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 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