Firewalls and Internet Security
Second Edition

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin

DRAFT COVER
as of 12/02

eastman
bring to you

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Chương 15: Phát hiện xâm nhập

“Kẻ ngốc nói rằng: ‘Đừng để tất cả trứng vào cùng một giỏ’ - đây chỉ là cách nói. Hãy ‘phân tán tiền và sự chú ý của bạn’. Nhưng người khôn ngoan nói rằng: ‘Hãy để tất cả trứng vào cùng một giỏ và... trông chừng cái giỏ đó!’”

— Puddin' Head Wilson's Calendar

Điều quan trọng là phải bố trí người canh gác gần những thứ bạn muốn bảo vệ, và hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) giúp thực hiện chức năng này. Là một sản phẩm thương mại, các công cụ bảo mật này đã được quảng bá như một giải pháp tối ưu cho các hành vi xâm nhập mạng, và nhiều nhà quản lý IT đã tuyên bố rằng mạng của họ an toàn vì họ đã cài đặt tường lửa và IDS mới nhất. Những điều này có thể hữu ích, nhưng chúng còn xa mới đạt đến mức lý tưởng.

Có một số loại hệ thống phát hiện xâm nhập. IDS mạng (Network IDS - NIDS) giám sát lưu lượng mạng để tìm các dấu hiệu của sự xâm nhập. Một số hệ thống dựa trên máy chủ quét các tệp hoặc lưu lượng truy cập để tìm virus; một số khác phân tích các mẫu cuộc gọi hệ thống hoặc kiểm tra các tệp bị thay đổi.

IDS phải đối mặt với một số hạn chế cố hữu. Dương tính giả (False positive) xảy ra khi IDS kết luận sai rằng một cuộc xâm nhập đã xảy ra. Âm tính giả (False negative) là các xâm nhập thực sự mà IDS bỏ sót. Với hầu hết các hệ thống phát hiện xâm nhập, cả hai vấn đề này đều không thể tránh khỏi và xảy ra với tần suất cao đến mức làm giảm đáng kể giá trị của chúng. Thông thường, cần có sự can thiệp của con người để xác định vấn đề hoặc thiếu sót, và một số nguồn gây ra lỗi trong các gói tin bị sai có thể quá khó để khắc phục.

Cuối cùng, các hệ thống IDS mạng thường hoạt động bằng cách “ngửi” lưu lượng mạng và ghép các gói tin lại thành dòng dữ liệu. Làm điều này một cách hợp lý nghe có vẻ đơn giản. Hầu hết các chương trình dò tìm chỉ làm điều đó, nhưng một số bài báo (như của Ptacek và Newsham [1998], Paxson [1998], và đặc biệt là Handley và cộng sự [2001]) chỉ ra rằng công việc này gần như không thể thực hiện chính xác. Vấn đề là một chương trình dò tìm cần biết trạng thái của các ngăn xếp TCP/IP ở cả hai đầu của liên lạc, cộng với các đặc điểm riêng của các chi tiết triển khai. Ví dụ, giả sử hai gói tin đến chứa dữ liệu chồng chéo nhau.

Vấn đề dữ liệu trùng lặp có vẻ như không phổ biến, nhưng các chương trình như fragrouter [Song *et al.*, 1999] được thiết kế để tạo luồng TCP/IP không bình thường nhằm gây nhầm lẫn cho các hệ thống phát hiện xâm nhập. Fragrouter sử dụng các kịch bản viết bằng một ngôn ngữ nhỏ để định nghĩa các vấn đề mong muốn trên luồng gói tin. Dữ liệu gửi đi có thể bị biến dạng đến mức hệ thống giám sát không thể giải mã được.

Dữ liệu chồng lấn có thể xuất hiện khi các gói tin được tái hợp lại và có hai phiên bản dữ liệu trùng lặp cho một vùng. Hệ thống sẽ sử dụng phiên bản nào? Các tiêu chuẩn RFC không đề cập đến vấn đề này, và các cách triển khai có thể khác nhau. Nếu dữ liệu trong hai gói tin không khớp, phiên bản nào mà Hệ thống phát hiện xâm nhập mạng (NIDS) sẽ cho là đúng?

Vấn đề dữ liệu chồng lấn nghe có vẻ hiếm, nhưng nó có thể xảy ra trong thực tế. Ví dụ, các chương trình như fragrouter [Song et al., 1999] cố tình thay đổi luồng TCP/IP để gây nhầm lẫn cho các hệ thống giám sát. Fragrouter sử dụng các đoạn mã nhỏ nhằm tạo ra các lỗi cụ thể trong dữ liệu gói tin. Kết quả là luồng gói tin đi ra có thể bị bóp méo đến mức hệ thống giám sát không thể giải mã luồng dữ liệu.

Có bốn nơi mà các luồng TCP/IP bất thường cần được xử lý đúng cách: khách hàng, máy chủ, tường lửa, và NIDS. [Handley et al., 2001] đề xuất sử dụng một thiết bị trung gian để chuẩn hóa luồng gói tin. Một cách tiếp cận khác là bổ sung chức năng này vào

tường lửa, làm cho nó hoạt động giống như một cổng mạch (circuit-level gateway). Một số tường lửa đã thực hiện điều này; chúng tái hợp các gói tin bị phân mảnh để bảo vệ khỏi các cuộc tấn công bằng gói tin ngắn. Các cổng mạch thực sự cũng có thể làm sạch luồng IP.

Vấn đề này là cơ sở cho khuyến nghị của chúng tôi trong lần xuất bản đầu tiên rằng các tổ chức nên tránh kết nối IP trực tiếp giữa mạng nội bộ và Internet, và thay vào đó sử dụng tường lửa ứng dụng hoặc tường lửa cấp độ mạch.

15.1 Nơi cần giám sát

Điều quan trọng là phải hiểu những hạn chế của Hệ thống Phát hiện Xâm nhập (IDS) trước khi triển khai. Một câu hỏi cần đặt ra là: "Mục đích của IDS là gì?" Một lý do chính đáng để cài đặt IDS ngoài tường lửa là để biện minh cho việc cấp ngân sách (vì đây là một mô hình mối đe dọa trong đó quản lý là "kẻ thù"). Không cần thiết phải giám sát lưu lượng ngoài mạng của bạn để xem liệu bạn có đang bị tấn công hay không — bạn biết mình là mục tiêu. Điều đó không có nghĩa là bạn nên bỏ qua lưu lượng bên ngoài, nhưng tốt hơn là ghi lại và lưu trữ lưu lượng bên ngoài để phân tích sau, thay vì cố gắng phát hiện xâm nhập trong thời gian thực.

Nếu bạn là nhà nghiên cứu học hỏi về các cuộc tấn công mới, thông tin như vậy là vô giá. Tuy nhiên, có quá nhiều lưu lượng xảy ra, và IDS là công cụ quá yếu để thực hiện phân tích thời gian thực. Đây là một công cụ tốt để huấn luyện những người mới làm quen với mạng và thiết bị IDS.

Thiết bị IDS trở nên hữu ích hơn khi được triển khai gần các tài sản quan trọng, bên trong các lớp bảo mật khác nhau. Chúng giống như một camera an ninh được lắp đặt trong két sắt của ngân hàng, cung cấp một lớp bảo đảm cuối cùng rằng mọi thứ đều ổn. Khi quyền truy cập thông thường vào mạng hoặc máy tính bị giới hạn nghiêm ngặt hơn, các quy tắc dành cho thiết bị phát hiện cũng cần phải nhạy cảm hơn. Con người không nên thực hiện các truy vấn web từ máy tính bảng lương.

15.2 Các loại IDS

Các loại IDS khác nhau có điểm mạnh và điểm yếu khác nhau.

IDS dựa trên chữ ký (Signature-based IDS):
Loại này có một cơ sở dữ liệu các cuộc tấn công đã biết; bất kỳ điều gì khớp với mục trong cơ sở dữ liệu sẽ bị gắn cờ. Bạn sẽ không gặp nhiều cảnh báo sai nếu hệ thống được điều chỉnh đúng cách, nhưng khả năng cao sẽ bỏ sót các cảnh báo đúng vì hệ thống chỉ nhận diện những gì nằm trong cơ sở dữ liệu. Thật không may, việc tìm được sự cân bằng giữa chữ ký rộng (khớp với lưu lượng bình thường) và chữ ký hẹp (dễ bị mã độc qua mặt) là rất khó. Tốt nhất, các hệ thống dựa trên chữ ký nên tích hợp ngữ cảnh thay vì chỉ dựa vào việc so khớp chuỗi.

IDS dựa trên bất thường (Anomaly-based IDS):
Những hệ thống này tìm kiếm các hành vi không bình thường và có khả năng đưa ra các cảnh báo sai hoặc bỏ sót cảnh báo đúng. Chúng hoạt động tốt nhất trong môi trường với phiên bản định nghĩa chặt chẽ về "bình thường," nơi dễ xác định khi một điều gì đó không nên xảy ra. Mục đích càng đặc thù của một máy, thì hành vi "bình thường" càng bị giới hạn, và khả năng cảnh báo sai càng giảm.

Phát hiện bất thường là một lĩnh vực nghiên cứu thú vị, nhưng đến nay vẫn chưa tạo ra nhiều công cụ thực tiễn. [Forrest et al., 1996] và [Ko et al., 2000] đã cho thấy một số kết quả đáng chú ý. Forrest phát triển một công cụ giám sát các quy trình chạy trên máy tính và kiểm tra các lệnh hệ thống. Công cụ này có khái niệm về mẫu lệnh "bình thường" và nhận ra khi

điều gì đó không đúng xảy ra. Nó sử dụng n-grams của các lệnh hệ thống và phân tích thứ tự thực thi để phát hiện bất thường.

IDS dựa trên máy chủ hoặc mạng (Host-based & Network-based IDS):
Hai loại này bổ sung cho nhau, không loại trừ nhau. Hệ thống dựa trên máy chủ thường biết trạng thái của chính máy đó, giúp xử lý dữ liệu dễ hơn, nhưng phần mềm có thể bị xâm phạm nếu máy chủ bị tấn công. Hệ thống dựa trên mạng là các thiết bị độc lập và thường ít bị tấn công hơn.

Một số môi trường như DMZ (vùng phi quân sự hóa) yêu cầu một loại IDS đặc biệt gọi là honeypot — một máy tính mà không ai được phép truy cập. Bất kỳ lưu lượng nào đến máy này có thể được xem là hành vi đáng ngờ. Honeypot không phù hợp trong môi trường sản xuất mở, nhưng nó phù hợp để phát hiện các cuộc tấn công mà không ảnh hưởng đến các tài nguyên dành riêng.

Một hệ thống honeypot (bẫy mật) trên mạng Internet công cộng có thể hữu ích để nghiên cứu hành vi của hacker, mặc dù một số hacker đã học cách né tránh chúng. Một trong những ví dụ đẹp nhất là *honeyd* của Niels Provos [Spitzner, 2002, Chương 8]. Nó mô phỏng một mạng lưới hoàn chỉnh, bao gồm nhiều loại máy móc khác nhau. Tuy nhiên, bạn không thể dựa vào nó để xác định liệu ai đó đã xâm nhập vào một máy đơn lẻ hay chưa; tối đa, nó chỉ có thể phát hiện các lượt quét. Để xử lý các cảnh báo dương tính giả và âm tính giả, một số người sử dụng nhiều hệ thống IDS (Hệ thống Phát hiện Xâm nhập) có đầu ra được đồng bộ hóa. Sự tương quan thời gian có thể được sử dụng để phát hiện các cuộc tấn công "chậm và âm thầm."

15.3 Quản trị một hệ thống IDS

Một hệ thống phát hiện xâm nhập (IDS) yêu cầu một lượng tài nguyên đáng kể. IDS phải được cài đặt ở các vị trí chiến lược, cấu hình đúng cách và giám sát thường xuyên. Trong hầu hết các môi trường, chúng sẽ phải xử lý một lượng lớn lưu lượng mạng không hợp lệ. Ví dụ, một trình điều khiển máy in HP mà chúng tôi đã sử dụng đã cố tìm mọi thứ trên mạng con mà không biết về mặt nạ mạng, dẫn đến quét toàn bộ mạng /16 để tìm một máy in HP. Phần mềm quản lý mạng đôi khi cũng làm điều tương tự. Người vận hành IDS phải biết cách xử lý loại lưu lượng này và cần có khả năng chịu đựng một lượng lớn "tiếng ồn" [Bellovin, 1993]. Họ cũng cần đảm bảo rằng họ không trở nên quá tự mãn vì IDS có xu hướng "báo động giả."

15.4 Công cụ IDS

Có rất nhiều công cụ IDS có sẵn, cả miễn phí lẫn thương mại. Các công cụ như snort (xem phần sau), ethereal, và bro [Paxson, 1998] rất hữu ích. Ethereal cung cấp một giao diện đồ họa (GUI) đẹp, cho phép bạn tái hiện các luồng TCP để xem dữ liệu ở cấp độ ứng dụng. Nó cũng có thể ghi lại lưu lượng mạng để phân tích sau.

Các sản phẩm thương mại dao động từ kém chất lượng đến khá hữu ích. Một số sản phẩm cố gắng áp dụng kỹ thuật trí tuệ nhân tạo để giải quyết vấn đề. Một số khác thu thập thông tin phân tán và cố gắng lắp ráp một cái nhìn tổng thể về cuộc tấn công.

15.4.1 Snort

Có lẽ chương trình phát hiện xâm nhập miễn phí phổ biến nhất là snort, được phát triển bởi Martin Roesch. Snort là mã nguồn mở, và có một cộng đồng lớn các người dùng và người đóng góp tích cực. Xem thêm tại:
http://www.snort.org/

Chương trình có sẵn trên nhiều nền tảng — nó hoạt động ở bất kỳ đâu mà libpcap chạy được.

Snort có thể được sử dụng theo nhiều cách khác nhau. Nó có thể "ngửi" mạng và tạo đầu ra theo định dạng tcpdump. Nó cũng có thể được sử dụng để ghi lại các gói tin, để các công cụ khai thác dữ liệu hoặc chương trình của bên thứ ba phân tích lưu lượng mạng sau đó. Tính năng thú vị nhất của snort là khả năng thiết kế một bộ quy tắc nhận diện các mẫu lưu lượng cụ thể. Nhiều quy tắc đã có sẵn cho snort và chúng thường được chia sẻ giữa người dùng và đăng tải trên Internet. Snort có thể được cấu hình để nhận diện các khảo sát bằng nmap, các cuộc tấn công tràn bộ đệm đã biết, các khai thác CGI đã biết, và các lưu lượng thăm dò như quét cổng.

Những nỗ lực để nhận dạng hệ điều hành dựa trên các đặc điểm của ngăn xếp mạng, và nhiều kiểu tấn công khác mà quản trị viên muốn cấu hình quy tắc. Dưới đây là một ví dụ quy tắc được lấy từ [Roesch, 1999]:

bash

Copy code

activate tcp !$HOME_NET any -> $HOME_EIET 143 (flags: PA; content: "|E8C0FFFFFF|bin|; activates: 1; msg: "(buffer overflow!");

dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by: 1; count: 50;);

Quy tắc trên chỉ ra rằng một cảnh báo sẽ được gửi khi một lỗi tràn bộ đệm IMAP được phát hiện. Tại thời điểm đó, 50 gói tin đến tiếp theo hướng đến cổng 143 sẽ được ghi lại. Một số trong những gói tin này có thể chứa thông tin quan trọng về cuộc tấn công mà một nhà phân tích hoặc quản trị viên mạng quan tâm.

Tuy nhiên, có một lỗ hổng: Quy định về cờ "PA" có nghĩa là cả hai bit PUSH và ACK phải được đặt trên gói tin để nó phù hợp với quy tắc này. Điều này khá dễ để kẻ tấn công né tránh bằng cách đảm bảo rằng PUSH không được đặt.

Như mong đợi từ các công cụ phát hiện xâm nhập hữu ích, Snort cung cấp các cơ chế cảnh báo linh hoạt, từ cửa sổ bật lên trên màn hình đến email và thông báo qua thiết bị nhắn tin. Có các nhóm người dùng Snort thường tụ họp để so sánh dữ liệu, chia sẻ tập luật, thảo luận về kết quả dương tính giả, và đề xuất các cải tiến có thể cho chương trình. Ngoài ra, còn có một diễn đàn trực tuyến với rất nhiều thông tin hữu ích tại http://snort.rapidnet.com/.

Và đúng vậy, luôn có một "cuộc chạy đua vũ trang" giữa những kẻ tấn công và các nhà phát triển script Snort.

Chương 19: Where do we go from here?

Chúng tôi hy vọng rằng đến thời điểm này, hai điểm sau đã được làm rõ: rằng thực sự có một mối đe dọa, nhưng mối đe dọa này có thể được kiểm soát thông qua các kỹ thuật phù hợp, bao gồm việc sử dụng tường lửa. Tuy nhiên, tường lửa không phải là giải pháp toàn diện cho bảo mật. Vẫn còn nhiều việc phải làm.

Đây là dự đoán của chúng tôi về tương lai. Chúng tôi đã từng sai trước đây và có lẽ sẽ sai nữa. (Một trong số chúng tôi, Steve, là một trong những nhà phát triển của NetNews. Ông từng dự đoán rằng lưu lượng của NetNews cuối cùng chỉ là một hoặc hai thông điệp mỗi ngày trong 50 đến 100 nhóm thảo luận.)

> *"Thật khó để đưa ra dự đoán, đặc biệt là về tương lai."*
> — **YOGI BERRA**

19.1 IPv6

Khi nào IPv6 sẽ được triển khai rộng rãi? IPv6 nên sớm được triển khai trong thế hệ điện thoại di động mới; hiện tại nó cũng đang được áp dụng tại Trung Quốc và Nhật Bản. Các bộ định tuyến xương sống hiện nay không hỗ trợ chuyển tiếp IPv6 ở mức phần cứng, và các phiên bản phần mềm không đủ hiệu quả để xử lý lưu lượng lớn. Vào cuối những năm 1990, các nhà cung cấp dịch vụ Internet (ISP) thường thay đổi bộ định tuyến trong vòng 18 tháng, di chuyển các bộ định tuyến lõi ra vùng biên. Xu hướng này đã chậm lại gần đây do sự suy thoái kinh tế.

Phần lớn các máy khách UNIX và Linux đã hỗ trợ IPv6. Windows XP có hỗ trợ dành cho nhà phát triển đối với IPv6; Microsoft đã công bố rằng hỗ trợ đầy đủ cho người dùng sẽ có trong bản phát hành chính tiếp theo của Windows, dự kiến vào khoảng năm 2004 nếu họ giữ đúng lịch trình. Trong vòng bốn năm sau đó, IPv6 có thể được triển khai rộng rãi. Nhưng liệu nó có được sử dụng hay không?

Chưa rõ các động lực kinh tế nào sẽ khiến các công ty bỏ thời gian và công sức để chuyển sang IPv6. Đúng là vấn đề thiếu không gian địa chỉ sẽ được giải quyết, nhưng hầu hết các mạng nội bộ lớn sử dụng không gian địa chỉ riêng và NAT để xử lý vấn đề này. Các công ty có thể muốn cải thiện khả năng kết nối với các điện thoại di động được đề cập trước đó (thoại qua IP?), mà không cần thông qua bộ dịch.

Một động lực mạnh mẽ là sự xuất hiện của các dịch vụ Internet trên IPv6 không khả dụng trên IPv4. Nhưng khó có thể tưởng tượng một trang web sẽ giới hạn mình chỉ ở giao thức mới. Thêm nữa, hầu hết các dịch vụ trên v6 đều có thể được thực hiện trên v4, miễn là có đủ không gian địa chỉ. Một ứng dụng tiềm năng là mạng ngang hàng (peer-to-peer) — nếu các ứng dụng hợp pháp trở nên phổ biến đủ mức.

Lý do rõ ràng nhất để chuyển sang IPv6 là vấn đề không gian địa chỉ, cũng là động lực ban đầu để thiết kế IPv6. Không gian IPv4 khan hiếm và được cho là có giá trị cao. Nếu những địa chỉ này được bán đấu giá và hình thành một thị trường không gian địa chỉ (chắc chắn không phải là truyền thống của Internet), thì sẽ có động lực kinh tế mạnh mẽ để chuyển đổi. Xem thêm [Rekhter et al., 1997] để biết thêm chi tiết.

Ba chúng tôi có ý kiến khác nhau về ngày triển khai IPv6 rộng rãi, nhưng đồng ý rằng năm 2008 là thời điểm sớm nhất chúng tôi có thể thấy việc sử dụng phổ biến.

19.2 DNSsec

Việc thiếu xác thực trong các phản hồi DNS là một trong những điểm yếu nhất của Internet. Trong bối cảnh Web, vấn đề này càng nghiêm trọng. Chúng ta cần một thứ như DNSsec, và khi các công cụ tấn công giả mạo DNS trở nên phổ biến hơn, việc sử dụng Web như hiện nay có thể bị đình trệ nếu không có biện pháp. Do đó, chúng tôi dự đoán rằng, mặc dù có những vấn đề liên quan đến PKI (ai là gốc?), DNSsec sẽ được triển khai. Bảo mật mà nó mang lại quá quan trọng, và các vấn đề nó giải quyết không thể được khắc phục bằng cách khác. Cuối cùng, một số khóa công khai sẽ được tích hợp trong các bản phân phối khách hàng DNS, và các phản hồi DNS sẽ được ký.

Tuy nhiên, việc triển khai rộng rãi DNSsec không phải là không có thách thức. Chúng ta có thể đủ khả năng để ký miền .COM không? Dấu ấn bộ nhớ của một miền cấp cao được ký sẽ rất lớn. Tuy nhiên, chúng tôi tin rằng những vấn đề này có thể được khắc phục. Nghiêm trọng hơn, quá nhiều trang web không quan tâm đến bảo mật cho đến khi họ thực sự bị tổn thất. Chúng ta chỉ có thể tiến xa bằng cách đưa các biện pháp bảo vệ vào cơ sở hạ tầng.

19.3 Microsoft và Bảo mật

Gần đây, truyền thông đưa tin rằng Microsoft sẽ tập trung vào bảo mật. Điều này dường như là thật, không chỉ là tuyên truyền. Họ đang cung cấp các khóa học nâng cao nhận thức và đào tạo bảo mật rộng rãi, phát triển các công cụ kiểm toán bảo mật mới, và văn hóa doanh nghiệp của họ đã bắt đầu thay đổi. Chúng tôi hoan nghênh nỗ lực này và hy vọng rằng các ngành khác sẽ noi gương.

Tuy nhiên, sẽ mất rất lâu để thấy kết quả thực sự. Ngoài cơ sở đã được cài đặt và yêu cầu tương thích ngược, khối lượng mã khổng lồ cần được xem xét và độ phức tạp của nó tạo ra nhiều cơ hội cho các hành vi bất thường.

19.4 Tính phổ biến của Internet

Rõ ràng, ngày càng nhiều thiết bị sẽ được kết nối với mạng nội bộ, nếu không phải là Internet. Các khóa cửa khách sạn, tủ lạnh, bộ điều nhiệt, lò sưởi, hệ thống liên lạc nội bộ trong nhà và thậm chí cả hộp thư đã được kết nối mạng. Nhưng làm thế nào để một công tắc đèn trong một ngôi nhà thông minh biết được ai là người đáng tin cậy?

Một trong số chúng tôi đã thực hiện nhiều thí nghiệm với một ngôi nhà có dây kết nối. Phần khó khăn không nằm ở thiết bị điện tử, thiết bị hoặc thậm chí là nghĩ ra những điều hữu ích để làm; mà chính là các nhiệm vụ quản trị hệ thống – những công việc mà bạn phải thêm vào danh sách việc nhà vào mỗi thứ Bảy. Liệu những hệ thống này có thể được triển khai ở quy mô lớn cho công chúng không? Nếu có, liệu ngôi nhà của chúng ta sẽ trở nên hữu ích hơn nhưng kém an toàn hơn?

Bên cạnh các ứng dụng thông thường của kết nối Internet liên tục đến nhà, còn có nhiều khả năng thú vị cho các dịch vụ mới. Các chương trình tự động có thể thông báo các cảnh báo thời tiết và các tình huống khẩn cấp khác. Chúng tôi từng nghe thấy các thông báo giọng nói về quỹ đạo vệ tinh và các sự kiện thiên văn khác, lời nhắc nhở mang rác đi đổ và tái chế, cùng nhiều thông báo khác. Nhiều dịch vụ trong số này có tính thời gian nhạy cảm và có thể được tiếp thị như một dịch vụ nếu có đủ nhu cầu.

Các dịch vụ như TiVo có thể giúp tích hợp giải trí gia đình với lập lịch động. Mạng ngang hàng (peer-to-peer) hiện đã cung cấp một lượng lớn nội dung âm nhạc, mặc dù theo cách ngẫu nhiên và có lẽ là bất hợp pháp. Một cách nào đó, việc tiếp cận giải trí sẽ ngày càng phát triển.

19.5 Bảo mật Internet

Bảo mật trên Internet đã suy giảm trong suốt 20 năm qua, và cuộc sống số sẽ trở nên nguy hiểm hơn trong tương lai. Những kẻ viết virus cho máy tính cá nhân có thể chiến thắng trong cuộc chiến với các phần mềm phòng chống virus. Hãy tưởng tượng một thế giới mà phần mềm kiểm tra virus hoàn toàn không hoạt động. Cuối cùng, vấn đề **halting problem** (vấn đề ngừng máy) không đứng về phía chúng ta. Ít nhất, các phần mềm kiểm tra virus sẽ phải tiêu tốn ngày càng nhiều thời gian CPU để xác định xem một tệp có bị nhiễm hay không. Nếu chúng ta không thể tin tưởng vào phần mềm kiểm tra virus, chúng ta sẽ phải quay lại sử dụng các biện pháp vệ sinh mạng tốt hơn, các tệp nhị phân đã được ký, và một cơ sở tính toán đáng tin cậy hơn (**Trusted Computing Base - TCB**).

Cơ sở hạ tầng Internet sẽ đối mặt với các cuộc tấn công ngày càng nhiều. Các điểm dễ bị tổn thương nhất là các máy chủ tên DNS, giao thức BGP, và các chế độ lỗi phổ biến của bộ định tuyến [Schneider, 1999].

Có một phong trào mạnh mẽ nhằm bảo mật quá trình khởi động và xác minh hệ điều hành cùng tất cả các ứng dụng trên hệ thống. Các nhà sản xuất phần cứng lớn, bao gồm Compaq, HP, IBM và Intel, đã thành lập **Liên minh Nền tảng Tính toán Tin cậy** (Trusted Computing Platform Alliance - TCPA). Ý tưởng này nhằm làm cho máy tính ít bị tổn thương hơn trước các mã độc như Trojan. Microsoft cũng là một phần của TCPA và đang tích cực phát triển **Palladium**, một nền tảng phần mềm được thiết kế để hỗ trợ TCPA. Các ứng dụng của nền tảng này bao gồm quản lý quyền kỹ thuật số (digital rights management) và đảm bảo an ninh toàn bộ hệ thống.

Nhiều kế hoạch như TCPA/Palladium và các nỗ lực bảo mật khác đặt ra nguy cơ tiềm tàng đối với quyền riêng tư, tính mở của các nền tảng, và khả năng các bên thứ ba phát triển phần mềm. Mặc dù những vấn đề này không phải là trọng tâm của cuốn sách, chúng là những yếu tố quan trọng phát sinh từ các nỗ lực đối phó với các mối đe dọa ngày càng tăng trên Internet. Có đáng để mua một máy tính an toàn hơn nhưng lại ít quyền riêng tư hơn và ít lựa chọn nhà cung cấp phần mềm hơn?

Ngoài ra, còn có các câu hỏi khác cần xem xét. Phiên bản Red Hat Linux tiếp theo có chứa khóa công khai trong ROM của máy tính xách tay IBM Thinkpad mới không? Điều này hoàn toàn có thể xảy ra. Nếu bạn mua một đầu DVD hỗ trợ Internet trên eBay, làm thế nào để nó được cài đặt lại để nhận diện bạn là chủ sở hữu mới, đồng thời thu hồi quyền truy cập của chủ sở hữu cũ? Làm thế nào để bảo mật một ngôi nhà được kết nối mạng? Nếu máy giặt muốn gửi dữ liệu về nhà sản xuất, các gói tin đó sẽ đi qua tường lửa của bạn bằng cách nào? Bạn có muốn cho phép không? (Liệu bảo hành của máy giặt có giới hạn số lần bạn được phép sử dụng? Máy giặt có thông báo cho nhà sản xuất rằng bạn đã vận hành nó không đúng cách không? Ai sở hữu dữ liệu của máy giặt đó và làm thế nào để chủ sở hữu kiểm soát việc sử dụng dữ liệu đó?)

19.6 Kết luận

Trong cuốn sách này, chúng tôi đã đề cập đến bảo mật Internet trong bối cảnh thế giới ngày nay. Mặc dù chúng tôi không biết những vấn đề tương tự sẽ được giải quyết ra sao trong tương lai, nhưng chúng tôi chắc chắn rằng những nguyên tắc bảo mật đã hướng dẫn con người trong ba thập kỷ qua, và có lẽ trong suốt 5000 năm qua, sẽ tiếp tục đúng.

Như Karger và Schell đã chỉ ra, chúng ta đang đi thụt lùi, không phải tiến lên; các hệ thống ngày nay thậm chí không đạt được mức bảo mật mà Multics đã có vào những năm 1970 [Karger và Schell, 2002]. Chúng ta đang mất lợi thế. Chúng ta không thể để điều này tiếp diễn, và cần làm tốt hơn.

> “Tôi đã quyết định rồi. Tôi muốn thấy núi non một lần nữa, Gandalf – những ngọn núi, và sau đó tìm một nơi mà tôi có thể nghỉ ngơi. Trong yên bình và tĩnh lặng, không bị họ hàng tò mò quấy rầy, không có những người khách không mời bấm chuông liên tục. Có lẽ tôi sẽ tìm một nơi để hoàn thành cuốn sách của mình. Tôi đã nghĩ đến một kết thúc đẹp cho nó: *và ông đã sống hạnh phúc mãi mãi đến cuối đời mình.*”

Gandalf cười lớn. “Tôi hy vọng ông sẽ như vậy. Nhưng không ai đọc cuốn sách đó, dù nó kết thúc ra sao.”

> “Ồ, có thể họ sẽ đọc, vào một ngày nào đó.”

Bilbo Baggins in Lord of the Rings - J.R.R.TOLKIEN