

Tài liệu đọc

Hỗ Trợ Công Nghệ Thông Tin

Khóa 5: Bảo mật CNTT chống lại các cuộc tấn công

Phần 1: Tài liệu đọc bổ trợ

Bài đọc 1	An ninh máy tính
	<ul style="list-style-type: none">1.1 Nguyên tắc CIA<ul style="list-style-type: none">- Bộ ba nguyên tắc CIA- Đặc điểm từng nguyên tắc1.2 Các thuật ngữ liên quan để an ninh máy tính
Bài đọc 2	Các mối đe dọa an ninh máy tính
	<ul style="list-style-type: none">2.1 Phần mềm độc hại<ul style="list-style-type: none">- Khái niệm về phần mềm độc hại- Phân loại và đặc điểm từng loại2.2 Tấn công mạng<ul style="list-style-type: none">- Tấn công giả mạo DNS- Tấn công xen giữa- Tấn công từ chối dịch vụ2.3 Các loại tấn công khác<ul style="list-style-type: none">- Chèn mã độc (XSS, SQL)- Tấn công mật khẩu (vét cạn, từ điển)- Lừa đảo (giả mạo)
Bài đọc 3	Mật mã học
	<ul style="list-style-type: none">3.1 Mã hóa và giải mã<ul style="list-style-type: none">- Các khái niệm về mã hóa và giải mã- Bảo vệ và tấn công hệ thống mã hóa

	<ul style="list-style-type: none"> - Ấn dữ liệu <p>3.2 Mã hóa đối xứng</p> <ul style="list-style-type: none"> - Khái niệm và nguyên lý thực thi - Phân loại - Các thuật toán mã hóa đối xứng (DES, AES, RC4) <p>3.3 Mã hóa bất đối xứng</p> <ul style="list-style-type: none"> - Khái niệm và nguyên lý thực thi - Chữ ký số - Mã xác thực thông điệp - Các thuật toán mã hóa bất đối xứng (RSA, DSA, DH, ECC) <p>3.4 Băm</p> <ul style="list-style-type: none"> - Giới thiệu và ứng dụng của băm - Các thuật toán băm (MD5, SHA-1/2/3, MIC) - Tấn công băm và cách thức phòng thủ <p>3.5 Hạ tầng khóa công khai</p> <ul style="list-style-type: none"> - Hạ tầng khóa công khai và chứng chỉ số - Các loại chứng chỉ số - Chuỗi CA tin cậy - Cấu trúc chứng chỉ số - Web of Trust <p>3.6 Phần cứng mã hóa</p>
Bài đọc 4	Bảo mật AAA
	<p>4.1 Giới thiệu bảo mật AAA</p> <p>4.2 Xác thực (Authentication)</p> <ul style="list-style-type: none"> - Mật khẩu mạnh - Xác thực đa yếu tố - Xác thực chứng chỉ số - Các giao thức xác thực (LDAP, RADIUS, Kerberos, TACACS+) - Đăng nhập một lần <p>4.3 Ủy quyền (Authorization)</p> <ul style="list-style-type: none"> - Khái niệm về ủy quyền - Hệ thống ủy quyền - Danh sách kiểm soát truy cập <p>4.4 Kiểm toán (accounting)</p>

Bài đọc 5	An ninh mạng
	<p>5.1 Tổng quan gia cố mạng</p> <p>5.2 Gia cố phần cứng mạng</p> <ul style="list-style-type: none"> - Tấn công giả mạo máy chủ DHCP và cách phòng thủ - Tấn công giả mạo ARP và cách phòng thủ - Tấn công giả mạo IP và cách phòng thủ - Xác thực mạng <p>5.3 Gia cố phần mềm mạng</p> <p>5.4 Bảo mật mạng không dây</p> <ul style="list-style-type: none"> - WEP - WPA/WPA2 - Gia cố mạng không dây <p>5.5 Giám sát mạng</p> <ul style="list-style-type: none"> - Bắt và kiểm tra gói tin - Bắt gói tin trong mạng không dây - Công cụ hỗ trợ (Tcpdump, Wireshark) - Hệ thống phát hiện/ngăn chặn xâm nhập
Bài đọc 6	Phòng thủ theo chiều sâu
	<p>6.1 Tấn công và phòng thủ</p> <p>6.2 Gia cố hệ thống</p> <ul style="list-style-type: none"> - Tắt các thành phần không cần thiết - Tường lửa - Ghi nhật ký và phân tích các bất thường - Phần mềm chống virus - Mã hóa toàn đĩa <p>6.3 Gia cố ứng dụng</p> <ul style="list-style-type: none"> - Cập nhật phần mềm - Chính sách ứng dụng
Bài đọc 7	Bảo mật trong công ty
	<p>7.1 Mục tiêu bảo mật</p> <p>7.2 Quét lỗ hổng bảo mật</p> <p>7.3 Quyền riêng tư</p> <ul style="list-style-type: none"> - Chính sách quyền riêng tư - Chính sách xử lý dữ liệu

7.4 [Người dùng](#)

- Thói quen người dùng
- Bảo mật bên thứ ba
- Văn hóa bảo mật

7.5 [Xử lý và khắc phục sự cố](#)

- Phản ứng với sự cố
- Xử lý sự cố
- Xác định mức độ nghiêm trọng
- Vấn đề đánh cắp dữ liệu
- Khôi phục hệ thống

7.6 [Bảo mật điện thoại](#)

Phần 2: Hướng dẫn trả lời câu hỏi - Quiz

Phần 1

TÀI LIỆU ĐỌC BỔ TRỢ

Bài đọc 1: An Ninh Máy Tính

1. Nguyên tắc CIA

Bộ ba nguyên tắc CIA

Bộ ba nguyên tắc gồm nguyên tắc về tính bảo mật (Confidentiality), nguyên tắc về tính toàn vẹn (Integrity) và nguyên tắc về tính sẵn sàng (Availability), gói tắt là CIA, đã trở thành nền tảng quan trọng để hướng dẫn thiết kế các chính sách bảo mật thông tin trong máy tính. Bộ nguyên tắc CIA này sẽ giúp chúng ta phát triển các chính sách an ninh máy tính tại nơi làm việc và môi trường cá nhân của chúng ta.



Đặc điểm từng nguyên tắc

Bảo mật có nghĩa là giữ mọi thứ được giấu kín. Nó có nghĩa là giữ cho dữ liệu ẩn đi một cách an toàn khỏi những đối tượng không mong muốn. Một phương pháp bảo mật cơ bản mà chúng ta có thể sử dụng là bảo vệ bằng mật khẩu. Để bảo mật hoạt động, chúng ta cần giới hạn quyền truy cập vào dữ liệu. Chỉ những người liên quan mới được cấp quyền truy cập vào dữ liệu này.

Tính toàn vẹn có nghĩa là giữ cho dữ liệu được chính xác và không bị can thiệp. Dữ liệu gửi hoặc nhận phải được giữ nguyên vẹn trong toàn bộ tiến trình. Hãy tưởng tượng nếu chúng ta tải xuống một tập tin từ Internet và trang web đang tải cho biết tập tin đó gồm 3 MB. Tuy nhiên, khi tải xuống, nó biến thành 30 MB. Đó là một dấu hiệu đỏ. Đã xảy ra sự cố trong quá trình tải xuống, một điều gì đó có thể không an toàn. Một tập tin không mong muốn có thể đang tồn tại trên ổ cứng của chúng ta.

Tính khả dụng có nghĩa là thông tin có thể dễ dàng truy cập được đối với những người cần có thông tin đó. Điều này có thể có nhiều ý nghĩa, chẳng hạn như chuẩn bị sẵn sàng nếu dữ liệu bị mất hoặc nếu hệ thống gặp sự cố. Các cuộc tấn công bảo mật được thiết kế để đánh cắp mọi thứ. Chẳng hạn như chúng đánh cắp thời gian mà chúng ta cần bỏ ra để sao lưu và chạy các dịch vụ. Số khác nắm giữ hệ thống làm con tin cho đến khi chúng ta trả tiền chuộc.

2. Các thuật ngữ liên quan đến an ninh máy tính

Trước khi đi vào các vấn đề an ninh máy tính, chúng ta cần đi qua một số thuật ngữ phổ biến liên quan. Đầu tiên là **rủi ro bảo mật** (security risk). Nó là thuật ngữ chỉ khả năng bị tổn thất trong trường hợp hệ thống bị tấn công. Giả sử chúng ta mua một chiếc điện thoại mới. Một biện pháp bảo mật có thể thực hiện để bảo vệ thiết bị của mình, là thiết lập khóa màn hình bằng mật khẩu hoặc mẫu hình. Khóa màn hình là một tính năng bảo mật giúp ngăn chặn truy cập không mong muốn bằng cách tạo một hành động phải làm để có được quyền truy cập. Nếu chúng ta chọn không thêm khóa màn hình, rủi ro có thể gặp phải là ai đó có thể dễ dàng truy cập vào điện thoại và lấy cắp dữ liệu của chúng ta. Ngay cả khi thêm thứ gì đó đơn giản như mật mã hoặc khóa màn hình cũng có thể giúp chúng ta bảo vệ dữ liệu cá nhân hoặc công ty của mình không bị rơi vào tay kẻ xấu.

Tiếp theo là thuật ngữ **lỗ hổng** (vulnerability). Một lỗ hổng trong hệ thống có thể bị lợi dụng để xâm nhập hệ thống. Các lỗ hổng có thể là những lỗ hổng mà chúng ta có thể nhận thức được hoặc không. Có thể chúng ta đi nghỉ dài ngày và khóa mọi cửa ra vào và cửa sổ trong nhà trước khi rời đi. Nhưng lại quên khóa cửa sổ phòng tắm. Cửa sổ phòng tắm đó bây giờ là một lỗ hổng mà kẻ trộm có thể sử dụng để đột nhập vào nhà. Một ví dụ khác là khi chúng ta đang viết một ứng dụng web và kích hoạt tài khoản kiểm thử để thử nghiệm trong quá trình phát triển nhưng lại quên tắt nó trước khi phát hành ứng dụng. Giờ đây, ứng dụng tồn tại một lỗ hổng mà kẻ tấn công có thể phát hiện ra.

Có một loại lỗ hổng đặc biệt được gọi là lỗ hổng Zero-day, tạm dịch là lỗ hổng 0 ngày. Đây là một lỗ hổng mà nhà phát triển hoặc nhà cung cấp phần mềm chưa biết những kẻ tấn công đã biết. Tên gọi mô tả đến khoảng thời gian mà nhà phát triển phần mềm đã phản ứng và sửa chữa lỗ hổng bảo mật này là không ngày. Những kẻ tấn công sẽ khai thác các lỗ hổng được tìm thấy trong

phần mềm để gây hại cho hệ thống. Giả sử kẻ tấn công phát hiện ra lỗ hổng zero-day. Hắn quyết định tận dụng lỗi này bằng cách viết mã khai thác zero-day. Mã đó sẽ nhắm mục tiêu cụ thể như truy cập và gây ra thiệt hại cho hệ thống.

Thuật ngữ tiếp theo cần biết là **các mối đe dọa** (threat). Chúng là những cuộc tấn công nguy hiểm có thể xảy ra. Có thể ví chúng như những kẻ trộm. Không phải tất cả những tên trộm sẽ cố gắng đột nhập vào nhà chúng ta, nhưng chúng là một mối đe dọa tiềm tàng.

Một **hacker** trong thế giới bảo mật là người cố gắng đột nhập hoặc khai thác một hệ thống. Hầu hết chúng ta liên hệ hacker với những nhân vật nguy hiểm. Nhưng thực tế có hai loại hacker phổ biến. Hacker mũ đen là những kẻ cố gắng xâm nhập vào hệ thống để làm điều gì đó gây hại. Nhưng cũng có những hacker mũ trắng cố gắng tìm ra điểm yếu trong một hệ thống và cảnh báo cho chủ sở hữu để họ có thể sửa chữa nó trước khi người khác làm điều gì đó hư hại. Mặc dù còn nhiều loại hacker khác nữa nhưng đây là hai loại chính và quan trọng nhất mà chúng ta cần biết.

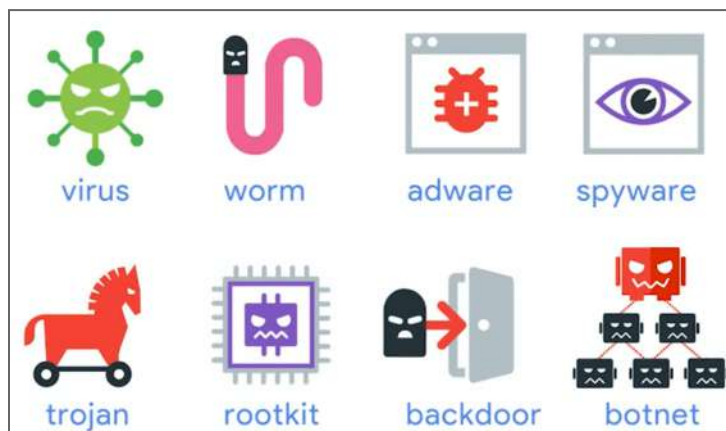
Thuật ngữ cuối cùng cần biết là **tấn công** (attack). Đó là một nỗ lực thực sự nhằm gây hại cho hệ thống. Điều cực kỳ quan trọng là phải nhận thức được các mối đe dọa và lỗ hổng bảo mật có thể xảy ra đối với hệ thống để có thể chuẩn bị tốt hơn. Mặc dù luôn có các cuộc tấn công vào hệ thống, nhưng cũng sẽ có nhiều cách để chúng ta có thể phát hiện và giảm thiểu các cuộc tấn công.

Bài đọc 2: Các Mối Đe Dọa An Ninh Máy Tính

1. Phần mềm độc hại

Khái niệm về phần mềm độc hại

Phần mềm độc hại (malware) là một loại phần mềm có thể được sử dụng để lấy thông tin nhạy cảm, xóa hoặc sửa đổi các tập tin. Về cơ bản, nó có thể được sử dụng cho bất kỳ và tất cả các mục đích không mong muốn nào. Các loại phần mềm độc hại phổ biến nhất như virus, sâu, phần mềm quảng cáo, phần mềm gián điệp, trojan, rootkit, backdoor, botnet, v.v...



Phân loại và đặc điểm từng loại

Virus là loại phần mềm độc hại được biết đến nhiều nhất và chúng hoạt động giống như cách thức hoạt động của virus trong cơ thể chúng ta. Khi chúng ta bị bệnh, một loại virus sẽ gắn vào một tế bào khỏe mạnh trong cơ thể, sau đó tự nhân lên và lây lan sang các tế bào khỏe mạnh khác. Virus máy tính cũng gắn vào mã thực thi của một chương trình. Khi chương trình chạy, nó tương tác với nhiều tập tin, mỗi tập tin bây giờ bị nhiễm virus. Vì vậy, vì rút tự sao chép chính chúng và thực hiện các công việc độc hại mà nó dự định thực hiện và lặp đi lặp lại điều này cho đến khi nó lan rộng hết mức có thể.

Sâu máy tính (worm) cũng tương tự như virus ngoại trừ việc thay vì phải bám vào thứ gì đó để phát tán, sâu máy tính có thể tự sống và lây lan qua các kênh như mạng. Một trường hợp về một loại sâu máy tính nổi tiếng là ILOVEYOU hoặc Love Bug đã lây lan sang hàng triệu máy Windows. Con sâu này lây lan qua

email. Một người gửi email có dòng tiêu đề “I Love You” và một tập tin đính kèm thực sự là sâu máy tính được ngụy trang dưới dạng tập tin thư tình. Khi được mở, nó sẽ thực hiện nhiều cuộc tấn công như sao chép chính nó vào một số tập tin và thư mục, khởi chạy phần mềm độc hại khác, thay thế tập tin và sau đó tự ẩn sau khi hoàn tất. Loại sâu này lây lan bằng cách đánh cắp địa chỉ e-mail trong máy tính của nạn nhân và các ứng dụng trò chuyện. Sau đó, nó tiến hành gửi email đó đến mọi người trong sổ địa chỉ. Love bug lan rộng khắp thế giới và gây thiệt hại hàng tỷ đô la. Đây chỉ là một trong nhiều lý do tại sao chúng ta không bao giờ nên mở các tệp đính kèm email mà chúng ta không biết rõ về chúng.



Phần mềm quảng cáo (adware) là một trong những dạng phần mềm độc hại dễ thấy nhất, hầu hết chúng ta đều nhìn thấy nó hàng ngày. Phần mềm quảng cáo chỉ là phần mềm hiển thị quảng cáo và thu thập dữ liệu. Đôi khi chúng ta tải xuống phần mềm quảng cáo một cách hợp pháp. Điều đó xảy ra khi chúng ta đồng ý với các điều khoản dịch vụ cho phép chúng ta sử dụng phần mềm miễn phí để đổi lấy việc hiển thị quảng cáo. Tuy nhiên, một số phần mềm khác có thể được cài đặt mà không có sự đồng ý của chúng ta và chúng có thể làm những điều gây hại khác ngoài việc hiển thị quảng cáo.

Trong thần thoại Hy Lạp, có một câu chuyện nổi tiếng về cuộc xâm lược thành Troy. Những người Hy Lạp, những người cố gắng tiếp cận thành phố có tường bao quanh, cuối cùng đã quyết định ẩn mình trong một bức tượng khổng lồ bằng gỗ của một con ngựa dưới vỏ bọc của một món quà. Người trong thành cho phép món quà vào bên trong và đêm đến, quân Hy Lạp xông ra khỏi bức tượng và tấn công thành phố. Trong bảo mật máy tính, chúng ta có phần mềm độc hại hoạt động giống như một con ngựa thành Troy và nó được đặt theo tên này. **Trojan** là phần mềm độc hại tự ngụy trang thành một thứ nhưng lại làm một thứ khác. Giống như cách con ngựa thành Troy lịch sử được công dân thành Troy chấp nhận vào thành phố, Trojan máy tính phải được người dùng chấp nhận, nghĩa là chương trình phải được người dùng thực thi. Không ai sẵn sàng

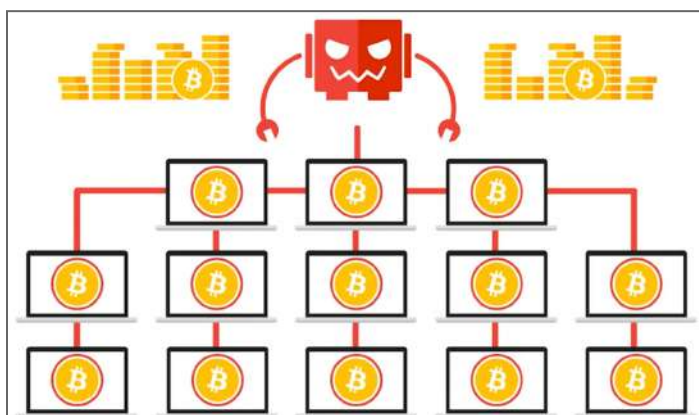
cài đặt phần mềm độc hại vào máy của họ, đó là lý do tại sao trojan nhằm mục đích lôi kéo chúng ta cài đặt chúng bằng cách ngụy trang thành phần mềm khác.



Phần mềm gián điệp (spyware) là loại phần mềm độc hại nhằm theo dõi người dùng. Điều đó có nghĩa là theo dõi màn hình máy tính, phím bấm, webcam, sau đó báo cáo hoặc phát trực tuyến tất cả thông tin này cho một bên khác. Keylogger là một loại phần mềm gián điệp phổ biến được sử dụng để ghi lại mọi thao tác gõ phím của người dùng. Nó có thể nắm bắt tất cả các tin nhắn được nhập, thông tin bí mật, mật khẩu và thậm chí còn nhiều thứ hơn nữa.

Ransomware là một kiểu tấn công bắt giữ dữ liệu trong hệ thống làm con tin cho đến khi được trả một số loại tiền chuộc. Một ransomware gần đây là cuộc tấn công ransomware WannaCry vào tháng 5 năm 2017. Phần mềm độc hại này đã lợi dụng một lỗ hổng trong các hệ thống Windows phiên bản cũ để lây nhiễm cho hàng trăm nghìn máy trên khắp thế giới. Đáng chú ý nhất là cuộc tấn công làm tắt hệ thống của Dịch vụ Y tế Quốc gia ở Anh, gây ra một cuộc khủng hoảng liên quan đến sức khỏe. Cuộc tấn công bằng ransomware WannaCry đã tàn phá các hệ thống trên khắp thế giới.

Điều gì sẽ xảy ra nếu những kẻ tấn công không chỉ ăn cắp dữ liệu mà còn ăn cắp tài nguyên máy tính như CPU? **Botnet** là một mạng lưới hay một tập hợp các con bot sử dụng sức mạnh của các máy kết nối Internet để thực hiện một số chức năng phân tán. Một số nhiệm vụ phân tán như việc đào Bitcoin. Đào Bitcoin yêu cầu một máy thực hiện một số tính toán để có thể kiếm được các đồng tiền số. Vì vậy, thay vì có một máy tính chạy tính toán, những kẻ tấn công giờ đây có thể có hàng nghìn máy tính chạy tính toán và kiếm được ngày càng nhiều Bitcoin.



Cửa hậu (backdoor) là một cách để xâm nhập vào hệ thống nếu các phương pháp khác thông thường để vào hệ thống không được phép, đó là một lối vào bí mật cho những kẻ tấn công. Backdoor thường được cài đặt sau khi kẻ tấn công có quyền truy cập vào hệ thống và muốn duy trì quyền truy cập đó. Ngay cả khi phát hiện ra hệ thống của mình đã bị xâm nhập, chúng ta có thể không nhận ra rằng có một cửa hậu hệ thống tồn tại. Chúng ta cần kiểm tra và khóa các cửa hậu lại trước khi chúng có thể gây ra nhiều thiệt hại hơn.

Rootkit theo tên gọi là một bộ công cụ dành cho tài khoản root trên Linux. Đó đồng nghĩa là một tập hợp các phần mềm hoặc công cụ mà quản trị viên sẽ sử dụng. Nó cho phép sửa đổi cấp quản trị đối với một hệ điều hành. Rootkit có thể khó bị phát hiện vì nó có thể tự ẩn mình khỏi hệ thống bằng cách sử dụng chính quyền hệ thống. Bộ rootkit có thể đang chạy rất nhiều tiến trình độc hại, nhưng đồng thời những tiến trình đó sẽ không hiển thị trong trình quản lý tác vụ vì nó có thể ẩn sự hiện diện của chính nó.

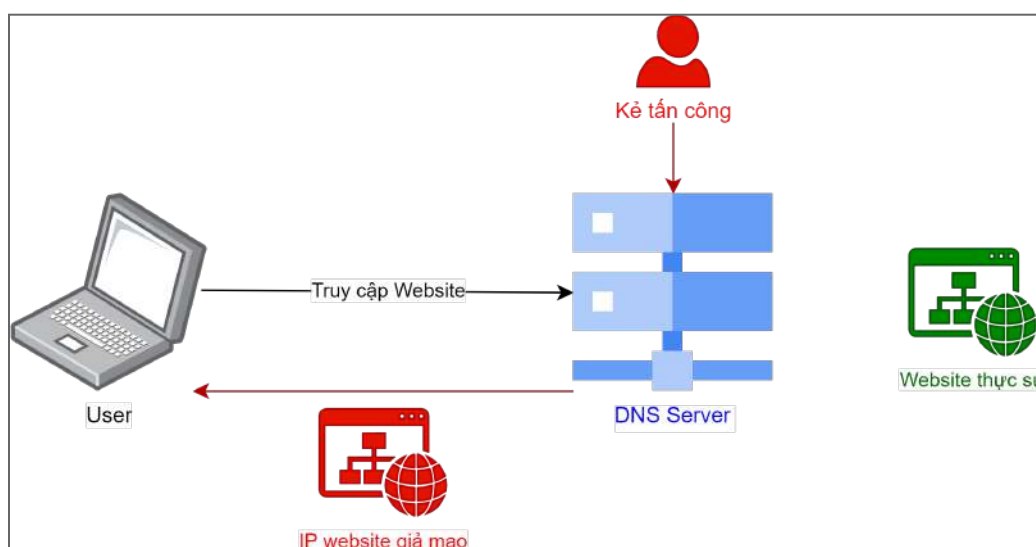
Bom logic (logic bomb) là một loại phần mềm độc hại được cài đặt có chủ đích. Sau khi một sự kiện hoặc thời gian nhất định, nó sẽ được kích hoạt và chạy chương trình độc hại. Có một bom logic phổ biến đã xảy ra vào năm 2006, trong đó một quản trị viên hệ thống ác ý tại một ngân hàng đã gây ra một quả bom logic và hạ bệ các dịch vụ của một công ty trong nỗ lực giảm giá cổ phiếu của họ.

2. Tấn công mạng

Tấn công giả mạo DNS

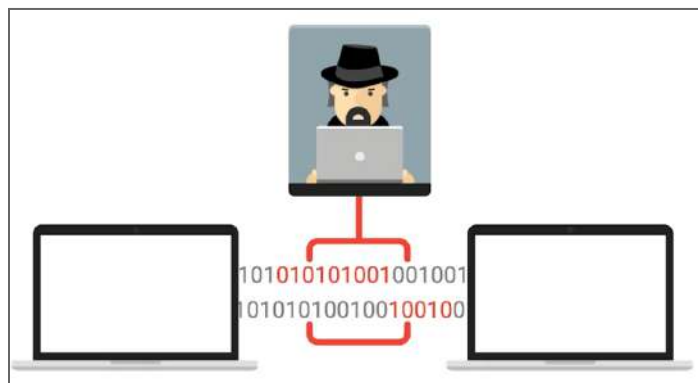
Máy chủ DNS giúp thực hiện phân giải tên miền thành địa chỉ IP cụ thể. Một cuộc tấn công giả mạo DNS (DNS spoofing, DNS cache poisoning attack) hoạt động bằng cách lừa máy chủ DNS chấp nhận một bản ghi DNS giả mạo mà nó hướng chúng ta đến một máy chủ DNS đã bị kiểm soát. Sau đó, nó cung cấp địa chỉ giả khi chúng ta cố gắng truy cập các trang web hợp pháp. Không chỉ vậy, giả mạo DNS cũng có thể lây lan sang các mạng khác. Nếu các máy chủ DNS đang lấy thông tin từ một máy DNS bị xâm nhập, chúng sẽ phân phát các mục DNS xấu đó cho các máy chủ khác.

Vài năm trước, đã có một cuộc tấn công giả mạo DNS quy mô lớn ở Brazil. Có vẻ như những kẻ tấn công đã tìm cách đầu độc bộ nhớ cache DNS của một số ISP cục bộ, bằng cách chèn các bản ghi DNS giả mạo cho các trang web phổ biến khác nhau như Google, Gmail hoặc Hotmail. Khi ai đó cố gắng truy cập một trong những trang web đó, họ sẽ nhận được một bản ghi DNS giả mạo và được gửi đến một máy chủ mà kẻ tấn công kiểm soát. Sau đó, người dùng sẽ bị lừa cài đặt applet, đây thực sự là một trojan độc hại được thiết kế để đánh cắp thông tin đăng nhập ngân hàng.

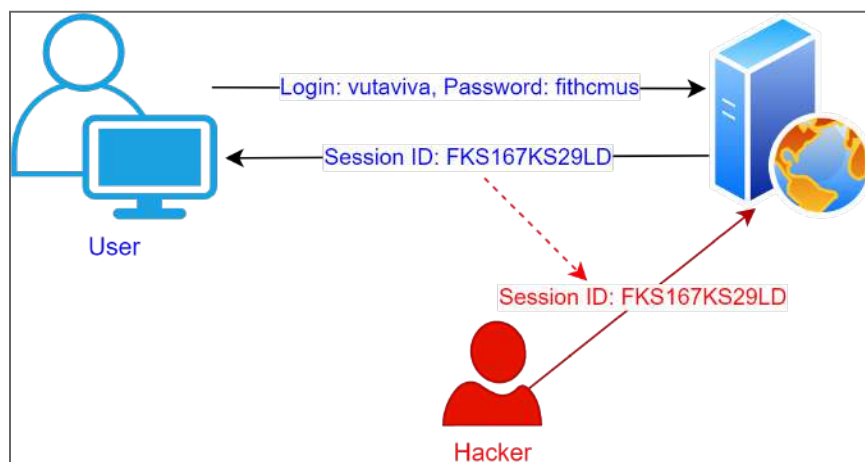


Tấn công xen giữa

Tấn công xen giữa (man-in-the-middle attack) là một cuộc tấn công đặt kẻ tấn công vào giữa hai đối tượng mà họ nghĩ rằng đang giao tiếp trực tiếp với nhau. Cuộc tấn công sẽ theo dõi thông tin đến và đi và có khả năng sửa đổi thông tin đó khi chuyển tiếp.

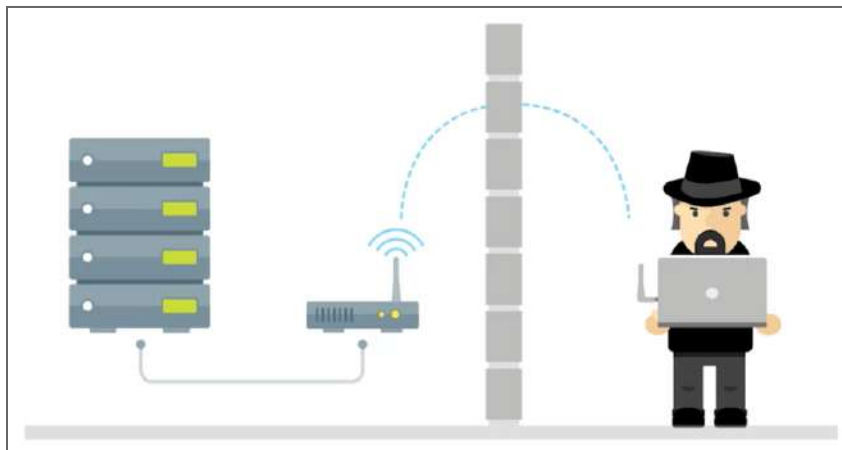


Loại tấn công xen giữa phổ biến là tấn công phiên (session hijacking, cookie hijacking). Giả sử chúng ta đã xác thực chính mình để truy cập vào trang web và tạo mã phiên cho quyền truy cập vào trang web đó. Nếu một người tấn công phiên, họ có thể đánh cắp mã đó và mạo danh chúng ta để truy cập trang web.

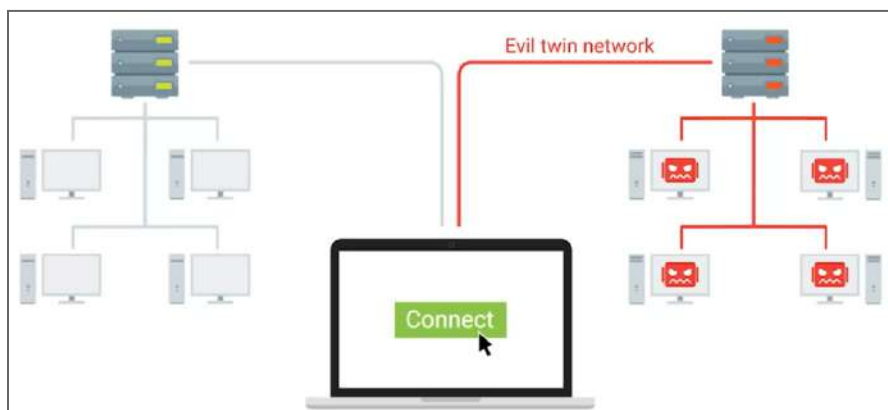


Một cách khác để thiết lập một cuộc tấn công xen giữa là một cuộc tấn công AP giả mạo (rogue AP). AP giả mạo là một điểm truy cập được cài đặt trên mạng mà quản trị viên không hề hay biết. Đôi khi, trong môi trường công ty, ai đó có thể cấm bộ định tuyến vào mạng công ty để tạo một mạng không dây

đơn giản. Điều này thực sự có thể khá nguy hiểm và có thể cấp quyền truy cập trái phép vào một mạng được xác thực.



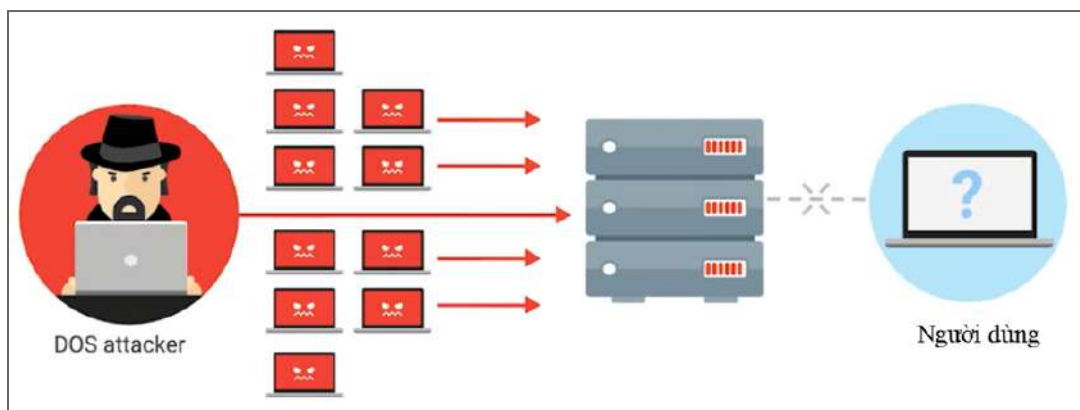
Một phương pháp khác nữa của tấn công xen giữa gọi là evil twin. Nó tương tự như ví dụ AP giả mạo nhưng có một sự khác biệt nhỏ nhưng quan trọng. Tiền đề của một cuộc tấn công evil twin là để chúng ta kết nối với một mạng giống hệt với mạng của chúng ta. Mạng giống hệt này được kiểm soát bởi kẻ tấn công. Sau khi chúng ta kết nối với mạng này, chúng có thể giám sát các luồng trao đổi của chúng ta.



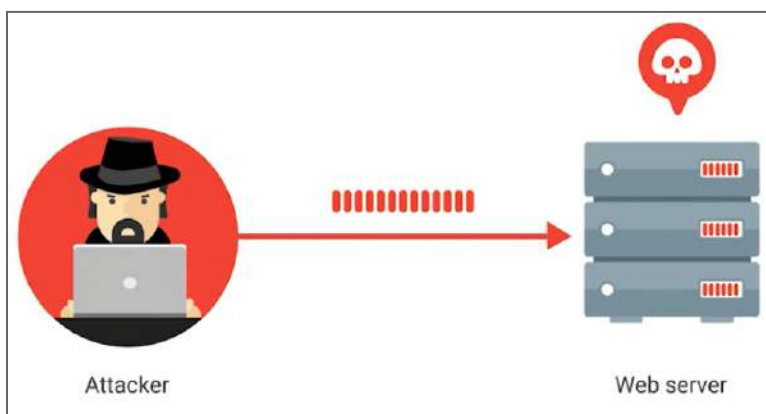
Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ, hay còn gọi là tấn công DoS (denial-of-service attack), là một cuộc tấn công cố gắng ngăn chặn quyền truy cập vào dịch vụ của những người dùng thông thường bằng cách gây áp đảo mạng hoặc máy chủ. Hãy tưởng tượng chúng ta có một trang web chỉ có thể phục vụ 10 người

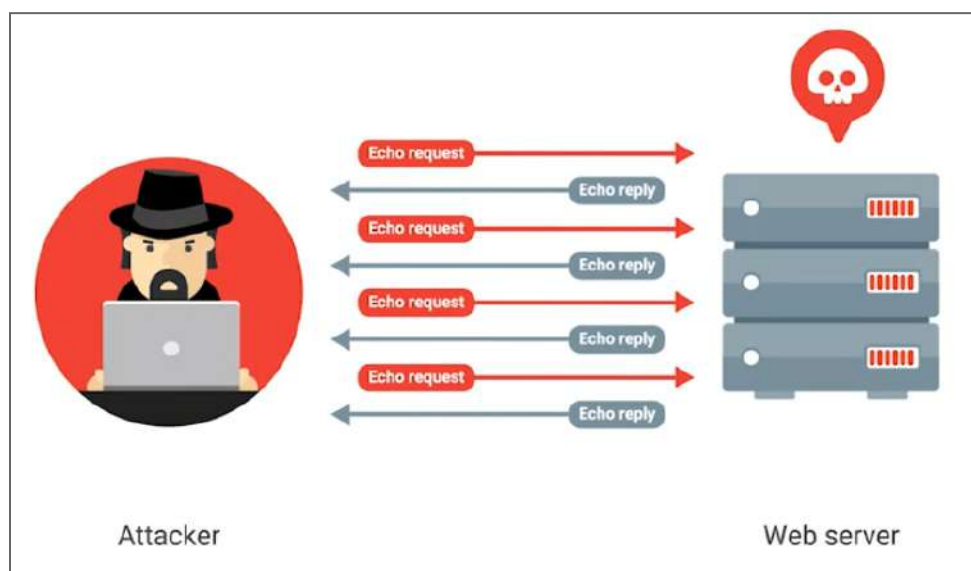
dùng. Nếu ai đó đang thực hiện một cuộc tấn công từ chối Dịch vụ, họ sẽ chiếm tất cả 10 điểm truy cập trong số đó và những người dùng khác sẽ bị từ chối dịch vụ, vì không còn chỗ cho họ.



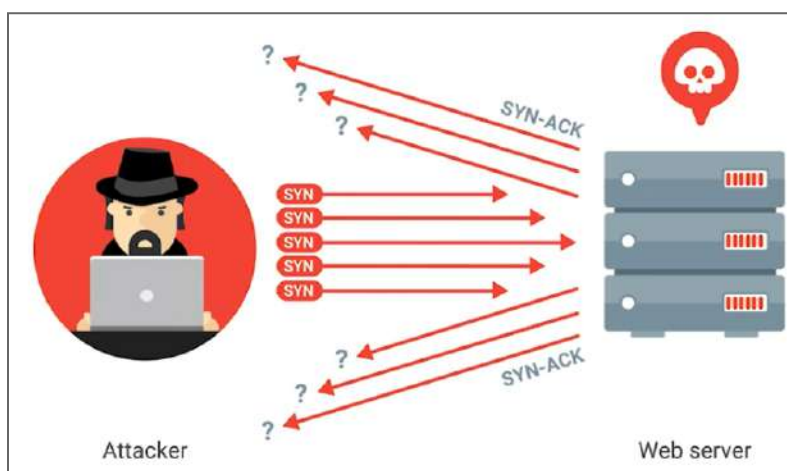
Ping of Death (PoD) là một ví dụ khá đơn giản về cuộc tấn công DoS. Nó hoạt động bằng cách gửi một ping không đúng định dạng đến một máy tính. Ping này có kích thước lớn hơn so với những gì giao thức internet được tạo ra để xử lý. Vì vậy, nó dẫn đến tràn bộ đệm. Điều này có thể khiến hệ thống gặp sự cố và có khả năng cho phép thực thi mã độc.



Một cách khác là ping flood, nó sẽ gửi hàng tấn gói tin ping đến một hệ thống. Cụ thể hơn, nó gửi các yêu cầu ICMP echo. Vì mỗi ping mong đợi một số lượng tương đương các phản hồi ICMP echo. Nếu một máy tính không thể theo kịp điều này, thì nó sẽ dễ bị quá tải và bị đánh sập.

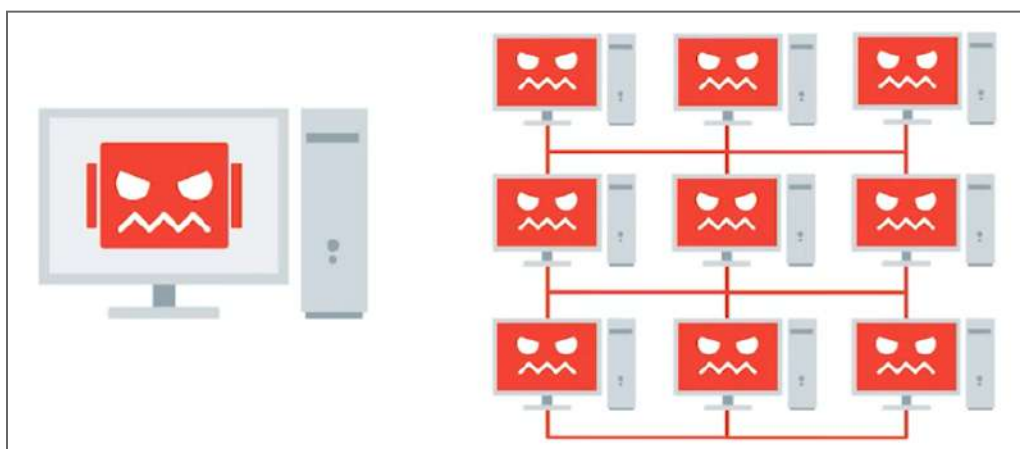


Tương tự như ping flood là SYN flood. Để tạo kết nối TCP, một máy khách sẽ gửi một gói SYN đến một máy chủ mà nó muốn kết nối. Tiếp theo, máy chủ sẽ gửi lại một thông điệp SYN-ACK, sau đó máy khách gửi lại thông điệp ack. Trong một đợt SYN, máy chủ đang bị tấn công bởi các gói SYN. Máy chủ gửi lại gói SYN-ACK nhưng kẻ tấn công không gửi tin nhắn xác nhận ack. Điều này có nghĩa là kết nối vẫn mở và đang chiếm tài nguyên của máy chủ. Những người dùng khác sẽ không thể kết nối với máy chủ, đây là một vấn đề lớn. Vì kết nối TCP còn dang dở nên SYN flood cũng được gọi là các cuộc tấn công half-open.



Các cuộc tấn công DoS cho đến nay chỉ sử dụng một máy duy nhất để thực hiện một cuộc tấn công. Nhưng điều gì sẽ xảy ra nếu những kẻ tấn công có thể

sử dụng nhiều máy? Một cuộc tấn công DoS sử dụng nhiều hệ thống, được gọi là cuộc tấn công từ chối dịch vụ phân tán hoặc DDoS (Distributed denial-of-service attack). Các cuộc tấn công DDoS cần một khối lượng lớn hệ thống để thực hiện một cuộc tấn công và chúng thường được trợ giúp bởi những kẻ tấn công botnet. Trong trường hợp đó, chúng có thể truy cập vào khối lượng lớn máy móc để thực hiện một cuộc tấn công. Vào tháng 10 năm 2016, một cuộc tấn công DDoS đã xảy ra ở nhà cung cấp dịch vụ DNS, Dyn. DNS giả từ botnet gửi các yêu cầu theo cách SYN flood đã làm quá tải hệ thống. Dyn đảm nhiệm DNS cho các trang web lớn như Reddit, GitHub, Twitter, v.v. Vì vậy, khi sự cố đó xảy ra, nó cũng đã hạ gục khách hàng của mình và khiến các dịch vụ đó không thể truy cập được.



3. Các loại tấn công khác

Tấn công tiêm mã độc

Tấn công tiêm mã độc (injection attack) là cách thức khai thác lỗi máy tính do xử lý dữ liệu không hợp lệ. Để dễ hiểu, chúng ta liên tưởng đến chiếc xe hơi. Chúng ta giữ cho chiếc xe hoạt động bằng cách đổ xăng cho nó. Bây giờ, giả sử một người muốn làm điều gì đó gây hại cho chiếc xe này. Người đó bơm sinh tố vào bình xăng. Điều này có thể làm hỏng chiếc xe. Các cuộc tấn công tiêm mã độc trong các trang web hoạt động theo cùng một cách. Các cuộc tấn công tiêm mã độc có thể được hạn chế với các nguyên tắc phát triển phần mềm tốt, như xác thực dữ liệu đầu vào và làm sạch nó.

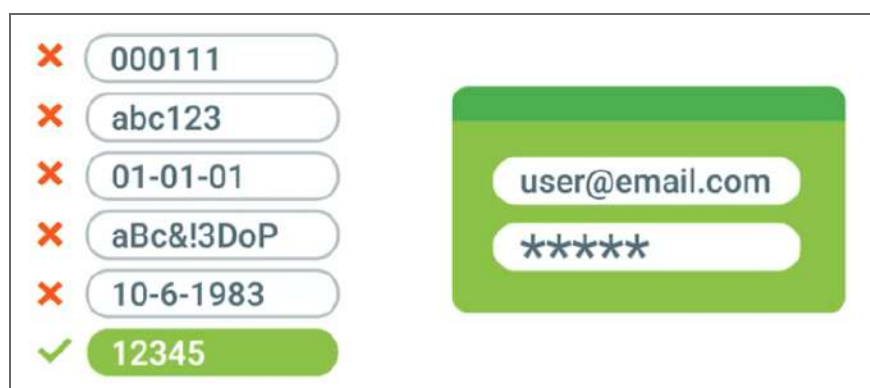
Cross-site scripting, hay còn gọi là tấn công XSS, là một loại tấn công chèn mã độc và nhắm mục tiêu vào người dùng dịch vụ. Các cuộc tấn công XSS thường để chiếm được phiên đăng nhập. Nó đơn giản như việc nhúng một tập lệnh độc hại vào một trang web và người dùng vô tình thực thi tập lệnh đó trong trình duyệt của họ. Sau đó, tập lệnh có thể thực hiện những điều như ăn cắp cookie của nạn nhân và dùng nó để đăng nhập vào một trang web.



Một kiểu tấn công tiêm khác là tiêm mã độc SQL (SQL injection). Không giống như XSS nhắm mục tiêu người dùng, tấn công SQL injection nhắm mục tiêu toàn bộ trang web nếu trang web đang sử dụng cơ sở dữ liệu SQL. Những kẻ tấn công có thể chạy các lệnh SQL cho phép chúng xóa dữ liệu trang web, sao chép nó và chạy các lệnh độc hại khác.

Tấn công mật khẩu

Mật khẩu là biện pháp bảo vệ chung an toàn nhất mà chúng ta có để ngăn chặn truy cập tài khoản trái phép. Một cuộc tấn công phổ biến xảy ra để giành quyền truy cập vào tài khoản là cuộc tấn công mật khẩu (password attack). Cuộc tấn công này sử dụng phần mềm bẻ khóa mật khẩu để thử và đoán mật khẩu.



Tấn công bằng mật khẩu thông dụng là tấn công vét cạn (brute force). Nó liên tục thử các tổ hợp ký tự và chữ cái khác nhau cho đến khi có quyền truy cập. Vì tấn công này yêu cầu kiểm tra rất nhiều tổ hợp mật khẩu, nên thường mất một khoảng thời gian để thực hiện. CAPTCHA được sử dụng để phân biệt người với máy móc. Trong một tấn công mật khẩu, nếu chúng ta không được trang bị CAPTCHA, phần mềm tự động có thể tiếp tục cố gắng đăng nhập vào tài khoản cho đến khi tìm thấy mật khẩu phù hợp. Nhưng với CAPTCHA, nó ngăn không cho các cuộc tấn công này thực hiện.

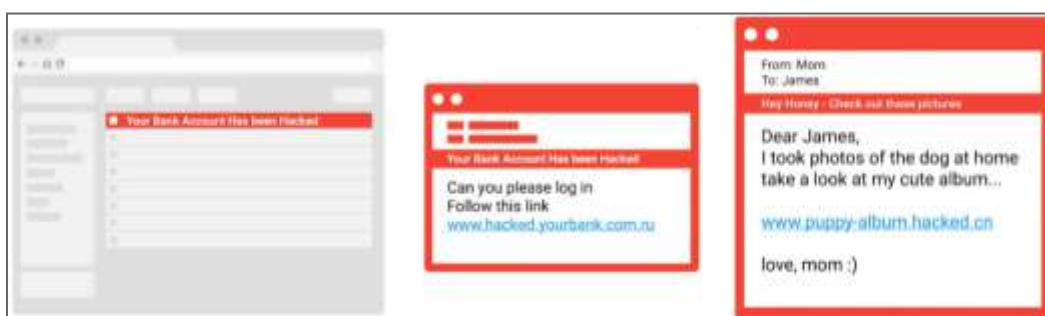
Một kiểu tấn công mật khẩu khác là tấn công từ điển (dictionary attack). Một cuộc tấn công từ điển không kiểm tra các tổ hợp vét cạn như abc123 hoặc ABC345. Thay vào đó, nó thử các từ thường được sử dụng trong mật khẩu, như bóng đá, hoa hồng, v.v.... Cách tốt nhất để ngăn chặn cuộc tấn công bằng mật khẩu là sử dụng các mật khẩu mạnh. Hạn chế đưa các từ trong từ điển vào và đảm bảo sử dụng kết hợp cả viết hoa, chữ số và ký hiệu. Nếu không có bất kỳ bảo mật dự phòng nào như CAPTCHA hoặc các biện pháp bảo vệ tài khoản khác, một ứng dụng bẻ khóa mật khẩu kinh điển sẽ mất khoảng một phút để bẻ khóa mật khẩu như sandwich. Nhưng sẽ lâu hơn đáng kể để bẻ khóa một từ giống như s, @, n, D, w, h, 1, c, h.

Tấn công phi kỹ thuật

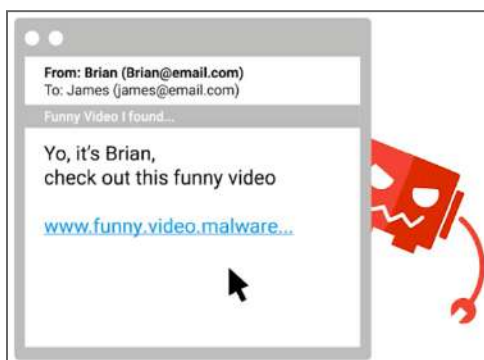
Tấn công phi kỹ thuật (social engineering attack) là một phương pháp tấn công chủ yếu dựa vào tương tác với con người thay vì máy tính. Chúng ta có thể chi hàng triệu đô la để trang bị cơ sở hạ tầng bảo mật tân tiến nhất. Nhưng nếu quản trị viên hệ thống có tất cả quyền truy cập và bị lừa xử lý thông tin đăng nhập, chúng ta không thể làm gì để ngăn chặn điều đó. Con người luôn là mắt xích yếu nhất trong hệ thống bảo mật. Tấn công phi kỹ thuật là một loại trò lừa đảo trong đó những kẻ tấn công sử dụng các kỹ thuật lừa đảo để có được quyền truy cập vào thông tin cá nhân hoặc lừa nạn nhân thực hiện điều nào đó.



Một loại tấn công phi kỹ thuật phổ biến là phishing. Phishing thường xảy ra khi một email độc hại được gửi đến nạn nhân được nguy trang dưới dạng một thứ gì đó hợp pháp. Một cuộc tấn công phishing phổ biến là email cho biết tài khoản ngân hàng của chúng ta đã bị xâm phạm. Và sau đó, cung cấp một liên kết để đặt lại mật khẩu. Khi truy cập vào liên kết, nó trông giống như trang web của ngân hàng nhưng thực chất đó là một trang web giả mạo. Vì vậy, chúng ta đã bị lừa nhập mật khẩu và thông tin đăng nhập hiện tại của mình để đặt lại mật khẩu. Một biến thể khác của lừa đảo là spear phishing. Cả hai cách lừa đảo đều có cùng mục tiêu cuối cùng, nhưng spear phishing nhắm vào cá nhân hoặc nhóm cụ thể. Các email giả mạo có thể chứa một số thông tin cá nhân như tên của chúng ta hoặc tên của bạn bè hoặc gia đình. Vì vậy, chúng trông có vẻ đáng tin cậy hơn.



Giả mạo (spoofing) là khi một nguồn giả mạo thành một thứ khác. Hãy nghĩ về một email giả mạo. Đây là những gì sẽ xảy ra khi chúng ta nhận được một email có địa chỉ người gửi gây hiểu lầm.



Không phải tất cả tấn công phi kỹ thuật đều xảy ra trực tuyến. Trên thực tế, có trường hợp tấn công xảy ra thông qua tiếp xúc vật lý thực tế. Một trong số đó là tấn công mồi nhử (baiting), dùng để dụ nạn nhân làm điều gì đó. Ví dụ, kẻ tấn công có thể để lại ổ USB ở đâu đó với hy vọng rằng có người sẽ cắm nó vào máy của họ. Nhưng khi cắm vào, họ đã cài phần mềm độc hại vào máy mình mà không hề hay biết.

Một cuộc tấn công khác có thể xảy ra ngoại tuyến được gọi là tailgating, tạm dịch là trà trộn. Về cơ bản, đó là cách thức xâm nhập vào một khu vực hạn chế hoặc tòa nhà bằng cách theo chân một nhân viên thực sự. Trong hầu hết các môi trường công ty, quyền truy cập vào tòa nhà bị hạn chế thông qua việc sử dụng thẻ khóa hoặc một số phương thức khác. Nhưng một kẻ trà trộn có thể sử dụng các chiến thuật phi kỹ thuật để lừa một nhân viên nghĩ rằng họ ở đó vì một lý do chính đáng như bảo trì tòa nhà hoặc giao các gói hàng. Sau khi thâm nhập, họ có quyền truy cập vào tài sản công ty.



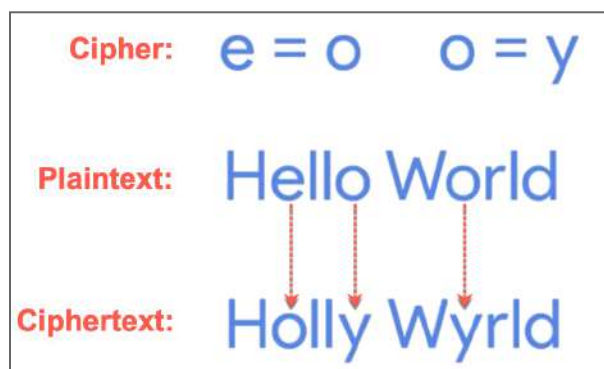
Bài đọc 3: Mật Mã Học

1. Mã hóa và giải mã

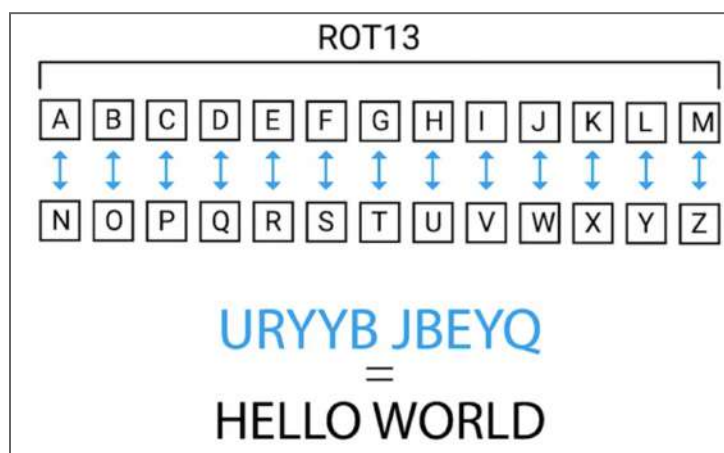
Các khái niệm về mã hóa và giải mã

Chủ đề về mật mã, hay ẩn thông điệp khỏi những kẻ thù tiềm tàng, đã có từ hàng nghìn năm trước. Nó phát triển rất nhiều với sự ra đời của công nghệ hiện đại, máy tính và viễn thông. Mã hóa (encryption) là hành động lấy một thông điệp, được gọi là bản rõ (plaintext), và áp dụng một phép toán cho nó, được gọi là phép mã hóa (cipher). Vì vậy, chúng ta nhận được một thông điệp bị cắt xén và không thể đọc được. Đây được gọi là bản mã (ciphertext). Quá trình ngược lại, lấy đầu ra bị mã hóa và chuyển nó trở lại thành văn bản thuần túy có thể đọc được, gọi là giải mã (decryption).

Ví dụ, xem xét một phép mã hóa đơn giản sau. Chúng ta thay thế chỗ có ký tự e bằng ký tự o và chỗ có ký tự o bằng ký tự y. Chúng ta sẽ lấy bản rõ Hello World và đưa nó vào phép mã hóa cơ bản này. Kết quả chúng ta có bản mã là Holly Wyrld. Khá dễ dàng để giải mã bản mã vì đây là một ví dụ rất cơ bản.



Một cách mã khác như đổi 13 ký tự đầu của bảng chữ cái với 13 ký tự sau. Mặc dù nó vẫn đơn giản để phá nhưng so với cách đầu có phần phức tạp hơn. Chúng ta vẫn còn nhiều cách thức mã hoặc thuật toán phức tạp và an toàn hơn và sẽ được đề cập ở các phần sau.



Phép mã hóa thực sự được tạo thành từ hai thành phần, thuật toán mã hóa (encryption algorithm) và khóa (key). Thuật toán mã hóa là logic hoặc quy trình cơ bản được sử dụng để chuyển bản rõ thành bản mã. Các thuật toán này thường là các phép toán rất phức tạp. Thành phần quan trọng khác của mật mã là chìa khóa, nó giới thiệu một cái gì đó độc đáo vào thuật toán. Chính xác nó là đoạn thông tin điều khiển hoạt động của thuật toán mã hóa nhằm giúp cá biệt hóa quá trình này. Nếu không có chìa khóa, bất kỳ ai sử dụng cùng một thuật toán sẽ có thể giải mã tin nhắn của chúng ta và chúng ta sẽ không thực sự có bất kỳ bí mật nào. Vì vậy, để tóm tắt lại, trước tiên, chúng ta chọn một thuật toán mã hóa muốn sử dụng để mã hóa thông điệp của mình, sau đó chọn một khóa. Tiếp theo, chúng ta có thể chạy mật mã qua bản rõ thông điệp của mình và nhận được một bản mã đã mã hóa sẵn sàng để gửi ra ngoài, an toàn và bảo mật khỏi những con mắt tò mò.

Bảo vệ và tấn công hệ thống mã hóa

Mục đích cơ bản của mật mã là để bảo vệ bí mật khỏi bị đọc bởi các bên trái phép. Điều đó có nghĩa là ít nhất một số thành phần của mật mã cũng cần được giữ bí mật. Một số người cho rằng bằng cách giữ bí mật thuật toán mã hóa, thông điệp sẽ được bảo mật. Đây là phương pháp được mô tả với thuật ngữ, bảo mật dựa trên sự mập mờ (security through obscurity, STO). Về cơ bản, nếu không ai biết thuật toán nào đang sử dụng, thì chúng ta sẽ an toàn trước những kẻ tấn công. Tuy nhiên, hãy liên tưởng cách này với việc giấu chìa khóa nhà dưới tấm thảm chùi chân, chỉ cần tên trộm không biết rằng chúng ta giấu chìa khóa dự phòng dưới tấm thảm, thì chúng ta vẫn an toàn. Nhưng một khi thông tin đó

được phát hiện, tất cả bảo mật sẽ đi ra ngoài cửa sổ cùng với các vật có giá trị. Vì vậy, bảo mật dựa trên sự mập mờ không phải là thứ mà chúng ta nên dựa vào để đảm bảo an ninh thông tin hoặc hệ thống.

Nguyên tắc của Kerckhoff nói rằng một hệ thống mật mã vẫn còn phải an toàn, ngay cả khi mọi thứ về hệ thống đều được biết ngoại trừ khóa. Điều này có nghĩa là ngay cả khi kẻ thù của chúng ta biết thuật toán mã hóa chính xác mà chúng ta sử dụng để bảo mật dữ liệu, chúng vẫn không thể khôi phục bản rõ từ một bản mã bị chặn. Chúng ta cũng có thể nghe nguyên tắc này được gọi là châm ngôn của Shannon hay kẻ thù biết hệ thống.

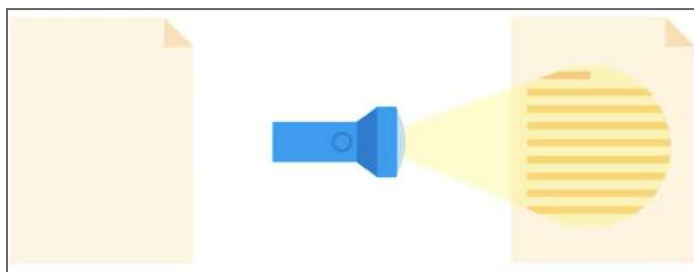
Hệ thống phải được bảo mật, ngay cả khi đối thủ của chúng ta biết chính xác loại hệ thống mã hóa đang sử dụng, miễn là các khóa vẫn an toàn. Việc thực hiện mã hóa và ẩn thông điệp từ các bên thứ ba được gọi là mật mã (cryptology). Nghiên cứu về thực hiện này được gọi là mật mã học (cryptography). Ngược lại với việc tìm kiếm thông điệp ẩn hoặc cố gắng giải mã thông điệp được mã hóa được gọi là phân tích mật mã (cryptanalysis). Hai lĩnh vực này đã cùng phát triển trong suốt lịch sử, với các mật mã và hệ thống mật mã mới được phát triển khi các trường trước đó bị hỏng hoặc bị phát hiện là dễ bị tấn công. Hai lĩnh vực này đã cùng phát triển trong suốt lịch sử với các mật mã và hệ thống mật mã mới được phát triển khi cái trước đó bị phá hay bị phát hiện là dễ bị tấn công.

Một trong những mô tả sớm nhất được ghi lại về phương pháp phá mã là của một nhà toán học Ả Rập ở thế kỷ thứ 9. Ông ta đã mô tả phương pháp phân tích tần số để phá vỡ các thông điệp được mã hóa. Phân tích tần số (frequency analysis) là thực hiện thống kê tần suất mà các chữ cái xuất hiện trong bản mã. Tiền đề đằng sau kiểu phân tích này là trong ngôn ngữ viết, một số chữ cái nhất định xuất hiện thường xuyên hơn những chữ cái khác và một số chữ cái thường được nhóm lại với nhau hơn những chữ cái khác. Ví dụ, các chữ cái được sử dụng phổ biến nhất trong tiếng Anh là e, t, a và o. Các cặp chữ cái thường thấy nhất là th, er, on và an. Một số thuật toán mã hóa, đặc biệt là thuật toán mã chuyển dịch và thay thế cổ điển bảo toàn tần số tương đối của các chữ cái trong bản rõ. Và do đó, chúng có thể dễ bị tổn thương bởi loại phân tích này.

Ẩn dữ liệu

Steganography là thuật ngữ mô tả quá trình che giấu thông tin khỏi những người quan sát, nhưng không mã hóa nó. Nói cách khác, thông điệp ở dạng văn bản rõ ràng và không cần giải mã để đọc nhưng nó bị ẩn khỏi tầm nhìn. Nó giống như chúng ta viết một thông điệp bằng cách sử dụng mực vô hình. Mực vô hình được hiển thị bằng cách sử dụng một cơ chế đặc thù.

Các kỹ thuật steganography hiện đại bao gồm nhúng thông điệp và thậm chí tập tin vào các tập tin khác như hình ảnh hoặc video. Đối với một người quan sát bình thường, họ sẽ chỉ nhìn thấy hình ảnh của một vật thể thông thường. Nhưng nếu đưa hình ảnh đó vào phần mềm steganography, nó sẽ trích xuất một thông điệp ẩn.

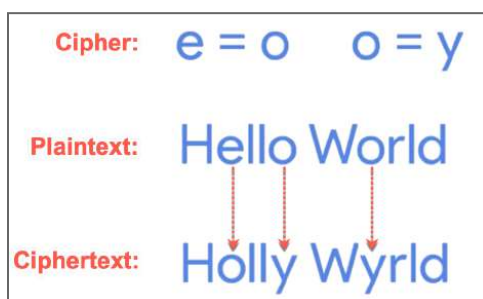


2. Mã hóa đối xứng

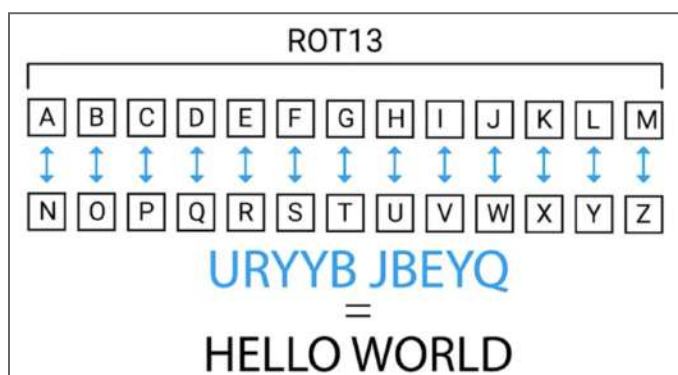
Khái niệm và nguyên lý thực thi

Mã hóa đối xứng (symmetric cryptography) là cách thức sử dụng cùng một khóa để mã hóa và giải mã thông điệp. Thực tế, các khóa mã hóa và giải mã có thể giống hệt nhau hoặc có thể có một sự chuyển đổi đơn giản. Các khóa đại diện cho bí mật được chia sẻ giữa hai hoặc nhiều bên và có thể được sử dụng để duy trì liên kết thông tin riêng tư.

Mật mã thay thế (substitution cipher) là một cơ chế mã hóa thay thế các phần của bản rõ để được bản mã. Cách mã hóa chuỗi hello world bên dưới là một ví dụ về mật mã thay thế vì chúng ta thay thế một số ký tự bằng các ký tự khác. Trong trường hợp này, chìa khóa sẽ là ánh xạ các ký tự giữa bản rõ và bản mã mà không cần biết chữ cái nào được thay thế. Nếu có khóa hoặc bảng thế, thì chúng ta có thể dễ dàng đảo ngược quy trình và giải mã thông điệp được mã hóa bằng cách thực hiện thao tác ngược lại.



Một ví dụ nổi tiếng về mã hóa thay thế là mã Caesar. Thuật toán này thay thế các ký tự trong bảng chữ cái bằng những ký tự khác thông qua phép dời hoặc xoay bảng chữ cái. Số bước dời chính là chìa khóa. Ví dụ với ROT13 nghĩa là bảng chữ cái được xoay 13 vị trí. Như vậy, khóa của mã hóa này là 13. Khi áp dụng bảng ROT13 này lên chuỗi Hello World, chúng ta sẽ có được bản mã như hình dưới. Để đảo ngược quá trình này và quay trở lại bản rõ, chúng ta chỉ thực hiện thao tác ngược lại bằng cách tra cứu các ký tự ở phía đầu ra của bảng ánh xạ.

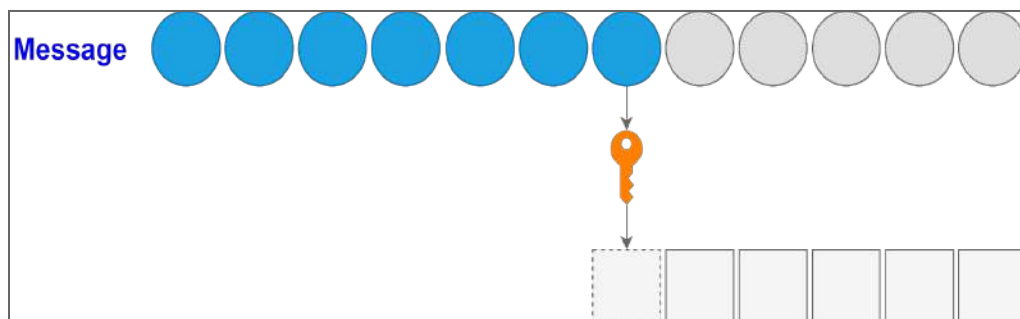


Phân loại

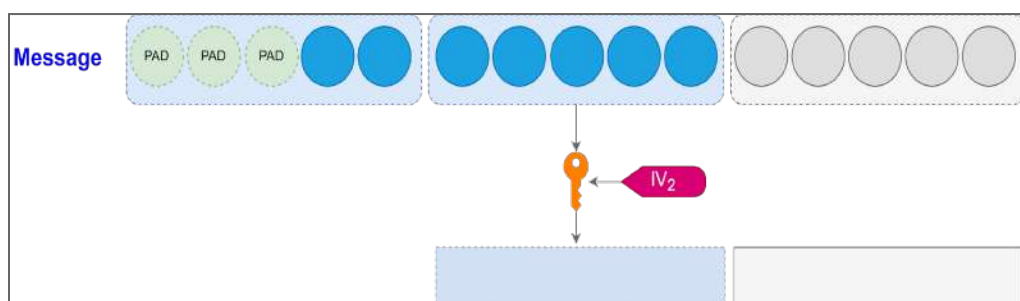
Một cách phân loại mã hóa đối xứng nữa là mã hóa dòng (stream cipher) và mã hóa khối (block cipher). Các cách mã hóa này liên quan đến thuật toán mã hóa hoạt động trên bản rõ.

Mã hóa dòng nhận liên tiếp ký tự đầu vào và mã hóa từng ký tự này. Vì vậy, có một mối quan hệ 1-1 giữa dữ liệu ban đầu và dữ liệu được mã hóa. Nhìn chung, mã hóa dòng thực hiện nhanh hơn và ít phức tạp hơn, nhưng chúng có thể kém an toàn hơn so với mã hóa khối. Nếu việc tạo và xử lý khóa không được thực

hiện đúng cách, hay nếu cùng một khóa được sử dụng để mã hóa dữ liệu nhiều lần, thì hệ thống mã hóa có nguy cơ bị phá.



Trong khi đó, mã hóa khối nhận dữ liệu và chia dữ liệu thành các khối có kích thước cố định, sau đó mã hóa toàn bộ khối đó thành một đơn vị. Nếu dữ liệu không đủ lớn để lấp đầy khối, thì không gian còn lại sẽ được đệm thêm. Để tránh sử dụng lại khóa, người ta sử dụng vectơ khởi tạo (IV). Đó là dữ liệu ngẫu nhiên được tích hợp vào khóa để tạo thành khóa mới. Khóa kết hợp này sử dụng để mã hóa dữ liệu. Bằng cách này, khóa mã hóa được sử dụng chỉ một lần. Để giải mã, vectơ khởi tạo phải được gửi ở dạng bản rõ cùng với thông điệp được mã hóa.

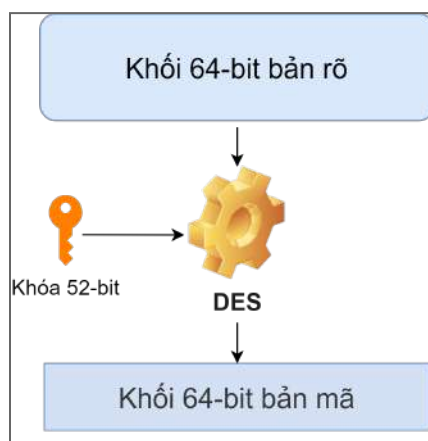


Các thuật toán

Thuật toán DES

Một trong những chuẩn mã hóa sớm nhất là DES, viết tắt của Data Encryption Standard. DES được thiết kế vào những năm 1970 bởi IBM, với sự hợp tác của Cơ quan An ninh Quốc gia Hoa Kỳ. DES đã được thông qua như một FIPS, đó là tiêu chuẩn xử lý thông tin liên bang chính thức cho Hoa Kỳ. Điều này có nghĩa là DES đã được chấp nhận như một tiêu chuẩn liên bang để mã hóa và bảo mật dữ liệu của chính phủ. DES là một mã hóa khối đối xứng sử dụng kích thước khóa

64-bit và hoạt động trên các khối có kích thước 64-bit. Mặc dù kích thước khóa về mặt kỹ thuật là độ dài 64 bit, nhưng 8 bit trong số đó được sử dụng để kiểm tra chẵn lẻ, đó là một dạng kiểm tra lỗi đơn giản. Điều này có nghĩa là độ dài khóa thực cho DES chỉ còn 56-bit.

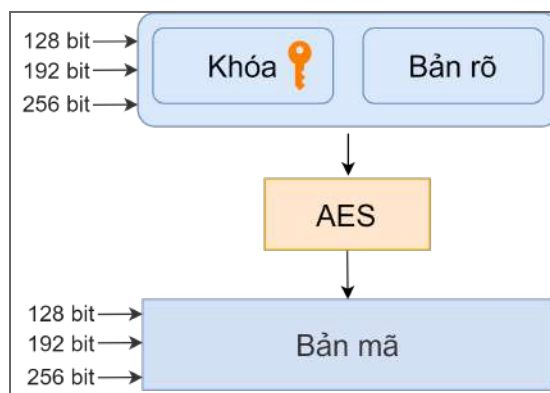


Độ dài khóa cực kỳ quan trọng trong mật mã vì về cơ bản nó xác định sức mạnh tiềm năng tối đa của hệ thống. Giả sử một thuật toán mã hóa đối xứng không có điểm yếu nào trong chính thuật toán thì cách duy nhất để kẻ tấn công có thể phá vỡ mã hóa là tấn công khóa thay vì thuật toán. Một phương pháp tấn công là đoán khóa và xem liệu thông điệp có được giải mã chính xác không. Đây được coi là một cuộc tấn công vét cạn (brute force). Trong thuật toán DES, độ dài khóa 56 bit cho tối đa 2^{56} , tức khoảng 72 triệu tỷ khả năng. Đó có vẻ như là một con số rất lớn vào những năm 1970. Nhưng khi máy tính trở nên nhanh hơn, các khóa DES trở nên không còn quá lớn. Năm 1998, tổ chức có tên EFF, Electronic Frontier Foundation, đã giải mã một thông điệp được mã hóa bằng DES chỉ trong 56 giờ.

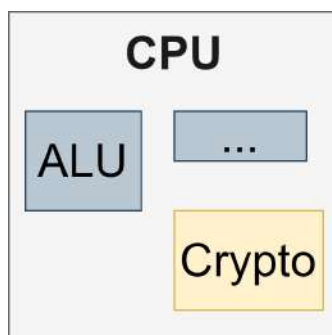
Thuật toán AES

Năm 1997, NIST, Viện Tiêu chuẩn và Công nghệ Quốc gia, muốn thay thế DES bằng một thuật toán mới, và vào năm 2001, đã thông qua AES (Advanced Encryption Standard) sau một cuộc thi quốc tế. AES cũng là mật mã công khai đầu tiên và duy nhất được Cơ quan An ninh Quốc gia Hoa Kỳ chấp thuận sử dụng với thông tin tuyệt mật. AES cũng là một mã hóa khối đối xứng tương tự như DES. Nhưng AES sử dụng khối 128 bit, gấp đôi kích thước của khối DES và hỗ trợ độ dài khóa 128 bit, 192 bit hoặc 256 bit. Do kích thước khóa lớn, các

cuộc tấn công vét cạn (brute-force) vào AES hiện chỉ là lý thuyết, bởi vì sức mạnh tính toán cần thiết vượt quá bất cứ điều gì khả thi hiện nay.



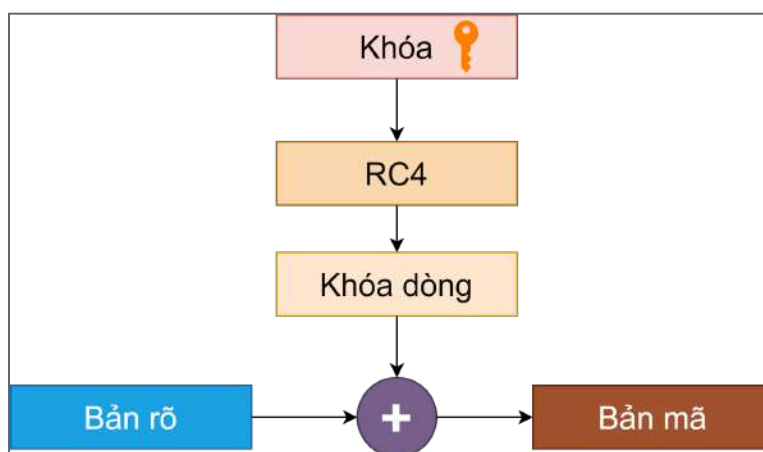
Một điều quan trọng khác cần ghi nhớ khi xem xét các thuật toán mã hóa là tốc độ và tính dễ thực hiện. Một thuật toán không nên quá khó thực hiện vì việc triển khai phức tạp có thể dẫn đến lỗi và khả năng mất bảo mật do các lỗi được đưa vào trong quá trình triển khai. Tốc độ rất quan trọng vì đôi khi dữ liệu sẽ được mã hóa bằng cách chạy dữ liệu qua thuật toán mã hóa nhiều lần. Các loại thực thi mã hóa này thường được thực hiện bởi các thiết bị, vì vậy chúng thực hiện càng nhanh với tác động tối thiểu đến hệ thống thì càng tốt. Đây là lý do tại sao một số nền tảng triển khai các thuật toán mật mã này trong phần cứng để tăng tốc quá trình và loại bỏ một số gánh nặng từ CPU. Ví dụ, các CPU hiện đại của Intel hoặc AMD có các lệnh AES được tích hợp sẵn trong CPU. Điều này cho phép tốc độ tính toán và hiệu quả cao hơn nhiều khi làm việc với các tác vụ mật mã.



Thuật toán RC4

RC4 (Rivest Cipher 4), là một mã hóa dòng đối xứng đã được áp dụng rộng rãi vì tính đơn giản và tốc độ của nó. RC4 hỗ trợ kích thước khóa từ 40-bit đến 2.048-bit. Vì vậy, điểm yếu của RC4 không phải do các cuộc tấn công vét cạn (brute-force), mà bản thân thuật toán mã hóa có những điểm yếu và lỗ hổng. Một ví dụ gần đây về việc RC4 bị phá là cuộc tấn công RC4 NOMORE. Cuộc tấn công này có thể khôi phục cookie xác thực từ kết nối được mã hóa TLS chỉ trong 52 giờ.

Vì đây là một cuộc tấn công vào bản thân mật mã RC4, bất kỳ giao thức nào sử dụng mật mã này đều có khả năng bị tấn công. Mặc dù vậy, RC4 đã được sử dụng trong một loạt các giao thức mã hóa phổ biến, như WEP để mã hóa không dây và WPA, kế thừa của WEP. Nó cũng được hỗ trợ trong SSL và TLS cho đến năm 2015 khi RC4 bị loại bỏ trong tất cả các phiên bản TLS vì những điểm yếu cố hữu. Vì lý do này, hầu hết các trình duyệt web lớn đã ngừng hỗ trợ RC4 hoàn toàn, cùng với tất cả các phiên bản SSL và thay vào đó sử dụng TLS. Cấu hình an toàn được ưu tiên là TLS 1.2 với AES GCM. Đây là chế độ hoạt động cho mã hóa khối AES về cơ bản biến nó thành mã hóa dòng. GCM hoạt động bằng cách lấy giá trị ngẫu nhiên, tăng giá trị này và mã hóa giá trị, tạo ra các khối bản mã được đánh số liên tục. Các bản mã sau đó được kết hợp vào bản rõ để được mã hóa. GCM cực kỳ phổ biến do tính bảo mật của nó dựa trên mã hóa AES, cùng với hiệu suất của nó. Nó có thể chạy song song với hiệu năng cao.



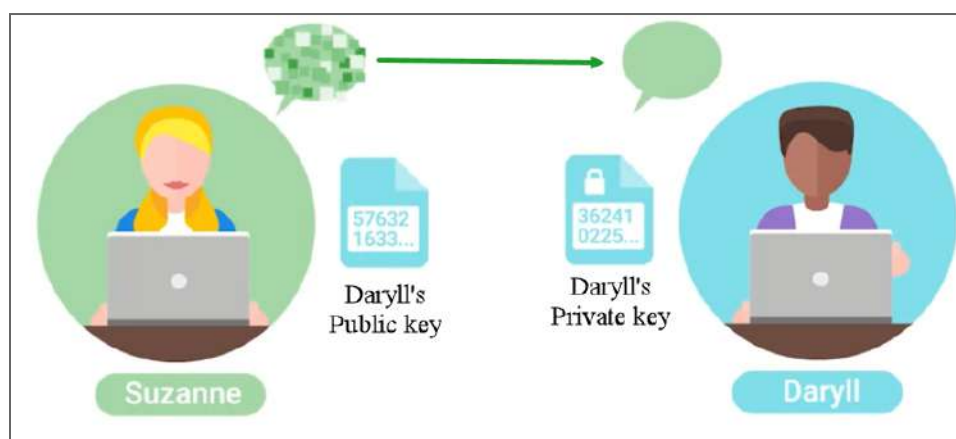
Do tính chất đối xứng của quá trình mã hóa và giải mã, nó tương đối dễ thực hiện và bảo trì. Các thuật toán đối xứng cũng rất nhanh và hiệu quả trong việc

mã hóa và giải mã hàng loạt dữ liệu lớn. Tuy nhiên, do chỉ có một khóa dùng chung cho cả mã hóa và giải mã nên việc trao đổi khóa trở nên phức tạp. Ví dụ, làm sao để chia sẻ mật khẩu Wifi an toàn, việc thay đổi khóa thường xuyên khiến phải cập nhật rất nhiều thiết bị hợp lệ.

3. Mã hóa bất đối xứng

Khái niệm và nguyên lý thực thi

Mã hóa bất đối xứng (asymmetric encryption) là cách thức sử dụng khóa khác nhau cho quá trình mã hóa và giải mã. Trong mã hóa bất đối xứng, một cặp khóa được sử dụng. Cặp khóa này bao gồm một khóa được gọi là khóa công khai (public key). Khóa này dùng để mã hóa dữ liệu. Một khóa khác là khóa bí mật (private key) được dùng để giải mã dữ liệu đã được khóa bởi khóa công khai. Khóa công khai không thể dùng để mở chính thông điệp mà được khóa bởi chính nó. Tương tự, khóa bí mật không dùng để khóa thông điệp. Ví dụ minh họa, giả sử có một người tên là Suzanne muốn gửi thông điệp bí mật đến Daryll. Cô ta sẽ lấy khóa công khai được phát hành rộng rãi bởi Daryll và mã hóa thông điệp cô ta muốn gửi đi. Khi thông điệp này được di chuyển, không có người nào có thể giải mã nếu như không có khóa bí mật. Do đó, chỉ có Daryll có thể giải mã thông điệp này với khóa anh ta cất giữ bí mật.



Chữ ký số

Chữ ký số (digital signature) là một kỹ thuật toán học để xác thực thông điệp điện tử. Ví dụ, Suzanne muốn gửi một tin nhắn cho Darryll và cô ấy muốn đảm bảo rằng Daryll biết thông điệp đến từ cô ấy chứ không phải ai khác đồng thời

nó không bị sửa đổi hay giả mạo. Cô ấy có thể làm điều này bằng cách soạn thông điệp, kết hợp nó với khóa cá nhân của mình để tạo chữ ký điện tử. Sau đó, cô ấy gửi tin nhắn này cùng với chữ ký điện tử đến Daryll. Giờ đây, Daryll có thể xác minh nguồn gốc và tính xác thực của thông điệp bằng cách kết hợp chữ ký điện tử và khóa công khai của Suzanne. Nếu thư thực sự được ký bằng khóa riêng tư của Suzanne chứ không phải của người khác và thư không được sửa đổi gì cả, thì chữ ký điện tử sẽ được xác thực. Nếu thông điệp bị sửa đổi, dù chỉ bằng một ký tự khoảng trắng, thì việc xác thực sẽ không thành công và Daryll không nên tin tưởng vào thông điệp này. Đây là một thành phần quan trọng của hệ thống mật mã không đối xứng.

Ba khái niệm mà hệ thống mật mã không đối xứng cấp cho chúng ta là tính bảo mật (confidentiality), tính xác thực (authenticity) và tính chống thoái thác (non-repudiation). Bảo mật được đảm bảo thông qua cơ chế mã hóa-giải mã. Tính xác thực được cấp bởi cơ chế chữ ký số, vì thông điệp có thể được xác thực hoặc xác minh rằng nó không bị giả mạo. Chống thoái thác nghĩa là tác giả của thông điệp không thể phủ nhận nguồn gốc của thông điệp. Nói cách khác, điều này cho phép chúng ta đảm bảo rằng thông điệp đến từ người tự xưng là tác giả.

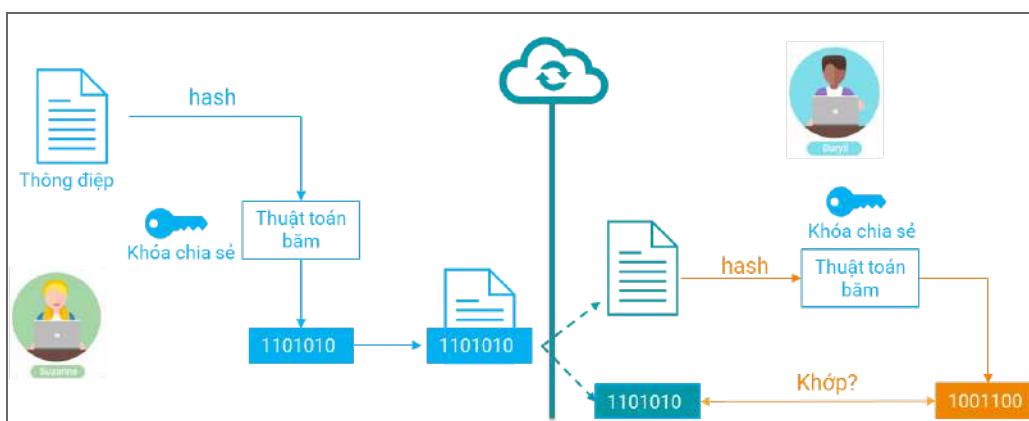
Mặc dù mã hóa bất đối xứng hoạt động tốt trong các môi trường không tin cậy, nhưng nó cũng tốn chi phí hơn và phức tạp hơn về mặt tính toán. Trong khi đó, các thuật toán mã hóa đối xứng nhanh hơn, hiệu quả hơn và mã hóa một lượng lớn dữ liệu. Trên thực tế, người ta phối hợp lợi ích tương đối của cả hai loại mã hóa này cho các mục đích khác nhau. Thuật toán mã hóa bất đối xứng được chọn làm cơ chế trao đổi khóa hoặc mật mã. Điều này có nghĩa là khóa mã hóa đối xứng được truyền an toàn cho bên kia bằng cách sử dụng mã hóa bất đối xứng. Sau khi nhận được khóa này, dữ liệu có thể được gửi nhanh chóng, hiệu quả và an toàn bằng cách sử dụng mã hóa đối xứng.

Mã xác thực thông điệp

Mã xác thực thông điệp (Message Authentication Codes, MAC) là một mẫu thông tin cho phép xác thực thông điệp đã nhận, đảm bảo rằng thông điệp đó đến từ người gửi thực sự chứ không phải bên thứ ba giả mạo họ. Nó cũng đảm bảo rằng thông điệp không bị sửa đổi. Điều này nghe có vẻ giống với chữ ký điện tử. Tuy nhiên điểm khác biệt là thuật toán băm (hash) có sử dụng khóa bí

mật và khóa này được sử dụng giống nhau ở cả người gửi và người nhận. Kỹ thuật băm là gì chúng ta sẽ bàn chi tiết trong các phần sau.

Quá trình diễn ra cơ bản gồm sau khi băm thông điệp cùng với khóa để có được MAC, nó sẽ được gửi cùng với thông điệp đến bên nhận. Phía người nhận xác minh bằng cách thực hiện thao tác tương tự trên thông điệp đã nhận, sau đó so sánh MAC đã tính toán với MAC nhận được. Nếu MAC giống nhau, thì thông điệp được xác thực.



Một loại MAC phổ biến và an toàn được gọi là HMAC (Keyed-Hash Message Authentication Code). HMAC sử dụng hàm băm mật mã cùng với khóa bí mật để tạo MAC. Bất kỳ hàm băm mật mã nào cũng có thể được sử dụng như SHA-1 hoặc MD5 và sức mạnh hoặc tính bảo mật của MAC phụ thuộc vào tính bảo mật cơ bản của hàm băm mật mã được sử dụng.

Ngoài ra còn có các MAC dựa trên mã hóa đối xứng, khối hoặc dòng như DES hoặc AES, được gọi là CMAC (Cipher-Based Message Authentication Code). Quá trình này tương tự như HMAC, nhưng thay vì sử dụng hàm băm để tạo mã, một thuật toán mã hóa đối xứng được sử dụng. Một dạng CMAC là CBC-MAC (Cipher Block Chaining Message Authentication Code) sử dụng mã hóa khối. Nó hoạt động bằng cách lấy thông điệp và mã hóa nó bằng phương pháp mã hóa khối hoạt động ở chế độ CBC. Chế độ CBC là cách thức kết hợp khối đã được mã hóa trước đó làm thành phần khóa cho khối tiếp theo. Vì vậy, nó xây dựng một chuỗi các khối được mã hóa đầy đủ và không bị sửa đổi để có thể giải mã được. Nói cách khác, chuỗi khối được mã hóa phụ thuộc lẫn nhau này có nghĩa là bất kỳ sửa đổi nào đối với văn bản sẽ dẫn đến kết quả cuối cùng là toàn bộ văn bản sẽ không giải mã được.

Các thuật toán mã hóa bất đối xứng

RSA

Một trong những mã hóa bất đối xứng đầu tiên được phát triển là RSA, tên viết tắt của ba nhà đồng sáng chế. Hệ thống mật mã này đã được cấp bằng sáng chế vào năm 1983 và được RSA Security phát hành ra công chúng vào năm 2000. Hệ thống RSA chỉ định cơ chế tạo và phân phối khóa cùng với hoạt động mã hóa và giải mã bằng cách sử dụng các khóa này. Chúng ta sẽ không đi vào chi tiết của thuật toán vì nó khá phức tạp để có thể trình bày trong phạm vi khóa học này. Nhưng điều quan trọng cần biết là quá trình tạo khóa phụ thuộc vào việc chọn hai số nguyên tố duy nhất, ngẫu nhiên và rất lớn.

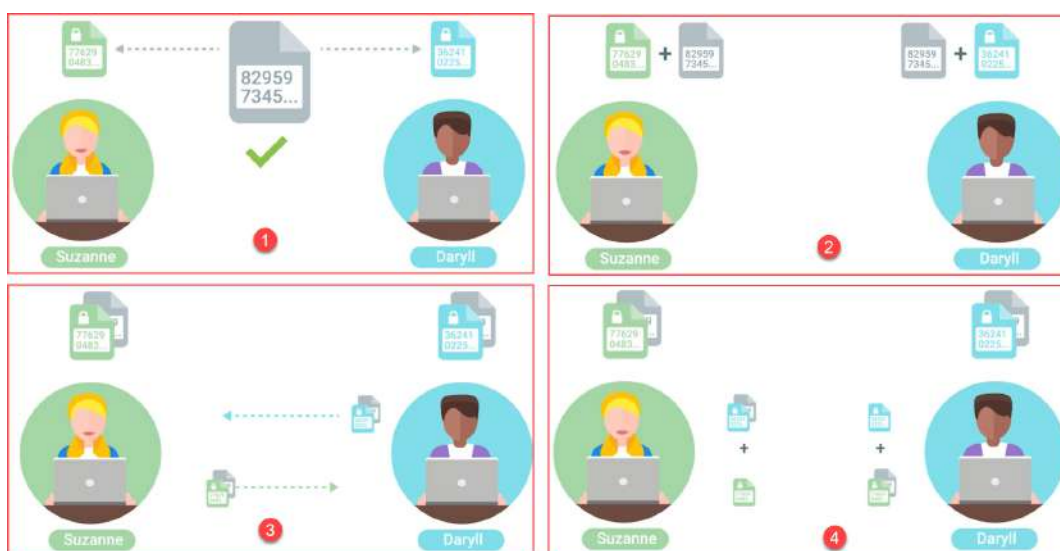
DSA

DSA (Digital Signature Algorithm) là một ví dụ khác về thuật toán mã hóa bất đối xứng, mặc dù nó chủ yếu được sử dụng để ký và xác minh dữ liệu. Nó đã được cấp bằng sáng chế vào năm 1991 và là một phần của Tiêu chuẩn Xử lý Thông tin Liên bang của chính phủ Hoa Kỳ. Tương tự như RSA, đặc điểm kỹ thuật bao gồm quá trình tạo khóa cùng với việc ký và xác minh dữ liệu bằng cách sử dụng các cặp khóa. Điều quan trọng cần nói là tính bảo mật của hệ thống này phụ thuộc vào việc chọn một giá trị gốc ngẫu nhiên được kết hợp vào quá trình ký. Nếu giá trị này bị rò rỉ hoặc nếu nó có thể được suy ra do số nguyên tố không ngẫu nhiên, thì kẻ tấn công có thể khôi phục khóa bí mật. Điều này thực sự đã xảy ra vào năm 2010 với Sony và máy chơi game PlayStation 3 của họ. Hóa ra họ đã không đảm bảo giá trị ngẫu nhiên này được thay đổi cho mọi chữ ký. Điều này dẫn đến việc một nhóm hacker có tên Fail0verflow có thể khôi phục khóa bí mật mà Sony đã sử dụng để ký phần mềm cho nền tảng của họ. Điều này dẫn đến việc vi phạm bản quyền trò chơi trở thành một vấn đề đối với Sony.

DH

Một thuật toán trao đổi khóa phổ biến khác là DH hoặc Diffie-Hellman được đặt tên cho những người đồng sáng chế. Hãy xem qua cách hoạt động của thuật toán trao đổi khóa DH. Giả sử chúng ta có hai người muốn giao tiếp qua một kênh không an toàn. Đầu tiên, họ thống nhất một con số bắt đầu sẽ là số nguyên tố ngẫu nhiên và rất lớn. Con số này sẽ khác nhau cho mỗi phiên và

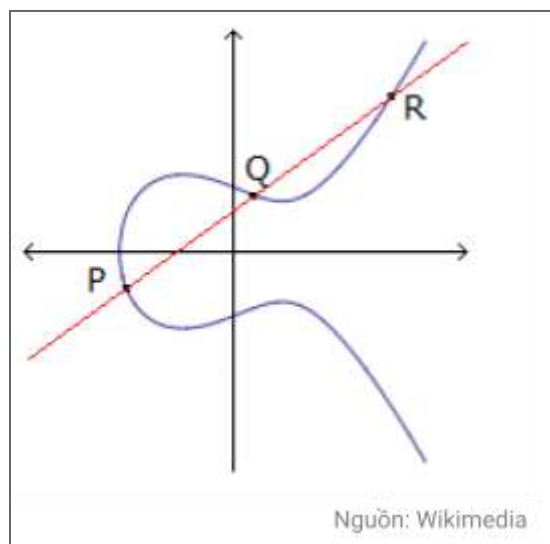
không cần phải bí mật. Tiếp theo, mỗi người chọn một số lớn ngẫu nhiên khác nhưng số này được giữ bí mật. Sau đó, họ kết hợp số được chia sẻ của họ với số bí mật tương ứng của họ và gửi hỗn hợp kết quả cho nhau. Tiếp theo, mỗi người kết hợp số bí mật của họ với giá trị kết hợp mà họ nhận được từ bước trước. Kết quả là một giá trị mới giống nhau ở cả hai bên mà không tiết lộ đủ thông tin cho bất kỳ kẻ nghe trộm tiềm năng nào để tìm ra bí mật được chia sẻ. Thuật toán này được thiết kế chủ yếu để trao đổi khóa, mặc dù đã có những nỗ lực để điều chỉnh nó cho mục đích mã hóa. Nó thậm chí còn được sử dụng như một phần của hệ thống PKI mà chúng ta sẽ bàn sau.



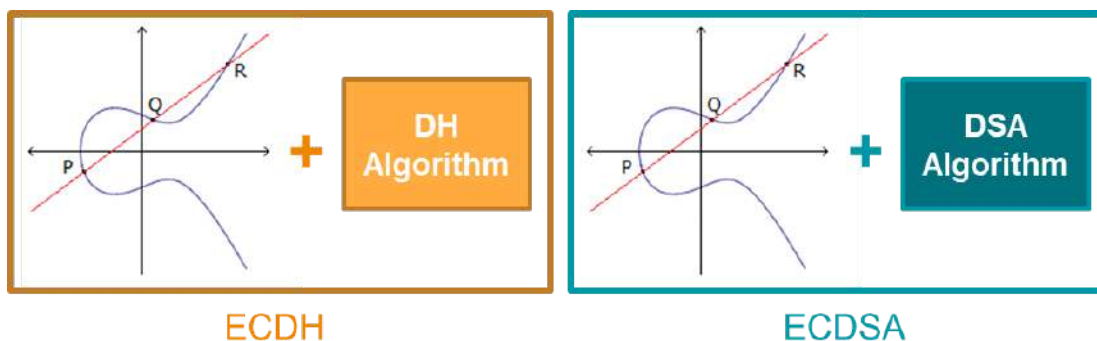
ECC

ECC (Elliptic curve cryptography) là thuật toán mã hóa khóa công khai sử dụng cấu trúc đại số của đường cong elliptic trên các trường hữu hạn để tạo khóa an toàn. Các hệ thống khóa công khai truyền thống sử dụng tính toán các số nguyên tố lớn trong khi ECC sử dụng đường cong elip. Đường cong này bao gồm một tập hợp các tọa độ thỏa một phương trình như $y^2 = x^3 + ax + b$. Đường cong elliptic có một vài đặc tính thú vị và độc đáo. Một là nó đối xứng qua trục hoành. Tiếp theo là mọi đường chéo sẽ cắt đường cong nhiều nhất ở ba vị trí. Thuộc tính này cho phép sử dụng đường cong elliptic trong mã hóa. Lợi ích của các hệ thống mã hóa dựa trên đường cong elliptic là chúng có thể đạt được tính bảo mật tương tự như các hệ thống khóa công khai truyền thống nhưng với kích thước khóa nhỏ hơn. Ví dụ, một khóa đường cong elliptic 256 bit,

sẽ có thể so sánh với khóa RSA 3072 bit. Điều này thực sự có lợi vì nó làm giảm lượng dữ liệu cần thiết được lưu trữ và truyền đi khi xử lý các khóa.



Cả DH và DSA đều có các biến thể đường cong elliptic, được gọi là ECDH và ECDSA. Tổ chức US NEST khuyến nghị sử dụng mã hóa EC và cơ quan quan ninh quốc gia NSA cho phép sử dụng mã hóa này để bảo vệ dữ liệu tuyệt mật bằng khóa EC 384 bit. Tuy nhiên, NSA đã bày tỏ lo ngại về việc mã hóa EC có khả năng dễ bị tấn công bởi các cuộc tấn công điện toán lượng tử, nhất là khi công nghệ điện toán lượng tử đang tiếp tục phát triển mạnh mẽ.



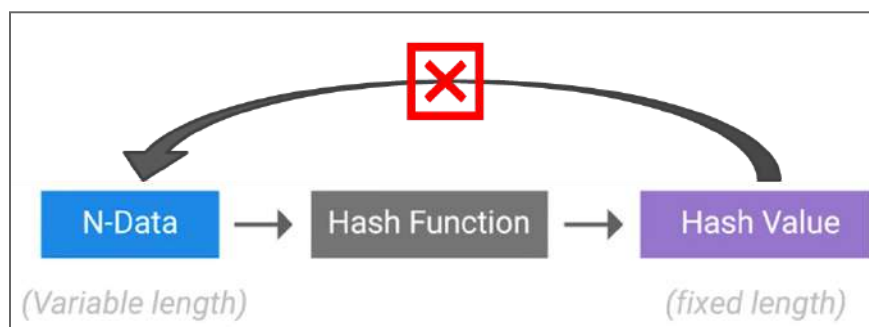
4. Băm

Giới thiệu và ứng dụng của băm

Hàm băm (hash function) là một loại hàm hoặc thao tác nhận đầu vào dữ liệu tùy ý và ánh xạ nó tới đầu ra có kích thước cố định. Kích thước đầu ra thường được xác định bằng bit dữ liệu và thường được bao gồm trong tên hàm băm. Điều này có nghĩa là chúng ta nạp bất kỳ dữ liệu nào vào một hàm băm và kết quả đầu ra sẽ luôn có cùng kích thước. Nhưng đầu ra phải là duy nhất đối với đầu vào, tức là hai đầu vào khác nhau không được trả về cùng một giá trị đầu ra. Hàm băm có nhiều ứng dụng trong máy tính nói chung và trong mật mã nói riêng. Đối với lĩnh vực mật mã học, hàm băm được sử dụng để xác thực, kiểm tra tính toàn vẹn của thông điệp, kiểm tra dấu vân tay, phát hiện lỗi dữ liệu và chữ ký số.

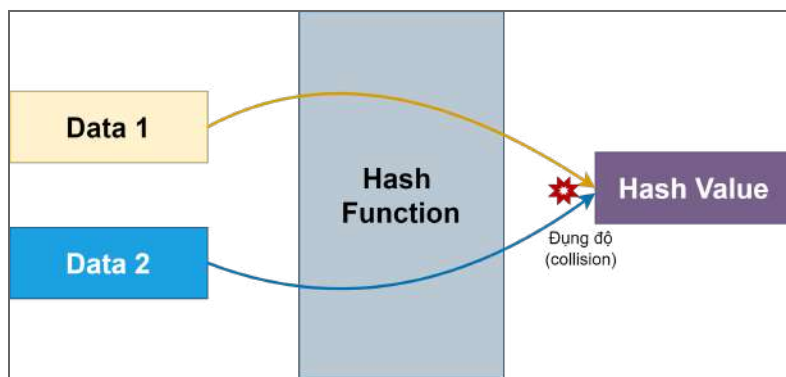


Hàm băm mã hóa (cryptographic hashing) khác biệt rõ ràng với việc mã hóa vì các hàm băm mã hóa là hàm một chiều. Nghĩa là nó chỉ có chuyển dữ liệu thành giá trị băm nhưng không thể phục hồi giá trị này thành dữ liệu ban đầu.



Hàm băm mã hóa lý tưởng phải có tính xác định, có nghĩa là cùng một giá trị đầu vào phải luôn trả về cùng một giá trị băm. Hàm phải được tính toán nhanh chóng và hiệu quả. Không thể đảo ngược và khôi phục văn bản ban đầu từ giá trị băm. Một thay đổi nhỏ trong đầu vào sẽ dẫn đến thay đổi đầu ra, do đó không có mối tương quan giữa sự thay đổi của đầu vào và sự thay đổi dẫn đến

kết quả của đầu ra. Cuối cùng, hàm cần hạn chế vấn đề đụng độ (hash collision). Đụng độ nghĩa là hai đầu vào khác nhau ánh xạ đến cùng một đầu ra.



Các thuật toán băm

MD5 là một hàm băm mã hóa phổ biến được thiết kế vào đầu những năm 1990. Nó hoạt động trên một khối 512 bit và tạo ra các giá trị băm 128 bit. Một lỗ hổng thiết kế đã được phát hiện vào năm 1996. Tuy nhiên, lỗ hổng này không được coi là nghiêm trọng, vì vậy hàm băm tiếp tục được sử dụng và chấp nhận rộng rãi. Năm 2004, người ta phát hiện ra rằng MD5 dễ bị đụng độ. Điều này cho phép kẻ xấu tạo ra một tập tin độc hại cùng giá trị MD5 như một tập tin hợp pháp khác. Vào năm 2008, các nhà nghiên cứu bảo mật đã tiến thêm một bước nữa và chứng minh khả năng tạo chứng chỉ SSL giả mạo, được xác thực do sự đụng độ của hàm băm MD5. Vì vậy, MD5 được khuyến cáo không sử dụng cho các ứng dụng mật mã ngày nay.

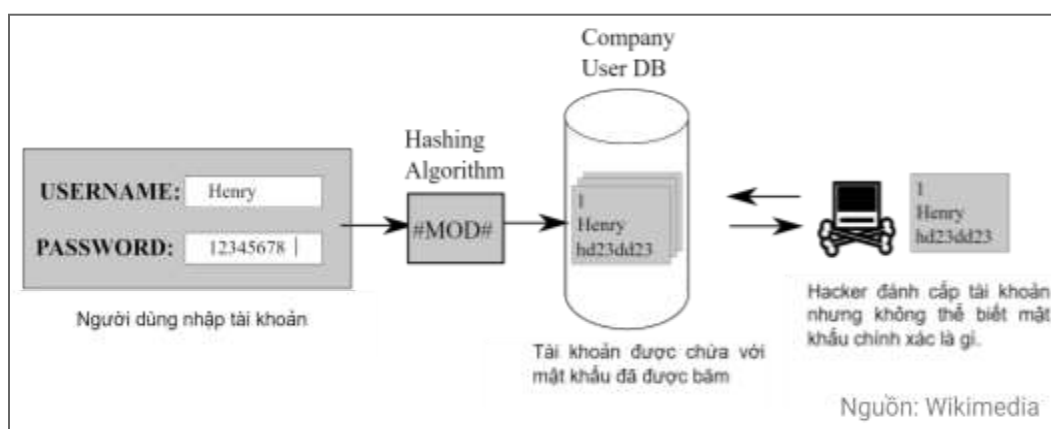
```
$ echo 'Hello World' | md5sum  
e59ff97941044f85df5297e1c302d260
```

SHA-1 là một phần của bộ thuật toán băm an toàn, được thiết kế bởi NSA và xuất bản vào năm 1995. Nó vận hành một khối 512 bit và tạo ra giá trị băm 160 bit. SHA-1 được sử dụng trong các giao thức phổ biến như TLS/SSL, PGP SSH và IPsec. SHA-1 cũng có những điểm yếu và lỗ hổng bảo mật. Những gì trước đây chỉ có thể về mặt lý thuyết, giờ đây đã trở nên khả thi với các phương pháp tấn công hiệu quả hơn với hiệu suất tính toán cao hơn, đặc biệt là sự hỗ trợ tăng tốc của GPU và điện toán đám mây. Vào đầu năm 2017, hiện tượng đụng độ đầy đủ

đầu tiên của SHA-1 được công bố. Sử dụng tài nguyên CPU và GPU đáng kể, hai tập tin PDF đã được tạo để dẫn đến cùng một giá trị băm SHA-1. Vì vậy, nhiều tổ chức đã khuyến cáo thay thế SHA-1 bằng SHA-2 hoặc SHA-3. Các nhà cung cấp trình duyệt lớn đã thông báo ngừng hỗ trợ chứng chỉ SSL sử dụng SHA-1 vào năm 2017.

MIC (Message integrity check) về cơ bản là một bản giá trị băm của thông điệp. Chúng ta có thể xem nó như một giá trị tổng kiểm (checksum) cho thông điệp, đảm bảo rằng nội dung của thông điệp không bị sửa đổi khi truyền nhận. Nhưng điều này hoàn toàn khác với MAC mà chúng ta đã nói trước đây. Nó không sử dụng khóa bí mật, có nghĩa là thông điệp không được xác thực. Không có gì ngăn được kẻ tấn công thay đổi thông điệp, tính toán lại tổng kiểm và sửa đổi MIC đính kèm trong thông điệp. MIC chỉ nên được xem là biện pháp bảo vệ chống lại sự cố hư hỏng hoặc mất mát, nhưng không để bảo vệ chống lại các hành động giả mạo.

Mật khẩu không nên được lưu trữ dưới dạng văn bản thô vì nếu hệ thống bị xâm phạm, mật khẩu cho các tài khoản sẽ là phần thưởng cho kẻ tấn công. Thay vào đó, chúng ta lưu trữ giá trị băm của mật khẩu. Khi đăng nhập vào tài khoản, mật khẩu đã nhập sẽ được chạy qua hàm băm và sau đó kết quả băm được so sánh với giá trị băm đã được lưu trước đó. Nếu các giá trị này khớp nhau, thì mật khẩu là chính xác. Bằng cách chỉ lưu trữ các giá trị băm mật khẩu, kẻ tấn công không thể biết mật khẩu trước khi băm là gì.



Tấn công băm và cách phòng thủ

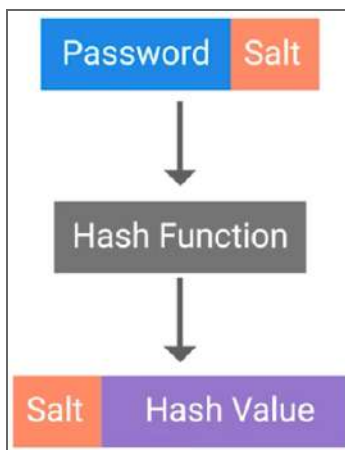
Để tìm lại bản rõ của giá trị băm, kẻ tấn công có thể thực hiện một cuộc tấn công vét cạn (brute force). Trong đó, chúng thử tất cả các giá trị đầu vào có thể có cho đến khi kết quả băm khớp với giá trị mà chúng đang cố gắng khôi phục. Một cuộc tấn công brute force có thể rất tiêu tốn về mặt tính toán tùy thuộc vào hàm băm được sử dụng. Nếu kẻ tấn công có thời gian và tài nguyên không giới hạn, bất kỳ hệ thống nào cũng có thể bị phá. Tuy nhiên, chúng ta có thể bảo vệ khỏi những cuộc tấn công dạng này bằng cách giới hạn thời gian và tài nguyên để nó không khả thi trên thực tế. Một phương pháp phổ biến khác giúp nâng cao khả năng bảo vệ là chạy dữ liệu qua hàm băm nhiều lần, đôi khi hàng nghìn lần. Điều này sẽ yêu cầu tính toán nhiều hơn đáng kể cho mỗi lần thử đoán mật khẩu.

Kẻ tấn công có thể sử dụng bảng cầu vồng. Bảng này giúp tăng tốc quá trình khôi phục mật khẩu từ các hàm băm mật khẩu bị đánh cắp. Bảng cầu vồng chỉ là một bảng được tính toán trước của tất cả các giá trị mật khẩu có thể có và các giá trị băm tương ứng của chúng. Kẻ tấn công có thể xác định mật khẩu bằng cách chỉ cần tra cứu giá trị băm trong bảng cầu vồng của chúng.

Vậy cách nào bảo vệ khỏi những bảng cầu vồng được tính toán trước này? Chúng ta sẽ sử dụng muối mật khẩu. Muối mật khẩu là dữ liệu ngẫu nhiên được bổ sung thêm vào hàm băm để tạo ra giá trị băm khác nhau của cùng một mật khẩu. Cách nó hoạt động như sau, một giá trị muối ngẫu nhiên đủ lớn được nối vào phần cuối của mật khẩu. Sau đó chuỗi kết hợp được chạy qua hàm băm để tạo ra giá trị băm. Giá trị này được lưu lại cùng với muối của nó. Điều này có nghĩa là bây giờ đối với kẻ tấn công chúng phải tính toán một bảng cầu vồng cho mỗi giá trị muối có thể có. Nếu kích thước muối đủ lớn, các yêu cầu về tính toán và lưu trữ để tạo ra các bảng cầu vồng cần thiết trở nên gần như không khả thi.



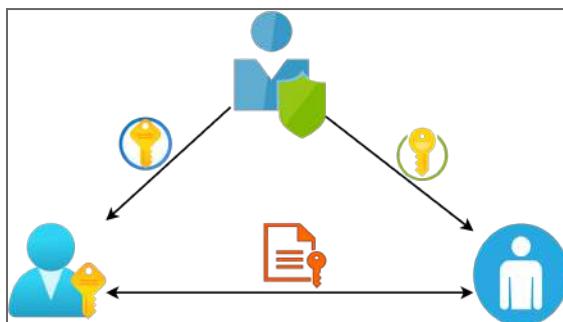
Password	Hash
123456	e10adc983ad09dca098da02320e
password	09dca09e10a0232dc983ad834ds
qwerty	h566adc983ad09d432fgsdcg432
baseball	123dsa3ad09dca3fer34r4653323
dragon	12409dca098dsa42363412467s2
kittycat	2ws3d4c983ad23wsd34565f4643
000111	344rfwc9834564dca09756324t72



5. Hạ tầng khóa công khai

Hạ tầng khóa công khai và chứng chỉ số

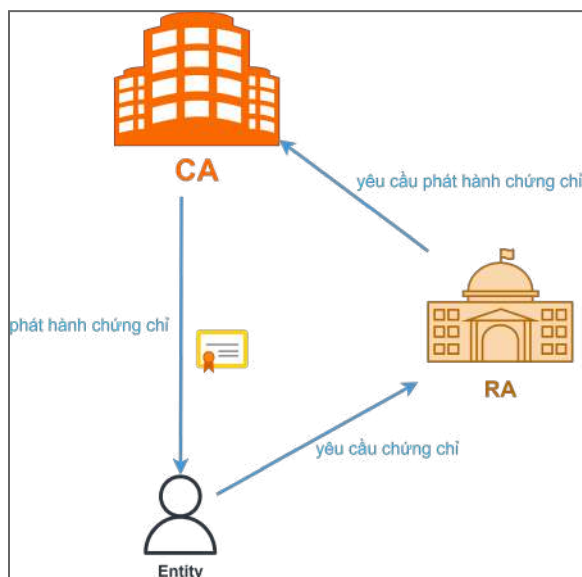
Hạ tầng khóa công khai (public key infrastructure, PKI) là một hệ thống để cho một bên thứ 3 cung cấp và xác thực danh tính của các bên tham gia vào quá trình trao đổi. PKI định nghĩa việc tạo, lưu trữ và phân phối chứng chỉ số.



Chứng chỉ số (digital certificate) là một tập tin chứng minh rằng một thực thể sở hữu một khóa công khai nhất định. Chứng chỉ chứa thông tin về khóa công khai, tổ chức mà nó thuộc về và chữ ký số từ một bên khác đã xác minh thông tin này. Nếu chữ ký hợp lệ và chúng ta tin tưởng tổ chức đã cấp chứng chỉ thì chúng ta có thể tin tưởng khóa công khai sẽ được sử dụng để giao tiếp an toàn với tổ chức sở hữu nó.



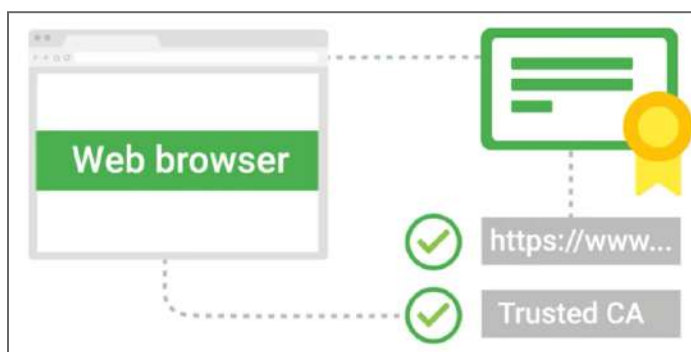
Thực thể chịu trách nhiệm lưu trữ, phát hành và ký chứng chỉ được gọi là nhà cung cấp chứng chỉ số (certificate authority, CA). Đó là một thành phần quan trọng của hệ thống PKI. CA cần tổ chức một kho lưu trữ trung tâm để lưu trữ và lập chỉ mục các chứng chỉ một cách an toàn. Hệ thống quản lý này cũng tổ chức quyền truy cập vào chứng chỉ một cách dễ dàng và nhanh chóng.



RA (registration authority, RA) là cơ quan chịu trách nhiệm xác minh danh tính của bất kỳ thực thể nào yêu cầu chứng chỉ. Sau đó, gửi yêu cầu đến CA để phát hành nó.

Các loại chứng chỉ số

Ứng dụng khác nhau sử dụng các loại chứng chỉ khác nhau. Chứng chỉ máy chủ SSL hoặc TLS (SSL/TLS server certificate) là loại thông dụng nhất. Đây là chứng chỉ mà máy chủ web cung cấp cho máy khách như một phần của thiết lập bảo mật ban đầu của kết nối SSL/TLS. Trình duyệt web trên máy khách sẽ xác minh chủ thể của chứng chỉ khớp với tên máy chủ mà người dùng đang kết nối đến. Ngoài ra, nó cũng sẽ xác minh rằng chứng chỉ được ký bởi tổ chức phát hành tin cậy. Một chứng chỉ cũng có thể hợp lệ cho nhiều tên miền. Trong một số trường hợp, chứng chỉ với ký tự đại diện (dấu hoa thị) có thể được cấp để biểu thị tính hợp lệ cho tất cả các tên máy chủ trong một tên miền xác định.



Máy chủ cũng có thể sử dụng chứng chỉ được gọi là chứng chỉ tự ký (self sign certificate). Về cơ bản, máy chủ sẽ ký khóa công khai của nó bằng cách sử dụng khóa bí mật của chính nó. Trừ khi chúng ta đã tin cậy khóa này, chứng chỉ này gần như không thể xác minh.

Một loại chứng chỉ khác là chứng chỉ máy khách SSL hoặc TLS (SSL/TLS client certificate). Đây là một thành phần tùy chọn của kết nối SSL/TLS và ít phổ biến hơn chứng chỉ máy chủ. Như tên của nó, đây là những chứng chỉ được ràng buộc với máy khách và được sử dụng để xác thực máy khách với máy chủ, cho phép kiểm soát truy cập vào dịch vụ SSL/TLS. Thông thường, nhà điều hành dịch vụ sẽ có CA nội bộ của riêng họ để phát hành và quản lý các chứng chỉ máy khách cho dịch vụ của họ.

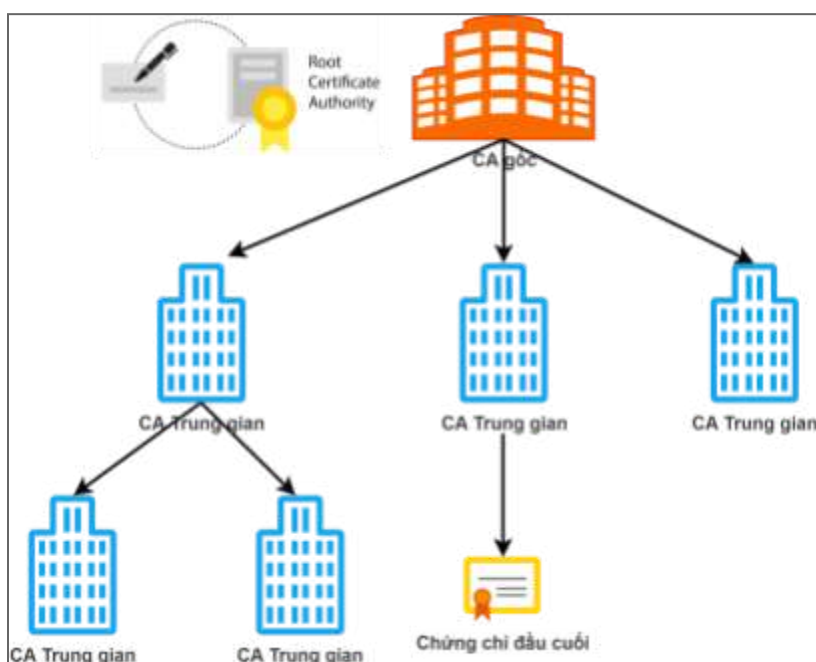
Ngoài ra còn có các chứng chỉ ký mã nguồn (code signing certificate) được sử dụng để ký các chương trình thực thi. Điều này cho phép người dùng của các ứng dụng xác minh chữ ký và đảm bảo rằng ứng dụng không bị giả mạo. Nó cũng cho phép họ xác minh rằng ứng dụng đến từ tác giả phần mềm.

Chuỗi CA tin cậy

PKI phụ thuộc rất nhiều vào mối quan hệ tin cậy giữa các thực thể và xây dựng mạng lưới hoặc chuỗi tin cậy. Chuỗi tin cậy này bắt đầu từ CA gốc. Các chứng chỉ gốc này được tự ký bởi vì chúng là sự khởi đầu của chuỗi tin cậy. Vì vậy, không có cơ quan quyền lực nào cao hơn có thể ký thay cho họ.

Cơ quan cấp chứng chỉ gốc này có thể sử dụng chứng chỉ tự ký và khóa cá nhân để bắt đầu ký các khóa công khai khác. Nó xây dựng một loại cấu trúc cây với CA gốc ở trên cùng của cấu trúc. Nếu CA gốc ký một chứng chỉ và đặt một trường trong chứng chỉ được gọi là CA thành true, thì điều này đánh dấu chứng chỉ là CA trung gian hoặc cấp dưới. Điều này có nghĩa là pháp nhân mà chứng chỉ này được cấp hiện có thể ký các chứng chỉ khác. Và CA này có cùng độ tin cậy với CA gốc. Một CA trung gian cũng có thể ký các CA trung gian khác. Chúng ta có thể thấy cách mở rộng niềm tin này từ một CA gốc đến những CA trung gian có thể bắt đầu xây dựng một chuỗi. Chứng chỉ không có thẩm quyền như CA được gọi là chứng chỉ thực thể cuối hoặc chứng chỉ Lá.

Để khởi động chuỗi tin cậy này, chúng ta phải tin cậy chứng chỉ CA gốc, nếu không thì toàn bộ chuỗi là không đáng tin cậy. Điều này được thực hiện bằng cách phân phối chứng chỉ CA gốc qua các kênh thay thế. Mỗi nhà cung cấp hệ điều hành lớn cung cấp một số lượng lớn chứng chỉ CA gốc đáng tin cậy với hệ điều hành của họ. Và họ thường có các chương trình riêng để tạo điều kiện phân phối các chứng chỉ CA gốc. Hầu hết các trình duyệt sau đó sẽ sử dụng kho lưu trữ chứng chỉ gốc do hệ điều hành cung cấp.

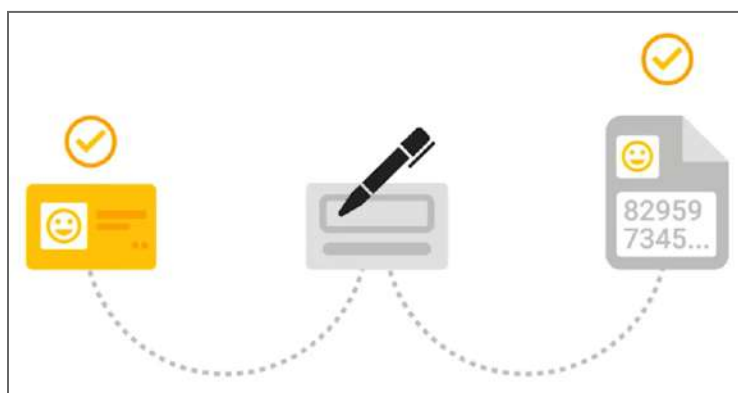


Cấu trúc chứng chỉ số

Chuẩn X.509 là tiêu chuẩn mô tả cấu trúc của một chứng chỉ số. Nó cũng định nghĩa danh sách thu hồi chứng chỉ. Đó là một cách thức để phân phối danh sách các chứng chỉ không còn giá trị. Chuẩn X.509 được ban hành lần đầu tiên vào năm 1988. Các trường được mô tả trong chứng chỉ theo chuẩn X.509 gồm các thành phần sau. Version là trường mô tả phiên bản nào của chuẩn X.509. Kế tiếp là số sê-ri, đây là một số nhận dạng đơn nhất cho chứng chỉ do CA gán. Trường thứ ba là thuật toán ký chứng chỉ, trường này cho biết thuật toán nào được sử dụng cho khóa công khai và thuật toán băm nào được sử dụng để ký chứng chỉ. Trường tiếp theo là tên nhà phát hành, trường này chứa thông tin về cơ quan đã ký chứng chỉ. Trường mô tả tính hợp lệ gồm hai trường con là Not before và Not after, để mô tả khoảng thời gian mà chứng chỉ còn hợp lệ. Tiếp theo là chủ thể, trường này chứa thông tin về pháp nhân mà chứng chỉ được cấp. Trường thông tin khóa công khai chứa thuật toán của khóa công khai cùng với chính khóa công khai. Thuật toán ký chứng chỉ, giống như trường thông tin khóa công khai, hai trường này phải khớp với nhau. Giá trị chữ ký chứng chỉ là dữ liệu chữ ký điện tử của chính nó. Ngoài ra còn có các trường như dấu vân tay chứng chỉ, nó không thực sự là các trường trong chính chứng chỉ, nhưng được máy khách sử dụng khi xác thực hoặc kiểm tra chứng chỉ. Đó là giá trị băm của toàn bộ chứng chỉ.

Web of Trust

Một mô hình thay thế cho mô hình PKI nhằm thiết lập sự tin cậy và danh tính ràng buộc gọi là Web of Trust. Web of Trust là nơi các cá nhân thay vì tổ chức phát hành chứng chỉ ký các khóa công khai của các cá nhân khác. Trước khi một cá nhân ký khóa, trước tiên họ phải xác minh danh tính của người đó thông qua một cơ chế đã được thỏa thuận. Thông thường bằng cách kiểm tra một số mẫu giấy tờ tùy thân như căn cước công dân, bằng lái xe, hộ chiếu, v.v. Khi họ xác định được người đó là ai, việc ký vào khóa công khai của họ về cơ bản là xác nhận người này. Bạn đang nói rằng bạn tin tưởng khóa công khai thuộc về cá nhân này. Quá trình này có đi có lại, có nghĩa là cả hai bên sẽ ký vào khóa của nhau. Thông thường, những người quan tâm đến việc thiết lập Web of Trust sẽ tổ chức cái được gọi là buổi tiệc ký khóa. Nơi mà những người tham gia thực hiện cùng một quá trình xác minh và ký. Vào cuối buổi, khóa công khai của mọi người sẽ được ký bởi những người tham gia thiết lập Web of Trust này. Trong tương lai, khi một trong những người tham gia buổi tiệc ký khóa ban đầu này thiết lập niềm tin với thành viên mới, Web of Trust sẽ được mở rộng. Quá trình này cho phép các Web of Trust riêng biệt được kết nối bởi các cá nhân và cho phép nó phát triển.



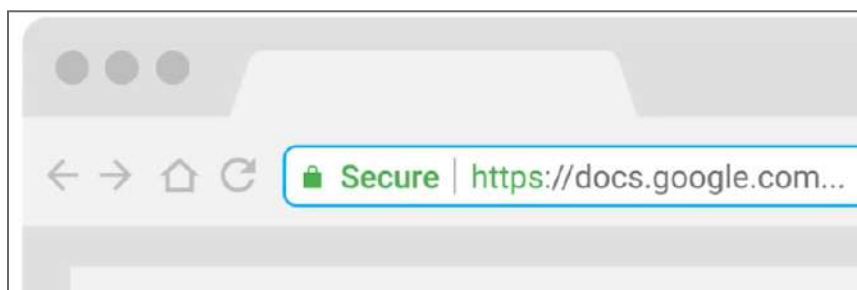
6. Bảo mật mạng

Giao thức SSL/TLS

HTTPS là phiên bản bảo mật của HTTP được sử dụng trong trình duyệt web. HTTPS cũng có thể được gọi là HTTP qua SSL/TLS vì nó về cơ bản đóng gói dữ liệu HTTP qua một kênh được mã hóa, bảo mật sử dụng SSL/TLS. Chúng ta có

thể nghe thấy SSL và TLS được sử dụng thay thế cho nhau, nhưng SSL 3.0, bản sửa đổi mới nhất của SSL, đã không còn được dùng từ năm 2015 và TLS 1.2 là bản sửa đổi được đề xuất hiện tại. TLS cũng được sử dụng để bảo mật các thông tin liên lạc khác ngoài duyệt web, chẳng hạn như các cuộc gọi VoIP như Skype hoặc Hangouts, email, nhắn tin và thậm chí là bảo mật mạng Wifi.

TLS cung cấp cho chúng ta ba thứ. Thứ nhất là một đường truyền thông tin an toàn, có nghĩa là dữ liệu được truyền đi được bảo vệ khỏi những kẻ nghe trộm tiềm ẩn. Thứ hai, khả năng xác thực cả hai bên giao tiếp, mặc dù thông thường, chỉ máy chủ được xác thực bởi máy khách. Và thứ ba, tính toàn vẹn của thông tin liên lạc, nghĩa là có các biện pháp kiểm tra để đảm bảo rằng các thông điệp không bị mất hoặc bị thay đổi khi chuyển tiếp.

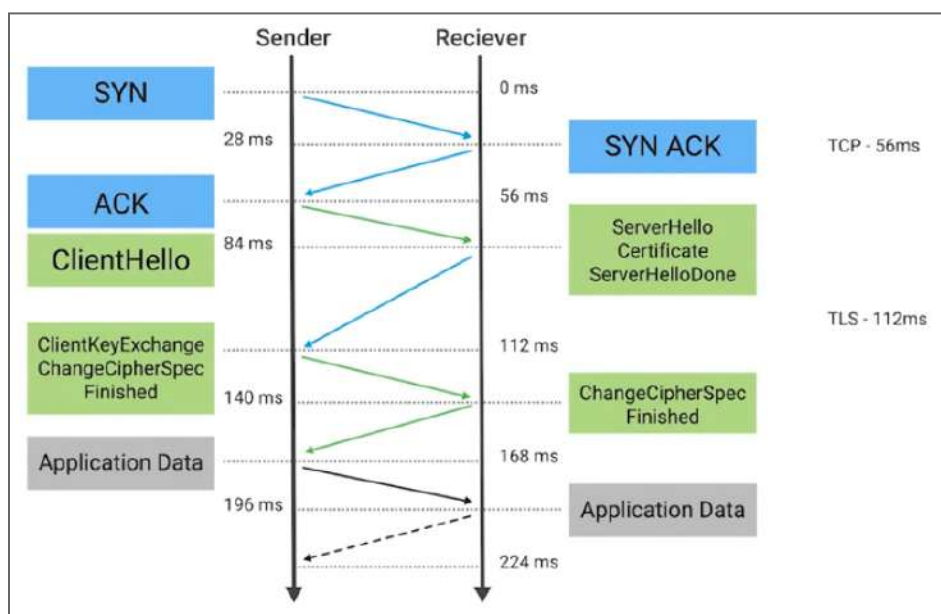


Cơ chế bắt tay TLS

Về cơ bản, TLS cung cấp một kênh an toàn để ứng dụng giao tiếp với một dịch vụ, nhưng phải có một cơ chế để thiết lập kênh này ban đầu. Đây là những gì được gọi là bắt tay TLS.

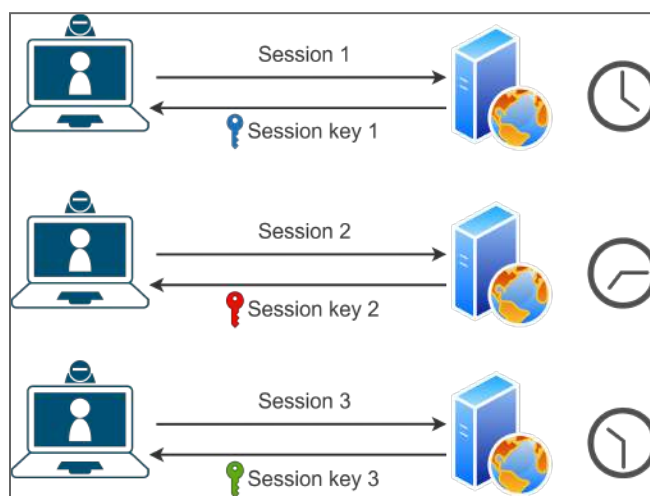
Quá trình bắt tay bắt đầu với việc một máy khách thiết lập kết nối với dịch vụ hỗ trợ TLS, được gọi là ClientHello. Điều này bao gồm thông tin về máy khách, như phiên bản TLS mà máy khách hỗ trợ, danh sách các bộ mã và có thể một số tùy chọn TLS bổ sung. Sau đó, máy chủ phản hồi bằng một thông điệp ServerHello, trong đó nó chọn phiên bản giao thức cao nhất chung với máy khách và chọn một bộ mã từ danh sách để sử dụng. Nó cũng truyền chứng chỉ kỹ thuật số và một thông điệp ServerHelloDone. Sau đó, máy khách sẽ xác thực chứng chỉ mà máy chủ đã gửi để đảm bảo rằng nó đáng tin cậy và dành cho máy chủ thích hợp. Giả sử chứng chỉ được thông qua, máy khách sau đó sẽ gửi một thông điệp ClientKeyExchange. Đây là khi máy khách chọn cơ chế trao đổi khóa để thiết lập an toàn bí mật được chia sẻ với máy chủ, cơ chế này sẽ được

sử dụng với mã hóa đối xứng để mã hóa tất cả các thông tin liên lạc tiếp theo. Máy khách cũng gửi một thông điệp ChangeCipherSpec cho biết rằng nó đang chuyển sang truyền thông an toàn khi nó có tất cả thông tin cần thiết để bắt đầu giao tiếp qua kênh an toàn. Tiếp theo là một thông điệp Finished được mã hóa cũng dùng để xác minh rằng quá trình bắt tay đã hoàn tất thành công. Máy chủ trả lời bằng ChangeCipherSpec và thông điệp Finished được mã hóa sau khi khóa chia sẻ được nhận. Sau khi hoàn tất, dữ liệu ứng dụng có thể bắt đầu truyền qua kênh được bảo mật.



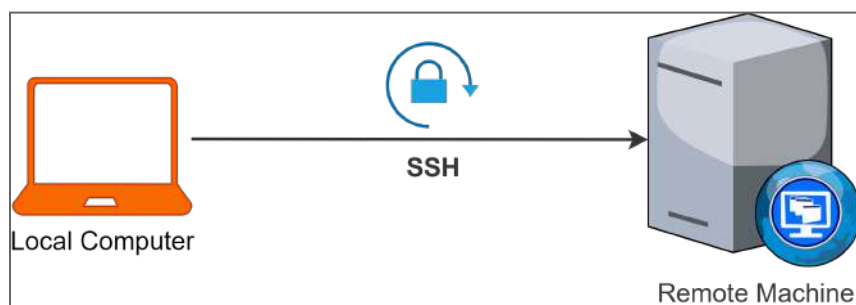
Khóa phiên và bảo mật chuyển tiếp

Trong quá trình bắt tay TLS, hai bên giao tiếp tạo tới 4 khóa phiên khi bắt đầu bất kỳ phiên giao tiếp nào. Khóa phiên (session key) là khóa đối xứng được chia sẻ sử dụng các phiên TLS để mã hóa dữ liệu được gửi qua lại. Vì khóa này có nguồn gốc từ khóa công khai-bí mật, nên nếu khóa bí mật bị đánh cắp, kẻ tấn công có khả năng giải mã tất cả các thông điệp đã truyền trước đó. Để bảo vệ chống lại điều này, chúng ta sử dụng bảo mật chuyển tiếp (forward secrecy). Đây là một thuộc tính của hệ thống mật mã để ngay cả trong trường hợp khóa bí mật bị đánh cắp, các khóa phiên vẫn an toàn.



Các giao thức và ứng dụng bảo mật mạng

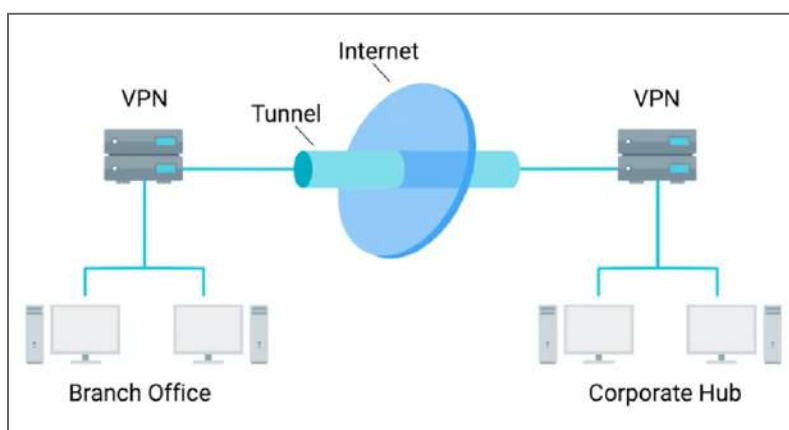
SSH (secure shell) là một giao thức mạng bảo mật sử dụng mã hóa để cho phép truy cập vào dịch vụ mạng trên các môi trường không an toàn. Chúng ta thường thấy SSH được sử dụng để đăng nhập từ xa vào hệ thống qua giao diện dòng lệnh. Tuy nhiên, giao thức này cực kỳ linh hoạt và có các điều khoản cho phép các mạng và dữ liệu truy cập tùy ý qua các cổng đó được mã hóa. SSH sử dụng mã hóa khóa công khai để xác thực máy từ xa mà máy khách đang kết nối và có các điều khoản cho phép xác thực người dùng thông qua chứng chỉ máy khách, nếu cần. Giao thức SSH rất linh hoạt và có tính mô-đun, đồng thời hỗ trợ nhiều cơ chế trao đổi khóa khác nhau như DH, cùng với nhiều loại mã hóa đối xứng khác. Nó cũng hỗ trợ nhiều phương pháp xác thực, bao gồm cả những phương thức mà chúng ta tự viết. Khi sử dụng xác thực khóa công khai, một cặp khóa được tạo bởi người dùng muốn xác thực. Sau đó, họ phải phân phối các khóa công khai đó cho tất cả các hệ thống mà họ muốn xác thực để sử dụng cặp khóa. Khi xác thực, SSH sẽ đảm bảo rằng khóa công khai đang được dùng khớp với khóa bí mật.



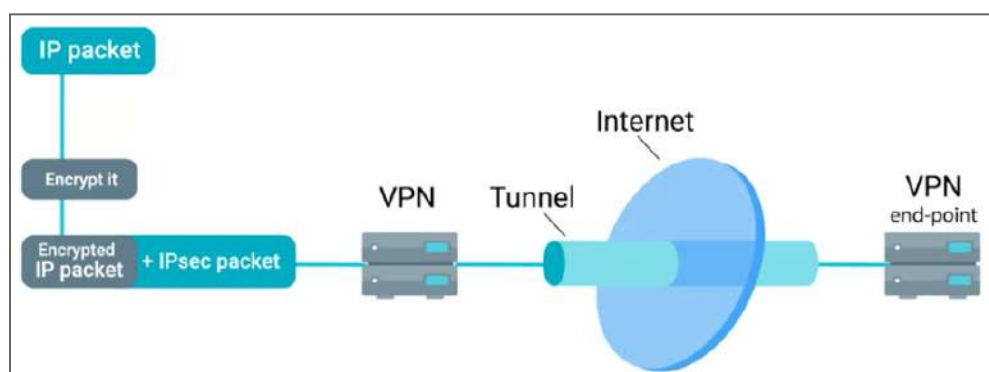
PGP (Pretty Good Privacy) là một ứng dụng mã hóa cho phép xác thực dữ liệu cùng với quyền riêng tư từ các bên thứ ba dựa trên mã hóa bất đối xứng. Nó sử dụng phổ biến để liên lạc qua email được mã hóa, nhưng nó cũng là một giải pháp mã hóa toàn bộ ổ đĩa, tập tin hay thư mục tùy ý. PGP sử dụng khóa không dưới 128 bit và được nhiều người coi là rất an toàn, không có cơ chế nào được biết đến để phá mã thông qua các phương tiện mật mã hoặc tính toán. Nó được so sánh với mã hóa cấp quân sự và có rất nhiều trường hợp cảnh sát và chính phủ không thể khôi phục dữ liệu được bảo vệ bằng mã hóa PGP. Trong những trường hợp này, cơ quan thực thi pháp luật có xu hướng sử dụng biện pháp pháp lý để buộc chuyển giao mật khẩu hoặc khóa. Ban đầu, PGP sử dụng thuật toán RSA, nhưng cuối cùng nó đã được thay thế bằng DSA để tránh các vấn đề về giấy phép bản quyền.



VPN (Virtual Private Network) là một cơ chế cho phép chúng ta kết nối từ xa một máy chủ hoặc mạng riêng nội bộ, truyền dữ liệu qua một kênh công cộng, chẳng hạn như Internet. Chúng ta có thể coi đây là một loại đường hầm được mã hóa, nơi tất cả lưu thông mạng của hệ thống từ xa sẽ chảy qua. VPN cũng có thể là kết nối điểm-điểm, nơi hai cổng được kết nối thông qua VPN. Đây là cầu nối hai mạng riêng thông qua một đường hầm được mã hóa. Có một loạt các giải pháp VPN sử dụng các cách tiếp cận và giao thức khác nhau với những lợi ích và sự cân bằng khác nhau. Chúng ta cùng xem xét một số cái phổ biến.



IPsec (Internet Protocol Security), là một giao thức VPN được thiết kế cùng với IPv6. Ban đầu nó được thiết kế tiêu chuẩn tuân thủ với việc triển khai IPv6, nhưng cuối cùng đã bị loại bỏ theo yêu cầu. Bây giờ, nó chỉ là tùy chọn để sử dụng với IPv6. IPsec hoạt động bằng cách mã hóa một gói IP và đóng gói gói đã mã hóa bên trong một gói IPsec. Sau đó, gói được mã hóa này được chuyển đến điểm cuối VPN, nơi gói được mở ra và giải mã, và được gửi đến đích cuối cùng.

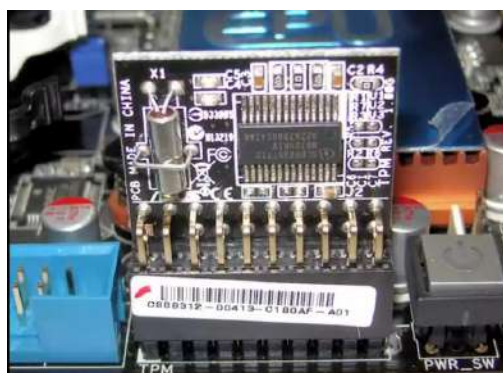


IPsec hỗ trợ hai chế độ hoạt động, chế độ vận chuyển và chế độ đường hầm. Khi chế độ vận chuyển được sử dụng, chỉ có phần dữ liệu của gói IP được mã hóa, không ảnh hưởng đến IP header. Các giá trị header được băm và xác minh, cùng với tầng vận chuyển và tầng ứng dụng. Điều này sẽ ngăn việc sử dụng bất kỳ thứ gì có thể sửa đổi các giá trị này. Trong chế độ đường hầm, toàn bộ gói IP header, dữ liệu được mã hóa và đóng gói bên trong một gói IP mới với các header mới.

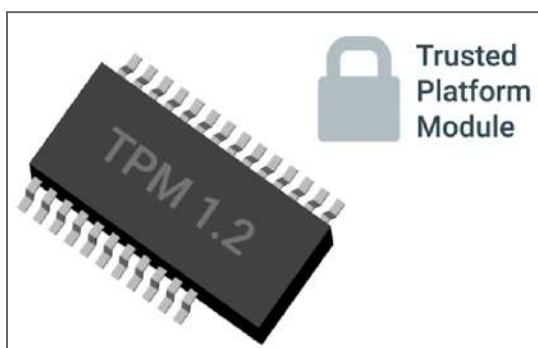
Mặc dù bản thân không phải là một giải pháp VPN, nhưng **L2TP** (Layer 2 Tunneling Protocol) thường được sử dụng để hỗ trợ VPN. Việc triển khai L2TP kết hợp với IPsec là cần thiết, vì L2TP không tự mã hóa chính nó. Đây là một giao thức đường hầm đơn giản cho phép đóng gói các giao thức khác hoặc lưu thông qua mạng không hỗ trợ loại lưu thông được gửi. L2TP cũng có thể tách riêng và quản lý lưu thông. Ví dụ, ISP sẽ sử dụng L2TP để cung cấp quyền truy cập mạng tới điểm cuối của khách hàng. Sự kết hợp của L2TP và IPsec được gọi là L2TP IPsec và đã được chuẩn hóa chính thức trong IETF RFC 3193.

7. Phần cứng mã hóa

TPM (Trusted platform module) là một thiết bị phần cứng thường được tích hợp vào phần cứng của máy tính, đó là một bộ xử lý mật mã chuyên dụng. TPM có khóa RSA bí mật duy nhất được ghi vào phần cứng tại thời điểm sản xuất, cho phép TPM thực hiện những thứ như xác thực phần cứng. Điều này có thể phát hiện các thay đổi phần cứng trái phép đối với hệ thống.



TPM cung cấp khả năng tạo khóa bảo mật, tạo số ngẫu nhiên, chứng thực từ xa, ràng buộc và niêm phong dữ liệu. Chứng thực từ xa là ý tưởng về một hệ thống xác thực cấu hình phần mềm và phần cứng của nó với một hệ thống từ xa. Điều này cho phép hệ thống từ xa xác định tính toàn vẹn của nó. TPM thực hiện quá trình này bằng cách tạo một hàm băm bảo mật của cấu hình hệ thống, sử dụng khóa RSA duy nhất được nhúng trong chính TPM. Một công dụng khác của khóa mã hóa được hỗ trợ bởi phần cứng bí mật này là ràng buộc và niêm phong dữ liệu. Nó liên quan đến việc sử dụng khóa bí mật để lấy một khóa duy nhất sau đó được sử dụng để mã hóa dữ liệu. Về cơ bản, điều này ràng buộc dữ liệu được mã hóa với TPM. Hay nói cách khác, chỉ có các khóa được lưu trữ trong phần cứng TPM mới có thể giải mã dữ liệu được. Việc niêm phong dữ liệu tương tự như ràng buộc vì dữ liệu được mã hóa bằng khóa mã hóa được hỗ trợ bởi phần cứng. Tuy nhiên, để dữ liệu được giải mã, TPM phải ở trạng thái xác định.



TPM là một chuẩn với một số phiên bản có thể được triển khai như một chip phần cứng rời, được tích hợp vào một chip khác trong hệ thống, được thực hiện trong phần mềm firmware hoặc ảo hóa bên dưới một phần mềm giám sát máy ảo. Cách triển khai an toàn nhất là chip rời, vì các chip này cũng kết hợp khả năng chống giả mạo vật lý để ngăn chặn các cuộc tấn công vật lý vào chip. Thiết bị di động có một cái gì đó tương tự được gọi là phần tử bảo mật. Tương tự như TPM, nó là một chip chống giả mạo thường được nhúng trong bộ vi xử lý hoặc tích hợp vào bo mạch chủ của thiết bị di động. Nó cung cấp khả năng lưu trữ an toàn các khóa mật mã và cung cấp một môi trường an toàn cho các ứng dụng.



TPM nhận được nhiều lời chỉ trích xung quanh việc tin tưởng vào nhà sản xuất. Vì khóa bí mật được ghi vào phần cứng tại thời điểm sản xuất, nhà sản xuất sẽ có quyền truy cập vào khóa này. Nhà sản xuất có thể lưu trữ các khóa sau đó có thể được sử dụng để sao chép TPM, điều này có thể phá vỡ tính bảo mật mà mô-đun cung cấp.

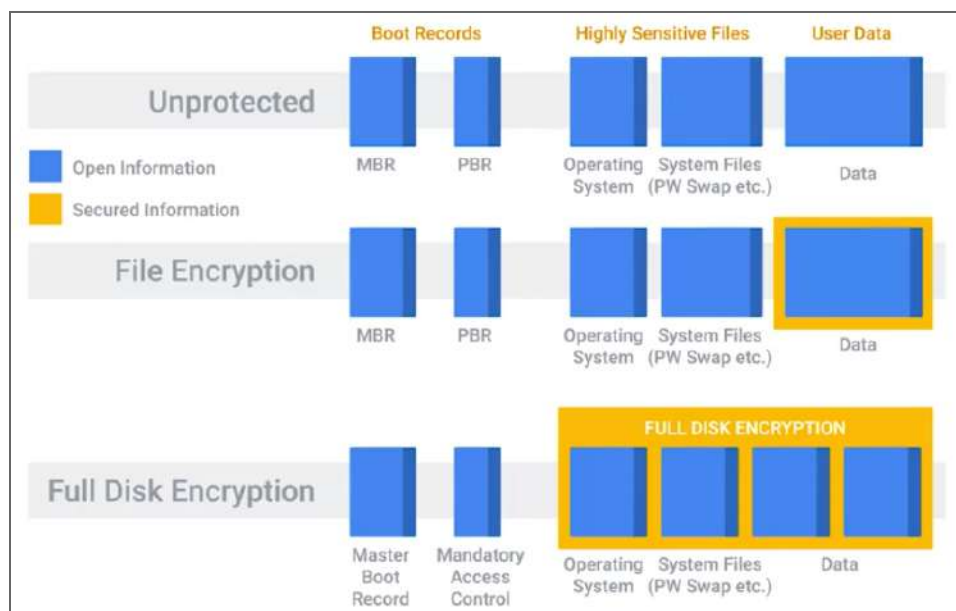
Có một báo cáo về một cuộc tấn công vật lý vào TPM cho phép một nhà nghiên cứu bảo mật xem và truy cập toàn bộ nội dung của TPM. Nhưng cuộc tấn công này yêu cầu sử dụng kính hiển vi điện tử và thiết bị có độ chính xác ở mức micromet để điều khiển mạch TPM. Mặc dù quá trình này tốn rất nhiều thời gian và đòi hỏi thiết bị chuyên dụng cao, nhưng nó đã chứng minh rằng một cuộc tấn công như vậy là có thể xảy ra.

Một sự phát triển của các yếu tố bảo mật là **TEE** (trusted execution environment). Nó cung cấp một môi trường thực thi cách ly toàn diện chạy cùng với hệ điều hành chính. Điều này giúp cách ly các ứng dụng khỏi hệ điều hành. Nó cũng cách ly các tiến trình bảo mật khỏi cái khác khi chạy trong TEE.



Mã hóa toàn đĩa (full disk encryption, FDE) là phương pháp mã hóa toàn bộ ổ đĩa trong hệ thống. Không chỉ các tập tin nhạy cảm trong hệ thống. Điều này cho phép chúng ta bảo vệ toàn bộ nội dung của đĩa khỏi bị đánh cắp hoặc giả mạo dữ liệu. Có một loạt các tùy chọn để triển khai FDE như sản phẩm thương mại PGP, Bitlocker của Microsoft, tích hợp rất tốt với TPM, Filevault 2 của Apple và phần mềm mã nguồn mở dm-crypt, cung cấp mã hóa cho các hệ thống Linux. Cấu hình FDE sẽ có một phân vùng chính hoặc phân vùng logic chứa dữ liệu được mã hóa. Tuy nhiên, để khởi động từ phân vùng được mã hóa, trước tiên nó phải được mở khóa. Vì ổ đĩa được mã hóa, BIOS không thể truy cập dữ liệu trên ổ đĩa này cho mục đích khởi động được. Đây là lý do tại sao các cấu hình FDE sẽ có một phân vùng khởi động nhỏ không được mã hóa chứa các phần tử như nhân, bộ nạp khởi động và initrd. Tại thời điểm khởi động, các phần tử này được tải lên và sau đó nhắc người dùng nhập cụm mật khẩu để mở khóa đĩa và tiếp tục quá trình khởi động. FDE cũng có thể kết hợp TPM, sử dụng các khóa mã hóa TPM để bảo vệ đĩa. Và, nó có tính toàn vẹn để ngăn chặn việc mở

khóa đĩa nếu cấu hình hệ thống bị thay đổi. Điều này bảo vệ chống lại các cuộc tấn công như giả mạo phần cứng và đánh cắp hoặc sao chép đĩa.



Lựa chọn các số ngẫu nhiên là một khái niệm rất quan trọng trong mã hóa vì nếu quá trình chọn số không thực sự ngẫu nhiên, thì có thể có một số mẫu mà kẻ thù có thể phát hiện ra thông qua quan sát chặt chẽ và phân tích các thông điệp được mã hóa theo thời gian. Một cái gì đó không thực sự ngẫu nhiên được gọi là giả ngẫu nhiên. Vì lý do này mà các hệ điều hành duy trì những gì được gọi là một hồ entropy. Đây thực chất là một nguồn dữ liệu ngẫu nhiên để giúp phát sinh số ngẫu nhiên hạt giống. Ngoài ra còn có các trình tạo số ngẫu nhiên chuyên dụng và trình tạo số giả ngẫu nhiên, có thể được kết hợp vào thiết bị bảo mật hoặc máy chủ để đảm bảo rằng các số thực sự ngẫu nhiên được chọn khi tạo khóa mật mã.

Bài đọc 4: Bảo Mật AAA

1. Giới thiệu bảo mật AAA

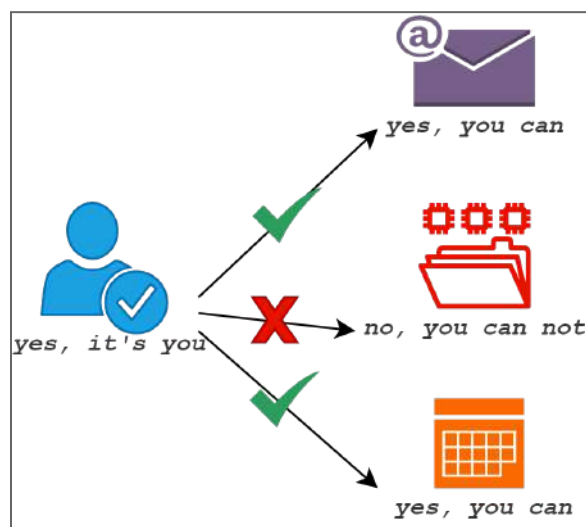
Bảo mật AAA là một nền tảng được sử dụng để kiểm soát và theo dõi các truy xuất bên trong một máy tính. AAA bao gồm việc xác thực (Authentication), ủy quyền (Authorization) và kế toán (Accounting).



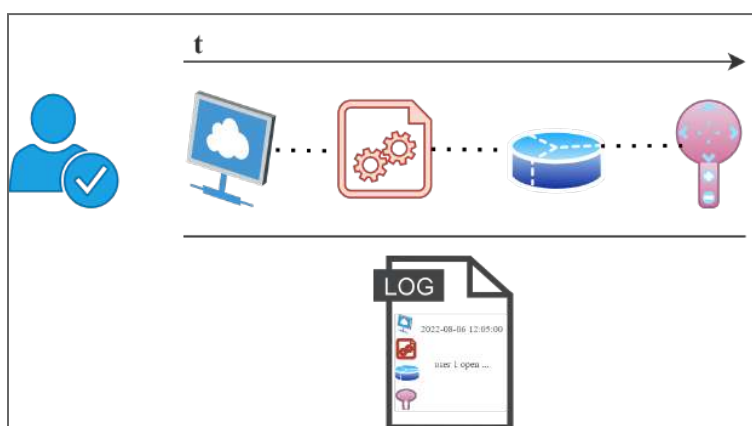
Đầu tiên, chúng ta đến với thuật ngữ xác thực. Xác thực là hành động chứng minh một khẳng định, chẳng hạn như chứng minh danh tính của người dùng hệ thống máy tính. Chúng ta cần phân biệt với khái niệm định danh (identification). Đó là hành động chỉ ra danh tính của một người hoặc một vật, trong khi xác thực là quá trình xác minh danh tính đó. Ví dụ, địa chỉ email là định danh của bạn khi đăng nhập vào một trang web. Nhưng làm thế nào để bạn chứng minh email đó là của bạn? Quá trình xác thực sẽ thực hiện điều đó. Để xác thực email, bạn cần cung cấp mật khẩu được liên kết với danh tính để chứng minh đó là bạn hoặc ít nhất bạn biết mật khẩu được liên kết với tài khoản email. Xác thực thường được viết tắt bằng từ authn.



Ủy quyền là chức năng chỉ định các quyền/đặc quyền truy cập vào tài nguyên trong hệ thống máy tính. Trong ví dụ đăng nhập tài khoản email, sau khi xác thực thành công, danh tính của bạn được quyền truy cập vào hộp thư của bạn, nhưng bạn không được quyền truy cập hộp thư của bất kỳ ai khác. Ủy quyền thường được viết tắt bằng từ authz.



Kế toán (accounting) là quá trình ghi lại các tài nguyên và dịch vụ người dùng đã truy xuất cũng như các thao tác của họ trên tài nguyên này. Điều này có thể bao gồm lượng thời gian hệ thống hoặc lượng dữ liệu được gửi và nhận trong một phiên thực hiện. Bản ghi được sử dụng để kiểm soát ủy quyền, khắc phục sự cố, phân tích xu hướng sử dụng tài nguyên và lập kế hoạch cho dung lượng lưu trữ cần thiết, v.v...



2. Xác thực

Mật khẩu mạnh

Để bảo vệ quá trình xác thực, chúng ta cần sử dụng một mật khẩu mạnh. Nhưng điều gì tạo nên một mật khẩu mạnh? Sau đây là một số yếu tố cần xem xét để có được mật khẩu mạnh và bảo vệ chúng một cách an toàn. Đầu tiên

mật khẩu cần đảm bảo độ dài tối thiểu nhất định như tối thiểu 8 ký tự, sử dụng các ký tự một cách phức tạp như kết hợp chữ, số và ký tự đặc biệt, kết hợp hoa thường. Tiếp theo là không dùng các từ trong từ điển. Điều này nghe có vẻ chúng ta sẽ tạo ra một mật khẩu mạnh nhưng lại rất khó nhớ. Tuy nhiên, có một số cách để vẫn có thể đảm bảo sự phức tạp trong chuỗi mật khẩu nhưng vẫn dễ nhớ cho chúng ta. Ví dụ, chúng ta có thể đặt mật khẩu bằng một câu có nghĩa sau đó thay thế một số ký tự bằng chữ viết hoa như ký tự đầu tiên của mỗi từ, tiếp theo biến đổi một số ký tự mà có hình dạng tương tự như ký tự I có thể thay bằng số 1, ký tự a bằng ký tự @, v.v... Lưu ý, cách thức này do tự chúng ta quy ước, tránh sử dụng các mẫu phổ biến vì hacker cũng sẽ biết các cách quy ước đó.



Diagram illustrating a password transformation:

Original Password: HelloWorld2022

↓

Transformed Password: H311oW0r1D2k22

Sau khi đã có được chuỗi mật khẩu mạnh, chúng ta cũng cần có các biện pháp bảo vệ nó như không được viết ra trên giấy ghi chú, không lưu trong văn bản thô. Chúng ta cũng không dùng lại một mật khẩu cho nhiều ứng dụng vì nếu một ứng dụng nào đó rò rỉ thông tin mật khẩu của chúng ta thì có thể ảnh hưởng đến bảo mật của các ứng dụng khác. Cuối cùng là chúng ta cần áp dụng chính sách thay đổi mật khẩu định kỳ. Chu kỳ thay đổi không nên quá ngắn vì sẽ gây phiền toái và dễ khiến chúng ta vi phạm các yêu cầu phía trên để có được sự thoải mái. Nói cách khác, chúng ta phải luôn cân bằng giữa bảo mật và tính tiện dụng.

Xác thực đa yếu tố

Xác thực đa yếu tố (multifactor authentication) là một hệ thống mà người dùng được xác thực bằng cách trình bày nhiều phần thông tin hoặc đối tượng. Nhiều yếu tố cấu thành hệ thống xác thực đa yếu tố có thể được phân loại thành ba loại gồm: cái gì đó bạn biết, cái gì đó bạn có và cái gì đó bạn là. Lý tưởng nhất là một hệ thống đa yếu tố sẽ kết hợp ít nhất hai trong số các yếu tố

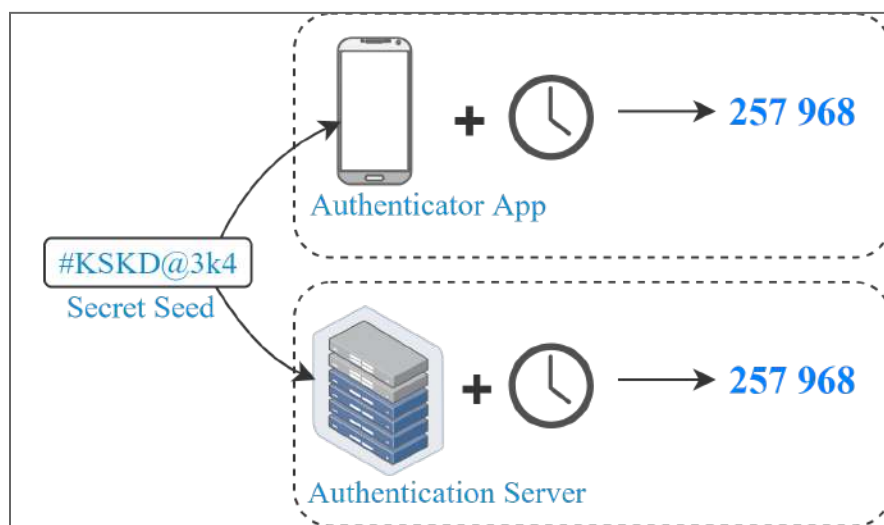
này. Cái gì đó bạn biết để cập đến những thứ mật khẩu, hoặc mã pin cho ngân hàng hoặc thẻ ATM của bạn. Cái gì đó bạn có thường là những thiết bị vật lý như thẻ ATM, điện thoại. Cái gì đó bạn là thường gắn liền với dữ liệu sinh trắc học như vân tay hoặc móng mắt.



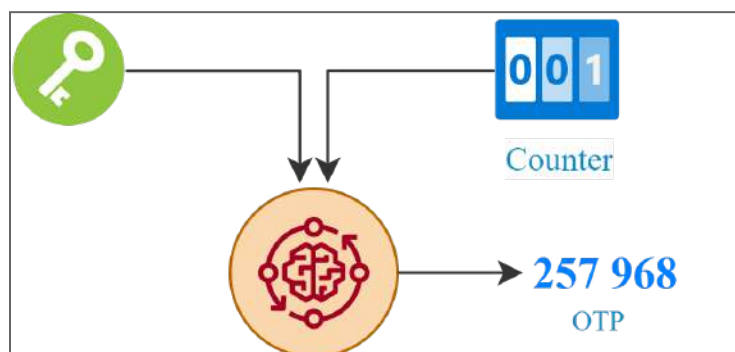
Tiền đề đằng sau xác thực đa yếu tố là kẻ tấn công sẽ gặp khó khăn hơn nhiều trong việc đánh cắp hoặc sao chép nhiều yếu tố xác thực. Nếu chúng ta sử dụng nhiều mật khẩu, bảo mật sẽ không được tăng cường đáng kể. Điều này là do mật khẩu, dù nhiều, vẫn dễ bị lừa đảo hoặc tấn công bằng chương trình keylogger. Bằng cách sử dụng mật khẩu kết hợp với mã token, khả năng bảo mật sẽ tăng lên. Ngay cả khi mật khẩu bị đánh cắp bởi một cuộc tấn công lừa đảo, kẻ tấn công cũng cần phải đánh cắp hoặc sao chép mã token vật lý để có thể truy cập vào tài khoản. Và điều đó ít có khả năng xảy ra hơn nhiều.

Mã token là một dạng mã bổ sung được tạo bởi các thiết bị vật lý hay thiết bị số nhằm cung cấp thêm yếu tố để xác thực người dùng. Thiết bị token vật lý có thể có một số dạng khác nhau như thiết bị USB có mã token trên đó, thiết bị độc lập tạo mã thông báo hoặc thậm chí là một chìa khóa đơn giản được sử dụng với khóa truyền thống. Một ví dụ về thiết bị này là RSA SecurID. Đó là một thiết bị nhỏ, chạy bằng pin với màn hình LCD hiển thị mã token định kỳ. Chúng ta thường phải mang theo các thiết bị này để xác thực. Nếu thiết bị bị mất hoặc bị hỏng, chúng ta sẽ không thể xác thực cho đến khi thiết bị được thay thế. Điều này cũng yêu cầu chi phí hỗ trợ, vì thiết bị sẽ bị lỗi, bị mất, hết pin và không đồng bộ với máy chủ. Sử dụng một ứng dụng trên điện thoại thông minh giải quyết một số vấn đề này, nhưng cũng không phải là quá thuận tiện. Khi được nhắc đăng nhập, người dùng phải lấy một thiết bị hoặc điện thoại từ túi của họ và ghi các số theo cách thủ công vào trang xác thực. Tuy nhiên, dù sao việc tăng cường tính bảo mật cũng sẽ đi đôi với việc giảm sự thuận tiện ở mức nhất định. Ở cuối phần này, chúng ta sẽ tìm hiểu một loại thiết bị token giải quyết một số sự bất tiện này.

OTP (one-time password) là một dạng mã token tồn tại trong thời gian ngắn, dùng một lần và có giá trị thay đổi liên tục. Đây là một mã token dựa trên thời gian nên đôi khi nó cũng được gọi là TOTP. OTP hoạt động bằng cách bắt đầu với một hạt giống bí mật hoặc giá trị được tạo ngẫu nhiên trên mã token mà đã đăng ký với máy chủ xác thực. Giá trị gốc được sử dụng cùng với thời gian hiện tại để tạo OTP. Lưu ý rằng thời gian giữa mã token xác thực và máy chủ xác thực cần được đồng bộ tương đối. Điều này thường đạt được bằng cách sử dụng giao thức thời gian mạng hoặc NTP. Kẻ tấn công sẽ cần phải đánh cắp thiết bị phát sinh mã token hoặc tạo bản sao mã token nếu chúng có thể đánh cắp giá trị hạt giống bí mật. Vì token này được đồng bộ với máy chủ sử dụng thời gian và điều này không phải là bí mật, nên kẻ tấn công có thể tạo bản sao mã token khi có được giá trị hạt giống. Các trình tạo mã token này có thể là thiết bị vật lý, thiết bị chuyên dụng hoặc chúng có thể là một ứng dụng được cài đặt trên điện thoại thông minh có chức năng tương tự.



Ngoài ra còn có các mã token dựa trên bộ đếm (counter-based token), sử dụng giá trị hạt giống bí mật cùng với giá trị bộ đếm bí mật được tăng lên mỗi khi mã token được tạo trên thiết bị. Giá trị sau đó được tăng lên trên máy chủ nếu xác thực thành công. Điều này an toàn hơn các mã token dựa trên thời gian vì hai lý do. Đầu tiên, kẻ tấn công sẽ cần khôi phục giá trị hạt giống và giá trị bộ đếm. Thứ hai, giá trị bộ đếm cũng tăng lên khi nó được sử dụng. Vì vậy, mã token nhân bản sẽ chỉ hữu ích trong một khoảng thời gian ngắn trước khi giá trị bộ đếm thay đổi quá nhiều và mã token nhân bản trở nên không được đồng bộ hóa từ mã token thực và máy chủ.



Một phương pháp rất phổ biến khác để xử lý đa yếu tố ngày nay, đó là gửi mã thông báo mật khẩu một lần bằng SMS. Nhưng điều này đã bị một số chỉ trích, vì các cuộc tấn công được quan sát thông qua kênh này. Vấn đề với việc dựa vào SMS để truyền yếu tố xác thực bổ sung là chúng ta đang phụ thuộc vào các quy trình bảo mật của nhà cung cấp dịch vụ di động. SMS không được mã hóa và cũng không phải là tin riêng tư. Và có thể tin nhắn SMS bị chặn bởi một kẻ tấn công được trang bị tốt. Tệ hơn nữa, đã có những tài khoản mã dựa trên SMS bị đánh cắp bằng cách gọi cho nhà cung cấp dịch vụ di động. Kẻ tấn công mạo danh chủ sở hữu của đường truyền dịch vụ để chuyển hướng các cuộc gọi điện thoại và tin nhắn SMS đến điện thoại mà kẻ tấn công kiểm soát. Nếu kẻ tấn công đã đánh cắp được mật khẩu và có thể nhận được SMS chuyển hướng đến chúng, thì giờ đây chúng sẽ có toàn quyền truy cập vào tài khoản.



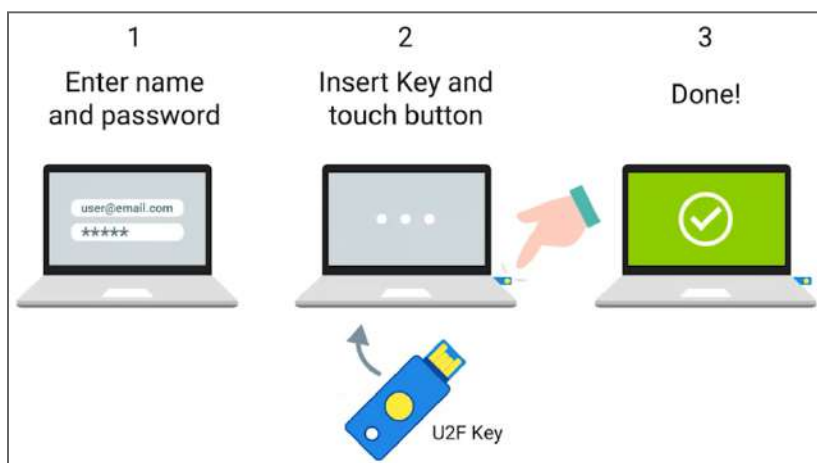
Các mã OTP cũng dễ bị tấn công lừa đảo theo kiểu trung gian. Người dùng có thể bị lừa vào trang xác thực giả bằng cách gửi email, tin nhắn lừa đảo. Ví dụ, email thông báo "tài khoản đã bị xâm phạm, yêu cầu đăng nhập và thay đổi mật khẩu ngay lập tức." Khi nạn nhân nhập thông tin đăng nhập của họ vào trang giả mạo, bao gồm cả mật khẩu dùng một lần, kẻ tấn công có tất cả thông tin cần thiết để chiếm đoạt tài khoản.

Một sự phát triển của token vật lý là U2F (Universal Second Factor). Đó cũng là một tiêu chuẩn được phát triển bởi Google, Yubico và NXP Semiconductors. U2F kết hợp cơ chế phản hồi-thử thách (challenge–response), cùng với khóa công khai để triển khai giải pháp xác thực yếu tố thứ hai an toàn hơn và thuận tiện hơn. Xác thực với U2F được tích hợp trong trình duyệt Chrome và trình duyệt Opera, với sắp tới là Firefox. Chia khóa bảo mật về cơ bản là các bộ xử lý mã hóa nhúng nhỏ, có khả năng lưu trữ an toàn các khóa bất đối xứng và các phần bổ sung để chạy mã nhúng.

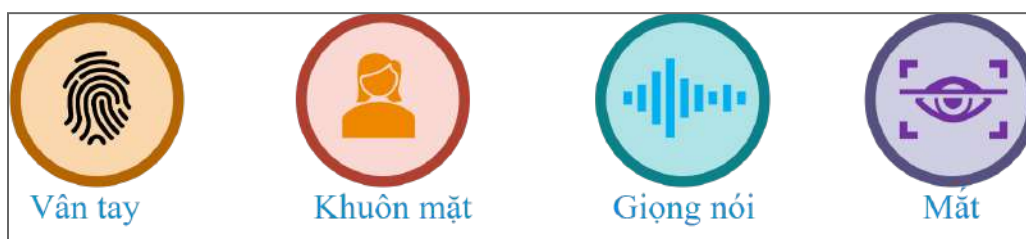
Từ góc độ bảo mật, đây là một thiết kế an toàn hơn nhiều so với OTP. Điều này là do, quy trình xác thực được bảo vệ khỏi các cuộc tấn công lừa đảo, dựa trên bản chất tương tác của quy trình. Mặc dù U2F không trực tiếp bảo vệ khỏi các cuộc tấn công xen giữa, nhưng quá trình xác thực sẽ diễn ra qua kết nối TLS an toàn, điều này sẽ cung cấp khả năng bảo vệ khỏi kiểu tấn công này. Khóa bảo mật cũng có khả năng chống sao chép hoặc giả mạo, bởi vì chúng có các bí mật độc đáo, được nhúng trên chúng và được bảo vệ khỏi giả mạo. Từ góc độ thuận tiện, đây là quy trình xác thực tốt hơn nhiều so với OTP vì người dùng không phải nhập một chuỗi số vào hộp thoại xác thực theo cách thủ công. Tất cả những gì họ phải làm là nhấn vào khóa bảo mật của họ.

Để sử dụng thiết bị này, đầu tiên chúng ta cần đăng ký, vì khóa bảo mật phải được đăng ký với một trang web hoặc dịch vụ. Tại thời điểm đăng ký, khóa bảo mật tạo một cặp khóa công khai-bí mật duy nhất cho trang web đó và gửi khóa công khai đến trang web để đăng ký. Nó cũng liên kết danh tính của trang web với cặp khóa. Lý do cho các cặp khóa duy nhất cho mỗi trang web là do bảo mật. Nếu một trang web bị tấn công, điều này sẽ ngăn việc tham chiếu chéo các khóa công khai đã đăng ký và phát hiện ra những điểm chung giữa các trang web dựa trên dữ liệu đăng ký. Sau khi đăng ký với trang web, lần sau khi được hỏi xác thực, bạn sẽ được yêu cầu nhập tên người dùng và mật khẩu của mình như bình thường. Nhưng sau đó, bạn sẽ được nhắc nhấn vào khóa bảo mật của mình. Khi bạn chạm thực tế vào khóa bảo mật, đó là một kiểm tra nhỏ về sự hiện diện của người dùng để đảm bảo phần mềm độc hại không thể xác thực thay mặt bạn mà bạn không biết. Thao tác nhấn này sẽ mở khóa các khóa cá nhân được lưu trữ trong khóa bảo mật, được sử dụng để xác thực. Quá trình xác thực xảy ra như một quy trình phản hồi-thử thách, bảo vệ chống lại các cuộc tấn công phát lại (replay attack). Điều này là do phiên xác thực không thể

được sử dụng lại bởi kẻ nghe trộm sau đó, vì thử thách và phản hồi kết quả sẽ khác với mỗi phiên xác thực. Điều xảy ra là trang web tạo ra một thử thách, về cơ bản, một số dữ liệu ngẫu nhiên và gửi dữ liệu này cho máy khách đang cố gắng xác thực. Sau đó, máy khách sẽ chọn khóa riêng phù hợp với trang web và sử dụng khóa này để ký xác nhận và gửi lại dữ liệu đã ký. Trang web hiện có thể xác minh chữ ký bằng khóa công khai đã được đăng ký trước đó. Nếu chữ ký được kiểm tra, người dùng đã được xác thực.



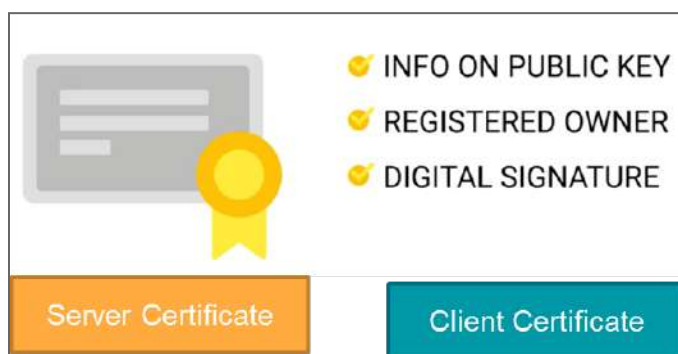
Một loại xác thực đa yếu tố khác là sinh trắc học (biometric authentication), đã trở nên phổ biến trong những năm gần đây, đặc biệt là trong các thiết bị di động. Xác thực sinh trắc học là quá trình sử dụng các đặc điểm sinh lý độc nhất của một cá nhân để định danh họ. Bằng cách xác nhận chữ ký sinh trắc học, cá nhân được xác thực. Một lợi thế của xác thực sinh trắc học so với các hệ thống dựa trên mật khẩu hoặc mã token, đó là việc xác định một cá nhân để xác thực đáng tin cậy hơn, vì các tính năng sinh trắc học thường không thể chia sẻ được. Ví dụ, bạn không thể cung cấp dấu vân tay cho bạn bè của mình để họ có thể đăng nhập với tư cách là bạn. Tuy nhiên, mọi thứ không diễn ra theo cách đó. Khi các trường học bắt đầu giới thiệu hệ thống điểm danh dựa trên dấu vân tay, học sinh tìm cách đánh lừa hệ thống này. Họ tạo dấu vân tay giả bằng cách sử dụng những thứ như keo dán. Ngoài ra, hệ thống sinh trắc học cũng gặp một số vấn đề như nó thường không dễ để thay đổi khi chúng ta muốn và cũng dễ bị vi phạm quyền riêng tư.



Hệ thống xác thực sinh trắc học được thực hiện bằng việc đăng ký, lưu trữ và so khớp dữ liệu sinh trắc. Một ứng dụng rất phổ biến trong các thiết bị di động là máy quét dấu vân tay để mở khóa điện thoại. Tính năng này hoạt động bằng cách đăng ký dấu vân tay của bạn trước, sử dụng cảm biến quang học để ghi lại hình ảnh của mẫu vân tay của bạn. Giống như cách mặt khẩu không bao giờ được lưu trữ dưới dạng văn bản thô, dữ liệu sinh trắc học được sử dụng để xác thực, do đó, nó cũng không bao giờ được lưu trữ trực tiếp. Điều này thậm chí còn quan trọng hơn để xử lý dữ liệu sinh trắc học. Không giống như mặt khẩu, sinh trắc học là một phần vốn có của con người. Vì vậy, có những tác động riêng tư đối với hành vi trộm cắp hoặc rò rỉ dữ liệu sinh trắc học. Đặc điểm sinh trắc học cũng có thể rất khó thay đổi trong trường hợp chúng bị xâm phạm không giống như mặt khẩu. Vì vậy, thay vì lưu trữ dữ liệu dấu vân tay trực tiếp, dữ liệu được chạy thông qua một thuật toán băm và kết quả là giá trị băm duy nhất. Khi xác thực, hệ thống sẽ so khớp sinh trắc học hiện tại với dữ liệu được lưu trữ.

Xác thực chứng chỉ số

Chứng chỉ số (digital certificate) là khóa công khai được tổ chức phát hành chứng chỉ hoặc CA ký như một dấu hiệu của sự tin cậy. Hay nói cách khác chứng chỉ số chứng minh thực thể sở hữu khóa công khai. Trong đó, nó chứa một số thông tin như khóa công khai, chủ sở hữu, chữ ký số. Ngoài chứng chỉ máy chủ, chúng ta cũng có chứng chỉ máy khách. Nó hoạt động rất giống với chứng chỉ máy chủ nhưng được thể hiện bởi máy khách và cho phép máy chủ xác thực và xác minh máy khách. Các hệ thống VPN hoặc Wifi doanh nghiệp sử dụng chứng chỉ khách để xác thực.



Quy trình xác thực chứng chỉ giống như xuất trình giấy tờ tùy thân tại sân bay. Bạn xuất trình ID hoặc chứng chỉ của mình để chứng minh bạn là ai. ID được kiểm tra để xem nó có được cấp bởi một cơ quan được người xác minh tin cậy hay không. Nó được cấp bởi một tổ chức chính phủ hay nó là một giấy phép mới từ một cửa hàng quà tặng? Rõ ràng, một trong những ID đó sẽ được chấp nhận tại sân bay, tương tự như một chứng chỉ được CA đáng tin cậy ký. Danh sách các CA đáng tin cậy cần được lưu trữ trước đó để phục vụ quá trình kiểm tra này.





Khi bạn ở sân bay, ngày hết hạn trên giấy tờ tùy thân của bạn cũng sẽ được kiểm tra để đảm bảo nó vẫn còn hiệu lực. Điều tương tự cũng áp dụng cho xác thực chứng chỉ, mặc dù chứng chỉ có hai ngày cần được xác minh (không hợp lệ trước và không hợp lệ sau). Không hợp lệ trước nghĩa là kiểm tra xem chứng chỉ có hợp lệ ở thời điểm hiện tại hay không vì có thể có chứng chỉ được cấp để sử dụng trong tương lai. Không hợp lệ sau ngày nghĩa là chứng chỉ hết hạn chưa.




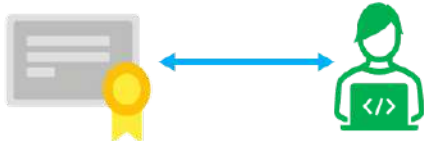
Các nhà chức trách sân bay cũng có một danh sách các ID cụ thể được gắn cờ. Nếu ID của bạn nằm trong danh sách đó, thì bạn sẽ bị từ chối đi máy bay. Tương tự, chứng chỉ sẽ được kiểm tra dựa trên danh sách thu hồi hoặc CRL. Đây là danh sách đã ký do CA công bố, xác định các chứng chỉ đã bị thu hồi một cách rõ ràng.

Một bước cuối cùng là chứng minh quyền sở hữu khóa tương ứng, vì chứng chỉ là khóa công khai đã ký. Nếu chúng ta không chứng minh được quyền sở hữu, thì không có gì ngăn được kẻ tấn công sao chép chứng chỉ, vì nó không được coi là bí mật và đóng giả là chủ sở hữu. Để tránh điều này, việc sở hữu khóa cá nhân được xác minh thông qua cơ chế thử thách-phản hồi. Máy chủ sẽ yêu cầu một bit dữ liệu ngẫu nhiên được ký bằng khóa bí mật tương ứng với

khóa công khai. Điều này tương tự như cách sân bay kiểm tra ảnh trên giấy tờ tùy thân của bạn để đảm bảo bạn trông giống người trong ảnh và không mạo danh họ.

Bảng sau tóm tắt các điểm tương ứng trên.

Bước	Kiểm tra thị thực	Xác thực chứng chỉ
1	<p>Xuất trình giấy tờ tùy thân (hộ chiếu, CCCD)</p> 	<p>Xuất trình chứng chỉ.</p> 
2	<p>ID được kiểm tra xem nó có được cấp bởi tổ chức chính phủ tin cậy?</p> 	<p>Chứng chỉ có được CA đáng tin cậy ký không?</p> 
3	<p>Vẫn còn thời gian hiệu lực?</p>	<p>Kiểm tra chứng chỉ có hợp lệ vào thời điểm hiện tại? (Not valid before, not valid after)</p>

4	<p>ID có nằm trong danh sách bị hạn chế?</p> 	<p>Chứng chỉ có nằm trong danh sách thu hồi (Certificate Revocation List, CRL) không?</p> 
5	<p>Kiểm tra ID có khớp với người xuất trình nó bằng cách kiểm tra khuôn mặt.</p> 	<p>Kiểm tra bên trình chứng chỉ có phải là sở hữu hợp lệ bằng cơ chế thử thách-phản hồi.</p> 

Các giao thức xác thực (LDAP, RADIUS, Kerberos, TACACS+)

LDAP

LDAP (Lightweight Directory Access Protocol) là một giao thức tiêu chuẩn công nghiệp mở để truy cập và duy trì các dịch vụ thư mục. Khi chúng ta nói dịch vụ thư mục (directory service), chúng ta đang đề cập đến một dạng cơ sở dữ liệu chứa và duy trì thông tin về người sử dụng và các tài nguyên trong mạng. Ví dụ, khi người dùng truy xuất một ứng dụng, ứng dụng này sẽ tham chiếu đến dịch vụ thư mục để đảm bảo người dùng hợp pháp và có quyền truy cập thư mục.

LDAP mô tả cấu trúc dữ liệu của thư mục. Và xác định các chức năng để tương tác với dịch vụ, như thực hiện tra cứu và cập nhật. Cấu trúc thư mục LDAP là một loại cấu trúc cây và được tối ưu hóa cho việc truy xuất dữ liệu hơn là cập nhật và sửa đổi. Các thư mục có thể được lưu trữ trên nhiều máy chủ

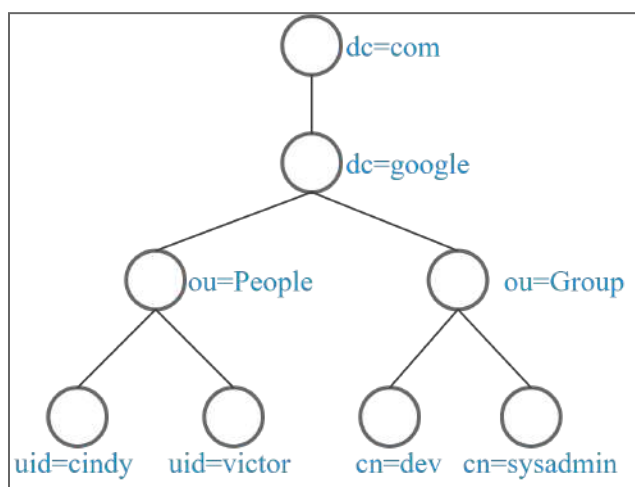
LDAP khác nhau để tạo điều kiện cho việc tra cứu nhanh hơn và được giữ đồng bộ thông qua việc nhân bản thư mục.

Một phần tử cho một người dùng cụ thể trong LDAP sẽ chứa thông tin liên quan đến tài khoản người dùng đó, như họ và tên, số điện thoại, địa chỉ email, shell đăng nhập và các dữ liệu khác. Bên cạnh các thuộc tính đối tượng, vị trí của phần tử trong cấu trúc dữ liệu tổng thể sẽ đại diện cho thông tin liên quan đến các đối tượng như mối quan hệ giữa chúng.

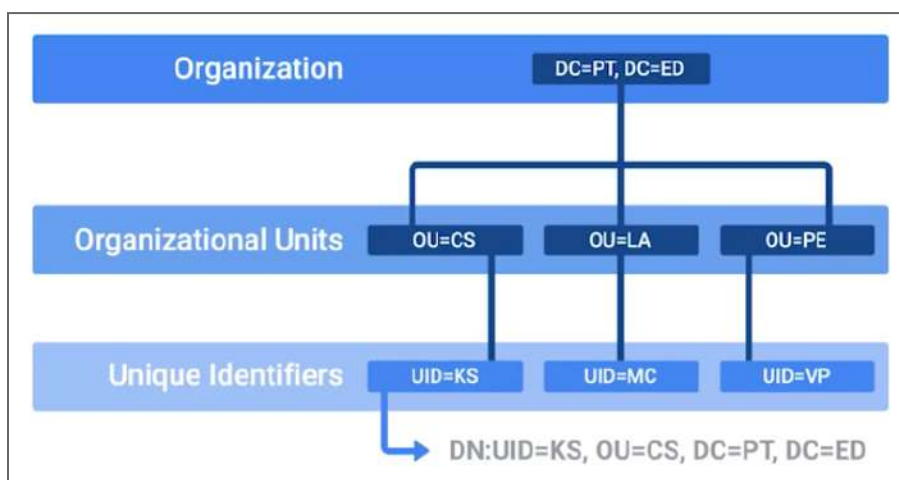
```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Nguồn: Wikipedia

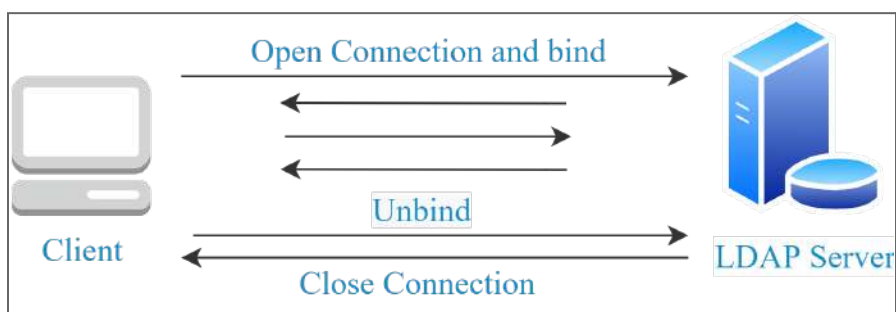
LDAP sử dụng cấu trúc cây được gọi là cây thông tin dữ liệu (Data Information Tree), trong đó các đối tượng sẽ có một cha và có thể có một hoặc nhiều con thuộc về đối tượng cha. Chúng ta cũng có thể xem nó giống như một hệ thống tập tin. Trong ngôn ngữ LDAP, các thư mục mà một đối tượng thuộc về được gọi là Đơn vị tổ chức. Chúng cho phép nhóm các đối tượng có liên quan hay tương tự nhau thành một đơn vị. Ví dụ, đơn vị tổ chức People hoặc Group để phân biệt giữa tài khoản người dùng cá nhân và nhóm mà tài khoản đó thuộc về. Cấu trúc cây này cũng cho phép kế thừa và lồng ghép các đối tượng, trong đó các thuộc tính của đối tượng cha có thể được kế thừa bởi các đối tượng con ở sâu bên dưới cây.



Do các phần tử trong thư mục có thể chia sẻ các thuộc tính, nên cần có một số định danh duy nhất cho mỗi mục. Chúng ta gọi nó là tên phân biệt (distinguished name, DN). Chúng ta có thể coi DN như một đường dẫn đầy đủ đến tập tin thay vì tên tập tin. Điều này là do có thể có nhiều tập tin có cùng tên trên một hệ thống tập tin. Đường dẫn đầy đủ đến tập tin sẽ giúp mô tả một tập tin duy nhất.



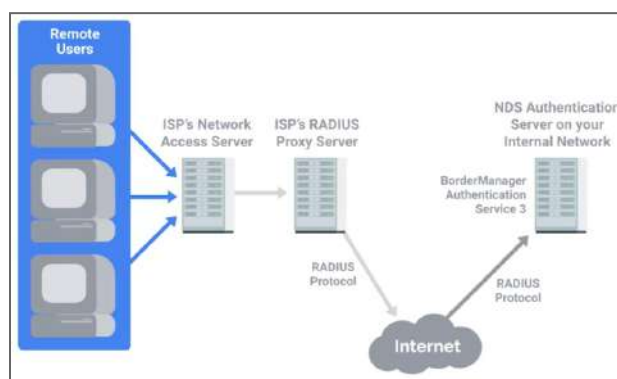
Máy khách có thể tương tác với máy chủ LDAP thông qua quá trình liên kết (bind), đó là cách máy khách xác thực với máy chủ. StartTLS, cho phép máy khách giao tiếp bằng LDAP qua TLS. Hiện nay, có nhiều cách triển khai máy chủ LDAP, như Active Directory của Microsoft và OpenLDAP cho triển khai mã nguồn mở.



RADIUS

RADIUS (Remote Authentication Dial-In User Service) là một giao thức cung cấp các dịch vụ AAA cho người dùng trên một mạng. Đó là một giao thức phổ biến được sử dụng để quản lý quyền truy cập vào mạng nội bộ, mạng WiFi, dịch vụ email và dịch vụ VPN. Ban đầu được thiết kế để vận chuyển thông tin xác thực cho người dùng quay số từ xa, Nó được phát triển để mang nhiều giao thức xác thực tiêu chuẩn như EAP (Extensible Authentication Protocol).

Máy khách muốn xác thực máy chủ RADIUS không trực tiếp tương tác với máy chủ đó. Thay vào đó, khi máy khách muốn truy cập tài nguyên được bảo vệ, máy khách sẽ xuất trình thông tin xác thực cho NAS (Network Access Server) và nó sẽ chuyển tiếp thông tin đăng nhập đến máy chủ RADIUS. Máy chủ RADIUS sau đó sẽ xác minh thông tin đăng nhập bằng cách sử dụng lược đồ xác thực đã được cấu hình. Máy chủ RADIUS có thể xác minh thông tin xác thực người dùng được lưu trữ trong một tập tin hoặc có thể tích hợp vào các nguồn bên ngoài như cơ sở dữ liệu SQL, LDAP, Kerberos hoặc Active Directory. Sau khi máy chủ RADIUS đã đánh giá yêu cầu xác thực của người dùng, nó sẽ trả lời bằng một trong ba thông báo từ chối truy cập, thử thách truy cập hoặc chấp nhận truy cập.

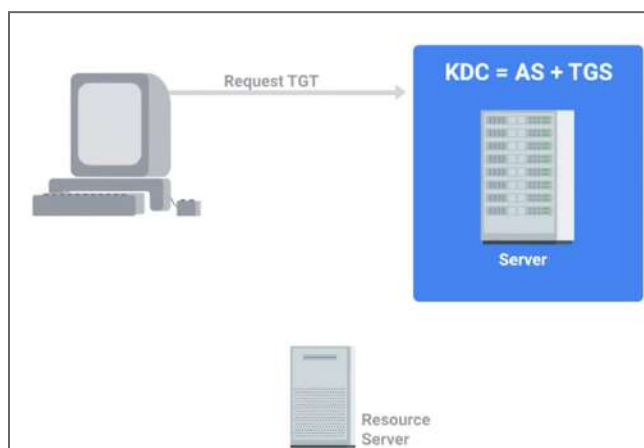


Kerberos

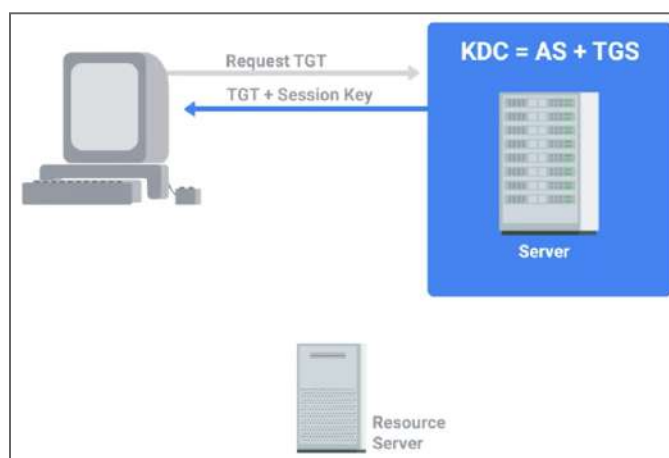
Kerberos là một giao thức xác thực mạng sử dụng vé để cho phép các thực thể chứng minh danh tính của nhau qua các kênh không an toàn. Nó cũng sử dụng mã hóa đối xứng để bảo vệ các thông điệp khỏi các cuộc tấn công nghe trộm và phát lại.

Vé xác thực (authentication ticket) là một loại mã thông báo chứng minh danh tính của bạn. Chúng có thể được sử dụng để xác thực với các dịch vụ được bảo vệ bằng cách sử dụng Kerberos hay nói cách khác là hoặc trong lĩnh vực Kerberos. Phiếu xác thực cho phép người dùng xác thực các dịch vụ mà không yêu cầu xác thực tên người dùng và mật khẩu cho từng dịch vụ riêng lẻ. Vé sẽ hết hạn sau một thời gian, nhưng nó có quy định về việc gia hạn vé tự động minh bạch.

Đầu tiên, người dùng nhập tên và mật khẩu của họ. Sau đó, phần mềm Kerberos trên máy của họ sẽ lấy mật khẩu và tạo khóa mã hóa đối xứng từ nó. Tiếp theo, máy khách gửi một tin nhắn văn bản thuần túy đến Kerberos AS chứa ID người dùng. Mật khẩu hoặc khóa bí mật lấy từ mật khẩu sẽ không được truyền đi. AS sử dụng ID người dùng để kiểm tra xem có tài khoản trong cơ sở dữ liệu xác thực hay không. Nếu có, AS sẽ tạo khóa bí mật bằng cách sử dụng mật khẩu băm được lưu trữ trong máy chủ trung tâm phân phối khóa.

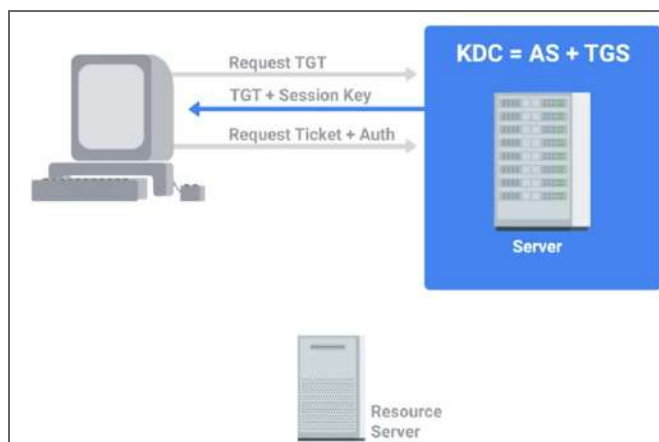


Sau đó AS sẽ sử dụng khóa bí mật để mã hóa và gửi một thông điệp có chứa khóa phiên TGS máy khách. Đây là khóa bí mật được sử dụng để mã hóa thông tin liên lạc với dịch vụ cấp vé. AS cũng gửi một thông điệp thứ hai với phiếu cấp vé (ticket granting ticket, TGT), được mã hóa bằng khóa bí mật TGS. TGT có thông tin như ID máy khách, thời hạn hiệu lực của vé và khóa phiên TGS máy khách. Vì vậy, thông điệp đầu tiên có thể được giải mã bằng cách sử dụng khóa bí mật được chia sẻ có nguồn gốc từ mật khẩu người dùng. Sau đó, nó cung cấp khóa bí mật có thể giải mã thông điệp thứ hai mà cung cấp cho máy khách phiếu cấp vé hợp lệ.

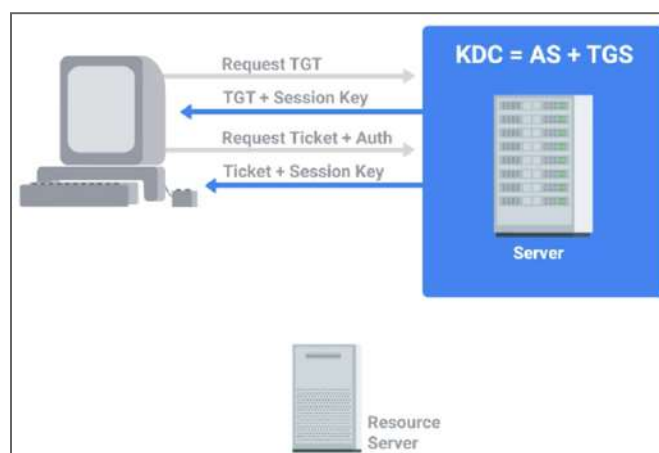


Vì máy khách đã xác thực và nhận được phiếu cấp vé hợp lệ, nên máy khách có thể sử dụng phiếu cấp vé để yêu cầu quyền truy cập vào các dịch vụ từ bên trong khu vực Kerberos. Điều này được thực hiện bằng cách gửi một tin nhắn đến dịch vụ cấp vé cùng với mã cấp vé đã được mã hóa nhận được từ AS trước

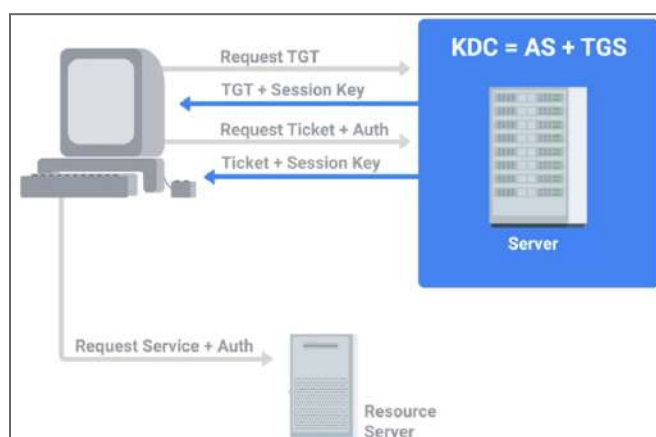
đó cùng với tên dịch vụ hoặc ID mà máy khách đang yêu cầu quyền truy cập. Máy khách cũng gửi một thông điệp chứa trong bộ xác thực mà có ID máy khách và thời gian được mã hóa bằng khóa phiên TGS máy khách.



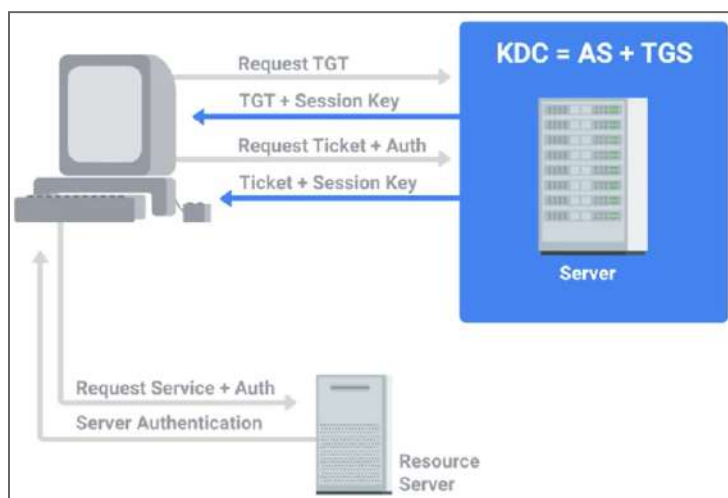
Dịch vụ cấp vé giải mã phiếu cấp vé bằng khóa bí mật TGS, khóa mà cung cấp TGS cho khóa phiên TGS máy khách. Sau đó, nó sử dụng khóa để giải mã thông điệp xác thực. Tiếp theo, nó kiểm tra ID máy khách của hai thông điệp này để đảm bảo chúng khớp với nhau. Nếu đúng, nó sẽ gửi lại hai thông điệp cho máy khách. Thông điệp đầu tiên chứa vé máy khách-đến-máy chủ bao gồm ID máy khách, địa chỉ máy khách, thời hạn hiệu lực và khóa phiên máy khách-máy chủ được mã hóa bằng khóa bí mật của dịch vụ. Thông điệp thứ hai, chứa chính khóa phiên máy khách-máy chủ và được mã hóa bằng khóa phiên TGS máy khách.



Cuối cùng, máy khách có đủ thông tin để xác thực chính nó với máy chủ dịch vụ. Máy khách gửi hai thông điệp đến SS. Thông điệp đầu tiên là vé máy khách đến máy chủ đã mã hóa nhận được từ Dịch vụ cấp vé. Thứ hai là trình xác thực mới với ID máy khách và thời gian được mã hóa bằng khóa phiên máy khách-máy chủ.



SS giải mã thông điệp đầu tiên bằng cách sử dụng khóa bí mật của nó. Công việc này cung cấp cho nó khóa phiên máy khách-máy chủ. Sau đó, khóa được sử dụng để giải mã thông điệp thứ hai và nó so sánh ID ứng dụng khách trong trình xác thực với ID có trong vé máy khách đến máy chủ. Nếu các ID này khớp nhau, thì SS sẽ gửi một thông điệp chứa nhãn thời gian từ bộ xác thực cung cấp máy khách được mã hóa bằng khóa phiên máy khách-máy chủ. Sau đó, máy khách sẽ giải mã thông điệp này và kiểm tra xem thời gian có xác thực đúng máy chủ hay không. Nếu tất cả điều này thành công, thì máy chủ cấp quyền truy cập vào dịch vụ được yêu cầu trên máy khách.



Kerberos có một điểm yếu. Nó một dịch vụ nguyên khối duy nhất. Điều này tạo ra một điểm thất bại nguy hiểm. Nếu dịch vụ Kerberos ngừng hoạt động, người dùng mới sẽ không thể xác thực và đăng nhập. Ngoài các vấn đề về tính khả dụng, nếu máy chủ Kerberos trung tâm bị xâm nhập, kẻ tấn công có thể mạo danh bất kỳ người dùng nào bằng cách tạo vé Kerberos hợp lệ cho tài khoản người dùng. Kerberos yêu cầu thời gian nghiêm ngặt, máy khách và máy chủ phải được đồng bộ hóa tương đối chặt chẽ, nếu không, quá trình xác thực sẽ không thành công. Điều này thường được thực hiện bằng cách sử dụng NTP để giữ cho cả hai bên được đồng bộ hóa bằng máy chủ NTP. Mô hình tin cậy của Kerberos cũng có vấn đề, vì nó yêu cầu máy khách và dịch vụ phải có sự tin cậy đã được thiết lập trong máy chủ Kerberos để mà xác thực bằng Kerberos. Điều này có nghĩa là người dùng không thể xác thực bằng cách sử dụng Kerberos từ các ứng dụng khách không xác định hoặc không đáng tin cậy. Vì vậy, những thứ như BYOD và điện toán đám mây không tương thích hoặc ít nhất là rất khó để triển khai an toàn với xác thực Kerberos.

TACACS+

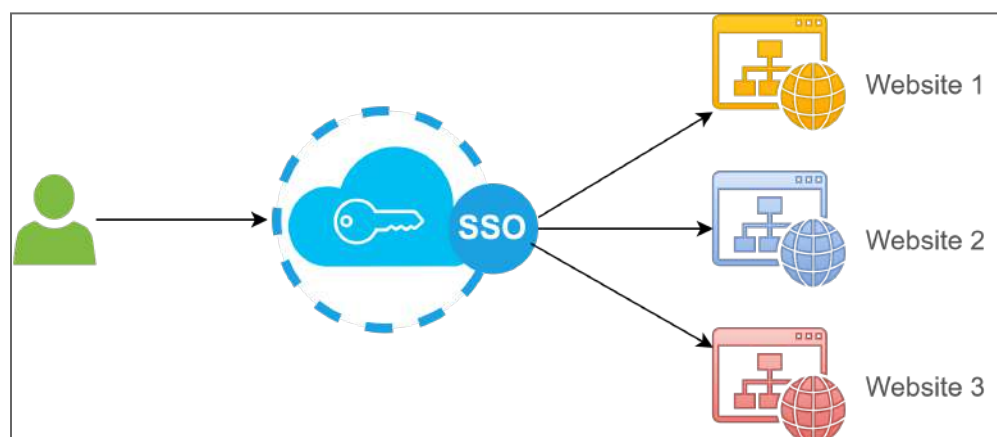
TACACS+ là một giao thức AAA do Cisco phát triển, được phát hành dưới dạng tiêu chuẩn mở vào năm 1993. Nó thay thế giao thức TACACS cũ hơn được phát triển vào năm 1984 cho MILNET. TACACS + cũng thay thế cho XTACACS hoặc Extended TACACS là một phần mở rộng độc quyền của Cisco trên TACACS. TACACS+ chủ yếu được sử dụng để quản trị thiết bị, xác thực, ủy quyền và kế toán, trái ngược với RADIUS, phần lớn được sử dụng để truy cập mạng AAA. Mặc dù sự khác biệt chủ yếu liên quan đến ủy quyền và các phần kế

toán, nhiều hơn là xác thực. TACACS + chủ yếu được sử dụng như một hệ thống xác thực cho các thiết bị hạ tầng mạng, có xu hướng trở thành mục tiêu giá trị cao cho những kẻ tấn công.

Đăng nhập một lần

Đăng nhập một lần (Single Sign-On, SSO) là công nghệ cho phép người dùng xác thực một lần để được cấp quyền truy cập vào nhiều dịch vụ và ứng dụng khác nhau. Vì không cần xác thực lại cho từng dịch vụ, người dùng không cần nhiều bộ tên người dùng và mật khẩu trên một hỗn hợp các ứng dụng và dịch vụ. SSO được thực hiện bằng cách xác thực với máy chủ xác thực trung tâm, như máy chủ LDAP. Sau đó, nó được một cookie hoặc mã token có thể được sử dụng để truy cập vào các ứng dụng được định cấu hình để sử dụng SSO. SSO thực sự rất tiện lợi. Nó cho phép người dùng có một bộ thông tin xác thực cấp quyền truy cập vào nhiều dịch vụ, giúp ít có khả năng mật khẩu bị ghi hoặc lưu trữ không an toàn. Điều này cũng sẽ giảm chi phí cho hỗ trợ mật khẩu và loại bỏ thời gian xác thực lại trong suốt ngày làm việc.

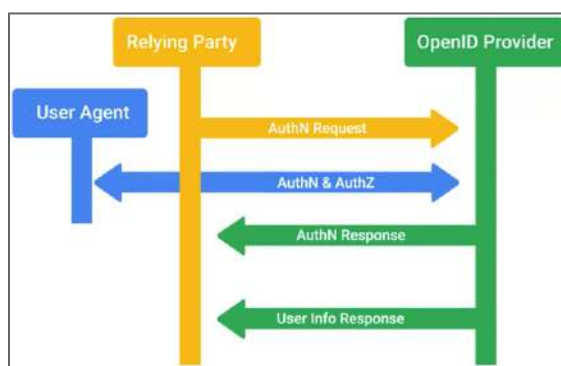
Kerberos là một ví dụ điển hình về dịch vụ xác thực SSO. Người dùng sẽ xác thực dịch vụ Kerberos một lần, sau đó nó sẽ cấp cho họ một phiếu cấp vé. Điều này sau đó có thể được xuất trình cho dịch vụ cấp vé thay cho thông tin đăng nhập truyền thống. Vì vậy, người dùng có thể nhập thông tin đăng nhập một lần và có quyền truy cập vào nhiều dịch vụ khác nhau.



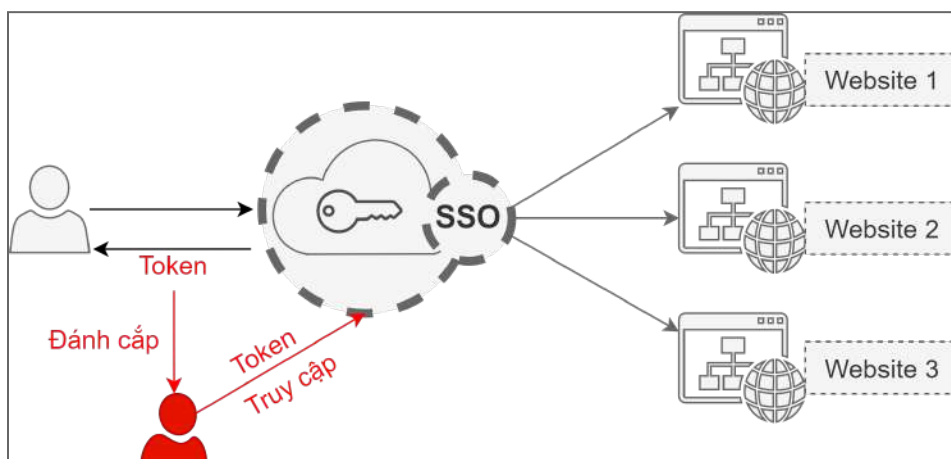
Ví dụ về hệ thống SSO là openID, đây là hệ thống xác thực phi tập trung. OpenID là một tiêu chuẩn mở cho phép các bên tham gia được gọi là bên phụ thuộc (relying party) xác thực người dùng qua bên thứ ba. Điều này giúp cho

các bên tham gia không cần phải xây dựng cơ sở hạ tầng xác thực phức tạp. Nó cũng cho phép người dùng truy cập trang web mà không yêu cầu họ tạo tài khoản mới, đơn giản hóa việc quản lý quyền truy cập trên nhiều trang web. Thay vào đó, người dùng chỉ cần có tài khoản với nhà cung cấp định danh.

Để yêu cầu xác thực, trước tiên bên phụ thuộc tra cứu nhà cung cấp openID, và thiết lập bí mật được chia sẻ với nhà cung cấp này. Bí mật được chia sẻ sẽ được sử dụng để xác thực thông điệp của nhà cung cấp openID. Tiếp theo, người dùng sẽ được chuyển hướng hoặc yêu cầu xác thực trong một cửa sổ mới thông qua nhật ký và quy trình của nhà cung cấp định danh. Sau khi xác thực, người dùng sẽ được nhắc xác nhận xem họ có tin tưởng bên phụ thuộc hay không. Khi hoàn tất xác nhận, thông tin đăng nhập được chuyển tiếp đến bên phụ thuộc, thường ở dạng mã token cho biết người dùng hiện đã được xác thực với dịch vụ.



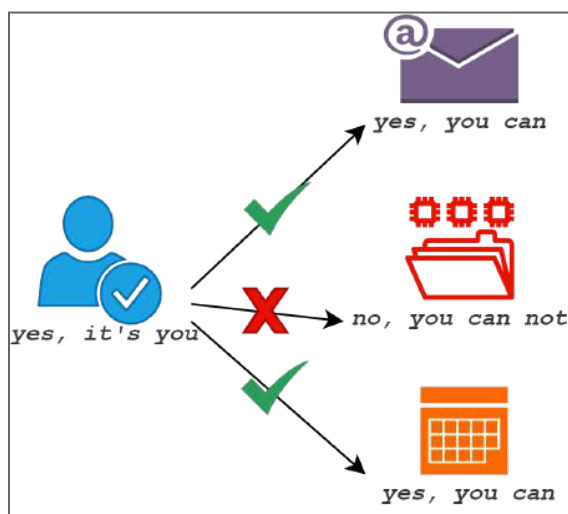
SSO mở ra một kênh tấn công mới, đó là đánh cắp cookie hoặc mã token phiên SSO. Thay vì nhắm mục tiêu trực tiếp vào thông tin đăng nhập, những kẻ tấn công có thể cố gắng đánh cắp mã token SSO trực tiếp, điều này sẽ cho phép truy cập rộng rãi ứng dụng ngay cả trong một khoảng thời gian ngắn. Đánh cắp các mã token này, cũng cho phép kẻ tấn công né tránh các biện pháp bảo vệ xác thực đa yếu tố vì mã token phiên cho phép truy cập mà không yêu cầu xác thực đầy đủ cho đến khi mã token hết hạn.



3. Ủy quyền

Khái niệm về ủy quyền

Ủy quyền thường được kết hợp chặt chẽ với xác thực. Xác thực liên quan đến việc xác minh danh tính người dùng, nhưng ủy quyền liên quan đến việc mô tả những gì tài khoản người dùng có quyền truy cập hoặc không có quyền truy cập. Người dùng có thể xác thực thành công hệ thống bằng cách xuất trình thông tin xác thực hợp lệ. Nhưng nếu tên người dùng mà họ xác thực cũng không được phép truy cập vào hệ thống được đề cập, họ sẽ bị từ chối quyền truy cập.



Khi chúng ta nói về Kerberos trước đó, người dùng đã xác thực và nhận được một phiếu cấp vé. Sau đó, điều này có thể được sử dụng để yêu cầu quyền truy cập vào một dịch vụ cụ thể bằng cách gửi yêu cầu đến dịch vụ cấp vé. Đây là lúc việc cấp phép có hiệu lực, vì dịch vụ cấp vé sẽ quyết định xem người dùng được đề cập có được phép truy cập vào dịch vụ đang được yêu cầu hay không. Nếu họ không được phép hoặc không được phép truy cập dịch vụ, yêu cầu sẽ bị từ chối bởi dịch vụ cấp vé. Nếu người dùng được ủy quyền, dịch vụ cấp vé sẽ trả lại một vé, cho phép người dùng truy cập dịch vụ.

Hệ thống ủy quyền

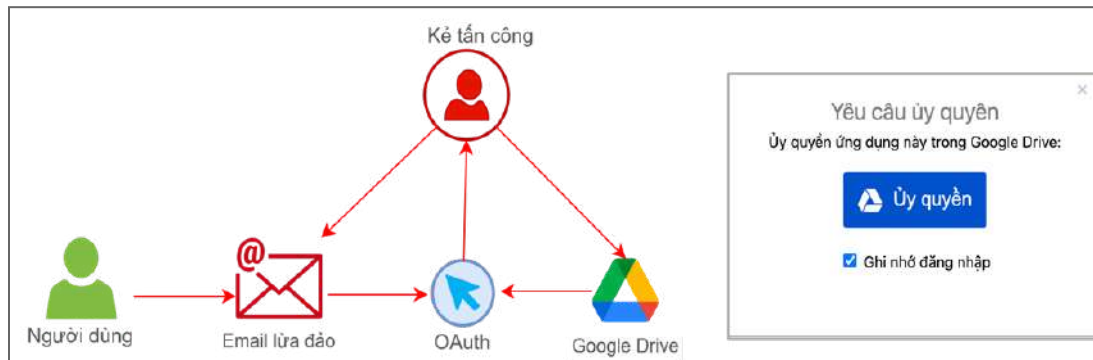
Một tiêu chuẩn mở rất phổ biến để ủy quyền và ủy quyền truy cập là OAuth, được sử dụng bởi các công ty như Google, Facebook và Microsoft. Với OAuth, người dùng có thể cấp cho các trang web và ứng dụng của bên thứ ba quyền truy cập vào thông tin của họ mà không cần chia sẻ thông tin đăng nhập tài khoản. Đây có thể được coi là một hình thức ủy quyền truy cập vì quyền truy cập vào tài khoản của người dùng đang được ủy quyền cho bên thứ ba.

OAuth được thực hiện bằng cách nhắc người dùng xác nhận rằng họ đồng ý cho phép bên thứ ba truy cập vào thông tin nhất định về tài khoản của họ. Thông thường, phần mềm hỗ trợ này sẽ liệt kê cụ thể những phần thông tin hoặc quyền truy cập nào đang được yêu cầu. Sau khi được xác nhận, nhà cung cấp định danh sẽ cung cấp cho bên thứ ba một mã token. Mã token này sau đó có thể được bên thứ ba sử dụng để truy cập dữ liệu hoặc dịch vụ do nhà cung cấp định danh trực tiếp thay mặt cho người dùng cung cấp.

Điều quan trọng là người dùng phải chú ý đến bên thứ ba nào đang yêu cầu quyền truy cập và chính xác những gì họ đang cấp quyền truy cập. Quyền OAuth có thể được sử dụng trong các cuộc tấn công theo kiểu lừa đảo để giành quyền truy cập vào tài khoản mà không yêu cầu thông tin xác thực bị xâm phạm. Điều này hoạt động bằng cách gửi email lừa đảo đến các nạn nhân tiềm năng trông giống như các yêu cầu ủy quyền OAuth hợp pháp, yêu cầu này đòi hỏi người dùng cấp quyền truy cập vào một số thông tin trong tài khoản của họ thông qua OAuth. Sau khi người dùng cấp quyền truy cập, kẻ tấn công có quyền truy cập vào tài khoản thông qua mã token ủy quyền OAuth.

Điều này đã được sử dụng trong một cuộc tấn công dựa trên OAuth vào đầu năm 2017. Đã có một loạt các email lừa đảo xuất hiện từ một người bạn hoặc

đồng nghiệp muốn chia sẻ tài liệu google. Khi liên kết chia sẻ được theo dõi, nạn nhân được nhắc đăng nhập và cấp quyền truy cập vào tài liệu email và danh bạ cho một số dịch vụ của bên thứ ba, dịch vụ này tự nhận mình là Google Apps. Nhưng nó thực sự là một dịch vụ độc hại, sau đó sẽ gửi email cho các liên hệ từ tài khoản email của họ.



Điều quan trọng là phải phân biệt giữa OAuth và OpenID. OAuth cụ thể là một hệ thống ủy quyền và OpenID là một hệ thống xác thực. Mặc dù chúng thường được sử dụng cùng nhau, OpenID Connect là một lớp xác thực được xây dựng trên OAuth 2.0 được thiết kế để cải thiện OpenID và tích hợp tốt hơn với các ủy quyền OAuth.

Vì TACACS+ là một hệ thống AAA đầy đủ, nó cũng xử lý ủy quyền cùng với xác thực. Điều này được thực hiện sau khi người dùng được xác thực bằng cách cho phép hoặc không cho phép truy cập tài khoản người dùng để chạy các lệnh nhất định hoặc truy cập vào các thiết bị nhất định. Ví dụ, bạn chịu trách nhiệm định cấu hình và quản trị thiết bị switch và router. Bạn có thể cấp quyền chỉ đọc cho thành viên của mình vì họ không cần thực hiện thay đổi để chuyển đổi cấu hình trong công việc của họ. Quyền truy cập chỉ đọc đủ để họ khắc phục sự cố. Phần còn lại của các tài khoản sẽ không có quyền truy cập và sẽ không được phép kết nối với cơ sở hạ tầng mạng. Điều này giúp bạn linh hoạt hơn nhiều trong cách cấp quyền truy cập cho những người dùng hoặc nhóm cụ thể trong tổ chức của bạn.

RADIUS cũng có chức năng quản lý cấp quyền truy cập mạng. Ví dụ, bạn có thể muốn cho phép một số người dùng có quyền truy cập Wifi và VPN trong khi những người khác có thể không cần điều này. Khi họ xác thực với máy chủ RADIUS, nếu xác thực thành công, máy chủ RADIUS sẽ trả về thông tin cấu hình

cho máy chủ truy cập mạng. Điều này bao gồm các ủy quyền chỉ định những dịch vụ mạng nào mà người dùng được phép truy cập.

Danh sách kiểm soát truy cập

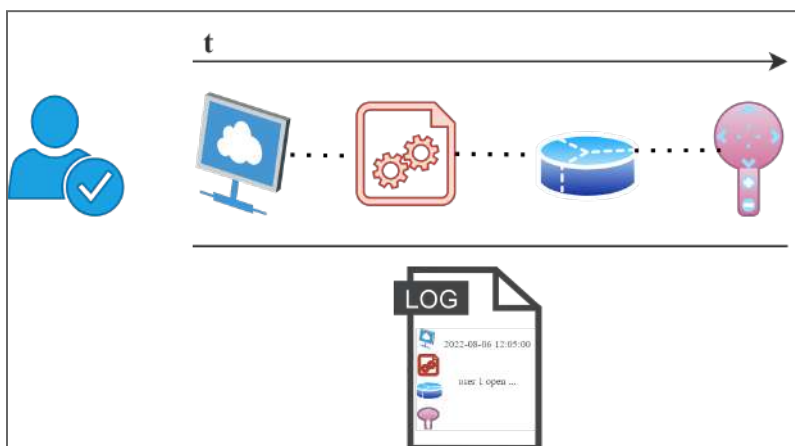
Danh sách kiểm soát truy cập (Access Control List, ACL) là một cách xác định quyền hoặc phân quyền cho các đối tượng. Trường hợp phổ biến nhất mà chúng ta có thể thấy ACL là thiết lập quyền đối với hệ thống tập tin. ACL trên hệ thống tập tin là một bảng hoặc cơ sở dữ liệu với danh sách các mục chỉ định quyền truy cập như đọc, ghi, thực thi cho từng người dùng hoặc nhóm khác nhau. Các quyền truy cập cho mỗi đối tượng được gọi là Mục Kiểm soát Truy cập (Access Control Entry) và chúng tạo nên ACL.

ACL cũng được sử dụng rộng rãi trong bảo mật mạng, áp dụng các điều khiển truy cập cho các thiết bị chuyển mạch bộ định tuyến và tường lửa. ACL mạng được sử dụng để hạn chế và kiểm soát quyền truy cập vào máy chủ hoặc dịch vụ chạy trên máy chủ trong mạng. ACL mạng có thể được dùng để kiểm soát lưu lượng đến và đi. Chúng cũng có thể được sử dụng để hạn chế quyền truy cập từ bên ngoài vào hệ thống và hạn chế lưu lượng gửi đi nhằm thực thi các chính sách hoặc để ngăn chặn việc truyền dữ liệu ra bên ngoài trái phép.



4. Kiểm toán

Điểm A cuối cùng trong Bộ ba A về bảo mật là kế toán (accounting). Điều này có nghĩa là, lưu giữ hồ sơ về những tài nguyên và dịch vụ mà người dùng truy cập hoặc những gì họ đã làm khi sử dụng hệ thống.

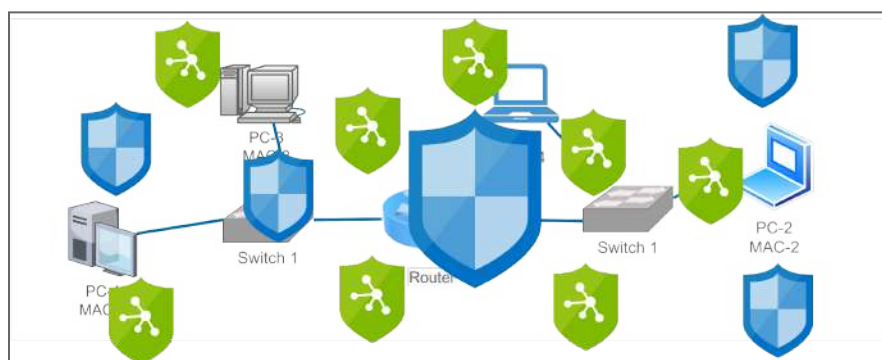


Mục tiêu là để đảm bảo rằng không có gì bất thường, hỗ trợ tìm ra nguyên nhân sự cố, và chuẩn bị cho các giải pháp nâng cấp hệ thống. Lưu ý, nếu chúng ta ghi lại việc sử dụng hệ thống, nhưng không định kỳ kiểm toán hay kiểm tra dữ liệu này thì điều đó không thực sự hữu ích.

Bài đọc 5: An Ninh Mạng

1. Tổng quan gia cố mạng

Gia cố mạng (network hardening) là quá trình đảm bảo an toàn cho mạng bằng cách giảm các lỗ hổng tiềm ẩn của nó thông qua các thay đổi cấu hình và thực hiện các bước cụ thể. Có một nguyên tắc bảo mật chung có thể được áp dụng cho hầu hết các lĩnh vực bảo mật, đó là khái niệm vô hiệu hóa các dịch vụ bổ sung không cần thiết hoặc hạn chế quyền truy cập vào chúng. Vì bất kỳ dịch vụ nào được kích hoạt và có thể truy cập đều có thể bị tấn công, nên nguyên tắc này cũng nên được áp dụng cho bảo mật mạng. Mạng sẽ an toàn hơn nhiều nếu bạn vô hiệu hóa quyền truy cập vào các dịch vụ mạng không cần thiết và thực thi các hạn chế truy cập.



Từ chối ngầm (implicit deny) là một khái niệm an ninh mạng, trong đó bất kỳ cái gì không được cho phép một cách tường minh sẽ bị từ chối. Điều này khác với việc chặn tất cả luồng truy cập, vì cấu hình từ chối ngầm sẽ cho phép luồng truy cập mà chúng ta đã liệt kê. Chúng ta có thể thực hiện việc này thông qua cấu hình ACL (Access Control List).

Rule	SIP	DIP	Sport	Dport	Proto
1	192.168.*.*	1.2.3.*	*	[2000, 3000]	TCP
2	192.168.*.*	1.2.3.*	*	[0, 1999]	TCP
...



Từ chối ngầm thường có thể được cấu hình trên tường lửa, giúp dễ dàng hơn trong việc xây dựng các quy tắc an toàn. Tường lửa (firewall) là một hệ thống bảo mật mạng dùng để theo dõi và kiểm soát các luồng vào ra dựa trên tập quy tắc đã được xác định. Thay vì yêu cầu phải chặn cụ thể tất cả luồng, với tường lửa, chúng ta có thể tạo các quy tắc cho luồng được phép đi qua. Chúng ta có thể coi đây là danh sách trắng, trái ngược với danh sách đen. Mặc dù điều này hơi kém tiện lợi, nhưng đó là một cấu hình an toàn hơn nhiều. Trước khi một dịch vụ mới hoạt động, một quy tắc mới phải được xác định.

Một thành phần quan trọng khác của an ninh mạng là giám sát và phân tích luồng truy cập trên mạng. Có một số lý do tại sao việc giám sát mạng lại quan trọng như vậy. Đầu tiên là nó cho phép thiết lập một mô hình cơ sở về luồng mạng điển hình. Đây là chìa khóa vì để biết luồng tấn công bất thường hoặc tiềm ẩn trông ra sao, chúng ta cần biết luồng truy cập bình thường trông như thế nào.



Phân tích nhật ký (analyzing logs) là hoạt động thu thập nhật ký từ các mạng khác nhau và đôi khi là các thiết bị khách trên mạng của chúng ta, sau đó thực hiện phân tích tự động trên chúng. Điều này sẽ làm nổi bật các cuộc xâm nhập tiềm ẩn, dấu hiệu nhiễm phần mềm độc hại hoặc một hành vi bất thường. Chúng ta sẽ phân tích những thứ như nhật ký tường lửa, nhật ký máy chủ xác thực và nhật ký ứng dụng. Các thiết bị bên ngoài thường phải chịu nhiều luồng truy cập độc hại tiềm ẩn hơn, làm tăng nguy cơ bị xâm phạm. Phân tích nhật ký sẽ liên quan đến việc tìm kiếm thông tin nhật ký cụ thể đáng quan tâm, như với nhật ký tường lửa. Các kết nối đã cố gắng tới một dịch vụ nội bộ từ một địa chỉ nguồn không đáng tin cậy có thể cũng cần được điều tra. Các kết nối từ mạng nội bộ đến các dải địa chỉ đã biết của các máy chủ điều khiển và lệnh Botnet có thể có nghĩa là có một máy đã bị xâm chiếm trong mạng.

Ghi nhật ký chi tiết và phân tích nhật ký sẽ cho phép xây dựng lại chi tiết các sự kiện dẫn đến vấn đề. Điều này cho phép nhóm bảo mật thực hiện những thay đổi thích hợp đối với hệ thống bảo mật để ngăn chặn các cuộc tấn công xảy ra trong tương lai. Nó cũng có thể giúp xác định mức độ và mức độ nghiêm trọng của vấn đề. Nó cũng sẽ cho chúng ta biết liệu có bất kỳ dữ liệu nào bị đánh cắp hay không và nếu có thì dữ liệu đó là gì.



Hệ thống phân tích nhật ký (logs analysis system) được định cấu hình bằng cách sử dụng các quy tắc do người dùng xác định để phù hợp với các mục nhật ký cần quan tâm. Sau đó, chúng có thể được hiển thị thông qua một hệ thống cảnh báo để cho phép các kỹ sư bảo mật điều tra. Một phần của quá trình cảnh báo này cũng sẽ liên quan đến việc phân loại cảnh báo, dựa trên quy tắc phù hợp. Chúng ta cũng cần thiết lập các mức độ ưu tiên để tạo điều kiện thuận lợi cho việc điều tra này và cho phép tìm kiếm hoặc lọc tốt hơn. Cảnh báo có thể ở dạng gửi email hoặc SMS với thông tin và liên kết đến sự kiện đã được phát hiện.



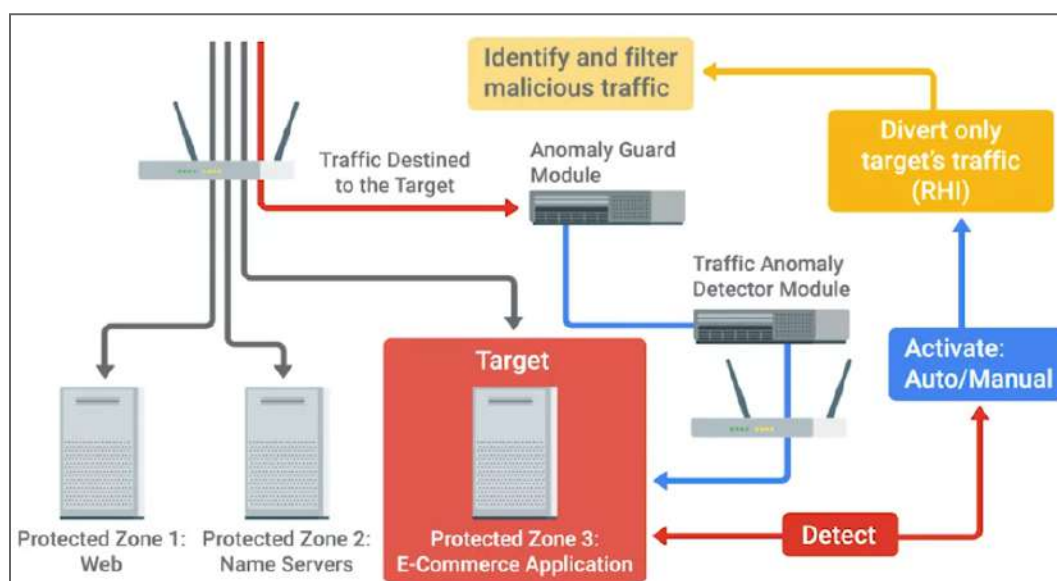
Chuẩn hóa dữ liệu nhật ký (normalizing log data) là một bước quan trọng, vì các bản ghi từ các thiết bị và hệ thống khác nhau có thể không được định dạng theo cách chung. Bạn có thể cần phải chuyển đổi các thành phần nhật ký thành một định dạng chung để phân tích dễ dàng hơn cho các nhà phân tích và hệ thống phát hiện dựa trên quy tắc, điều này cũng làm cho phân tích tương quan dễ dàng hơn.

Phân tích tương quan (correlation analysis) là quá trình lấy dữ liệu nhật ký từ các hệ thống khác nhau và so khớp các sự kiện giữa các hệ thống. Vì vậy, nếu chúng ta thấy một kết nối đáng ngờ đến từ một địa chỉ nguồn đáng ngờ, từ tường lửa ghi nhật ký và từ máy chủ xác thực, chúng ta có thể xem xét tương quan giữa các dữ liệu nhật ký đó. Loại phân tích nhật ký này cũng cực kỳ quan trọng trong việc điều tra và tái tạo lại các sự kiện đã xảy ra sau khi phát hiện ra sự xâm nhập. Đây thường được gọi là phân tích lỗi bài đăng (post-fail analysis), vì nó đang điều tra xem sự xâm nhập đã xảy ra như thế nào sau khi phát hiện vi phạm.

Một hệ thống phân tích nhật ký phổ biến và mạnh mẽ là Splunk, một hệ thống tìm kiếm và tổng hợp nhật ký rất linh hoạt và có thể mở rộng. Splunk có thể lấy dữ liệu nhật ký từ nhiều hệ thống và ở một lượng lớn định dạng. Nó cũng có thể được cấu hình để tạo cảnh báo và cho phép hiển thị trực quan mạnh mẽ hoạt động dựa trên dữ liệu đã ghi.

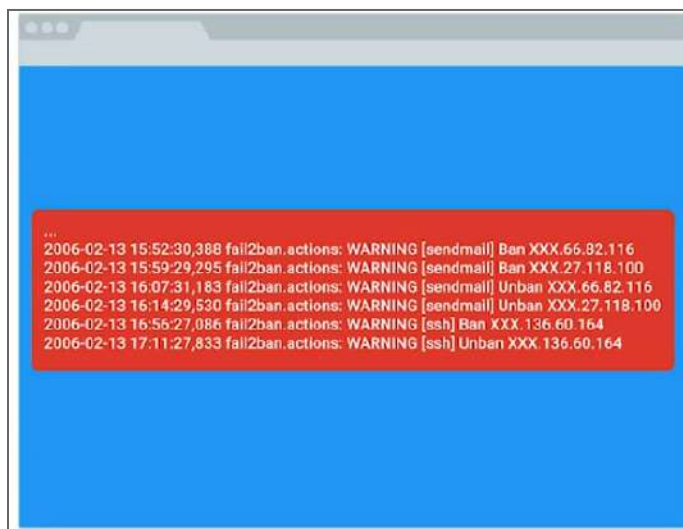


Flood Guard cung cấp bảo vệ chống lại các cuộc tấn công từ chối dịch vụ (DoS). Nó hoạt động bằng cách phát hiện các kiểu tấn công từ chối dịch vụ phổ biến như SYN flood hoặc UDP flood. Sau đó, nó sẽ kích hoạt cảnh báo khi đạt đến ngưỡng lưu lượng đã được cấu hình. Có một ngưỡng khác được gọi là ngưỡng kích hoạt. Khi đạt đến ngưỡng này, nó sẽ kích hoạt một hành động đã định. Hành động thường gặp sẽ là chặn luồng tấn công trong một khoảng thời gian cụ thể. Đây là một tính năng trên các bộ định tuyến hoặc tường lửa cấp doanh nghiệp, mặc dù đó là một khái niệm bảo mật chung.

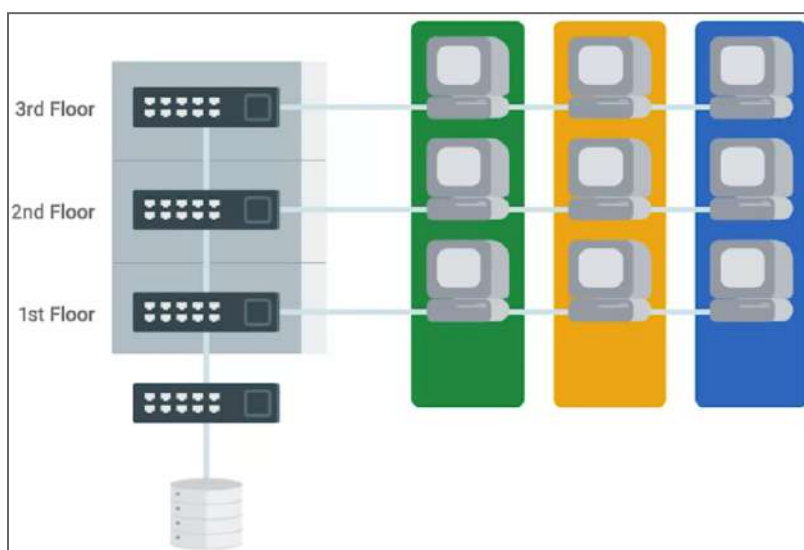


Một công cụ mã nguồn mở phổ biến để bảo vệ chống tấn công từ chối dịch vụ là Fail2ban. Nó theo dõi các dấu hiệu của một cuộc tấn công vào hệ thống và

chặn các nỗ lực tiếp theo từ một địa chỉ bị nghi ngờ tấn công. Fail2ban là một công cụ phổ biến cho các tổ chức quy mô nhỏ hơn.



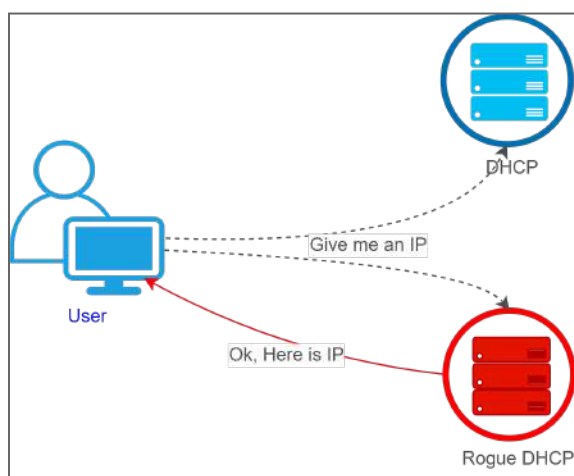
Phân tách mạng (network separation, network segmentation) là chia mạng thành các mạng con nhỏ hơn để quản lý. Đây là một nguyên tắc bảo mật tốt vì nó cho phép quản lý mạng linh hoạt hơn và cung cấp một số lợi ích bảo mật. Chúng ta có thể sử dụng VLAN để tạo mạng ảo cho các lớp hoặc loại thiết bị khác nhau. Ví dụ, chúng ta tạo ra các mạng ảo chuyên dụng cho nhân viên sử dụng, nhưng cũng có các mạng riêng để kết nối máy in. Bảo mật nằm ở chỗ các máy in sẽ không cần quyền truy cập đến cùng các tài nguyên mạng mà nhân viên sử dụng. Đó thực sự là một trong những lợi ích của việc tách mạng, vì chúng ta có thể kiểm soát và giám sát luồng giữa các mạng dễ dàng hơn. Để cấp cho nhân viên quyền truy cập vào máy in, chúng ta sẽ định cấu hình định tuyến giữa hai mạng trên bộ định tuyến của chúng ta. Chúng ta cũng triển khai ACL mạng cho phép luồng truy cập thích hợp.



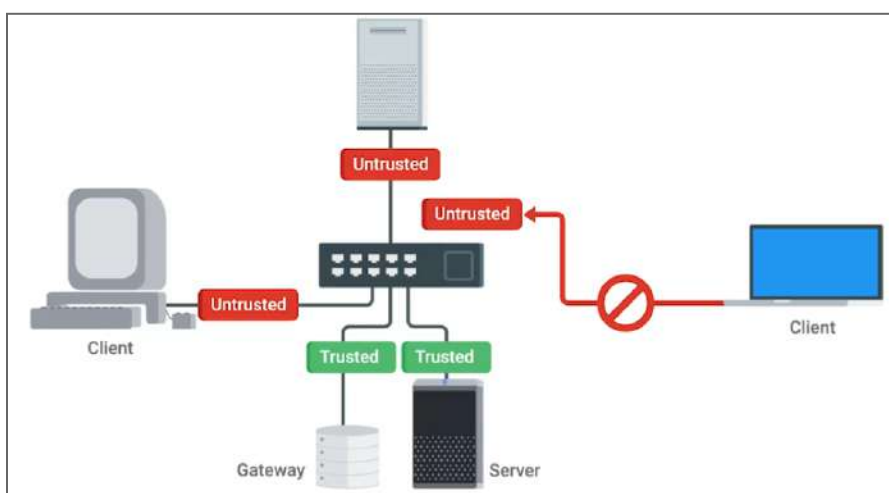
2. Gia cố phần cứng mạng

Tấn công giả mạo máy chủ DHCP và cách phòng thủ

DHCP là giao thức mà các thiết bị trên mạng được gán thông tin cấu hình quan trọng để giao tiếp trên mạng. Vì vậy, có thể thấy DHCP là mục tiêu của những kẻ tấn công vì tính chất quan trọng của dịch vụ mà nó cung cấp. Nếu kẻ tấn công có thể triển khai một máy chủ DHCP giả mạo trên mạng, chúng có thể theo dõi bất kỳ thông tin trao đổi nào trong mạng mà chúng muốn. Điều này bao gồm thiết lập địa chỉ gateway hoặc máy chủ DNS. Kiểu tấn công này được gọi là tấn công giả mạo máy chủ DHCP.



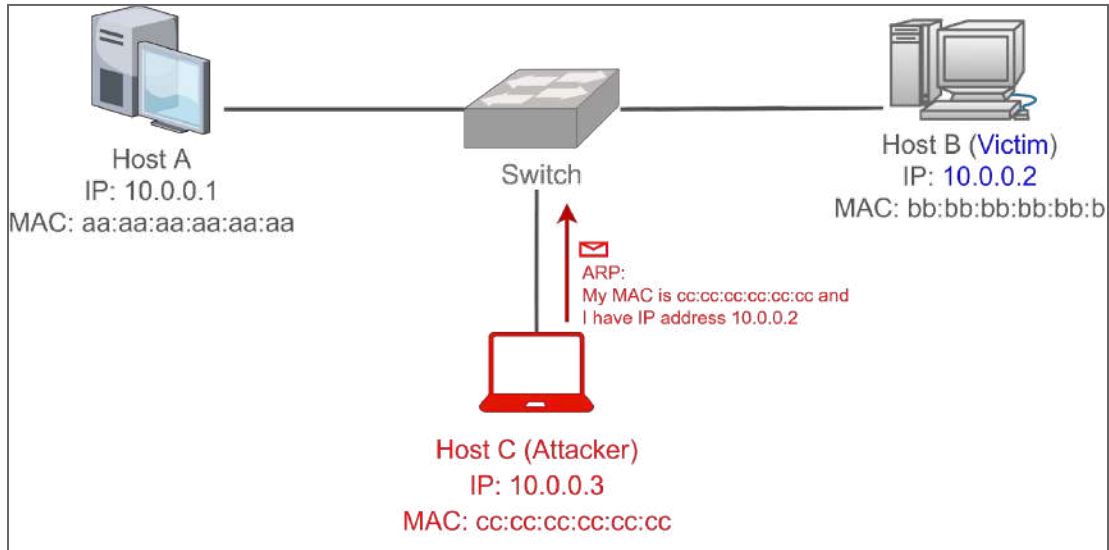
Để bảo vệ khỏi cuộc tấn công giả mạo máy chủ DHCP này, các thiết bị switch cung cấp một tính năng gọi là DHCP snooping. Một switch có DHCP snooping sẽ giám sát luồng DHCP được gửi qua nó. Nó cũng sẽ theo dõi việc gán IP và ánh xạ chúng đến các máy host được kết nối tới các cổng switch. Về cơ bản, điều này xây dựng một bản đồ các địa chỉ IP được gán cho các cổng switch vật lý. Thông tin này cũng có thể được sử dụng để bảo vệ khỏi các cuộc tấn công giả mạo IP và nhiễm độc ARP. DHCP snooping cũng cho phép chỉ định một IP máy chủ DHCP đáng tin cậy, nếu nó hoạt động như một trình trợ giúp DHCP và chuyển tiếp các yêu cầu DHCP tới máy chủ, hoặc chúng ta có thể cho phép DHCP snooping tin cậy trên cổng uplink, nơi các phản hồi DHCP hợp pháp sẽ đến. Giờ đây, bất kỳ phản hồi DHCP nào đến từ địa chỉ IP không đáng tin cậy hoặc từ một cổng switch downlink sẽ bị switch phát hiện là không đáng tin cậy và bị loại bỏ.



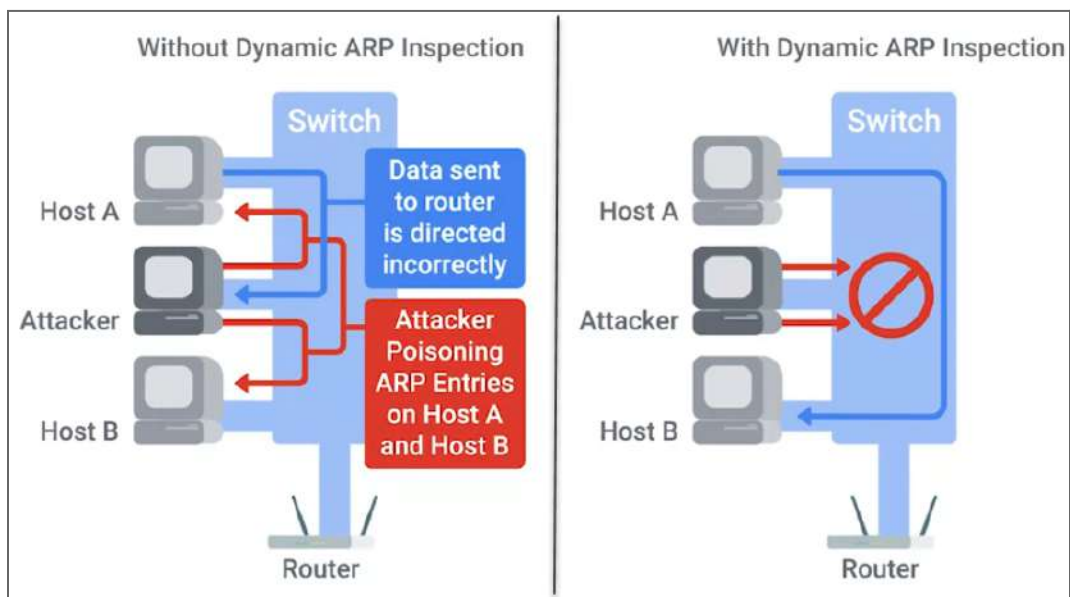
Tấn công giả mạo ARP và cách phòng thủ

ARP có thể bị tấn công xen giữa vì bản chất không được xác thực của ARP. Nó cho phép kẻ tấn công giả mạo phản hồi ARP (ARP spoofing), quảng bá địa chỉ MAC của nó như là địa chỉ vật lý khớp với địa chỉ IP của nạn nhân. Loại phản hồi ARP này được gọi là phản hồi ARP vô cơ, vì nó trả lời một truy vấn mà không ai thực hiện. Khi điều này xảy ra, tất cả các máy khách trên phân đoạn mạng cục bộ sẽ lưu vào bộ nhớ cache mục ARP này. Do mục ARP giả mạo, các máy trong mạng gửi các gói tin dành cho địa chỉ IP của nạn nhân đến máy của kẻ tấn công. Kẻ tấn công có thể kích hoạt chuyển tiếp IP, điều này sẽ cho phép chúng giám

sát một cách thông suốt luồng dữ liệu dành cho nạn nhân. Kẻ tấn công cũng có thể thao túng hoặc sửa đổi dữ liệu.



DAI (Dynamic ARP Inspection) là một tính năng khác trên thiết bị switch nhằm ngăn chặn tấn công giả mạo ARP. Nó yêu cầu sử dụng DHCP snooping để thiết lập một bảng ràng buộc tin cậy giữa các địa chỉ IP đến cổng switch. Nó dùng bảng này để phát hiện các gói ARP giả mạo vô cớ và loại bỏ chúng. DAI cũng thực thi giới hạn các gói ARP trên mỗi cổng để ngăn việc quét ARP do kẻ tấn công thường quét ARP trước khi thực hiện cuộc tấn công ARP.

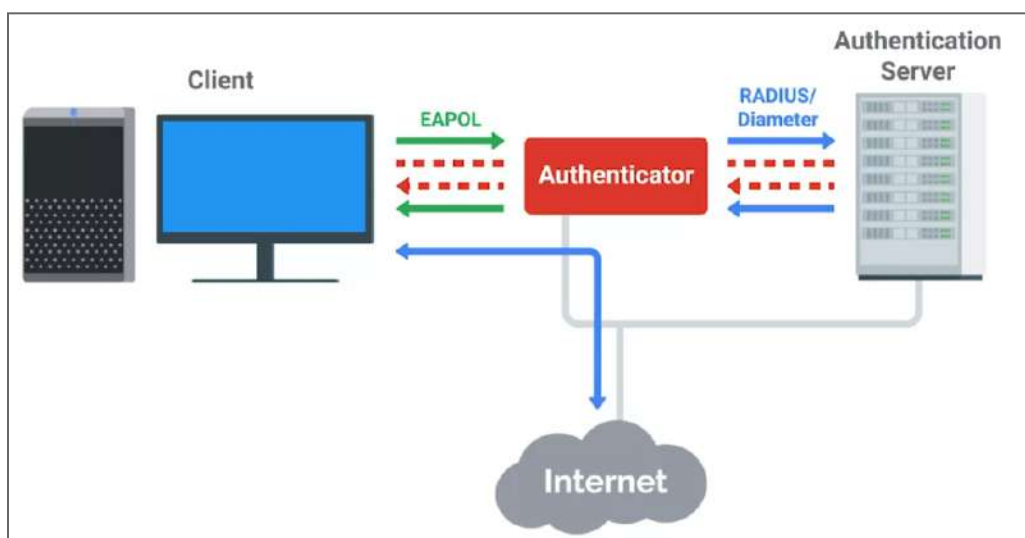


Tấn công giả mạo IP và cách phòng thủ

Để ngăn chặn các cuộc tấn công giả mạo IP, IPSG (IP source guard) có thể được kích hoạt trên các thiết bị switch cùng với DHCP snooping. Nó hoạt động bằng cách sử dụng bảng DHCP snooping để tạo động ACL cho mỗi cổng switch. Điều này giúp bỏ đi các gói không khớp với địa chỉ IP cho cổng dựa trên bảng DHCP snooping.

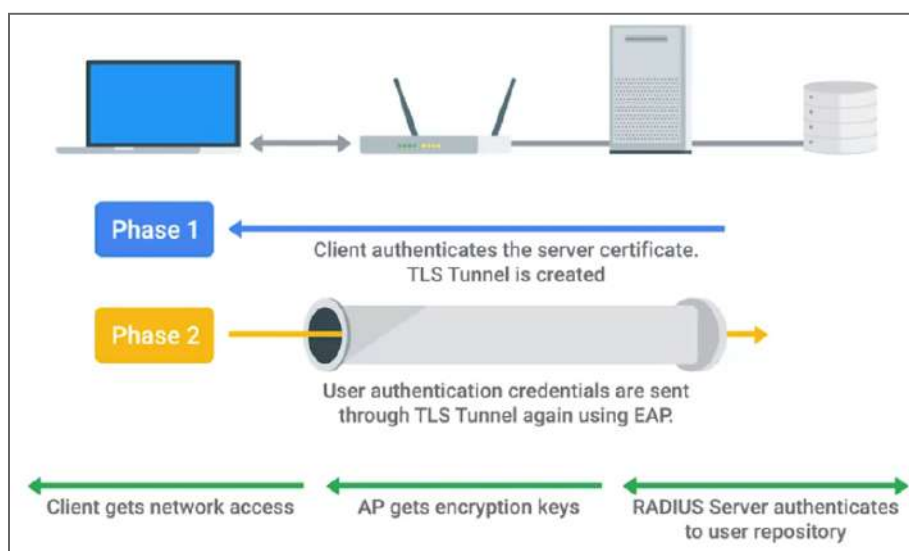
Xác thực mạng

Khi một máy khách muốn xác thực mạng sử dụng 802.1X, có ba bên tham gia. Thiết bị khách được gọi là thiết bị hỗ trợ. Nó đôi khi cũng được sử dụng để chỉ phần mềm chạy trên máy khách xử lý quá trình xác thực cho người dùng. Tiện ích nguồn mở Linux wpa_supplicant là một trong số đó. Thiết bị hỗ trợ sẽ giao tiếp với trình xác thực, nó hoạt động như một người gác cổng cho mạng. Nó yêu cầu các máy khách xác thực thành công với mạng trước khi họ được phép giao tiếp với mạng. Đây thường là một bộ switch hoặc một điểm truy cập AP trong trường hợp mạng không dây. Dù vậy, nó không thực sự là người đưa ra quyết định xác thực. Trình xác thực hoạt động giống như đi giữa và chuyển tiếp yêu cầu xác thực đến máy chủ xác thực. Đó là nơi xác minh và xác thực thông tin thực tế xảy ra. Máy chủ xác thực thường là máy chủ RADIUS.



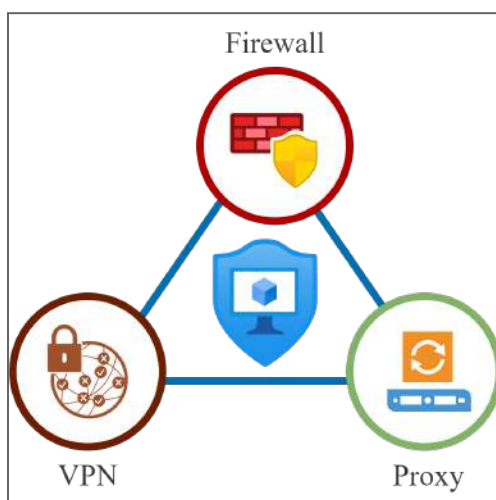
EAP-TLS là một loại xác thực được hỗ trợ bởi EAP (extensible authentication protocol) sử dụng TLS để cung cấp xác thực lẫn nhau của cả máy khách và máy chủ xác thực. Đây được coi là một trong những cấu hình an toàn hơn cho bảo

mật không dây. Các triển khai EAP-TLS đều yêu cầu chứng chỉ phía máy khách. Xác thực có thể dựa trên chứng chỉ, yêu cầu máy khách xuất trình chứng chỉ hợp lệ được ký bởi CA xác thực hoặc máy khách có thể sử dụng chứng chỉ kết hợp với tên người dùng, mật khẩu và thậm chí là yếu tố xác thực thứ hai, như mật khẩu một lần. Tính bảo mật của EAP-TLS bắt nguồn từ tính bảo mật vốn có mà giao thức TLS và PKI cung cấp. Điều đó cũng có nghĩa là các lỗ hổng đều giống nhau khi nói đến việc quản lý các yếu tố PKI đúng cách. Chúng ta phải bảo vệ các khóa riêng tư một cách thích hợp và đảm bảo phân phối chứng chỉ CA tới các thiết bị khách để cho phép xác minh phía máy chủ. Thậm chí, cấu hình an toàn hơn cho EAP-TLS sẽ là liên kết các chứng chỉ phía máy khách với nền tảng máy khách sử dụng TPM. Điều này sẽ ngăn chặn việc đánh cắp chứng chỉ từ các máy khách. Khi kết hợp điều này với FDE (mã hóa toàn bộ ổ cứng), ngay cả việc đánh cắp máy tính cũng sẽ ngăn chặn sự xâm nhập của mạng.

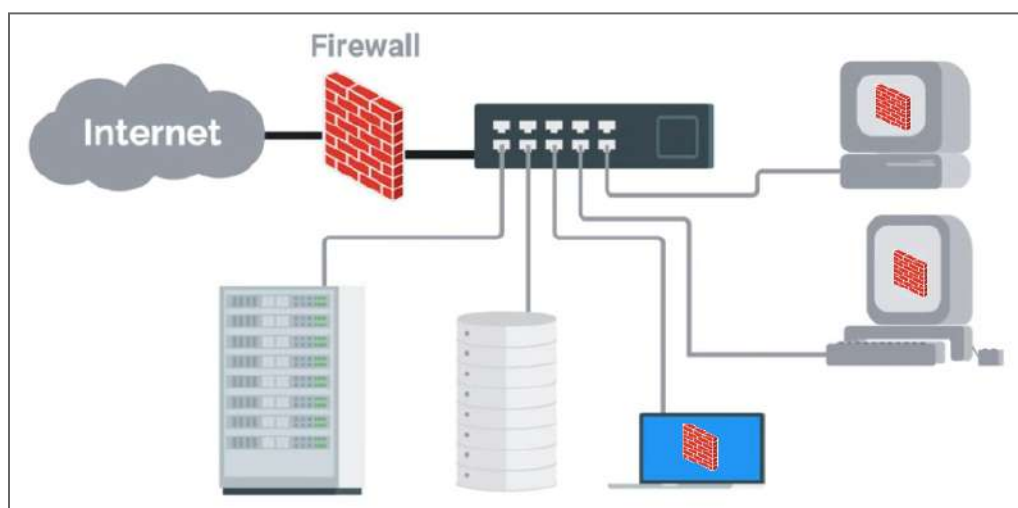


3. Gia cố phần mềm mạng

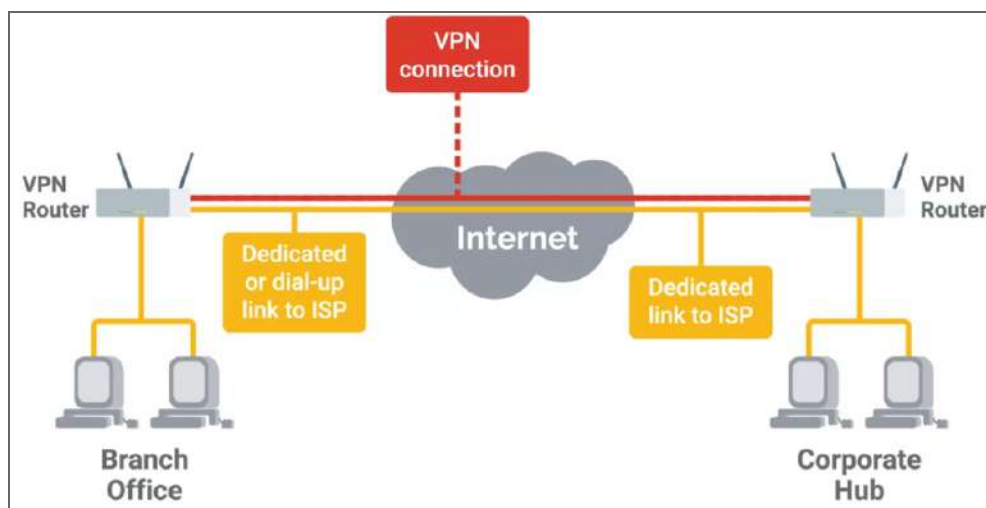
Cũng giống như việc gia cố phần cứng mạng, chúng ta cũng cần có cách thức để gia cố phần mềm mạng, bao gồm những thứ như tường lửa, proxy và VPN. Các giải pháp phần mềm bảo mật này sẽ đóng một vai trò quan trọng trong việc bảo mật mạng và luồng truy cập trong tổ chức của chúng ta.



Tường lửa rất quan trọng để bảo mật mạng. Chúng có thể được triển khai như các thiết bị hạ tầng mạng chuyên dụng, điều chỉnh luồng cho toàn mạng. Chúng có thể dựa trên máy trực tiếp (host-based firewall) dưới dạng phần mềm cung cấp khả năng bảo vệ chỉ cho một máy lưu trữ nó. Tường lửa máy trực tiếp cung cấp khả năng bảo vệ cho các thiết bị di động như máy tính xách tay có thể được sử dụng trong môi trường không đáng tin cậy, tiềm ẩn nguy cơ độc hại như điểm phát sóng Wifi ở sân bay. Tường lửa này cũng hữu ích để bảo vệ các máy khác không bị xâm nhập bởi thiết bị bị hỏng trên mạng nội bộ. Ngoài ra, còn có tường lửa mạng (network-based firewall) thường được tích hợp sẵn trong bộ định tuyến và các thiết bị mạng khác.

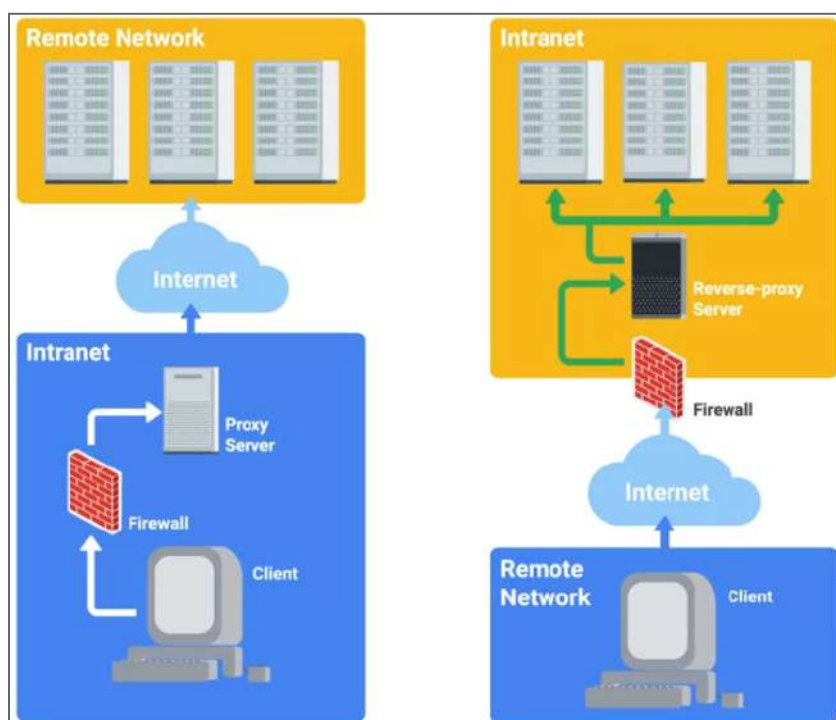


VPN cũng được khuyến nghị để cung cấp quyền truy cập an toàn vào tài nguyên nội bộ cho người dùng di động hoặc chuyển vùng. VPN thường được sử dụng để cung cấp quyền truy cập từ xa an toàn và liên kết hai mạng một cách an toàn. Giả sử chúng ta có hai văn phòng đặt tại các tòa nhà nằm đối diện với thị trấn. Chúng ta muốn tạo một mạng thống nhất cho phép người dùng ở mỗi vị trí, kết nối liền mạch với các thiết bị và dịch vụ ở cả hai vị trí. Chúng ta có thể sử dụng VPN site to site để liên kết hai văn phòng này. Đối với những người trong văn phòng, mọi thứ sẽ hoạt động. Họ có thể kết nối với một dịch vụ được lưu trữ trong văn phòng khác mà không cần bất kỳ cấu hình cụ thể nào. Sử dụng đường hầm VPN, tất cả lưu lượng giữa hai văn phòng có thể được bảo mật bằng cách sử dụng mã hóa. Điều này cho phép hai mạng từ xa kết nối với nhau một cách liền mạch. Bằng cách này, các máy khách trên một mạng có thể truy cập các thiết bị trên mạng khác mà không yêu cầu chúng kết nối riêng với dịch vụ VPN. Thông thường, cùng một cơ sở hạ tầng có thể được sử dụng để cho phép các dịch vụ VPN truy cập từ xa cho các máy khách cá nhân yêu cầu quyền truy cập vào tài nguyên nội bộ khi ở ngoài văn phòng.



Proxy thực sự hữu ích để bảo vệ thiết bị khách và luồng truy cập của chúng. Chúng cũng cung cấp quyền truy cập từ xa an toàn mà không cần sử dụng VPN. Một proxy web tiêu chuẩn có thể được định cấu hình cho các thiết bị khách. Điều này cho phép luồng truy cập web được ủy quyền thông qua một máy chủ proxy mà chúng ta kiểm soát cho nhiều mục đích. Cấu hình này có thể được sử dụng để ghi nhật ký các yêu cầu web của các thiết bị khách. Các thiết bị này có thể được sử dụng để ghi nhật ký, phân tích lưu lượng và điều tra sự cố.

Máy chủ proxy có thể được định cấu hình để chặn nội dung có thể độc hại, nguy hiểm hoặc chống lại chính sách của công ty. Reverse proxy có thể được định cấu hình để cho phép truy cập từ xa an toàn vào các dịch vụ dựa trên web mà không yêu cầu VPN. Bằng cách cấu hình reverse proxy ở rìa mạng, các yêu cầu kết nối tới các dịch vụ bên trong mạng đến từ bên ngoài sẽ bị proxy ngược chặn lại. Sau đó, chúng được chuyển tiếp đến dịch vụ nội bộ với reverse proxy hoạt động như một role. Điều này làm cầu nối giao tiếp giữa máy khách từ xa bên ngoài mạng và dịch vụ nội bộ. Thiết lập proxy này có thể được bảo mật hơn nữa bằng cách yêu cầu sử dụng chứng chỉ TLS của ứng dụng khách, cùng với xác thực tên người dùng và mật khẩu. Các ACL cụ thể cũng có thể được cấu hình trên reverse proxy ngược để hạn chế quyền truy cập hơn nữa. Rất nhiều giải pháp proxy phổ biến hỗ trợ cấu hình reverse proxy như HAProxy, Nginx và thậm chí cả máy chủ Web Apache.



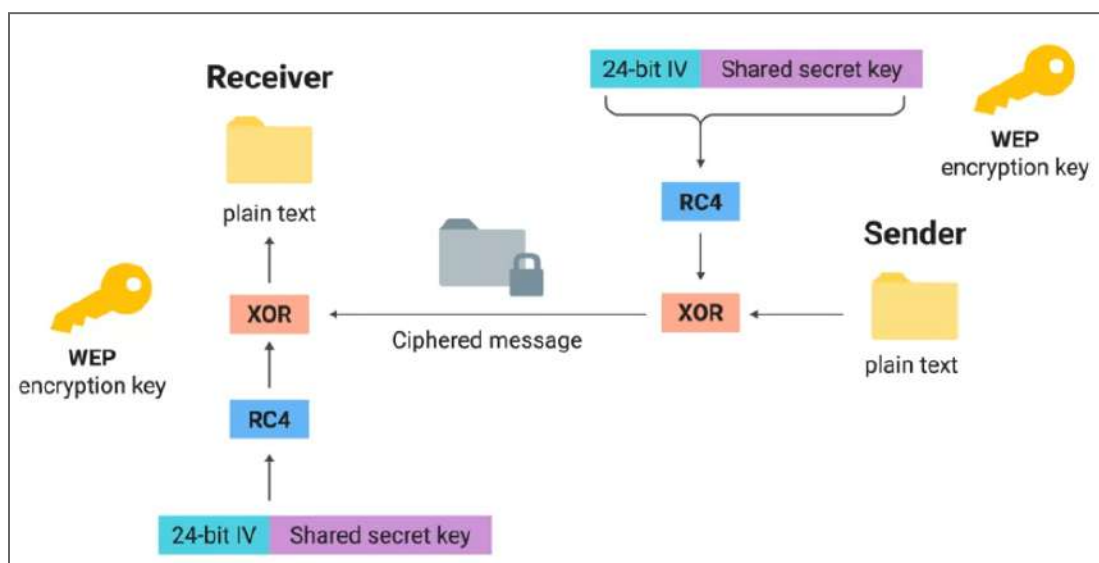
4. Bảo mật mạng không dây

WEP

Giao thức bảo mật đầu tiên được giới thiệu cho mạng Wifi là WEP (Wired Equivalent Privacy). Nó là một phần của tiêu chuẩn 802.11 ban đầu được giới

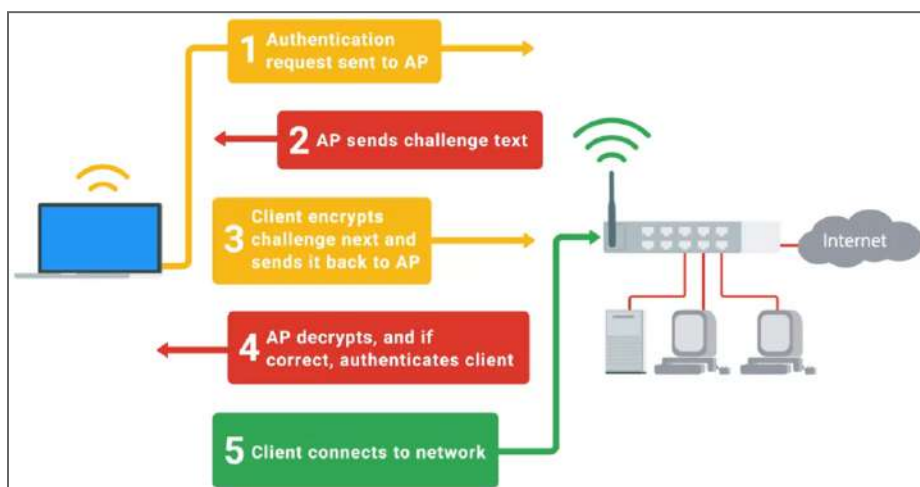
thiệu vào năm 1997. WEP nhằm cung cấp quyền riêng tư ngang bằng với mạng có dây, điều đó có nghĩa là thông tin được truyền qua mạng phải được bảo vệ khỏi sự nghe trộm của các bên thứ ba. Đây là một cân nhắc quan trọng khi thiết kế đặc điểm kỹ thuật không dây. Không giống như mạng có dây, các gói tin có thể bị chặn bởi bất kỳ ai ở gần điểm truy cập hoặc trạm khách. Nếu không có một số hình thức mã hóa để bảo vệ các gói, lưu lượng truy cập không dây sẽ có thể đọc được bởi bất kỳ ai ở gần muốn nghe. WEP được chứng minh là gặp vấn đề nghiêm trọng trong việc cung cấp tính bảo mật cho các mạng không dây. Nó nhanh chóng được thay thế vào năm 2004 để ủng hộ các hệ thống an toàn hơn. Chúng ta đề cập đến nó ở đây cho các mục đích lịch sử. Điều quan trọng là chúng ta phải hiểu đầy đủ tại sao WEP lại lỗi thời và thay vào đó cần phải làm gì.

WEP sử dụng mã hóa dòng đối xứng RC4 để mã hóa. Nó sử dụng khóa chia sẻ 40 bit hoặc 104 bit, nơi bắt nguồn từ khóa mã hóa cho các gói riêng lẻ. Khóa mã hóa thực tế cho mỗi gói được tính bằng cách lấy khóa chia sẻ do người dùng cung cấp và sau đó nhập với vectơ khởi tạo 24 bit, viết tắt là IV. Đó là một bit dữ liệu ngẫu nhiên để tránh sử dụng lại cùng một khóa mã hóa giữa các gói. Vì các bit dữ liệu này được nối với nhau, nên khóa chia sẻ 40 bit sẽ sử dụng khóa 64 bit để mã hóa và khóa 104 bit sử dụng khóa 128 bit. Ban đầu, mã hóa WEP chỉ được giới hạn ở 64-bit do các hạn chế xuất khẩu của Hoa Kỳ đặt ra đối với các công nghệ mã hóa. Giờ đây khi những luật đó được thay đổi, mã hóa 128-bit đã có thể sử dụng. Khóa chia sẻ được nhập dưới dạng 10 ký tự hexa cho WEP 40 bit hoặc 26 ký tự hexa cho WEP 104 bit. Mỗi ký tự hexa là 4 bit. Khóa cũng có thể được chỉ định bằng cách cung cấp 5 ký tự ASCII hoặc 13, mỗi ký tự ASCII đại diện cho 8 bit. Nhưng điều này thực sự làm giảm không gian khóa vì chỉ còn các ký tự ASCII hợp lệ thay vì tất cả các giá trị hex có thể có. Vì đây là một thành phần của khóa thực, khóa chia sẻ phải có số ký tự phù hợp với lược đồ mã hóa. Xác thực WEP ban đầu hỗ trợ hai chế độ khác nhau, xác thực hệ thống mở và xác thực khóa chia sẻ.



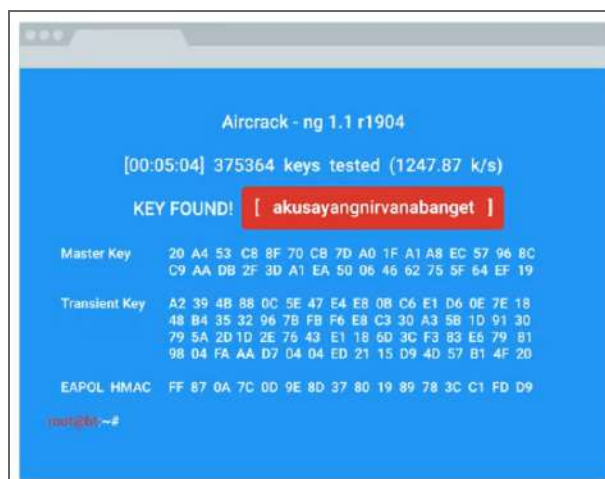
Chế độ hệ thống mở không yêu cầu máy khách cung cấp thông tin đăng nhập. Thay vào đó, họ được phép xác thực và liên kết với điểm truy cập. Điểm truy cập sẽ bắt đầu giao tiếp bằng khóa WEP được chia sẻ trước. Nếu máy khách không có khóa hoặc có khóa không chính xác, nó sẽ không thể giải mã dữ liệu đến từ điểm truy cập hoặc AP (Access Point). Nó cũng sẽ không thể liên lạc lại với AP.

Xác thực khóa chia sẻ hoạt động bằng cách yêu cầu máy khách xác thực thông qua quy trình thử thách-phản hồi bốn bước. Điều này về cơ bản, AP yêu cầu máy khách chứng minh rằng họ có khóa chính xác. Máy khách gửi một yêu cầu xác thực đến AP. AP trả lời với thử thách văn bản rõ, một chút dữ liệu ngẫu nhiên mà ứng dụng khách phải mã hóa bằng khóa WEP được chia sẻ. Máy khách trả lời AP với bản mã kết quả từ việc mã hóa văn bản thử thách này. AP xác minh điều này bằng cách giải mã phản hồi và kiểm tra nó với văn bản gốc ban đầu. Nếu chúng khớp, một phản hồi đồng ý sẽ được gửi lại. Chúng ta đang truyền cả văn bản gốc và văn bản mã hóa theo cách để lộ cả hai dữ liệu này cho những kẻ nghe tấn công tiềm năng. Điều này mở ra khả năng để kẻ tấn công lấy khóa mã hóa.



Một khái niệm chung trong bảo mật và mã hóa là không bao giờ gửi văn bản thô và bản mã cùng nhau, để những kẻ tấn công không thể tìm ra khóa được sử dụng để mã hóa. Nhưng điểm yếu thực sự của WEP không liên quan đến các sơ đồ xác thực, việc sử dụng mã hóa dòng RC4 và cách các IV được sử dụng để tạo khóa mã hóa đã dẫn đến sự sụp đổ cuối cùng của WEP. Mục đích chính của IV là đưa thêm các phần tử ngẫu nhiên vào khóa mã hóa để tránh sử dụng lại cùng một khóa. Khi sử dụng mật mã dòng như RC4, điều tối quan trọng là khóa mã hóa không được sử dụng lại. Điều này sẽ cho phép kẻ tấn công so sánh hai thông điệp được mã hóa bằng cùng một khóa và khôi phục thông tin. Nhưng khóa mã hóa trong WEP chỉ được tạo thành từ khóa chia sẻ, không thay đổi thường xuyên. Nó có 24 bit dữ liệu ngẫu nhiên, bao gồm cả IV nằm ở cuối nó. Điều này dẫn đến chỉ một nhóm 24 bit, nơi các khóa mã hóa duy nhất sẽ được lấy từ và sử dụng. Vì IV được tạo thành từ 24 bit dữ liệu, tổng số giá trị có thể có không lớn lắm theo các tiêu chuẩn máy tính hiện đại. Đó chỉ là khoảng 17 triệu IV duy nhất khả thi, có nghĩa là sau khoảng 5.000 gói, một IV sẽ được sử dụng lại. Khi một IV được sử dụng lại, khóa mã hóa cũng được sử dụng lại. Cũng cần lưu ý rằng IV được truyền ở dạng văn bản thô. Nếu nó đã được mã hóa, người nhận sẽ không thể giải mã nó. Điều này có nghĩa là kẻ tấn công chỉ cần theo dõi các IV và theo dõi các IV lặp lại. Cuộc tấn công thực tế cho phép kẻ tấn công khôi phục khóa WEP dựa trên các điểm yếu trong một số IV và cách mật mã RC4 tạo ra một dòng khóa được sử dụng để mã hóa tải trọng dữ liệu. Điều này cho phép kẻ tấn công xây dựng lại dòng khóa này bằng cách sử dụng các gói được mã hóa bằng IV yếu.

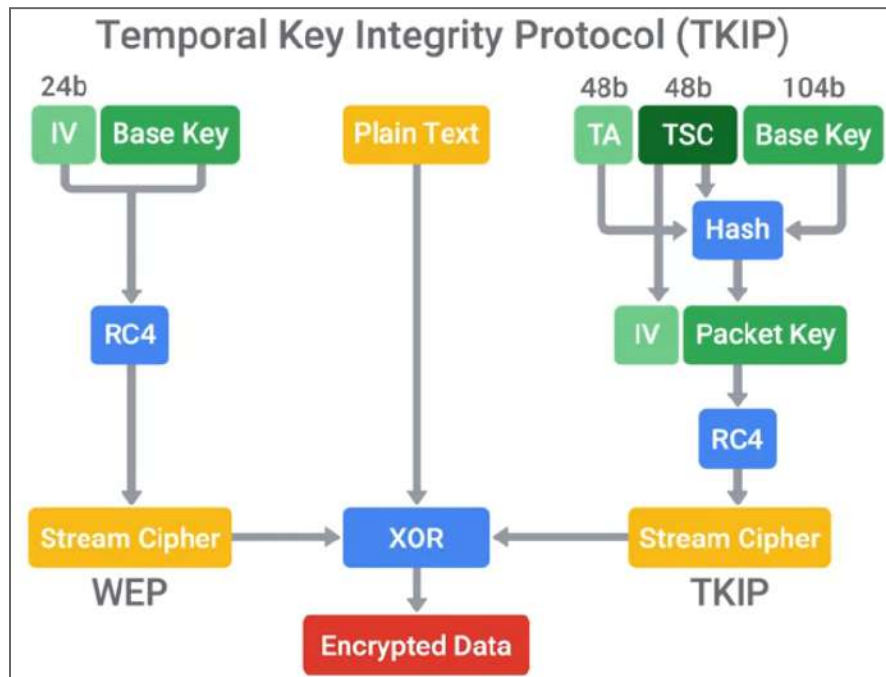
Chúng ta cũng có thể xem xét các công cụ mã nguồn mở chứng minh cuộc tấn công này có thể xảy ra, như Aircrack-ng hoặc AirSnort, chúng có thể khôi phục khóa WEP trong vài phút.



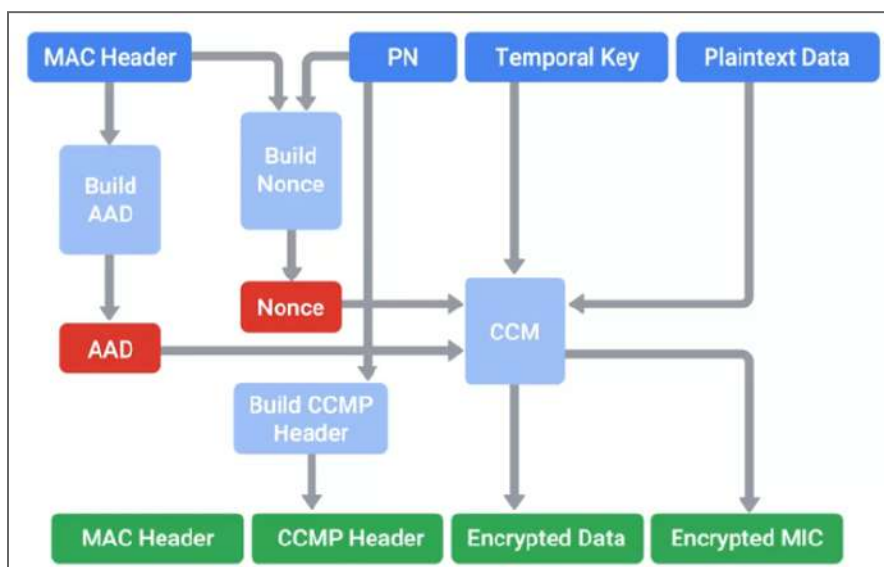
WPA/WAP2

Sự thay thế cho WEP từ Wifi Alliance là WPA. WPA được thiết kế như một sự thay thế ngắn hạn sẽ tương thích với phần cứng hỗ trợ WEP cũ hơn với một bản cập nhật firmware đơn giản. Điều này đã giúp người dùng chấp nhận vì nó không yêu cầu mua phần cứng Wifi mới. Để giải quyết những thiếu sót của bảo mật WEP, một giao thức bảo mật mới đã được giới thiệu có tên là TKIP.

TKIP đã triển khai ba tính năng mới làm cho nó an toàn hơn WEP. Đầu tiên, một phương pháp dẫn xuất khóa an toàn hơn đã được sử dụng để kết hợp an toàn IV vào khóa mã hóa. Thứ hai, một bộ đếm được thực hiện để ngăn chặn các cuộc tấn công phát lại bằng cách từ chối các gói không theo thứ tự. Thứ ba, MIC 64-bit được giới thiệu để ngăn chặn việc giả mạo hoặc làm hỏng các gói tin. TKIP vẫn sử dụng mật mã RC4 làm thuật toán mã hóa cơ bản. Nhưng nó đã giải quyết các điểm yếu tạo khóa của WEP bằng cách sử dụng chức năng trộn khóa để tạo các khóa mã hóa duy nhất cho mỗi gói. Nó cũng sử dụng các khóa dài 256 bit.

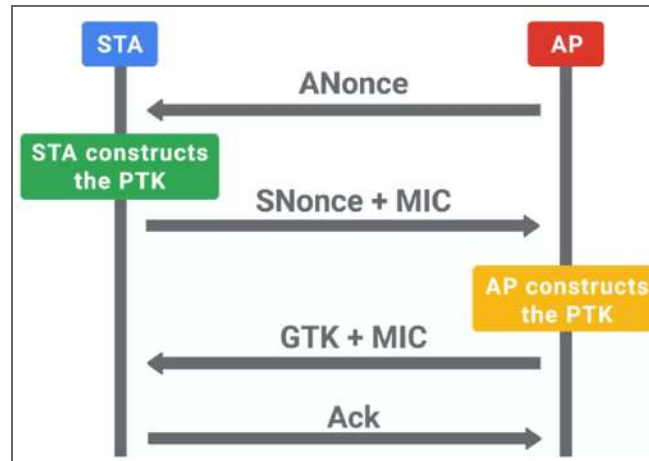


WPA2 cải thiện bảo mật WPA nhiều hơn nữa bằng cách triển khai CCMP. WPA2 là bảo mật tốt nhất cho các mạng không dây hiện có. Nó dựa trên mật mã AES. Quá trình dẫn xuất khóa và yêu cầu về khóa được chia sẻ trước không thay đổi so với WPA. Bộ đếm với CBC-MAC là một chế độ hoạt động cụ thể cho mã hóa khối. Nó cho phép mã hóa được xác thực, có nghĩa là dữ liệu được giữ bí mật và được xác thực. Điều này được thực hiện bằng cách sử dụng cơ chế xác thực, sau đó mã hóa. Thông điệp CBC-MAC được tính toán trước. Sau đó, mã xác thực kết quả được mã hóa cùng với thông điệp bằng mã hóa khối. Điều này biến mã hóa khối thành mã hóa dòng bằng cách sử dụng giá trị gốc ngẫu nhiên cùng với bộ đếm tăng dần để tạo dòng khóa cho mã hóa dữ liệu.



Quá trình bắt tay bốn bước trong WPA2 được tạo thành từ bốn lần trao đổi dữ liệu giữa máy khách và điểm truy cập (AP). Quá trình này cũng tạo ra khóa mã hóa tạm thời được sử dụng để mã hóa dữ liệu cho máy khách này. Nó được thiết kế để cho phép một AP xác nhận rằng máy khách có đúng khóa PMK hay khóa chia sẻ trước trong thiết lập WPA-PSK mà không cần tiết lộ khóa PMK. PMK là một chìa khóa không thay đổi trong một thời gian dài. Vì vậy, một khóa được gọi là PTK có nguồn gốc từ PMK được sử dụng để mã hóa và giải mã luồng dữ liệu giữa máy khách và AP. Khóa PTK tạo bằng cách sử dụng PMK, AP nonce, Client nonce, AP MAC address và Client MAC address. Tất cả chúng đều được nối với nhau và chạy qua một hàm. Các AP nonces và Client nonces chỉ là các bit dữ liệu ngẫu nhiên do mỗi bên tạo ra và được trao đổi. Địa chỉ MAC của mỗi bên sẽ được biết thông qua các header và cả hai bên đều đã có khóa PMK. Mỗi khóa trong PTK có mục đích riêng. Hai khóa được sử dụng để mã hóa và xác nhận các gói EAPoL, và giao thức đóng gói mang các thông điệp này. Hai khóa được sử dụng để gửi và nhận chuỗi kiểm tra toàn vẹn thông điệp. Và cuối cùng, có một khóa tạm thời, thực sự được sử dụng để mã hóa dữ liệu. AP cũng sẽ truyền khóa chuyển tiếp GTK theo nhóm. Nó được mã hóa bằng khóa mã hóa EAPoL có trong PTK, được sử dụng để mã hóa luồng phát đa hướng hoặc quảng bá. Vì loại luồng này phải được đọc bởi tất cả các máy khách kết nối với một AP, GTK này được chia sẻ giữa tất cả các máy khách. Nó được cập nhật và truyền lại theo định kỳ và khi máy khách ngắt kết nối AP. Tóm lại, bốn thông điệp được trao đổi theo thứ tự là, AP gửi anonce cho máy khách; máy khách sau đó

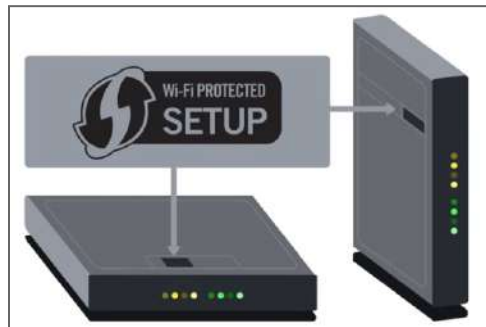
gửi snonce cho AP; AP gửi ngược lại GTK và máy khách trả lời bằng một Ack xác nhận giao tiếp thành công.



Tiêu chuẩn WPA và WPA2 cũng giới thiệu xác thực 802.1x cho mạng Wifi. Nó thường được gọi là WPA2-Enterprise. Các cấu hình không phải 802.1x được gọi là WPA2-Personal hoặc WPA2-PSK, vì chúng sử dụng khóa chia sẻ trước để xác thực máy khách. Điều khác biệt là AP đóng vai trò là người xác thực trong trường hợp này.

Mặc dù không phải là một tính năng bảo mật trực tiếp nhưng thiết lập được bảo vệ bằng WPS là một tính năng tiện lợi được thiết kế để giúp máy khách dễ dàng tham gia vào mạng được bảo vệ bằng WPA-PSK. Người dùng không cần phải nhập trực tiếp khóa chia sẻ trước. Điều này tạo điều kiện thuận lợi cho việc sử dụng các cụm mật khẩu dài và an toàn mà không làm cho nó trở nên phức tạp không cần thiết. WPS hỗ trợ xác thực mục nhập mã PIN, NFC hoặc USB hoặc xác thực bằng nút nhấn.

Cơ chế nút nhấn là một nút nhỏ ở đâu đó trên bộ định tuyến với hai mũi tên trở ngược chiều kim đồng hồ. Cơ chế nút nhấn hoạt động bằng cách yêu cầu nhấn một nút ở cả phía AP và phía máy khách. Điều này đòi hỏi tiếp xúc gần về mặt vật lý và một khoảng thời gian ngắn mà máy khách có thể xác thực. Phương thức NFC và USB cung cấp một kênh khác để truyền thông tin cho việc tham gia mạng. Phương pháp mã PIN tuy thú vị nhưng cũng là nơi xuất hiện lỗ hổng bảo mật.



WPA2 vẫn có thể bị tấn công bởi một số hình thức. Bắt tay xác thực bốn bước thực sự cũng dễ bị tấn công ngoại tuyến. Nếu kẻ tấn công có thể quản lý để nắm bắt quá trình bắt tay bốn bước, chúng có thể bắt đầu đoán khóa chia sẻ trước. Chúng có thể lấy các nonces và địa chỉ MAC từ các gói bắt tay bốn bước và các PTK. Gửi mã xác thực thông điệp, khóa bí mật được bao gồm như một phần của PTK. Phỏng đoán PMK chính xác sẽ mang lại một PTK xác thực thành công MIC. Đây là một cuộc tấn công vét cạn hoặc dựa trên từ điển, vì vậy nó phụ thuộc vào chất lượng của các lần đoán mật khẩu. Nó đòi hỏi một lượng lớn sức mạnh tính toán để tính toán PMK từ các cụm đoán mật khẩu và giá trị SSID. Nhưng phần lớn các yêu cầu tính toán nằm trong tính toán PMK. Điều này yêu cầu 4096 lần lặp lại của một hàm băm, có thể được tăng tốc hàng loạt thông qua việc sử dụng các tài nguyên tính toán GPU và điện toán đám mây. Do phần lớn các phép tính liên quan đến việc tính toán PMK, bằng cách kết hợp các dự đoán mật khẩu với SSID, chúng ta có thể tính toán trước hàng loạt PMK cho các SSID phổ biến và kết hợp mật khẩu. Điều này làm giảm các yêu cầu tính toán để lấy PTK từ các phần tử phiên duy nhất. Những tập hợp được tính toán trước này được gọi là bảng cầu vồng và chính xác là điều này đã được thực hiện. Bảng cầu vồng có sẵn để tải xuống cho 1000 SSID thường thấy nhất và 1 triệu mật khẩu.



Password	Hash
123456	e10adc983ad09dca098da02320e
password	09dca09e10a0232dc983ad834ds
qwerty	h566adc983ad09d432fgsdcg432
baseball	123dsa3ad09dca3fer34r4653323
dragon	12409dca098dsa42363412467s2
kittycat	2ws3d4c983ad23wsd34565f4643
000111	344rfwc9834564dca09756324t72

Gia cố mạng không dây

Bảo vệ mạng không dây của mình bằng cách sử dụng 802.1X và EAP-TLS. Nó được cho là cung cấp bảo mật tốt nhất hiện nay. Tuy nhiên, lựa chọn này cũng đòi hỏi nhiều phức tạp và chi phí bổ sung. Điều này là do nó yêu cầu tối thiểu phải sử dụng máy chủ RADIUS và một đầu cuối xác thực bổ sung. Nếu EAP-TLS được triển khai, thì tất cả các thành phần cơ sở hạ tầng khóa công khai cũng sẽ cần thiết. Điều này càng làm tăng thêm sự phức tạp và chi phí quản lý. Chúng ta không chỉ phải triển khai PKI an toàn trên đầu cuối để quản lý chứng chỉ mà còn phải có một hệ thống để ký chứng chỉ của máy khách. Chúng ta cũng phải phân phối chứng chỉ cho từng máy khách sẽ xác thực vào mạng. Điều này thường tốn nhiều chi phí hơn so với nhiều công ty sẵn sàng thực hiện. Nếu 802.1X quá phức tạp đối với một công ty, giải pháp thay thế tốt nhất tiếp theo sẽ là WPA2 với chế độ AES/CCMP.

Nhưng để bảo vệ khỏi các cuộc tấn công vét cạn hoặc bảng cầu vồng, chúng ta nên thực hiện một số bước để đẩy cao chi phí tính toán. Một cụm mật khẩu dài và phức tạp không được tìm thấy trong từ điển sẽ làm tăng lượng thời gian và tài nguyên mà kẻ tấn công sẽ cần để phá vỡ cụm mật khẩu. Thay đổi SSID thành một thứ gì đó không phổ biến và duy nhất, cũng sẽ làm cho các bảng cầu vồng ít khả năng được sử dụng hơn. Nó sẽ yêu cầu kẻ tấn công tự thực hiện các tính toán, làm tăng thời gian và nguồn lực cần thiết để thực hiện một cuộc tấn công. Chúng ta cũng cần đảm bảo rằng WPS không được bật trên các AP. Chúng ta cũng cần kiểm tra lại tính năng đã thực sự bị vô hiệu hóa chưa bằng cách sử dụng một số công cụ như Wash, công cụ này sẽ quét và liệt kê các thiết bị bật WPS. Xác minh độc lập này được khuyến cáo, vì một số nhà sản xuất

bộ định tuyến không cho phép chúng ta vô hiệu hóa WPS. Trong một số trường hợp, việc tắt tính năng thông qua bảng điều khiển quản lý không thực sự vô hiệu hóa tính năng này.

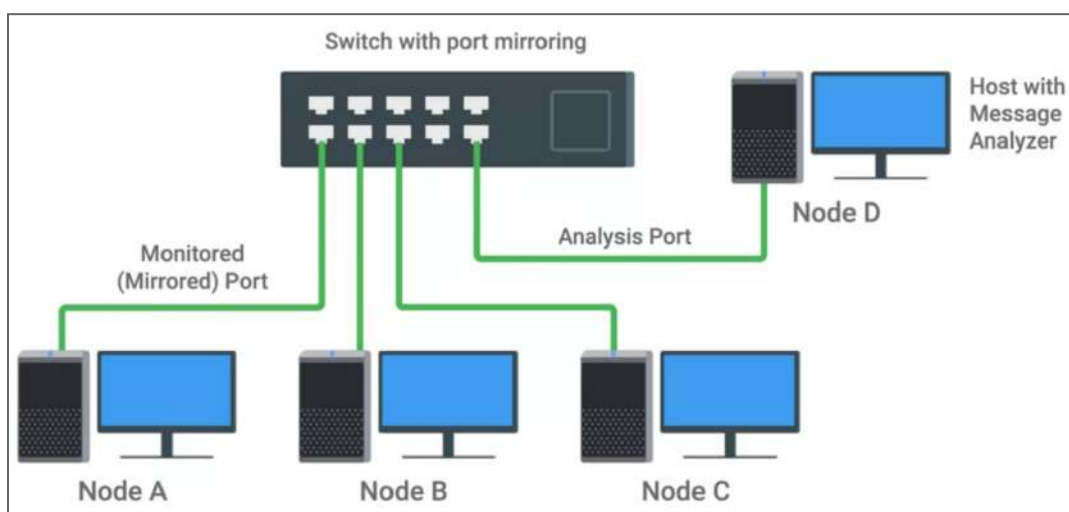
5. Giám sát mạng

Bắt và kiểm tra gói tin

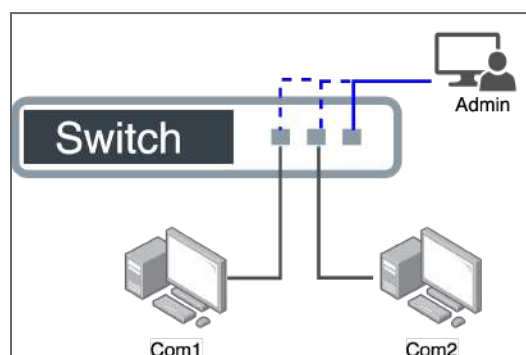
Bây giờ, để theo dõi loại luồng nào trên mạng, chúng ta cần một cơ chế để nắm bắt các gói từ luồng mạng để phân tích và ghi nhật ký tiềm năng. Packet Sniffing hay Packet Capture, là một quá trình chặn toàn bộ các gói mạng để phân tích.

Các card mạng và phần mềm mạng trên một hệ điều hành hoạt động giống như một trình thực thi tốt bụng. Nghĩa là chúng chỉ chấp nhận và xử lý các gói được đánh địa chỉ MAC của nó. Nếu gặp phải một gói có địa chỉ đích khác, card mạng sẽ thả gói đó. Tuy nhiên, nếu chúng ta muốn nắm bắt tất cả các gói mà một card mạng có thể nhìn thấy thì cách thức này sẽ gây khó khăn cho chúng ta. Để điều chỉnh, chúng ta đặt card mạng ở chế độ được gọi là chế độ hỗn tạp (promiscuous mode). Đây là một chế độ đặc biệt dành cho các card mạng Ethernet để bắt tất cả gói tin. Nhiều công cụ chụp gói tin cũng sẽ xử lý việc này cho chúng ta.

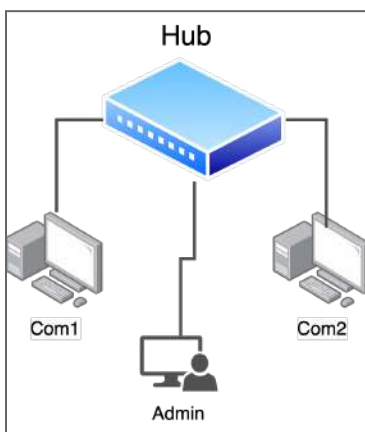
Một điều cực kỳ quan trọng cần xem xét khi thực hiện bắt gói tin là liệu chúng ta có quyền truy cập vào luồng mà chúng ta muốn bắt và theo dõi không. Giả sử chúng ta muốn phân tích tất cả luồng giữa các máy được kết nối đến cùng một switch. Trong trường hợp này, luồng truy cập duy nhất chúng ta có thể nắm bắt là luồng truy cập đến và đi từ máy của bạn mà thôi. Điều đó không có ý nghĩa cho phân tích luồng truy cập của các máy khác. Nếu các gói tin không được gửi đến card mạng của chúng ta thì chế độ hỗn tạp sẽ không giúp nhìn thấy chúng. Nếu máy của chúng ta xen giữa cổng uplink của switch và các máy thì chúng ta có quyền truy cập vào tất cả các gói trong và ngoài phân đoạn mạng cục bộ đó.



Các thiết bị switch trang bị trong doanh nghiệp thường có một tính năng gọi là Port Mirroring, giúp giải quyết điều kiện cần để bắt gói tin. Port Mirroring cho phép bộ chuyển mạch lấy tất cả các gói tin từ một cổng, dải cổng hoặc toàn bộ VLAN và phản chiếu các gói đến một cổng chuyển mạch được chỉ định. Điều này cho phép chúng ta có quyền truy cập vào tất cả các gói chuyển qua một bộ chuyển mạch một cách thuận tiện và an toàn hơn.



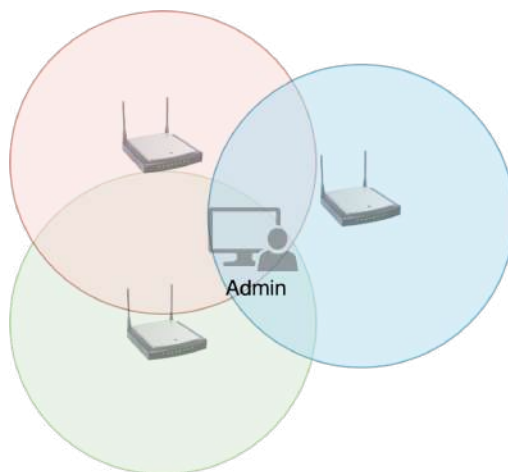
Có một cách khác mặc dù ít tiên tiến hơn là chèn một hub vào cấu trúc mạng và cho các máy chúng ta muốn giám sát kết nối đến hub này. Cách này thực hiện nhanh chóng và dễ dàng để bắt các gói tin. Tuy nhiên, chúng có nhiều nhược điểm như giảm băng thông và tiềm năng gây ra các độn độ.



Bắt gói tin trong mạng không dây

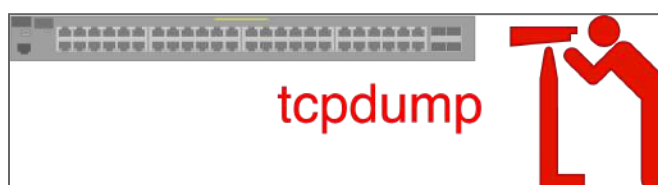
Chế độ hỗn tạp (promiscuous mode) được áp dụng cho một thiết bị không dây cho phép máy xử lý và nhận các gói từ mạng mà nó được liên kết. Nếu chúng ta muốn bắt tất cả luồng truy cập không dây trong khu vực xung quanh, chúng ta có thể đặt card mạng không dây của mình vào một chế độ được gọi là chế độ giám sát.

Chế độ giám sát (monitor mode) cho phép chúng ta quét qua các kênh để xem tất cả luồng truy cập không dây được gửi bởi các AP và máy khách. Không quan trọng chúng được sử dụng cho mạng nào và nó sẽ không yêu cầu thiết bị khách phải được liên kết hoặc kết nối với bất kỳ mạng không dây nào. Có một số tiện ích theo dõi và bắt gói tin không dây mã nguồn mở, như Aircrack-ng và Kismet. Lưu ý là nếu mạng không dây được mã hóa, chúng ta vẫn có thể bắt các gói tin, nhưng sẽ không thể giải mã dữ liệu nếu không biết mật khẩu.



Công cụ hỗ trợ (Tcpdump, Wireshark)

Tcpdump là một tiện ích dựa trên dòng lệnh được sử dụng để bắt và phân tích các gói tin. Tcpdump sử dụng thư viện libpcap mã nguồn mở. Đó là một thư viện bắt gói tin phổ biến được sử dụng trong rất nhiều công cụ thu thập và phân tích gói tin. Tcpdump cũng hỗ trợ ghi gói tin vào một tập tin, chia sẻ hoặc phát lại luồng truy cập sau này. Nó cũng hỗ trợ đọc các bản bắt gói tin trở lại từ một tập tin. Nó chuyển đổi thông tin quan trọng từ tầng ba trở lên thành các định dạng có thể đọc được bởi con người.

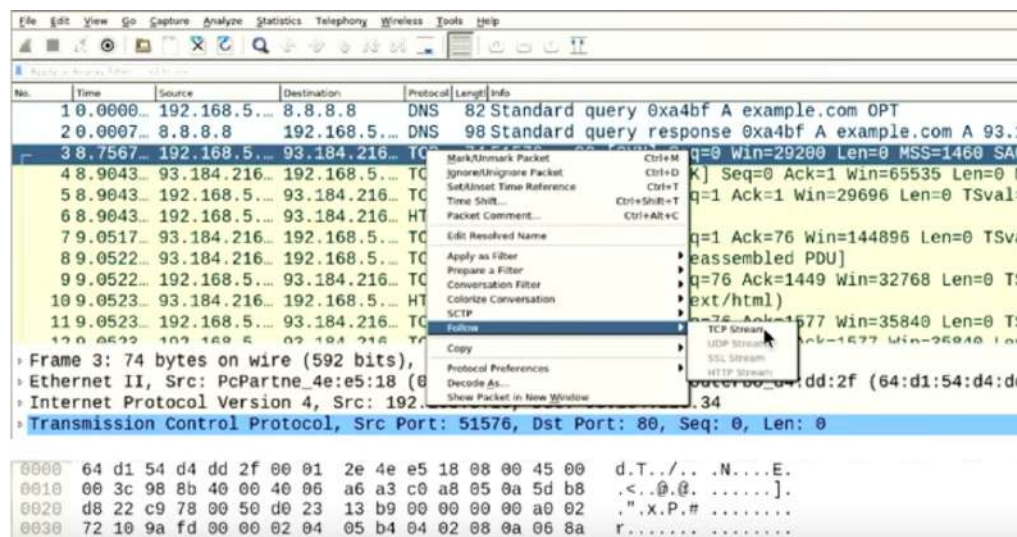


Thông tin gói tin mà tcpdump bắt và thể hiện như sau. Thông tin đầu là thời gian biểu thị thời điểm xảy ra gói tin. Tiếp theo, giao thức lớp ba, trong trường hợp này là IPv4. Sau đó, bộ bốn kết nối được thể hiện. Bộ này gồm địa chỉ nguồn, cổng nguồn, địa chỉ đích và cổng đích. Tiếp theo, cờ TCP và số thứ tự TCP được đặt trên gói, nếu có. Tiếp theo là số ack, kích thước cửa sổ TCP, sau đó là các tùy chọn TCP, nếu có. Cuối cùng là kích thước gói dữ liệu tính bằng byte. Tcpdump cũng hỗ trợ xem gói tin ở dạng thô.

```
spinel [clear] ~ 17-09-19 4:51PM
spinel% sudo tcpdump -i en0 ip and host example.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:52:00.416978 IP spinel.home.mrانت.0rg.49026 > 93.184.216.34.http: Flags [S], seq 2505083261, win 29200, options [mss 1460,sackOK,TS val 1410827528 ecr 0,nop,wscale 7], length 0
16:52:00.583154 IP 93.184.216.34.http > spinel.home.mrانت.0rg.49026: Flags [S.], seq 1959622244, ack 2505083262, win 65535, options [mss 1460,sackOK,TS val 1039848002 ecr 1410827528,nop,wscale 9], length 0
16:52:00.583166 IP spinel.home.mrانت.0rg.49026 > 93.184.216.34.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 1410827578 ecr 1039848002], length 0
```

Wireshark là một công cụ thu thập và phân tích gói tin. Nó có giao diện đồ họa và nhiều tính năng hơn so với tcpdump. Wireshark cũng sử dụng thư viện libpcap để bắt và phân giải các gói tin nhưng nó mở rộng hơn. Trong khi tcpdump thực hiện phân tích cơ bản về một số loại luồng truy cập thì Wireshark có thể giải mã các dữ liệu được mã hóa nếu biết khóa mã hóa. Nó cũng có thể xác định và trích xuất các dữ liệu từ việc truyền tập tin thông qua các giao thức như SMB hoặc HTTP. Wireshark hỗ trợ hơn 2.000 giao thức và tích hợp các bộ lọc để tạo sự dễ dàng trong quá trình phân tích. Wireshark không chỉ có khả

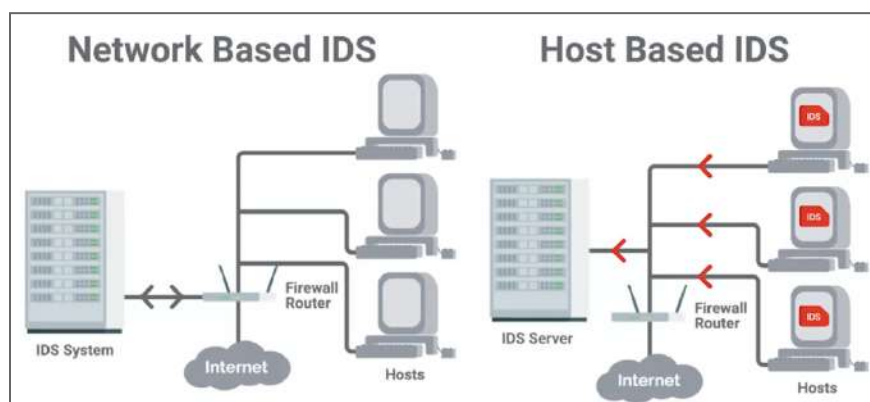
năng xử lý giao thức rất tiện dụng, nó còn hiểu và có thể theo dõi các luồng hoặc phiên TCP.



Hệ thống phát hiện/ngăn chặn xâm nhập

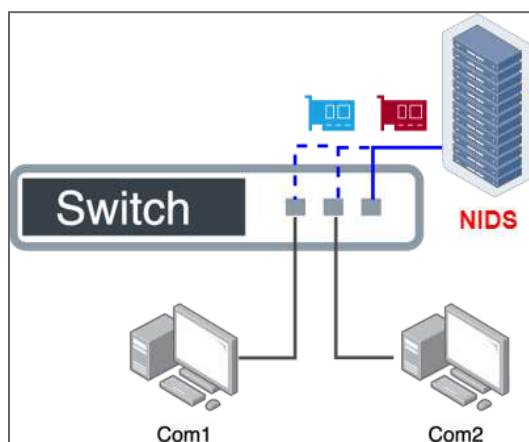
Hệ thống IDS (Intrusion Detection System, IDS) hoặc IPS (Intrusion Prevention System, IPS) hoạt động bằng cách giám sát luồng truy cập mạng và phân tích nó. Chúng tìm kiếm hành vi hoặc đặc điểm phù hợp có thể chỉ ra luồng truy cập nguy hại. Sự khác biệt giữa IDS và hệ thống IPS, IDS chỉ là một hệ thống phát hiện. Nó sẽ không thực hiện hành động để ngăn chặn một cuộc tấn công. Khi một cuộc tấn công được phát hiện, IDS chỉ ghi lại cảnh báo. Nhưng một hệ thống IPS có thể điều chỉnh các quy tắc tường lửa một cách nhanh chóng, để chặn hoặc loại bỏ luồng nguy hại khi nó được phát hiện.

Hệ thống IDS và IPS có thể dựa trên mạng hoặc dựa trên máy tính. Trong trường hợp hệ thống dựa trên mạng, hệ thống sẽ được triển khai ở một nơi nào đó trên mạng, nơi nó có thể giám sát luồng truy cập cho một phân đoạn mạng hoặc mạng con. Hệ thống dựa trên máy tính là một phần mềm được triển khai trên máy tính để giám sát luồng truy cập đến và đi từ máy tính đó. Nó cũng có thể giám sát các tập tin hệ thống để tìm các thay đổi trái phép.

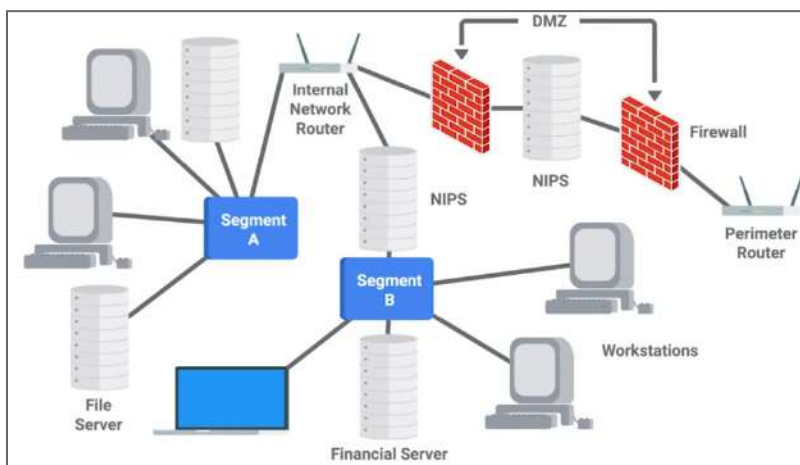


Hệ thống NIDS (network based IDS, NIDS) giống với tường lửa theo nhiều cách. Tuy nhiên, tường lửa được thiết kế để ngăn chặn sự xâm nhập bằng cách chặn luồng độc hại tiềm ẩn từ bên ngoài và thực thi danh sách ACL giữa các mạng. Hệ thống NIDS có nhiệm vụ phát hiện và cảnh báo về hoạt động nguy hiểm tiềm ẩn đến từ bên trong mạng. Ngoài ra, tường lửa chỉ có khả năng nhìn thấy luồng truy cập giữa các mạng mà chúng đã thiết lập để bảo vệ. Chúng thường không có khả năng nhìn thấy luồng truy cập giữa các máy tính bên trong mạng.

NIDS cần được đặt trong cấu trúc liên kết mạng, theo cách mà nó có quyền truy cập vào luồng mà chúng ta muốn theo dõi. Một cách tốt để có thể truy cập vào luồng mạng là sử dụng chức năng port mirroring được tìm thấy trong nhiều thiết bị switch. Điều này cho phép tất cả các gói trên một cổng, dải cổng hoặc toàn bộ VLAN được sao chép sang một cổng khác, nơi máy chủ NIDS sẽ được kết nối. Với cấu hình này, máy NIDS sẽ có thể thấy tất cả các gói truyền qua lại giữa các máy tính trên phân đoạn switch. Điều này cũng cho phép chúng ta giám sát các giao tiếp hay luồng truy cập từ các máy tính ra mạng bên ngoài, chẳng hạn như internet. Các máy NIDS sẽ phân tích luồng này bằng cách bật chế độ promiscuous trên cổng phân tích. Đây là card mạng được kết nối với cổng nhân bản trên switch, vì vậy nó có thể thấy tất cả các gói được truyền qua và thực hiện phân tích luồng truy cập. Vì card này được sử dụng để nhận các gói được sao chép từ mạng mà chúng ta muốn giám sát, máy chủ NIDS phải có ít nhất hai card mạng. Một cái dùng để theo dõi phân tích và một cái riêng biệt dùng để kết nối với mạng cho các mục đích quản lý và quản trị. Một số hệ thống NIDS hoặc NIPS phổ biến là Snort, Suricata và Bro NIDS.



Vị trí của hệ thống NIPS (network based IPS, NIPS) sẽ khác với hệ thống NIDS. Điều này là do hệ thống NIPS có thể thực hiện hành động chống lại một luồng truy cập bị nghi ngờ là độc hại. Để một thiết bị NIPS có thể chặn hoặc loại bỏ lưu lượng truy cập khỏi một mối đe dọa được phát hiện, nó phải được đặt phù hợp với luồng đang được giám sát. Điều này có nghĩa là luồng đang được giám sát phải đi qua thiết bị NIPS. Nếu không như vậy, máy chủ NIPS sẽ không thể thực hiện hành động đối với luồng bị nghi ngờ.



Việc phát hiện các mối đe dọa hoặc luồng độc hại thường được xử lý thông qua phát hiện dựa trên chữ ký, tương tự như cách phần mềm chống vi-rút phát hiện phần mềm độc hại. Chữ ký là đặc điểm duy nhất của luồng truy cập độc hại đã biết. Chúng có thể là các chuỗi gói tin cụ thể hoặc các gói tin có giá trị nhất định được mã hóa trong trường header xác định. Điều này cho phép hệ thống IDS/IPS dễ dàng và nhanh chóng nhận ra luồng truy cập xấu đã biết từ

các nguồn như botnet, sâu và các vectơ tấn công phổ biến khác trên internet. Các chữ ký cũng cần được thường xuyên cập nhật.

Tương tự như chống virus, các cuộc tấn công có chủ đích có thể không được phát hiện bởi hệ thống dựa trên chữ ký, vì có thể chưa có chữ ký được phát triển cho những trường hợp này. Chúng ta có thể tạo các quy tắc tùy chỉnh để phù hợp với luồng truy cập có thể được coi là đáng ngờ, nhưng không nhất thiết là độc hại. Điều này sẽ cho phép các nhà điều tra xem xét luồng truy cập chi tiết hơn để xác định mức độ xấu. Nếu luồng truy cập được phát hiện là độc hại, một chữ ký có thể được phát triển từ luồng truy cập và kết hợp nó vào hệ thống. Hệ thống có thể ghi lại sự kiện phát hiện cùng với một bản sao toàn bộ gói truy cập nghi ngờ. Cảnh báo cũng sẽ thường được kích hoạt để thông báo cho nhóm điều tra để xem xét luồng truy cập được phát hiện đó. Tùy thuộc vào mức độ nghiêm trọng của sự kiện, cảnh báo có thể chỉ gửi email cho một nhóm hoặc tạo một vé để theo dõi hoặc nó có thể đánh thức ai đó vào lúc nửa đêm nếu nó được xác định là mức độ nghiêm trọng thực sự cao và khẩn cấp. Những cảnh báo này thường cũng sẽ bao gồm thông tin tham khảo liên kết đến một lỗ hổng đã biết hoặc một số thông tin khác về bản chất của cảnh báo để giúp người điều tra xem xét sự kiện.

Bài đọc 6: Phòng Thủ Theo Chiều Sâu

1. Tấn công và phòng thủ

Lỗ hổng (vulnerability) là kẻ hở mà kẻ tấn công có thể lợi dụng để xâm nhập hệ thống. Có một loại lỗ hổng đặc biệt được gọi là lỗ hổng Zero-day, tạm dịch là lỗ hổng 0 ngày. Đây là một lỗ hổng mà nhà phát triển hoặc nhà cung cấp phần mềm chưa biết nhưng kẻ tấn công đã biết. Tên gọi mô tả đến khoảng thời gian mà nhà phát triển phần mềm đã phản ứng và sửa chữa lỗ hổng bảo mật này là không ngày. Khả năng xảy ra những sai sót chưa xác định này là điều chúng ta nên nghĩ đến khi tìm cách bảo vệ hệ thống và mạng máy tính của công ty mình. Mặc dù đó là một rủi ro chưa xác định, nó vẫn có thể được xử lý bằng cách thực hiện các biện pháp hạn chế và kiểm soát quyền truy cập vào hệ thống. Mục tiêu cuối cùng của chúng ta là giảm thiểu rủi ro.

Vectơ tấn công (attack vector) là phương pháp hoặc con đường mà kẻ tấn công hoặc phần mềm độc hại có được quyền truy cập vào mạng hoặc hệ thống. Một số vectơ tấn công là tập tin đính kèm email, giao thức hoặc dịch vụ mạng, card mạng và thao tác của người dùng. Đây là những cách tiếp cận hoặc con đường khác nhau mà kẻ tấn công có thể sử dụng để xâm nhập hệ thống nếu chúng có thể khai thác nó.

Bề mặt tấn công (attack surface) là tổng của tất cả các vectơ tấn công khác nhau trong một hệ thống nhất định. Chúng ta có thể coi đây là sự kết hợp của tất cả các cách mà kẻ tấn công có thể tương tác với hệ thống, bất kể các lỗ hổng đã biết hay chưa. Ngoài ra, chúng ta cũng không thể biết hết tất cả các lỗ hổng, nên cần nghĩ về tất cả các cách mà một tác nhân bên ngoài có thể tương tác với hệ thống của chúng ta như một bề mặt tấn công tiềm năng. Điểm quan trọng ở đây là giữ cho bề mặt tấn công càng nhỏ càng tốt. Điều này làm giảm khả năng kẻ tấn công phát hiện ra một lỗ hổng chưa biết và làm ảnh hưởng đến hệ thống. Có rất nhiều cách tiếp cận có thể sử dụng để giảm bớt bề mặt tấn công. Tất cả chúng đều hướng đến việc đơn giản hóa hệ thống và dịch vụ. Thứ gì đó càng ít phức tạp thì càng ít có khả năng có sai sót không bị phát hiện.

Phòng thủ theo chiều sâu (defense in depth) là cách thức tổ chức hệ thống phòng thủ đan xen nhau để bảo vệ hệ thống CNTT. Điều này đảm bảo một số lượng dự phòng cho các biện pháp phòng thủ. Nó cũng giúp tránh một thỏa

hiệp thảm khốc trong trường hợp một hệ thống bị lỗi hoặc một lỗ hổng được phát hiện trong một hệ thống. Chúng ta có thể xem nó giống như có nhiều tuyến phòng thủ. Nếu kẻ tấn công vượt qua tường lửa của bạn, bạn vẫn được bảo vệ bởi các hệ thống xác thực mạnh trong mạng. Điều này sẽ yêu cầu kẻ tấn công tìm ra nhiều lỗ hổng hơn trong nhiều hệ thống hơn trước khi thiệt hại thực sự có thể xảy ra.



2. Gia cố hệ thống

Tắt các thành phần không cần thiết

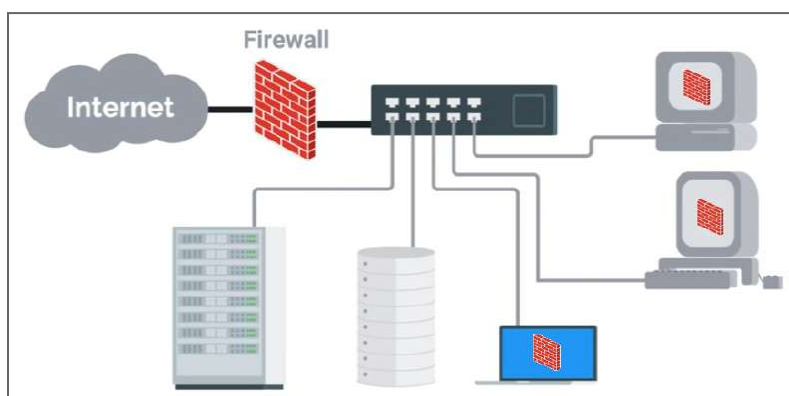
Hãy đảm bảo tắt bất kỳ dịch vụ hoặc giao thức bổ sung nào. Nếu chúng không hoàn toàn cần thiết, thì hãy tháo chúng ra. Mỗi dịch vụ bổ sung đang hoạt động đại diện cho bề mặt tấn công bổ sung, có thể có lỗ hổng chưa được phát hiện. Lỗ hổng đó có thể bị khai thác và dẫn đến phá hoại. Khái niệm tắt hay gỡ bỏ cũng áp dụng cho quyền truy cập và danh sách ACL. Chỉ cho phép truy cập khi thực sự cần thiết. Ví dụ, nhân viên có thể không cần thiết truy cập máy in từ bên ngoài mạng cục bộ. Chúng ta có thể điều chỉnh các quy tắc tường lửa để ngăn chặn kiểu truy cập đó. Một cách khác để giữ mọi thứ đơn giản là giảm triển khai phần mềm. Thay vì có năm giải pháp phần mềm khác nhau để hoàn thành năm nhiệm vụ riêng biệt, hãy thay thế chúng bằng một giải pháp thống nhất, nếu chúng ta có thể. Một giải pháp đó sẽ yêu cầu mã ít phức tạp hơn, giúp giảm số lượng lỗ hổng tiềm ẩn.

Chúng ta cũng nên đảm bảo vô hiệu hóa các tính năng không cần thiết hoặc không sử dụng trong phần mềm và hệ thống được triển khai. Bằng cách tắt các tính năng không được sử dụng, chúng ta thậm chí còn giảm nhiều dịch vụ công

nghe hơn nữa. Chúng ta không chỉ giảm số lượng cách kẻ tấn công có thể xâm nhập mà còn giảm thiểu số lượng mã nguồn đang hoạt động. Điều quan trọng là phải thực hiện phương pháp này ở mọi cấp độ của hệ thống và mạng do chúng ta quản lý. Có vẻ hiển nhiên khi thực hiện các biện pháp này trên cơ sở hạ tầng mạng và máy chủ quan trọng, nhưng điều này cũng quan trọng không kém đối với các nền tảng máy tính để bàn và máy tính xách tay mà nhân viên sử dụng. Rất nhiều hệ điều hành cá nhân cung cấp một loạt các dịch vụ và phần mềm mặc định, mà chúng ta có thể không sử dụng trong mạng hoặc môi trường doanh nghiệp. Ví dụ: truy cập Telnet cho một switch không có tác vụ kinh doanh nào cần phải bật nó trong môi trường thế giới thực. Chúng ta nên vô hiệu hóa nó ngay lập tức nếu tìm thấy nó trên thiết bị. Mọi quyền truy cập API dành riêng cho nhà cung cấp cũng sẽ bị vô hiệu hóa nếu chúng ta không có kế hoạch sử dụng các dịch vụ hoặc công cụ này. Dù chúng có thể vô hại, đặc biệt nếu đã thiết lập các quy tắc tường lửa và ACL mạng chặt chẽ, nhưng tại sao chúng ta lại phải chấp nhận bất kỳ rủi ro không cần thiết nào?

Tường lửa

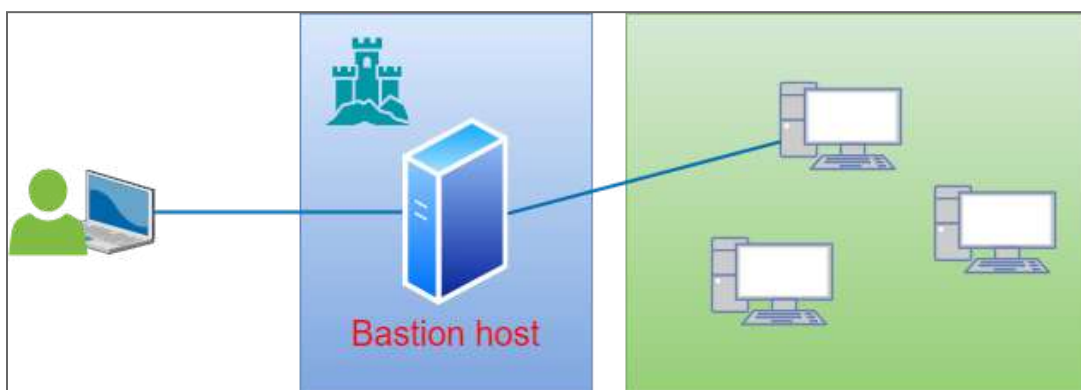
Chúng ta đã đề cập ngắn gọn đến tường lửa khi nói về hệ thống phát hiện xâm nhập và giám sát mạng. Tuy nhiên tường lửa cũng đóng vai trò quan trọng để tạo ra nhiều lớp bảo mật. Chúng ta nhắc lại một số đặc điểm của tường lửa trước khi đi vào vai trò cụ thể của nó trong bảo vệ đa lớp. Tường lửa là một hệ thống bảo mật mạng dùng để theo dõi và kiểm soát các luồng vào ra dựa trên tập quy tắc đã được xác định. Thay vì yêu cầu phải chặn cụ thể tất cả luồng, với tường lửa, chúng ta có thể tạo các quy tắc cho luồng được phép đi qua. Chúng ta có thể coi đây là danh sách trắng, trái ngược với danh sách đen. Trước khi một dịch vụ mới hoạt động, một quy tắc mới phải được xác định.



Tường lửa rất quan trọng để bảo mật mạng. Chúng có thể được triển khai như các thiết bị hạ tầng mạng chuyên dụng, điều chỉnh luồng cho toàn mạng. Chúng có thể dựa trên máy tính trực tiếp dưới dạng phần mềm cung cấp khả năng bảo vệ chỉ cho một máy lưu trữ nó. Tường lửa máy tính cung cấp khả năng bảo vệ cho các thiết bị di động như máy tính xách tay có thể được sử dụng trong môi trường không đáng tin cậy, tiềm ẩn nguy cơ độc hại như điểm phát sóng Wi-Fi ở sân bay. Tường lửa này cũng hữu ích để bảo vệ các máy khác không bị xâm nhập bởi thiết bị bị hỏng trên mạng nội bộ. Ngoài ra, còn có tường lửa mạng thường được tích hợp sẵn trong bộ định tuyến và các thiết bị mạng khác.

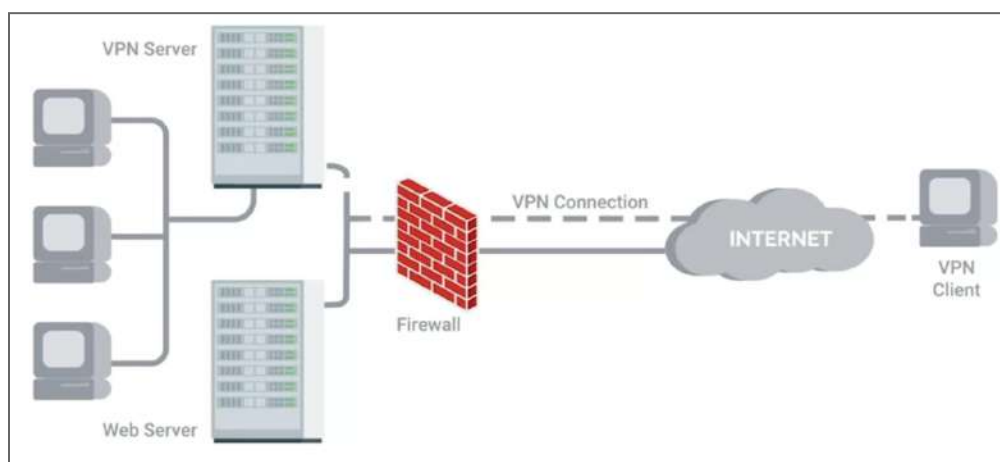
Ngoài chức năng bảo vệ các máy tính riêng lẻ khỏi bị xâm phạm khi chúng được sử dụng trong môi trường không đáng tin cậy và có khả năng độc hại, tường lửa máy tính cũng bảo vệ các máy tính ngay cả bên trong mạng đáng tin cậy. Trong khi tường lửa mạng có nhiệm vụ bảo vệ mạng nội bộ bằng cách lọc luồng truy cập vào và ra khỏi nó, thì tường lửa lưu trữ trên mỗi máy tính riêng lẻ sẽ bảo vệ máy đó. Khi thiết lập tường lửa máy tính, chúng ta cũng bắt đầu với quy tắc từ chối ngầm. Sau đó, chúng ta chọn các dịch vụ và cổng cụ thể được sử dụng. Điều này cho phép bắt đầu với một mặc định được bảo mật và sau đó chỉ cho phép luồng truy cập mà chúng ta biết và tin tưởng. Chúng ta có thể coi điều này giống như việc bắt đầu với một cấu hình tường lửa hoàn toàn an toàn và sau đó chọc lỗ vào đó cho luồng truy cập cụ thể mà chúng ta mong muốn. Tóm lại, tường lửa máy tính đóng một vai trò quan trọng trong việc giảm bớt những gì có thể truy cập được đối với kẻ tấn công bên ngoài. Nó cung cấp tính linh hoạt trong khi chỉ cho phép kết nối với các dịch vụ chọn lọc trên một máy tính nhất định từ các mạng hoặc dải IP cụ thể.

Khả năng hạn chế các kết nối từ một số nguồn nhất định thường được sử dụng để triển khai một máy tính có độ bảo mật cao với mạng. Từ đó, cho phép truy cập vào các hệ thống hoặc cơ sở hạ tầng quan trọng hoặc nhạy cảm. Chúng được gọi là máy chủ pháo đài (Bastion host).



Máy chủ pháo đài được gia cố một cách đặc biệt và được tối thiểu hóa để giảm những gì để chạy trên nó. Máy chủ lưu trữ pháo đài thường kết nối tới internet, vì vậy chúng ta cần chú ý đến việc tăng cường và khóa chúng lại để giảm khả năng bị xâm phạm. Chúng cũng có thể được sử dụng như một loại cổng truy cập vào các dịch vụ nhạy cảm hơn như máy chủ xác thực trung tâm hoặc bộ điều khiển miễn. Điều này sẽ cho phép chúng ta triển khai các cơ chế xác thực và ACL an toàn hơn trên các máy chủ Bastion mà không gây bất tiện cho toàn bộ công ty. Việc giám sát và ghi nhật ký có thể được ưu tiên cho các máy chủ này dễ dàng hơn. Thông thường, các máy chủ hoặc mạng này cũng sẽ có kết nối mạng bị hạn chế nghiêm trọng. Nó thường chỉ đến vùng an toàn mà chúng được thiết kế để bảo vệ chứ không phải nhiều thứ khác. Các ứng dụng được phép cài đặt và chạy trên các máy chủ này cũng sẽ bị hạn chế đối với những ứng dụng thực sự cần thiết, vì các máy này có một mục đích cụ thể.

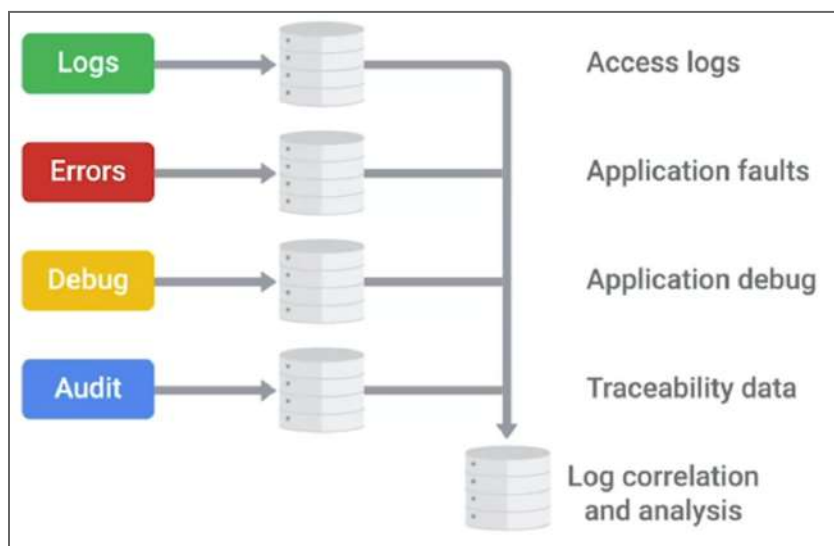
Một phần của các quy tắc tường lửa máy tính cung cấp các ACL mà cho phép truy cập từ mạng con VPN. Chúng ta cần giữ cho mạng mà các máy khách VPN kết nối riêng biệt bằng cách sử dụng kỹ thuật chia mạng con và VLAN. Điều này giúp chúng ta linh hoạt hơn để thực thi bảo mật trên các máy khách VPN này. Nó cũng cho phép xây dựng các lớp bảo vệ bổ sung vì các máy khách VPN vẫn là máy tính hoạt động trong môi trường nguy hiểm tiềm ẩn. Máy tính này sau đó sẽ kết nối từ xa vào mạng nội bộ đáng tin cậy của chúng ta. Khả năng giám sát riêng biệt lưu lượng truy cập đến và đi từ chúng là cực kỳ hữu ích.



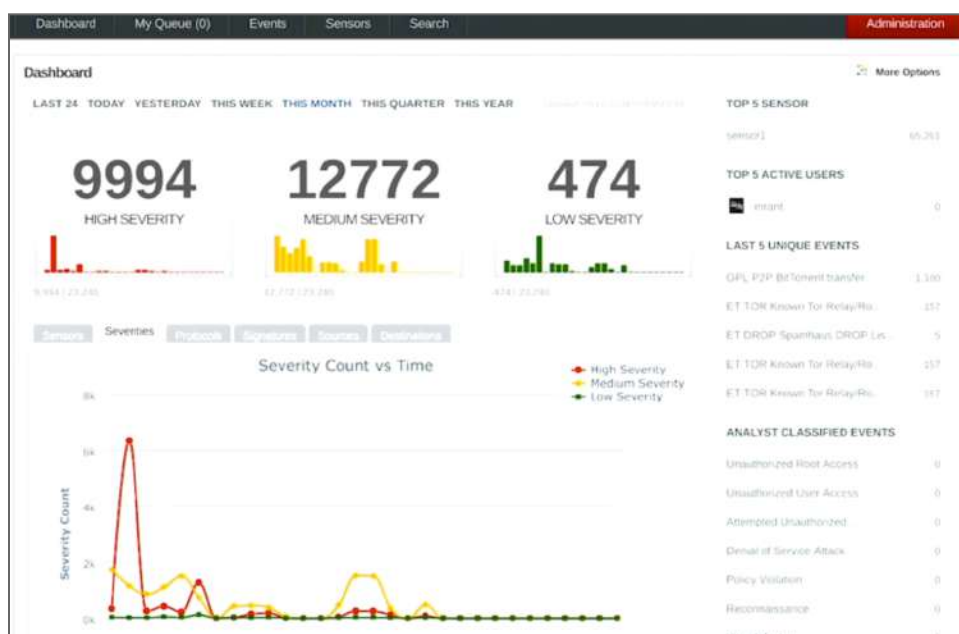
Nếu người dùng của hệ thống có quyền quản trị viên, thì họ có khả năng thay đổi cấu hình và quy tắc tường lửa. Đây là điều chúng ta nên lưu ý và đảm bảo theo dõi bản ghi nhật ký. Nếu các công cụ quản lý cho phép, chúng ta cũng nên ngăn chặn việc vô hiệu hóa tường lửa trên máy tính.

Ghi nhật ký và phân tích các bất thường

Một phần quan trọng của bất kỳ kiến trúc bảo mật nào là ghi nhật ký và cảnh báo. Chúng ta cần nhìn vào bên trong hệ thống an ninh để xem có loại luồng truy cập nào. Chúng ta cũng cần xem nhật ký của tất cả các thiết bị cơ sở hạ tầng và ứng dụng mà chúng ta quản lý. Nhưng chỉ có nhật ký thôi là chưa đủ, chúng ta còn cần các cách để bảo vệ nhật ký và giúp chúng dễ dàng phân tích và xem xét. Nhiều kỹ thuật phân tích cũng có thể được áp dụng để xử lý sự cố.



Khi có một số lượng lớn hệ thống đặt xung quanh mạng của chúng ta, mỗi hệ thống có định dạng nhật ký riêng, có thể là một thách thức để hiểu tất cả dữ liệu này. SIEM là mô tả về hệ thống quản lý sự kiện và thông tin bảo mật. SIEM có thể được coi như một máy chủ nhật ký tập trung. Nó cũng có một số tính năng phân tích bổ sung. Một hệ thống SIEM lấy nhật ký từ một loạt các hệ thống khác. Nó hợp nhất các bản ghi từ tất cả các nơi khác nhau và đặt nó vào một vị trí tập trung. Điều này làm cho việc xử lý nhật ký dễ dàng hơn rất nhiều.

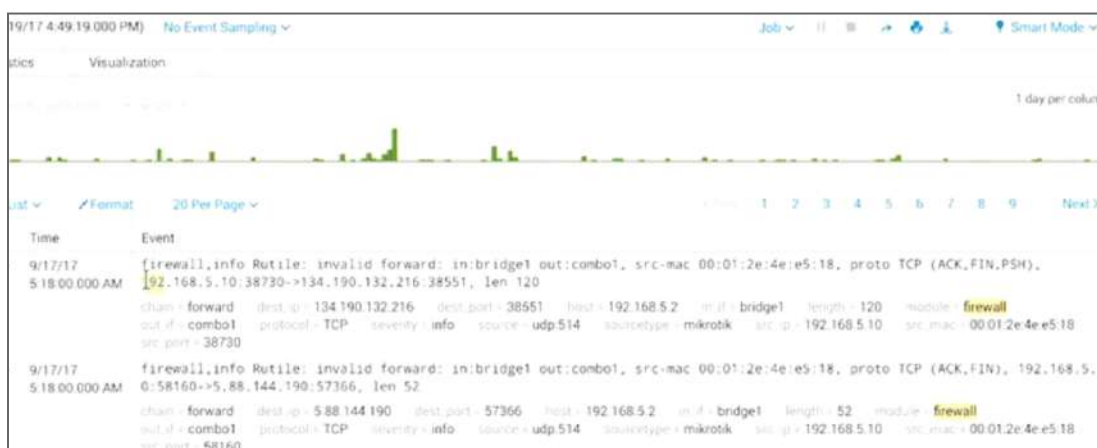


Ngoài hỗ trợ phân tích, một máy chủ tập trung cũng có các lợi ích về bảo mật. Bằng cách duy trì nhật ký trên một hệ thống chuyên dụng, việc bảo vệ hệ thống khỏi bị tấn công trở nên dễ dàng hơn. Các bản ghi thường là mục tiêu của những kẻ tấn công sau khi vi phạm, để chúng có thể che dấu vết của chúng. Bằng cách yêu cầu các hệ thống quan trọng gửi nhật ký đến máy chủ ghi nhật ký từ xa đã bị khóa, các chi tiết về vi phạm sẽ vẫn được ghi lại. Một nhóm phân tích sẽ có thể tái tạo lại các sự kiện dẫn đến xâm nhập.

Một bước quan trọng cần thực hiện trong phân tích nhật ký là chuẩn hóa. Đây là quá trình lấy dữ liệu nhật ký ở các định dạng khác nhau và chuyển đổi nó thành định dạng chuẩn hóa phù hợp với cấu trúc nhật ký xác định. Chúng ta có thể định cấu hình chuẩn hóa cho các nguồn nhật ký của mình. Ví dụ, các mục nhập nhật ký từ tường lửa có dạng thời gian theo năm/tháng/ngày, trong khi nhật ký từ các máy khách sử dụng định dạng ngày/tháng/năm. Để chuẩn hóa dữ

liệu này, chúng ta chọn một định dạng ngày tiêu chuẩn, sau đó xác định các trường dành cho các loại nhật ký cần được chuyển đổi. Khi nhận được nhật ký từ các máy này, các mục nhật ký sẽ được chuyển đổi thành chuẩn mà chúng ta đã xác định và được lưu trữ bởi máy chủ nhật ký. Điều này cho phép bạn phân tích và so sánh dữ liệu nhật ký giữa các loại nhật ký và hệ thống khác nhau theo cách dễ dàng và thống nhất hơn.

Nếu chúng ta ghi quá nhiều thông tin, rất khó để phân tích dữ liệu và tìm thông tin hữu ích. Thêm vào đó, các yêu cầu lưu trữ để lưu nhật ký trở nên rất tốn kém. Nhưng nếu chúng ta ghi quá ít, thì thông tin sẽ không cung cấp bất kỳ thông tin chi tiết hữu ích nào về hệ thống và mạng. Tìm kiếm điểm dung hòa có thể sẽ khó khăn. Nó sẽ khác nhau tùy thuộc vào các đặc điểm riêng của hệ thống đang được giám sát và loại hoạt động trên mạng. Bất kể sự kiện nào được ghi lại, tất cả chúng đều phải có thông tin giúp hiểu những gì đã xảy ra và tái tạo lại các sự kiện.



Có rất nhiều trường quan trọng cần ghi lại trong các mục nhật ký như thời gian, mã sự kiện hoặc mã lỗi, loại dịch vụ hoặc ứng dụng, tài khoản liên quan tới sự kiện và các thiết bị liên quan đến sự kiện. Thời gian là thứ cực kỳ quan trọng để hiểu khi nào một sự kiện xảy ra. Các trường như địa chỉ nguồn và địa chỉ đích sẽ cho chúng ta biết ai đang nói chuyện với ai. Đối với nhật ký ứng dụng, chúng ta có thể lấy thông tin hữu ích từ người dùng đã đăng nhập được liên kết với sự kiện và từ ứng dụng khách mà họ đã sử dụng.

Thông thường, khi xem nhật ký tổng hợp, chúng ta nên chú ý đến các mẫu và các kết nối giữa các luồng truy cập. Nếu nhận thấy một tỷ lệ lớn các máy đều

kết nối tới một địa chỉ cụ thể bên ngoài mạng, thì đó có thể đáng để điều tra. Nó có thể báo hiệu một sự lây nhiễm phần mềm độc hại. Khi nhật ký được tập trung và chuẩn hóa, chúng ta có thể viết cảnh báo tự động dựa trên các quy tắc. Ví dụ như thiết lập cảnh báo cho các nỗ lực xác thực lặp đi lặp lại không thành công với một máy chủ xác thực quan trọng. Ngoài ra, chúng ta có thể xem xét các giao thức thường được sử dụng trong mạng, xem những trao đổi hàng đầu trong mạng, kiểm tra các báo cáo lỗi để tìm ra các mẫu.

Một thành phần quan trọng khác đối với việc ghi nhật ký là khả năng duy trì nhật ký (log retention). Nhu cầu lưu trữ nhật ký sẽ khác nhau dựa trên số lượng hệ thống được ghi, số lượng nhật ký chi tiết và tốc độ tạo nhật ký. Thời gian muốn hoặc cần lưu giữ nhật ký cũng sẽ thực sự ảnh hưởng đến các yêu cầu lưu trữ đối với máy chủ nhật ký. Một số ví dụ về máy chủ ghi nhật ký và các giải pháp SIEMS như rsylog, Splunk Enterprise Security, IBM Security Qradar và RSA Security Analytics.

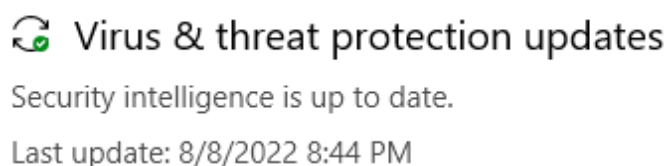
Phần mềm chống virus

Phần mềm chống virus (antivirus software) đã xuất hiện từ rất lâu nhưng một số chuyên gia bảo mật đặt câu hỏi về giá trị mà nó có thể cung cấp cho một công ty, đặc biệt là vì các phần mềm độc hại và các cuộc tấn công phức tạp hơn đã xuất hiện trong những năm gần đây. Phần mềm chống virus dựa trên chữ ký. Điều này có nghĩa là nó có cơ sở dữ liệu các chữ ký xác định phần mềm độc hại đã biết thông qua các giá trị băm tập tin. Hoặc có thể là đặc điểm lưu lượng mạng mà phần mềm độc hại sử dụng để giao tiếp với máy chủ điều khiển và chỉ huy.



Phần mềm chống virus sẽ theo dõi và phân tích những thứ như tập tin mới được tạo hoặc được sửa đổi trên hệ thống để theo dõi bất kỳ hành vi nào khớp với chữ ký phần mềm độc hại đã biết. Nếu phát hiện hoạt động khớp với chữ ký, tùy thuộc vào loại chữ ký, nó sẽ cố gắng chặn phần mềm độc hại. Nhưng một số chữ ký chỉ có thể phát hiện ra phần mềm độc hại sau khi quá trình lây nhiễm đã xảy ra. Trong trường hợp đó, nó có thể cố gắng cách ly các tập tin bị nhiễm. Nếu không thể, nó sẽ chỉ ghi lại và cảnh báo sự kiện phát hiện. Ở cấp độ cao, đây là cách hoạt động của tất cả các sản phẩm chống virus.

Tuy nhiên, có hai vấn đề với phần mềm chống virus. Đầu tiên là chúng phụ thuộc vào chữ ký chống virus được phân phối bởi nhà cung cấp phần mềm chống virus. Thứ hai là chúng phụ thuộc vào nhà cung cấp phần mềm chống virus phát hiện ra phần mềm độc hại mới và viết chữ ký mới cho các mối đe dọa mới được phát hiện. Cho đến khi nhà cung cấp có thể viết chữ ký mới và xuất bản và phổ biến chúng, phần mềm chống virus của bạn không thể bảo vệ bạn khỏi những mối đe dọa mới nổi này.



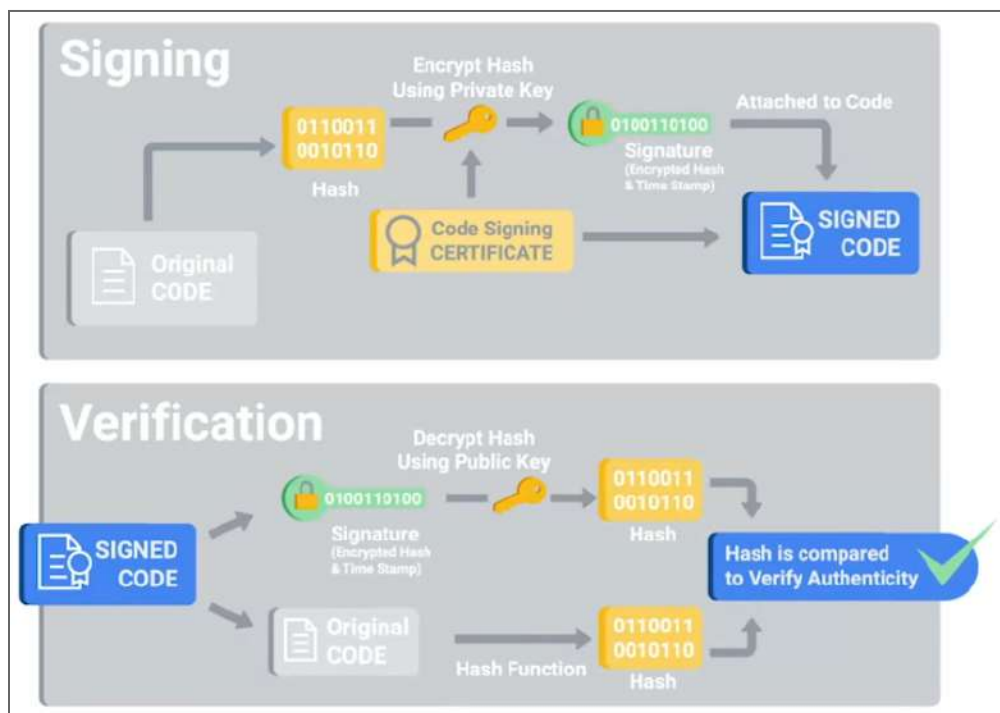
Phần mềm chống virus cũng đại diện cho một bề mặt tấn công bổ sung mà kẻ tấn công có thể khai thác. Một lỗ hổng đã được tìm thấy trong công cụ Sophos Antivirus vào năm 2012. Vì vậy, có vẻ như phần mềm chống virus không lý tưởng và có một số nhược điểm khá lớn. Vậy tại sao nó là một phần cốt lõi của thiết kế bảo mật? Câu trả lời ngắn gọn là nó bảo vệ chống lại các cuộc tấn công phổ biến nhất trên internet. Những thứ thực sự rõ ràng gây ra mối đe dọa cho hệ thống vẫn cần được bảo vệ chống lại. Phần mềm chống virus là một giải pháp dễ dàng để cung cấp sự bảo vệ đó. Một cách tốt để nghĩ về chống virus trong môi trường đe dọa bên ngoài ồn ào hiện nay là nó giống như một bộ lọc tiếng ồn tấn công trên internet. Nó cho phép chúng ta loại bỏ bớt tiếng ồn xung quanh và tập trung vào các mối đe dọa quan trọng hơn. Và theo khái niệm phòng thủ theo chiều sâu, chúng ta có nhiều lớp bảo vệ. Phần mềm chống virus chỉ là một phần trong hệ thống phòng thủ chống phần mềm độc hại mà thôi.

Trong khi phần mềm chống virus hoạt động theo mô hình danh sách đen, kiểm tra danh sách những điều xấu đã biết và chặn những gì phù hợp, có một loại phần mềm chống phần mềm độc hại làm theo cách ngược lại. Đó là danh sách các phần mềm tốt và đáng tin cậy được biết đến và chỉ những thứ có trong danh sách mới được phép chạy. Mọi thứ khác đều bị chặn. Chúng ta có thể coi điều này giống như việc áp dụng quy tắc ACL từ chối ngầm để thực thi phần mềm. Theo mặc định, mọi thứ đều bị chặn. Chỉ những thứ được phép thực thi một cách tường minh mới có thể thực hiện được.



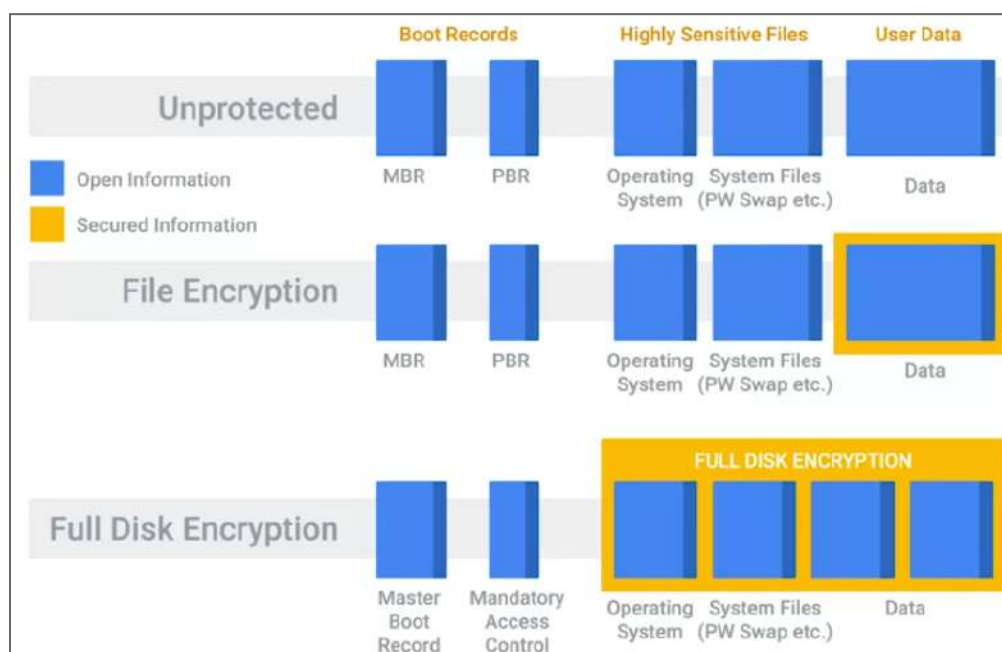
Nếu mọi bản cập nhật phải được đưa vào danh sách trắng trước khi nó có thể được áp dụng thì sẽ gây phiền phức. Chính vì lý do này mà phần mềm danh sách trắng nhị phân có thể tin cậy phần mềm bằng một vài cơ chế khác nhau. Đầu tiên là sử dụng hàm băm mã hóa duy nhất của các tập tin nhị phân được sử dụng để xác định các tập tin nhị phân duy nhất. Điều này được sử dụng để đưa vào danh sách trắng các tập tin thi hành riêng lẻ. Cơ chế tin cậy khác là chứng chỉ ký phần mềm. Nhà cung cấp phần mềm có thể ký mã hóa các tập tin nhị phân mà họ phân phối bằng cách sử dụng khóa bí mật. Chữ ký có thể được xác minh tại thời điểm thực thi bằng cách kiểm tra chữ ký bằng cách sử dụng khóa công khai được nhúng trong chứng chỉ và xác minh chuỗi tin cậy của khóa công khai. Nếu băm khớp và khóa công khai được tin cậy, thì phần mềm có thể được xác minh rằng nó đến từ một người nào đó có khóa bí mật ký mã của nhà cung cấp phần mềm. Hệ thống danh sách trắng nhị phân có thể được định cấu hình để tin cậy các chứng chỉ ký mã của nhà cung cấp cụ thể. Chúng cho phép tất cả các tập tin nhị phân với chứng chỉ đó chạy. Điều này rất hữu ích để tự động tin tưởng nội dung như các bản cập nhật hệ thống cùng với phần mềm đang được sử dụng phổ biến đến từ các nhà cung cấp có uy tín và đáng tin cậy. Tuy

nhân, kẻ tấn công có thể xâm phạm chứng chỉ ký mã của nhà cung cấp phần mềm và sử dụng chứng chỉ đó để ký phần mềm độc hại.



Mã hóa toàn đĩa

Mã hóa toàn đĩa (Full-disk encryption, FDE) là một yếu tố quan trọng trong mô hình bảo mật chuyên sâu về phòng thủ. Nó cung cấp sự bảo vệ khỏi một số hình thức tấn công vật lý. Các hệ thống có toàn bộ ổ cứng được mã hóa có khả năng chống lại hành vi trộm cắp dữ liệu. Chúng sẽ ngăn kẻ tấn công đánh cắp thông tin bí mật tiềm ẩn từ ổ cứng đã bị đánh cắp hoặc bị mất. Nếu không biết mật khẩu mã hóa hoặc có quyền truy cập vào khóa mã hóa, dữ liệu trên ổ cứng chỉ là những thứ vô nghĩa vô nghĩa. Đây là một cơ chế bảo mật rất quan trọng để triển khai cho nhiều thiết bị di động hơn như máy tính xách tay, điện thoại di động và máy tính bảng. Nhưng nó cũng được khuyến cáo cho máy tính để bàn và máy chủ. Vì mã hóa đĩa không chỉ cung cấp tính bảo mật mà còn là tính toàn vẹn. Điều này có nghĩa là kẻ tấn công có quyền truy cập vật lý vào hệ thống không thể thay thế các tập tin hệ thống bằng các tập tin độc hại hoặc cài đặt phần mềm độc hại. Đĩa được mã hóa hoàn toàn sẽ bảo vệ khỏi bị đánh cắp dữ liệu và giả mạo trái phép ngay cả khi kẻ tấn công có quyền truy cập vật lý vào đĩa.



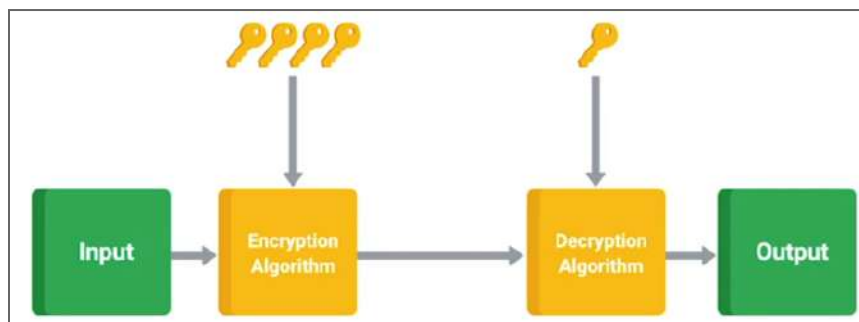
Để hệ thống có thể khởi động khi nó có thiết lập FDE, có một số tập tin quan trọng phải truy cập được. Chúng cần có sẵn trước khi đĩa chính có thể được mở khóa và quá trình khởi động có thể tiếp tục. Do đó, tất cả các thiết lập FDE đều có một phân vùng không được mã hóa trên đĩa, nơi chứa các tập tin khởi động quan trọng này. Ví dụ bao gồm những thứ như kernel và boot loader, rất quan trọng đối với hệ điều hành. Tuy nhiên, những tập tin này thực sự dễ bị thay thế bằng các tập tin độc hại tiềm ẩn đã được sửa đổi bởi kẻ tấn công có quyền truy cập vật lý. Mặc dù có thể xâm nhập một máy theo cách này, nhưng kẻ tấn công sẽ cần có phương pháp tấn công tinh vi và kiên trì để làm điều đó.



Để bảo vệ chống lại cuộc tấn công này, chúng ta có thể sử dụng giao thức khởi động an toàn, là một phần của kỹ thuật UEFI. Khởi động an toàn sử dụng

mã khóa công khai để bảo mật các thành phần của quá trình khởi động. Nó thực hiện điều này bằng cách tích hợp ký mã và xác minh các tập tin khởi động. Lúc bắt đầu, khởi động an toàn được cấu hình với khóa nền tảng, đây là khóa công khai tương ứng với khóa bí mật được sử dụng để ký các tập tin khởi động. Khóa nền tảng này được ghi vào chương trình cơ sở và được sử dụng tại thời điểm khởi động để xác minh chữ ký của các tập tin khởi động. Chỉ các tập tin được ký đúng và tin cậy mới được phép thực thi. Bằng cách này, khởi động an toàn bảo vệ khỏi sự giả mạo vật lý đối với phân vùng khởi động không được mã hóa. Có các giải pháp mã hóa toàn đĩa đến từ Microsoft và Apple được gọi là Bit Locker và FileVault2. Ngoài ra còn có một loạt các giải pháp mã nguồn mở và bên thứ ba. Trên Linux, gói dm-crypt rất phổ biến. Ngoài ra còn có các giải pháp từ PGP, TrueCrypt, VeraCrypt và rất nhiều giải pháp khác.

Các lược đồ mã hóa toàn đĩa dựa vào khóa bí mật cho các hoạt động mã hóa và giải mã. Chúng thường được bảo vệ bằng mật khẩu để truy cập vào khóa này. Nếu cần thay đổi khóa mã hóa, khóa người dùng có thể được hoán đổi mà không yêu cầu giải mã đầy đủ và mã hóa lại dữ liệu đang được bảo vệ. Khóa bảo vệ bằng mật khẩu hoạt động bằng cách yêu cầu cụm mật khẩu nhập của người dùng để mở khóa mã hóa. Sau đó, nó có thể được sử dụng để truy cập nội dung được bảo vệ trên đĩa. Trong nhiều trường hợp, mật khẩu này có thể giống với mật khẩu tài khoản người dùng để giữ mọi thứ đơn giản và giảm số lượng mật khẩu phải ghi nhớ.



Nếu cụm mật khẩu bị quên, thì nội dung của đĩa không thể khôi phục được. Đây là lý do tại sao nhiều giải pháp mã hóa đĩa có chức năng ký quỹ khóa. Ký quỹ khóa cho phép khóa mã hóa được lưu trữ an toàn ở một nơi để nhận lại về sau bởi một bên có thẩm quyền. Vì vậy, nếu ai đó quên cụm mật khẩu để mở khóa đĩa cho máy tính xách tay của họ, quản trị viên hệ thống có thể truy xuất

khóa ký quỹ hoặc cụm mật khẩu khôi phục để mở khóa đĩa. Nó thường là một cụm mật khẩu khóa riêng biệt có thể mở khóa đĩa bên cạnh cái của người dùng đang có. Điều này cho phép khôi phục nếu chúng ta quên mật khẩu.

Chúng ta cần phân biệt giữa mã hóa toàn đĩa với mã hóa dựa trên tập tin. Đó là nơi chỉ một số tập tin hoặc thư mục được mã hóa chứ không phải toàn bộ đĩa. Điều này thường được thực hiện dưới dạng mã hóa thư mục chính. Nó phục vụ một mục đích hơi khác so với FDE. Mã hóa tập tin hay thư mục chỉ đảm bảo tính bảo mật và tính toàn vẹn của các tập tin được bảo vệ bằng mã hóa. Các thiết lập này thường không mã hóa các tập tin hệ thống. Khi toàn bộ đĩa không được mã hóa, máy tính có thể khởi động từ xa mà không bị khóa. Nếu khởi động máy được mã hóa toàn đĩa, chúng ta phải nhập mật khẩu mở khóa đĩa trước khi máy khởi động xong. Vì vậy, mặc dù mã hóa dựa trên tập tin thuận tiện hơn một chút, nhưng nó ít được bảo vệ hơn trước các cuộc tấn công vật lý. Kẻ tấn công có thể sửa đổi hoặc thay thế các tập tin hệ thống và xâm phạm máy để có quyền truy cập vào dữ liệu được mã hóa.

3. Gia cố ứng dụng

Cập nhật phần mềm

Rất nhiều cuộc tấn công nhằm vào việc khai thác các lỗi trong phần mềm. Các loại lỗ hổng này có thể được sửa chữa thông qua các bản vá và cập nhật phần mềm. Các bản cập nhật phần mềm không chỉ cải thiện các sản phẩm phần mềm bằng cách thêm các tính năng mới, cải thiện hiệu suất và độ ổn định mà còn giải quyết các lỗ hổng bảo mật.

Hệ thống máy tính nên được kiểm tra, phân phối và xác minh các bản cập nhật phần mềm. Đây là một vấn đề phức tạp khi xem xét một tổ chức lớn với nhiều máy móc để quản lý chạy nhiều loại sản phẩm phần mềm. Đây là nơi mà các công cụ quản lý có thể giúp bạn tiếp cận công việc này dễ dàng hơn. Trên thực tế, các giải pháp như SCCM của Microsoft hoặc Puppet Labs và các công cụ khác cho phép quản trị viên có cái nhìn tổng quan về phần mềm nào được cài đặt trên nhiều hệ thống của họ. Điều này cho phép nhóm bảo mật phân tích phần mềm và phiên bản cụ thể nào được cài đặt, để hiểu rõ hơn về nguy cơ phần mềm dễ bị tấn công trong nhóm. Khi các bản cập nhật được phát hành và đẩy lên, các công cụ báo cáo này có thể giúp đảm bảo rằng các bản cập nhật

đã được áp dụng. SCCM thậm chí còn có khả năng buộc cài đặt các bản cập nhật sau khi đã qua một thời hạn nhất định.

Ngoài ra, cũng luôn có rủi ro rằng bản cập nhật phần mềm sẽ tạo ra một lỗi mới có thể ảnh hưởng đến chức năng của thiết bị hoặc nếu bản thân quá trình cập nhật sẽ gặp trục trặc và gây ra lỗi. Do đó, chúng ta cần có những giải pháp khắc phục để đảm bảo luôn cài đặt các bản vá quan trọng kịp thời.

Chính sách ứng dụng

Các chính sách ứng dụng (application policy) phục vụ hai mục đích. Chúng không chỉ xác định ranh giới của những ứng dụng được phép hay không, mà còn giúp hướng dẫn mọi người về cách sử dụng phần mềm an toàn hơn. Ví dụ như chính sách đảm bảo rằng phiên bản mới nhất của phần mềm đã được áp dụng. Chính sách không cài đặt hay sử dụng các phần mềm chia sẻ tập tin và phần mềm vi phạm bản quyền vì chúng có xu hướng liên quan đến việc lây nhiễm phần mềm độc hại. Trong trường hợp vẫn cần cài đặt các ứng dụng chia sẻ tập tin hay thậm chí trò chơi điện tử, nghĩa là những ứng dụng không phục vụ nghề nghiệp thì cần có chính sách rõ ràng tường minh về chúng.

Một lớp phần mềm mà chúng ta có thể muốn có các chính sách cụ thể là tiện ích mở rộng trong các trình duyệt. Vì hiện nay rất nhiều thao tác công việc chỉ tồn tại trong trình duyệt web, chúng đại diện cho một vectơ tiềm ẩn cho phần mềm độc hại thường bị bỏ qua. Các tiện ích mở rộng yêu cầu toàn quyền truy cập vào các trang web đã truy cập có thể gặp rủi ro vì nhà phát triển tiện ích mở rộng có quyền sửa đổi các trang đã truy cập. Một số tiện ích mở rộng thậm chí có thể gửi thông tin nhập vào của người dùng đến một máy chủ từ xa. Điều này có thể làm rò rỉ thông tin bí mật.



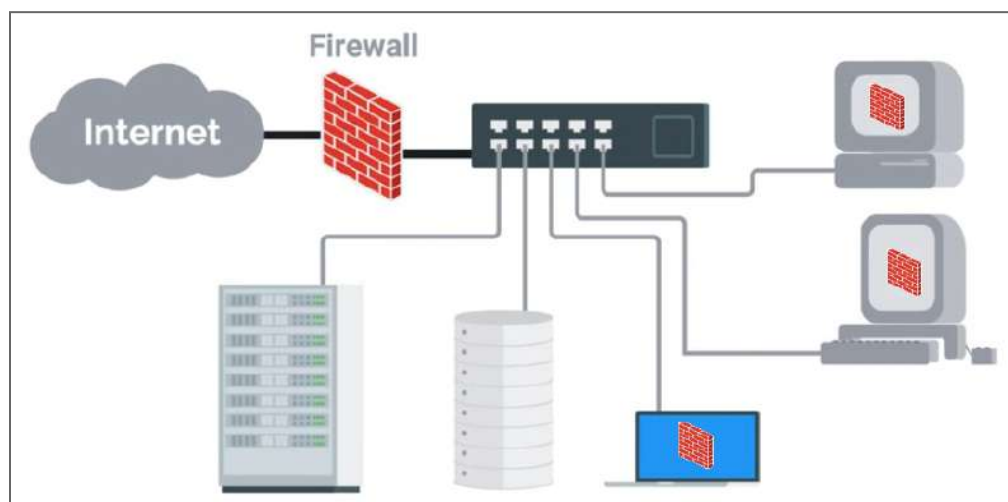
Bài đọc 7: Bảo Mật Trong Công Ty

1. Mục tiêu bảo mật

Bảo mật và năng suất là hai thứ luôn phải cân bằng. Khi chúng ta tăng cường bảo mật của hệ thống lên quá cao, chúng ta có thể đánh đổi năng suất của người dùng. Do đó, trước khi bắt đầu thiết kế một kiến trúc bảo mật, chúng ta cần xác định chính xác những gì muốn đạt được. Điều này sẽ phụ thuộc vào những gì công ty cho là quan trọng nhất. Chúng ta cũng cần biết liệu công ty có bất kỳ yêu cầu pháp lý nào khi nói đến bảo mật hay không. Chúng ta xem xét một ví dụ về các mục tiêu bảo mật được xác định rõ ràng. Một công ty cần xử lý các khoản thanh toán bằng thẻ tín dụng, do đó họ phải tuân theo PCI DSS, một tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán. PCI DSS được chia thành sáu mục tiêu lớn, mỗi mục tiêu có các yêu cầu cụ thể.



Mục tiêu đầu tiên là xây dựng và duy trì một mạng và hệ thống máy tính an toàn. Điều này bao gồm các yêu cầu về cài đặt và duy trì cấu hình tường lửa để bảo vệ dữ liệu của chủ thẻ và không sử dụng mật khẩu và các thông số bảo mật mặc định của nhà sản xuất. PCI DSS cũng cung cấp hướng dẫn cụ thể về những gì cấu hình tường lửa nên kiểm soát. Ví dụ: cấu hình tường lửa an toàn nên hạn chế kết nối giữa các mạng không đáng tin cậy và bất kỳ hệ thống nào trong môi trường dữ liệu của thẻ.



Mục tiêu thứ hai là bảo vệ dữ liệu của chủ thẻ. Trong mục tiêu này, yêu cầu đầu tiên là bảo vệ dữ liệu chủ thẻ được lưu trữ. Thứ hai là mã hóa việc truyền dữ liệu của chủ thẻ qua các mạng công cộng mở. PCI DSS cũng khuyến cáo nên sử dụng mật mã mạnh và đưa ra một số ví dụ. Nhưng không phải tất cả các yêu cầu đều mang tính chất kỹ thuật. Ví dụ, xem yêu cầu bảo vệ dữ liệu chủ thẻ được lưu trữ, nó có các yêu cầu đối với chính sách lưu giữ dữ liệu để đảm bảo rằng thông tin thanh toán nhạy cảm không được lưu trữ quá thời gian được yêu cầu. Sau khi thanh toán được ủy quyền, dữ liệu xác thực sẽ không cần thiết nữa và dữ liệu đó sẽ được xóa một cách an toàn. Điều này chứng tỏ các biện pháp bảo vệ an ninh tốt không chỉ về bản chất là kỹ thuật. Chúng cũng dựa trên các thủ tục và chính sách.

Mục tiêu thứ ba là duy trì một chương trình quản lý lỗ hổng bảo mật. Yêu cầu đầu tiên là bảo vệ tất cả các hệ thống chống lại phần mềm độc hại và thường xuyên cập nhật phần mềm hoặc chương trình chống vi-rút. Thứ hai là phát triển và duy trì các hệ thống và ứng dụng an toàn. PCI DSS sẽ đề cập đến những thứ như đảm bảo tất cả các hệ thống đều được cài đặt phần mềm chống vi-rút và đảm bảo phần mềm này được cập nhật. Nó cũng yêu cầu hoạt động quét được chạy thường xuyên và nhật ký được duy trì. Ngoài ra còn có các yêu cầu để đảm bảo hệ thống và phần mềm được bảo vệ khỏi các lỗ hổng bảo mật đã biết bằng cách áp dụng các bản vá bảo mật ít nhất một tháng kể từ khi phát hành bản vá bảo mật. Việc sử dụng cơ sở dữ liệu lỗ hổng bảo mật của bên thứ ba cũng được liệt kê để giúp xác định các lỗ hổng đã biết trong các hệ thống được quản lý.

Mục tiêu thứ tư là thực hiện các biện pháp kiểm soát truy cập mạnh mẽ. Mục tiêu này có ba yêu cầu. Đầu tiên là hạn chế quyền truy cập vào dữ liệu chủ thẻ. Thứ hai là xác định và xác thực quyền truy cập vào các thành phần hệ thống. Và thứ ba là hạn chế quyền truy cập vật lý vào dữ liệu chủ thẻ. Mục tiêu đầu tiên, hạn chế quyền truy cập vào dữ liệu, có nghĩa là bất kỳ dữ liệu nhạy cảm nào đều phải được hướng dẫn đến các chính sách truy cập dữ liệu để đảm bảo rằng dữ liệu khách hàng không bị lạm dụng. Một phần của yêu cầu này là thực thi xác thực mật khẩu để truy cập hệ thống và xác thực hai yếu tố để truy cập từ xa, đó là yêu cầu tối thiểu. Một phần quan trọng khác được đánh dấu bởi các yêu cầu PCI DSS là kiểm soát truy cập đối với truy cập vật lý. Đây là một khía cạnh bảo mật quan trọng cần lưu ý vì chúng ta cần bảo vệ hệ thống và dữ liệu khỏi cả hành vi trộm cắp vật lý và các cuộc tấn công ảo.



Mục tiêu thứ năm là thường xuyên theo dõi và kiểm tra mạng lưới. Yêu cầu đầu tiên là theo dõi và giám sát tất cả các truy cập vào tài nguyên mạng và dữ liệu của chủ thẻ. Thứ hai là thường xuyên kiểm tra các hệ thống và quy trình bảo mật. Yêu cầu về giám sát và kiểm tra mạng là một phần thiết yếu khác của một kế hoạch bảo mật tốt. Điều này đề cập đến những thứ như thiết lập và cấu hình hệ thống phát hiện xâm nhập và tiến hành quét lỗ hổng của mạng. Kiểm tra khả năng phòng thủ là một phần siêu quan trọng khác của việc này. Thực sự hữu ích khi kiểm tra các hệ thống phòng thủ thường xuyên để đảm bảo rằng chúng cung cấp sự bảo vệ mà chúng ta muốn. Nó cũng đảm bảo rằng các hệ thống cảnh báo đang hoạt động.

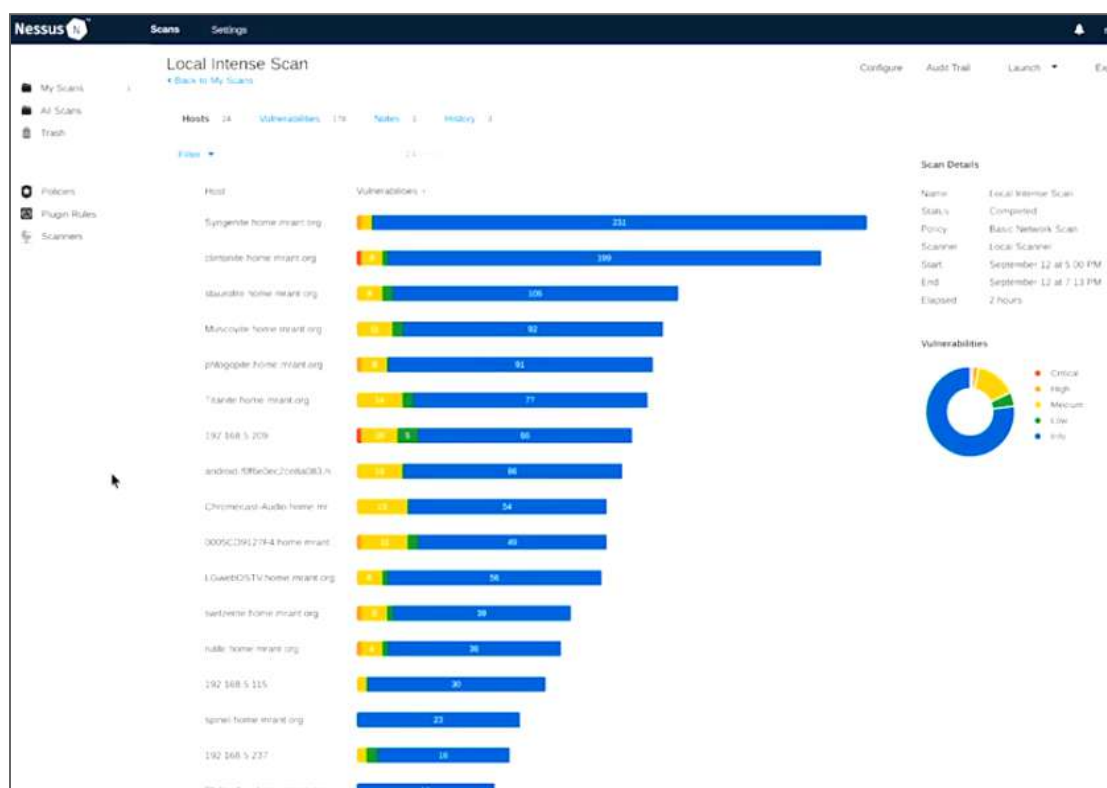
Mục tiêu thứ sáu và cuối cùng là duy trì chính sách bảo mật thông tin. Nó chỉ có một yêu cầu duy nhất là duy trì một chính sách để cập đến vấn đề bảo mật thông tin cho tất cả nhân viên. Yêu cầu này giải quyết lý do tại sao chúng ta cần có các chính sách bảo mật được thiết lập tốt. Chúng giúp quản lý và điều chỉnh hành vi của người dùng khi nói đến các khía cạnh bảo mật thông tin. Điều quan trọng cần lưu ý là yêu cầu này đề cập rằng chính sách phải dành cho tất cả nhân

sự. Trách nhiệm bảo mật thông tin không chỉ thuộc về các nhóm bảo mật. Mọi thành viên của tổ chức đều có trách nhiệm bảo mật thông tin. Các chính sách bảo mật được thiết kế tốt giải quyết các câu hỏi hoặc trường hợp sử dụng phổ biến nhất mà người dùng sẽ có dựa trên các chi tiết cụ thể của tổ chức. Mọi người sử dụng hệ thống đều có thể liên quan đến vấn đề an ninh. Họ có thể không cố ý, nhưng họ có thể làm giảm tính bảo mật tổng thể bởi các hành động của họ. Đó là lý do tại sao việc áp dụng các chính sách bảo mật được cân nhắc kỹ lưỡng cũng cần phải dễ tìm và dễ đọc.

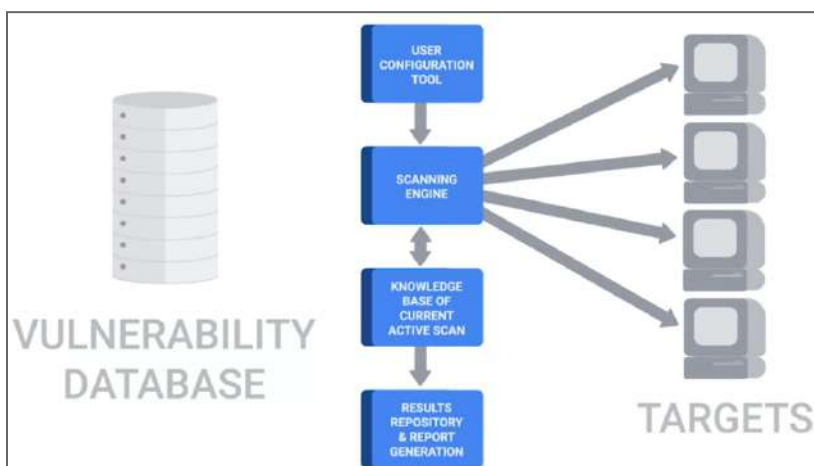
Rủi ro bảo mật (security risk) là tất cả về việc xác định rủi ro hoặc khả năng xảy ra các cuộc tấn công và thiết kế các biện pháp phòng thủ xung quanh những rủi ro này để giảm thiểu tác động của một cuộc tấn công. Đánh giá rủi ro bảo mật bắt đầu với mô hình hóa mối đe dọa. Đầu tiên, chúng ta xác định các mối đe dọa có thể xảy ra đối với hệ thống của mình, sau đó gán độ ưu tiên tương ứng với mức độ nghiêm trọng và xác suất xảy ra. Chúng ta làm điều này bằng cách suy nghĩ từ góc độ của một kẻ tấn công bên ngoài, đặt mình vào vị trí của tin tặc. Nó hữu ích để bắt đầu bằng cách tìm ra mục tiêu có giá trị cao mà kẻ tấn công có thể muốn theo đuổi. Từ đó, các vectơ tấn công thường nhằm vào các tài sản có giá trị cao. Dữ liệu có giá trị cao thường bao gồm thông tin tài khoản, như tên người dùng và mật khẩu, cơ sở dữ liệu xác thực. Thông thường, bất kỳ loại dữ liệu người dùng nào đều được coi là có giá trị cao, đặc biệt nếu có liên quan đến việc xử lý thanh toán.

2. Quét lỗ hổng bảo mật

Một phần khác của đo lường rủi ro là hiểu được các lỗ hổng bảo mật trên hệ thống và mạng máy tính. Một cách để tìm ra những điều này là thực hiện quét lỗ hổng bảo mật thường xuyên. Quét lỗ hổng là quá trình tìm các lỗ hổng bảo mật có thể có trong hệ thống. Có rất nhiều giải pháp mã nguồn mở và thương mại. Chúng có thể được cấu hình để thực hiện quét tự động theo lịch trình của các hệ thống hoặc mạng được chỉ định để tìm kiếm các lỗ hổng. Sau đó, chúng tạo một báo cáo. Một số công cụ trong số này như Nessus, OpenVas và Qualys.



Công cụ quét lỗ hổng bảo mật là các dịch vụ chạy trên hệ thống trong tầm kiểm soát của chúng ta, thực hiện quét định kỳ các mạng. Sau đó, dịch vụ sẽ tiến hành quét để tìm và phát hiện ra các máy tính trên mạng. Khi các máy tính được tìm thấy thông qua quét ping hoặc quét cổng, các bản quét chi tiết hơn sẽ được thực hiện với các lần quét máy tính được phát hiện. Quá trình quét các cổng chung hoặc tất cả các cổng hợp lệ có thể được thực hiện dựa trên các máy tính đã phát hiện để xác định dịch vụ nào đang lắng nghe. Các dịch vụ này sau đó sẽ được kiểm tra để cố gắng khám phá thêm thông tin về loại dịch vụ và phiên bản đang nghe trên cổng liên quan. Thông tin này sau đó có thể được kiểm tra dựa trên cơ sở dữ liệu về các lỗ hổng đã biết. Nếu một phiên bản dịch vụ dễ bị tấn công được phát hiện, máy quét sẽ thêm nó vào báo cáo. Sau khi quá trình quét kết thúc, các lỗ hổng được phát hiện và máy tính được tổng hợp trong một báo cáo, theo cách đó và các nhà phân tích có thể nhanh chóng và dễ dàng xem các khu vực có vấn đề nằm ở đâu trên mạng.



Các lỗ hổng được tìm thấy được ưu tiên theo mức độ nghiêm trọng và phân loại khác. Mức độ nghiêm trọng có tính đến một số thứ, như khả năng bị khai thác lỗ hổng bảo mật. Nó cũng xem xét loại truy cập mà lỗ hổng sẽ cung cấp cho kẻ tấn công và liệu nó có thể bị khai thác từ xa hay không. Các lỗ hổng và báo cáo sẽ có các liên kết đến thông tin chi tiết và tiết lộ về lỗ hổng. Trong một số trường hợp, nó cũng sẽ có các hướng dẫn về cách thoát khỏi nó. Máy quét lỗ hổng bảo mật sẽ phát hiện ra rất nhiều thứ, từ các dịch vụ được định cấu hình sai dẫn đến rủi ro tiềm ẩn, đến phát hiện sự hiện diện của các cửa sau và hệ thống. Điều quan trọng cần nói là tính năng quét lỗ hổng chỉ có thể phát hiện các lỗ hổng cũng như cấu hình không an toàn đã biết và đã lộ diện. Đó là lý do tại sao cần tiến hành quét lỗ hổng bảo mật tự động thường xuyên. Chúng ta cũng cần phải cập nhật cơ sở dữ liệu về lỗ hổng bảo mật để đảm bảo các lỗ hổng mới được phát hiện nhanh chóng.

Quét lỗ hổng bảo mật không phải là cách duy nhất để kiểm tra khả năng phòng thủ. Thực hiện các bài kiểm tra thâm nhập (penetration test) thường xuyên cũng thực sự được khuyến khích để kiểm tra khả năng phòng thủ nhiều hơn. Các thử nghiệm này cũng sẽ đảm bảo hệ thống phát hiện và cảnh báo vẫn đang hoạt động bình thường. Kiểm tra thâm nhập là cố gắng đột nhập vào hệ thống hoặc mạng để kiểm tra tính an toàn của nó. Nó giống như chúng ta đóng vai một kẻ xấu, chỉ để kiểm tra hệ thống. Qua đó, chúng ta đặt suy nghĩ của mình như một kẻ tấn công và sử dụng các công cụ và kỹ thuật giống như chúng. Kết quả của các báo cáo thử nghiệm thâm nhập cũng sẽ cho chúng ta thấy, đâu là điểm yếu hoặc điểm mù tồn tại. Các bài kiểm tra này giúp cải thiện khả năng phòng thủ và hướng dẫn các dự án bảo mật trong tương lai. Chúng có

thể được tiến hành bởi các thành viên trong đội an ninh nội bộ. Nếu nhóm nội bộ của chúng ta không có đủ nguồn lực cho bài kiểm tra này, chúng ta có thể thuê một công ty bên thứ ba cung cấp dịch vụ thử nghiệm thâm nhập. Chúng ta thậm chí có thể làm cả hai. Điều đó sẽ giúp chúng ta có thêm cái nhìn về hệ thống phòng thủ của mình.

3. Quyền riêng tư

Chính sách quyền riêng tư

Khi chúng ta đang hỗ trợ các hệ thống xử lý dữ liệu khách hàng, điều tối quan trọng là phải bảo vệ dữ liệu đó khỏi bị truy cập trái phép và không phù hợp. Nó không chỉ để bảo vệ khỏi các mối đe dọa bên ngoài, nó còn bảo vệ dữ liệu đó chống lại việc nhân viên sử dụng sai mục đích. Chính sách quyền riêng tư (privacy policy) giám sát việc truy cập và sử dụng dữ liệu nhạy cảm. Nó cũng xác định những gì thích hợp và cho phép sử dụng, và những quy định hoặc hạn chế nào được áp dụng khi nói đến cách dữ liệu được sử dụng. Lưu ý rằng mọi người có thể không xem xét các tác động bảo mật của các hành động của họ, vì vậy cả chính sách quyền riêng tư và quyền truy cập dữ liệu đều quan trọng trong việc hướng dẫn và thông báo cho mọi người cách duy trì bảo mật trong khi xử lý dữ liệu nhạy cảm.

Các chính sách bảo mật được xác định và thiết lập tốt là một phần quan trọng của quá trình thi hành tốt về quyền riêng tư. Nhưng chúng ta cũng cần một cách để thực thi các chính sách này. Kiểm tra định kỳ đối với các trường hợp dữ liệu nhạy cảm bị truy cập có thể đưa chúng ta đến đó. Điều này đã được kích hoạt bởi hệ thống ghi nhật ký và giám sát. Việc kiểm tra nhật ký truy cập dữ liệu là cực kỳ quan trọng, nó giúp chúng ta đảm bảo rằng dữ liệu nhạy cảm chỉ được truy cập bởi những người được phép truy cập và họ sử dụng dữ liệu đó đúng lý do. Cách thực hiện tốt là áp dụng nguyên tắc ít đặc quyền nhất, nghĩa là không cho phép truy cập vào loại dữ liệu này theo mặc định. Chúng ta nên yêu cầu bất kỳ ai cần quyền truy cập trước tiên phải đưa ra yêu cầu truy cập kèm theo lý do để lấy dữ liệu. Nhưng nó không thể chỉ là các yêu cầu truy cập mơ hồ hoặc chung chung, họ phải chỉ định dữ liệu nào họ cần truy cập. Thông thường, loại yêu cầu này cũng sẽ có giới hạn thời gian. Bằng cách đó, chúng ta có thể đảm bảo rằng quyền truy cập dữ liệu chỉ được phép vì lý do kinh doanh hợp pháp, điều này làm giảm khả năng truy cập hoặc sử dụng dữ liệu không phù hợp. Bất

kỳ quyền truy cập nào không có yêu cầu tương ứng sẽ bị gắn cờ là vi phạm tiềm ẩn với mức độ ưu tiên cao cần được điều tra càng sớm càng tốt.

Chính sách xử lý dữ liệu

Các chính sách của công ty đóng vai trò là hướng dẫn trong các nguồn thông tin về cách thức như thế nào được, và như thế nào không được truy cập và xử lý dữ liệu. Chúng đều quan trọng như nhau. Các chính sách sẽ bao gồm từ xử lý dữ liệu nhạy cảm đến dữ liệu có thể công bố công khai. Các chính sách xử lý dữ liệu phải bao gồm các chi tiết về cách các dữ liệu khác nhau được phân loại. Điều gì làm cho một số dữ liệu nhạy cảm thay vì không nhạy cảm? Dữ liệu bí mật được coi là gì? Khi các lớp dữ liệu khác nhau được xác định, chúng ta nên tạo các hướng dẫn về cách xử lý các loại dữ liệu khác nhau này. Nếu thứ gì đó được coi là nhạy cảm hoặc bí mật, chúng ta có thể có quy định rằng dữ liệu này không được lưu trữ trên các phương tiện dễ bị mất hoặc bị đánh cắp, như USB, CD hoặc ổ cứng di động. Các thiết bị này thường được sử dụng mà không có bất kỳ mã hóa nào. Hãy tưởng tượng nếu một nhân viên bị mất ổ cứng di động không được mã hóa chứa đầy thông tin khách hàng thì thật là thảm họa. Đó chính xác là tình huống mà chính sách truy cập dữ liệu cố gắng tránh. Cũng có thể hợp lý khi đưa máy tính xách tay và thiết bị di động vào loại phương tiện rất dễ bị mất hoặc bị đánh cắp. Việc đưa ra các khuyến cáo về cách xử lý tình huống một cách an toàn sẽ giúp ích cho chúng ta như đưa ra một giải pháp mã hóa thích hợp, cung cấp hướng dẫn và hỗ trợ về việc sử dụng nó.

4. Người dùng

Thói quen người dùng

Chúng ta có thể xây dựng hệ thống bảo mật tốt nhất thế giới, nhưng chúng sẽ không bảo vệ chúng ta nếu người dùng đang thực hành bảo mật không an toàn. Người dùng được xem là mắt xích yếu nhất trong hệ thống bảo mật. Do đó, chúng ta cần phải nhắc nhở người dùng khi nói đến bảo mật. Nó siêu quan trọng và có vẻ hiển nhiên, nhưng nó thường bị bỏ qua. Nếu người dùng viết mật khẩu của họ trên một ứng dụng ghi chú, dán nó vào màn hình chính của máy tính xách tay, sau đó để máy tính xách tay mở khóa và không có người giám sát tại một quán cà phê, chúng ta có thể gặp phải thảm họa. Nhưng việc đảm bảo rằng người dùng thực hiện các biện pháp phòng ngừa bảo mật hợp lý sẽ tốn

nhieu công sức và có thể thực sự khó khăn. Chúng ta phải đảm bảo rằng người dùng có thói quen và hành động liên quan đến chính sách bảo mật. Tuy nhiên, chúng ta có thể làm nhiều hơn thế để đảm bảo rằng người dùng của mình luôn siêng năng duy trì bảo mật.

Giả sử rằng nhân viên của chúng ta luôn hành động với mục đích tốt, việc rò rỉ và tiết lộ là do vô ý. Có thể tránh được rò rỉ và tiết lộ bằng cách hiểu nhân viên cần gì để hoàn thành công việc của họ. Chúng ta cũng cần đảm bảo rằng họ có các công cụ phù hợp để hoàn thành công việc mà không ảnh hưởng đến bảo mật. Ví dụ, nếu một nhân viên cần chia sẻ tập tin bí mật với đối tác bên ngoài và nó quá lớn để gửi qua email, họ có thể phải tải tập tin đó lên trang web chia sẻ tập tin của bên thứ ba mà họ có tài khoản cá nhân. Đây là một hành động đầy rủi ro. Chúng ta không bao giờ được tải thông tin bí mật lên dịch vụ của bên thứ ba mà công ty chưa đánh giá. Nếu chia sẻ tập tin lớn với các đối tác bên ngoài là hoạt động phổ biến, thì tốt nhất chúng ta nên tìm một giải pháp đáp ứng nhu cầu mà vẫn đảm bảo các nguyên tắc bảo mật. Bằng cách này, người dùng ít có khả năng để tổ chức gặp rủi ro không cần thiết.

Một vấn đề khác liên quan đến người dùng là họ có thể lừa dối về những thứ bảo mật. Họ không thích ghi nhớ những mật khẩu dài phức tạp, nhưng điều này cực kỳ quan trọng để giữ an toàn cho công ty. Vậy chúng ta phải làm thế nào để giải quyết mâu thuẫn này. Nếu chúng ta yêu cầu mật khẩu 20 ký tự phải được thay đổi ba tháng một lần, người dùng gần như chắc chắn sẽ viết chúng ra. Điều này làm ảnh hưởng đến tính bảo mật mà chính sách mật khẩu phức tạp đã đề ra. Điều quan trọng là phải hiểu các chính sách mật khẩu phải bảo vệ chống lại những mối đe dọa nào, bằng cách đó, chúng ta có thể cố gắng tìm ra sự cân bằng tốt hơn giữa bảo mật và khả năng sử dụng. Yêu cầu mật khẩu dài và phức tạp được thiết kế để bảo vệ chống lại các cuộc tấn công vét cạn, tấn công hệ thống xác thực, hoặc nếu cơ sở dữ liệu mật khẩu bị đánh cắp. Vì các cuộc tấn công vét cạn trực tiếp chống lại cơ sở hạ tầng xác thực nên dễ dàng bị phát hiện và chặn bởi các hệ thống phòng chống xâm nhập, chúng có thể được coi là rủi ro khá thấp. Nhưng việc đánh cắp cơ sở dữ liệu mật khẩu sẽ là một vi phạm siêu nghiêm trọng. Chúng ta có rất nhiều lớp bảo mật bổ sung để ngăn chặn một xâm nhập nghiêm trọng như vậy xảy ra ngay từ đầu. Vì vậy, hai cuộc tấn công mà mật khẩu phức tạp chủ yếu được thiết kế để bảo vệ chống lại, có nguy cơ khá thấp. Bây giờ, chúng ta có thể nới lỏng các yêu cầu

mật khẩu một chút và không yêu cầu những mật khẩu quá dài. Chúng ta thậm chí có thể điều chỉnh khoảng thời gian cập nhật mật khẩu bắt buộc.

Sử dụng lại mật khẩu là một hành vi phổ biến khác của người dùng. Mọi người không muốn ghi nhớ nhiều mật khẩu, nhiều người dùng thấy dễ dàng hơn khi sử dụng cùng một mật khẩu, cho cả tài khoản email cá nhân và tài khoản công việc của họ. Nhưng điều này làm suy yếu tính bảo mật của mật khẩu công việc của họ. Nếu một dịch vụ trực tuyến bị xâm nhập và cơ sở dữ liệu mật khẩu bị rò rỉ, họ sẽ gặp rắc rối. Mật khẩu trong cơ sở dữ liệu đó sẽ tìm đường vào các tập tin mật khẩu được sử dụng để bẻ khóa mật khẩu và tấn công vét cạn. Một khi mật khẩu không phải là bí mật, nó sẽ không được sử dụng nữa. Khả năng một kẻ xấu có thể sử dụng mật khẩu là quá cao. Đó là lý do tại sao điều quan trọng là đảm bảo nhân viên sử dụng mật khẩu mới và duy nhất, đồng thời không sử dụng lại chúng từ các dịch vụ khác. Ngoài ra, cũng cần có hệ thống kiểm tra các mật khẩu cũ để ngăn người dùng thay đổi mật khẩu của họ trở lại mật khẩu có khả năng bị xâm phạm đã sử dụng trước đó.

Một rủi ro lớn hơn nhiều ở nơi làm việc mà người dùng nên được huấn luyện là đánh cắp thông tin xác thực từ các email lừa đảo. Email lừa đảo khá hiệu quả. Nó lợi dụng khuynh hướng của mọi người mở email mà không cần xem xét chúng kỹ. Nếu một email xác thực dẫn đến một trang đăng nhập giả mạo, người dùng có thể nhập thông tin đăng nhập của họ vào trang web giả mạo một cách mù quáng và tiết lộ thông tin đăng nhập của họ cho kẻ tấn công. Mặc dù xác thực hai yếu tố giúp bảo vệ chống lại kiểu tấn công này, nhưng các giải pháp hai yếu tố dựa trên OTP vẫn có khả năng bị tấn công.

Nếu ai đó đã nhập mật khẩu của họ vào một trang web lừa đảo hoặc thậm chí nghi ngờ họ đã làm vậy, điều quan trọng là phải thay đổi mật khẩu càng sớm càng tốt. Nếu có thể, tổ chức nên cố gắng phát hiện những loại tiết lộ mật khẩu này bằng cách sử dụng các công cụ như cảnh báo mật khẩu. Đây là một tiện ích mở rộng của Chrome từ Google có thể phát hiện khi chúng ta nhập mật khẩu của mình vào một trang web không phải là trang của Google. Có thể phát hiện khi mật khẩu được nhập vào một trang web có khả năng không đáng tin cậy, cho phép một tổ chức phát hiện các tấn công lừa đảo tiềm ẩn.

Bảo mật bên thứ ba

Đôi khi, chúng ta cần phải dựa vào các giải pháp của bên thứ ba hoặc các nhà cung cấp dịch vụ vì chúng ta không thực hiện được mọi thứ. Trong trường hợp này, bên thứ ba sẽ có nhiều dữ liệu hoặc quyền truy cập đến dữ liệu nhạy cảm. Vì vậy, làm thế nào không phải đối mặt với vô số rủi ro không cần thiết? Điều quan trọng là phải thuê các nhà cung cấp đáng tin cậy và có uy tín bất cứ khi nào có thể. Chúng ta cũng cần quản lý các cam kết một cách có kiểm soát. Điều này liên quan đến việc thực hiện đánh giá rủi ro của nhà cung cấp hoặc đánh giá bảo mật.

Trong đánh giá bảo mật nhà cung cấp, chúng ta yêu cầu nhà cung cấp hoàn thành bảng câu hỏi bao gồm các khía cạnh khác nhau của các thủ tục và biện pháp bảo vệ chính sách bảo mật của họ. Bảng câu hỏi được thiết kế để xác định xem họ có triển khai các thiết kế bảo mật tốt trong tổ chức của họ hay không. Đối với các dịch vụ phần mềm hoặc nhà cung cấp phần cứng, chúng ta cũng có thể yêu cầu kiểm tra phần mềm/phần cứng. Bằng cách này, chúng ta có thể đánh giá các lỗ hổng bảo mật tiềm ẩn hoặc các mối quan tâm trước khi quyết định ký hợp đồng với dịch vụ của họ. Điều quan trọng là phải hiểu các đối tác kinh doanh của bạn được bảo vệ tốt như thế nào trước khi quyết định làm việc với họ. Nếu họ có các biện pháp bảo mật kém, bảo mật của tổ chức chúng ta có thể gặp rủi ro.

Mặc dù mô hình bảng câu hỏi là một cách nhanh chóng để đánh giá bên thứ ba, nhưng nó không phải là lý tưởng. Nó phụ thuộc vào việc tự báo cáo các thực thi, điều này không đáng tin cậy. Không có cách nào để chứng minh những gì được nêu trong bảng câu hỏi, chúng ta chỉ tin tưởng rằng công ty đang trả lời một cách trung thực. Mặc dù chúng ta hy vọng rằng một công ty bạn đang kinh doanh sẽ trung thực, nhưng tốt nhất là chúng ta nên xác minh. Nếu chúng ta có thể, hãy yêu cầu báo cáo đánh giá bảo mật của bên thứ ba. Một số thông tin trên bảng câu hỏi có thể được xác minh, chẳng hạn như kết quả đánh giá bảo mật của bên thứ ba và báo cáo kiểm tra thâm nhập. Trong trường hợp là phần mềm của bên thứ ba, chúng ta có thể tiến hành một số đánh giá và kiểm tra lỗ hổng cơ bản để đảm bảo sản phẩm có một số bảo mật hợp lý. Nếu dịch vụ của bên thứ ba liên quan đến việc lắp đặt bất kỳ thiết bị cơ sở hạ tầng nào trên trang web, hãy chú ý đến cách họ thực hiện. Bạn phải đảm bảo thiết bị này được quản lý theo cách không ảnh hưởng tiêu cực đến an ninh tổng thể. Giả sử,

công ty cung cấp yêu cầu quyền truy cập từ xa vào thiết bị cơ sở hạ tầng để thực hiện bảo trì. Nếu đúng như vậy, hãy thực hiện các điều chỉnh thích hợp đối với các quy tắc tường lửa để hạn chế quyền truy cập này. Bằng cách đó, bạn sẽ đảm bảo rằng nó không thể được sử dụng như một điểm vào mạng của bạn. Việc giám sát bổ sung cũng sẽ được khuyến cáo cho thiết bị của bên thứ ba này vì nó đại diện cho một bề mặt tấn công tiềm năng mới trong mạng của bạn. Nếu nhà cung cấp cho phép bạn, hãy đánh giá phần cứng trong môi trường phòng thí nghiệm trước. Tại đó, bạn có thể chạy các đánh giá chuyên sâu về lỗ hổng bảo mật và kiểm tra khả năng thâm nhập của phần cứng và đảm bảo rằng không có bất kỳ lỗ hổng rõ ràng nào trong sản phẩm. Báo cáo phát hiện của chúng ta cho nhà cung cấp và yêu cầu họ giải quyết bất kỳ vấn đề nào được phát hiện.

Văn hóa bảo mật

Không thể có các phương pháp bảo mật tốt tại công ty nếu nhân viên và người dùng không được huấn luyện tốt. Điều này sẽ thúc đẩy văn hóa công ty lành mạnh và thái độ tổng thể đối với bảo mật. Một môi trường làm việc khuyến khích mọi người lên tiếng khi họ cảm thấy có điều gì đó không ổn là điều cần thiết, nó khuyến khích họ làm điều đúng đắn. Để giúp tạo ra bối cảnh này, điều quan trọng là nhân viên phải có cách để họ có thể đặt câu hỏi khi họ thắc mắc. Đây có thể là hộp thư nơi người dùng có thể đặt câu hỏi về các mối quan tâm về bảo mật hoặc báo cáo những điều họ nghi ngờ là rủi ro bảo mật. Có kênh giao tiếp được chỉ định để mọi người có thể cảm thấy thoải mái khi đặt câu hỏi và nhận lại câu trả lời rõ ràng là điều cực kỳ quan trọng. Giúp người khác lưu ý đến vấn đề bảo mật sẽ giúp giảm bớt gánh nặng bảo mật mà chúng ta gặp phải. Nó cũng sẽ làm cho an ninh tổng thể của tổ chức tốt hơn. Tạo ra một nền văn hóa ưu tiên bảo mật không phải là điều dễ dàng. Chúng ta phải củng cố và khen thưởng những hành động giúp tăng cường an ninh cho tổ chức.

Nhưng xây dựng một nền văn hóa bao gồm các nguyên tắc bảo mật không phải lúc nào cũng đủ. Có một số điều mà tất cả nhân viên nên biết. Đó là lúc một khóa đào tạo bảo mật không thường xuyên. Cũng có thể là một đoạn video ngắn hoặc bản trình bày, sau đó là câu hỏi để xem liệu nhân viên có hiểu các khái niệm chính được đề cập trong khóa đào tạo hay không. Yêu cầu nhân viên thực hiện lại khóa đào tạo mỗi năm một lần hoặc lâu hơn, đảm bảo rằng mọi người được cập nhật về khóa đào tạo của họ. Chúng ta cũng có thể đưa các

khái niệm mới vào để cập nhật các chính sách khi cần thiết. Loại hình đào tạo này nên bao gồm các kiểu tấn công phổ biến nhất và cách tránh trở thành nạn nhân của chúng. Điều này bao gồm những thứ như email lừa đảo và các cách thức tốt về việc sử dụng mật khẩu. Các khóa đào tạo này thường bao gồm các tình huống có thể giúp kiểm tra sự hiểu biết của người dùng về một chủ đề cụ thể. Các khóa đào tạo như thế này sẽ là tuyến phòng thủ cuối cùng mà chúng ta và công ty cần phải có để đảm bảo chúng ta được an toàn nhất có thể, càng lâu càng tốt.

5. Xử lý và khắc phục sự cố

Phản ứng với sự cố

Chúng ta cố gắng hết sức để bảo vệ hệ thống và mạng máy tính của mình. Nhưng rất có thể một sự cố nào đó sẽ xảy ra. Đây có thể là bất cứ điều gì từ việc xâm nhập toàn bộ hệ thống và đánh cắp dữ liệu, cho đến ai đó vô tình làm rò rỉ bản ghi nhớ. Bất kể bản chất của sự việc là gì, việc xử lý sự cố thích hợp là rất quan trọng để hiểu chính xác những gì đã xảy ra, nó đã xảy ra như thế nào, khắc phục nó ra sao và làm thế nào để tránh nó xảy ra lần nữa.

Xử lý sự cố

Bước đầu tiên của việc xử lý một sự cố là phát hiện nó ngay từ đầu. Hy vọng rằng, các hệ thống phát hiện xâm nhập của chúng ta đã nắm bắt được các dấu hiệu cho thấy một cuộc tấn công đang diễn ra và cảnh báo cho chúng ta về mối đe dọa. Sự cố cũng có thể được chú ý theo những cách khác. Một nhân viên có thể đã nhận thấy điều gì đó đáng ngờ và báo cho đội an ninh để điều tra, hoặc có thể họ đã làm rò rỉ thông tin.

Bước tiếp theo là phân tích nó và xác định ảnh hưởng và phạm vi thiệt hại. Đó có phải là một rò rỉ dữ liệu? Hay công bố thông tin? Nếu vậy, thông tin nào được đưa ra ngoài? Thực hư ra sao? Hệ thống có bị xâm phạm không? Những hệ thống nào? Và họ đã quản lý để có được cấp độ truy cập nào? Nó có phải là một sự lây nhiễm phần mềm độc hại, những hệ thống nào đã bị nhiễm? Một số cuộc tấn công thực sự rõ ràng với các dấu hiệu xâm nhập rất rõ ràng như trang web bị phá hoại hoặc quá trình bất thường tiêu thụ tất cả tài nguyên trong hệ thống. Những thứ khác có thể tinh vi hơn và hầu như không thể bị phát hiện, chẳng hạn như một thay đổi nhỏ đối với một tập tin cấu hình hệ thống. Đây là lý

do tại sao việc giám sát tốt là rất quan trọng cùng với việc hiểu biết cơ sở của chúng ta. Sau khi chúng ta tìm ra luồng truy cập bình thường trên mạng của mình và những dịch vụ mong đợi sẽ thấy, các ngoại lệ sẽ dễ dàng phát hiện hơn. Điều này rất quan trọng vì mọi sự dẫn dắt sai mà nhóm ứng phó sự cố phải điều tra đều có nghĩa là thời gian và nguồn lực bị lãng phí. Điều này có khả năng cho phép các cuộc xâm nhập thực sự không bị phát hiện và không bị điều tra lâu hơn.

Trong quá trình phát hiện và xác định phạm vi, dữ liệu tương quan từ các hệ thống khác nhau có thể tiết lộ bức tranh lớn hơn nhiều về những gì đã xảy ra. Nó có thể hiển thị cách kẻ xâm nhập có được quyền truy cập. Ví dụ: chúng ta có thể thấy một sự kiện kết nối được tường lửa ghi lại từ một địa chỉ IP đáng ngờ, việc tìm kiếm các sự kiện khác liên quan đến địa chỉ IP này có thể tiết lộ các nỗ lực ghi nhật ký và nhật ký xác thực cho hệ thống. Điều này sẽ cung cấp thông tin chi tiết về nơi mà kẻ tấn công đến và những gì chúng đã cố gắng thực hiện trên mạng. Nhật ký xác thực cũng sẽ cho biết chúng có thể đăng nhập thành công vào tài khoản hay không. Nếu vậy, điều đó cho chúng ta biết tài khoản nào bị xâm phạm.

Khi phạm vi của sự cố được xác định, bước tiếp theo là ngăn chặn. Chúng ta cần phải ngăn chặn vi phạm để ngăn thiệt hại thêm. Đối với các trường hợp xâm phạm hệ thống và lây nhiễm phần mềm độc hại, đây là một bước khá nhạy cảm. Chúng ta không muốn phần mềm độc hại hoặc kẻ tấn công sử dụng một máy bị xâm nhập để chuyển sang các máy khác trong mạng. Điều này có thể mở rộng phạm vi tỷ lệ và gây ra nhiều thiệt hại hơn. Các chiến lược ngăn chặn sẽ khác nhau tùy thuộc vào bản chất của vụ việc. Nếu tài khoản bị xâm phạm, hãy thay đổi mật khẩu ngay lập tức. Nếu chủ sở hữu không thể thay đổi mật khẩu ngay lập tức, hãy khóa tài khoản. Ngoài ra, thu hồi bất kỳ mã thông báo xác thực tồn tại lâu dài nào, vì kẻ tấn công cũng có thể có một trong những mã đó. Nếu đó là phần mềm độc hại, phần mềm chống phần mềm độc hại có thể cách ly không? Hoặc loại bỏ các mã độc không? Nếu không, máy bị nhiễm cần phải được gỡ bỏ khỏi mạng càng sớm càng tốt để ngăn chặn chuyển động ngang xung quanh mạng. Để làm điều này, chúng ta có thể điều chỉnh các quy tắc tường lửa mạng để cách ly máy một cách hiệu quả. Chúng ta cũng có thể di chuyển máy sang một VLAN riêng biệt được sử dụng cho mục đích cách ly bảo mật. Đây sẽ là một VLAN với các hạn chế và bộ lọc nghiêm ngặt được áp dụng để ngăn chặn

việc lây nhiễm thêm các hệ thống và mạng khác. Trong giai đoạn này, điều quan trọng là phải nỗ lực để tránh việc phá hủy bất kỳ nhật ký hoặc bằng chứng nào. Những kẻ tấn công thường cố gắng che giấu dấu vết của chúng bằng cách sửa đổi nhật ký và xóa tệp, đặc biệt khi chúng nghi ngờ mình đã bị phát hiện. Chúng sẽ thực hiện các biện pháp để đảm bảo rằng chúng vẫn giữ quyền truy cập vào các hệ thống bị xâm phạm. Điều này có thể liên quan đến việc cài đặt một backdoor hoặc một số loại phần mềm độc hại truy cập từ xa. Một bước khác cần chú ý là tạo một tài khoản người dùng mới mà họ có thể sử dụng để xác thực trong tương lai. Với các cấu hình và hệ thống ghi nhật ký hiệu quả, các hoạt động này sẽ hiển thị trong nhật ký đánh giá. Vì vậy, loại truy cập này nên được phát hiện trong quá trình điều tra sự cố, sau đó có thể thực hiện các hành động để loại bỏ quyền truy cập.

Một phần khác của phân tích sự cố là xác định mức độ nghiêm trọng, tác động và khả năng phục hồi của sự cố. Mức độ nghiêm trọng bao gồm các yếu tố như cái gì và bao nhiêu hệ thống đã bị xâm phạm và vi phạm ảnh hưởng như thế nào đến các chức năng kinh doanh. Ví dụ, một sự cố làm ảnh hưởng đến một loạt các máy trong mạng sẽ nghiêm trọng hơn một sự cố trong đó một máy chủ web duy nhất bị tấn công. Bạn có thể tưởng tượng rằng nỗ lực cần thiết để sửa chữa một tấn công quy mô lớn sẽ ảnh hưởng tiêu cực đến khả năng thực hiện công việc bình thường. Vì vậy, ảnh hưởng của sự cố cũng là một vấn đề quan trọng cần quan tâm. Nếu tổ chức chỉ có một máy chủ web và nó đã bị xâm phạm, nó có thể được coi là một vi phạm có mức độ nghiêm trọng cao hơn nhiều. Nó có thể có tác động trực tiếp từ bên ngoài có thể nhìn thấy được đối với doanh nghiệp.

Đánh cắp dữ liệu (data exfiltration) là việc chuyển dữ liệu trái phép từ máy tính. Nó cũng là một mối quan tâm rất quan trọng khi một sự cố bảo mật xảy ra. Tin tặc có thể cố gắng đánh cắp dữ liệu vì một số lý do. Chúng có thể muốn đánh cắp thông tin tài khoản để cung cấp quyền truy cập sau này. Chúng có thể nhắm mục tiêu dữ liệu kinh doanh để công khai trực tuyến nhằm gây tổn thất tài chính hoặc tổn hại đến danh tiếng của tổ chức. Trong một số trường hợp, kẻ tấn công có thể chỉ muốn gây ra thiệt hại và phá hủy, có thể liên quan đến việc xóa hoặc làm hỏng dữ liệu.

Một sự cố có thể được khôi phục bằng cách khôi phục đơn giản từ bản sao lưu bằng cách làm theo các quy trình được coi là cách dễ dàng. Tuy nhiên, một

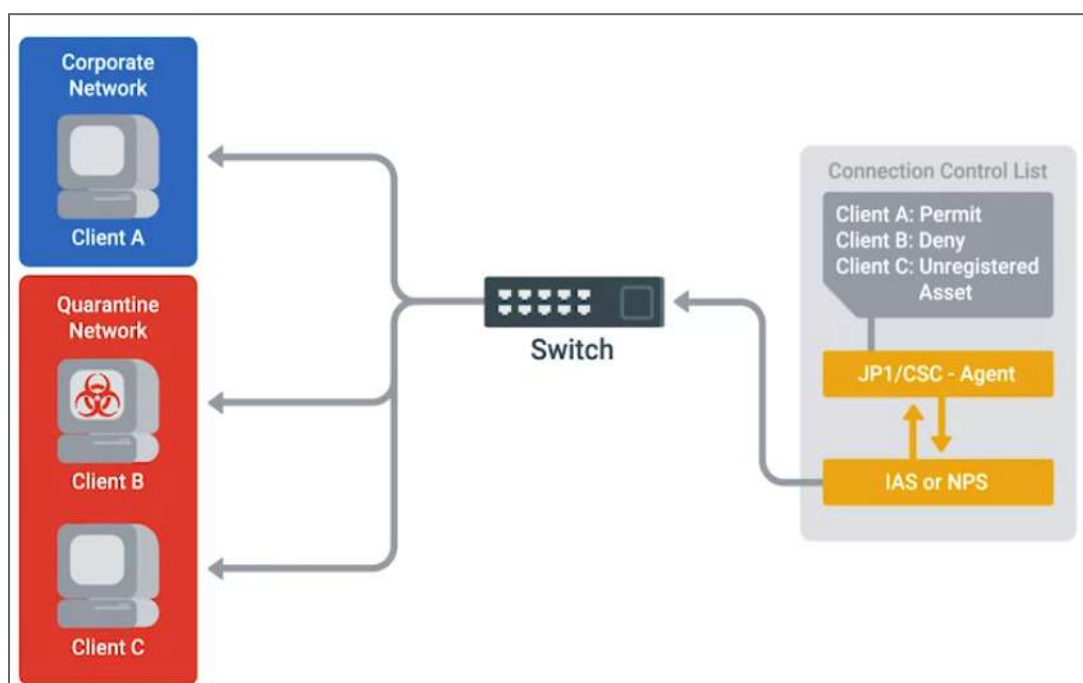
sự cố trong đó kẻ tấn công đã xóa một lượng lớn thông tin khách hàng và tàn phá rất nhiều hệ thống cơ sở hạ tầng quan trọng sẽ khó khôi phục hơn. Có thể hoàn toàn không thể khôi phục được. Trong một số trường hợp, tùy thuộc vào cấu hình và hệ thống sao lưu, một số dữ liệu có thể bị mất vĩnh viễn và không thể khôi phục được. Bản sao lưu sẽ không chứa bất kỳ thay đổi hoặc dữ liệu mới nào được thực hiện sau lần chạy sao lưu cuối cùng.

Bước tiếp theo là phân tích nó và xác định ảnh hưởng và phạm vi thiệt hại. Đó có phải là một rò rỉ dữ liệu? Hay công bố thông tin? Nếu vậy, thông tin nào được đưa ra ngoài? Thực hư ra sao? Hệ thống có bị xâm phạm không? Những hệ thống nào? Và họ đã quản lý để có được cấp độ truy cập nào? Nó có phải là một sự lây nhiễm phần mềm độc hại, những hệ thống nào đã bị nhiễm? Một số cuộc tấn công thực sự rõ ràng với các dấu hiệu xâm nhập rất rõ ràng như trang web bị phá hoại hoặc quá trình bất thường tiêu thụ tất cả tài nguyên trong hệ thống. Những thứ khác có thể tinh vi hơn và hầu như không thể bị phát hiện, chẳng hạn như một thay đổi nhỏ đối với một tập tin cấu hình hệ thống. Đây là lý do tại sao việc giám sát tốt là rất quan trọng cùng với việc hiểu biết cơ sở của chúng ta. Sau khi chúng ta tìm ra luồng truy cập bình thường trên mạng của mình và những dịch vụ mong đợi sẽ thấy, các ngoại lệ sẽ dễ dàng phát hiện hơn. Điều này rất quan trọng vì mọi sự dẫn dắt sai mà nhóm ứng phó sự cố phải điều tra đều có nghĩa là thời gian và nguồn lực bị lãng phí. Điều này có khả năng cho phép các cuộc xâm nhập thực sự không bị phát hiện và không bị điều tra lâu hơn.

Trong quá trình phát hiện và xác định phạm vi, dữ liệu tương quan từ các hệ thống khác nhau có thể tiết lộ bức tranh lớn hơn nhiều về những gì đã xảy ra. Nó có thể hiển thị cách kẻ xâm nhập có được quyền truy cập. Ví dụ: chúng ta có thể thấy một sự kiện kết nối được tường lửa ghi lại từ một địa chỉ IP đáng ngờ, việc tìm kiếm các sự kiện khác liên quan đến địa chỉ IP này có thể tiết lộ các nỗ lực ghi nhật ký và nhật ký xác thực cho hệ thống. Điều này sẽ cung cấp thông tin chi tiết về nơi mà kẻ tấn công đến và những gì chúng đã cố gắng thực hiện trên mạng. Nhật ký xác thực cũng sẽ cho biết chúng có thể đăng nhập thành công vào tài khoản hay không. Nếu vậy, điều đó cho chúng ta biết tài khoản nào bị xâm phạm.

Khi phạm vi của sự cố được xác định, bước tiếp theo là ngăn chặn. Chúng ta cần phải ngăn chặn vi phạm để ngăn thiệt hại thêm. Đối với các trường hợp xâm

phạm hệ thống và lây nhiễm phần mềm độc hại, đây là một bước khá nhạy cảm. Chúng ta không muốn phần mềm độc hại hoặc kẻ tấn công sử dụng một máy bị xâm nhập để chuyển sang các máy khác trong mạng. Điều này có thể mở rộng phạm vi tỷ lệ và gây ra nhiều thiệt hại hơn. Các chiến lược ngăn chặn sẽ khác nhau tùy thuộc vào bản chất của vụ việc. Nếu tài khoản bị xâm phạm, hãy thay đổi mật khẩu ngay lập tức. Nếu chủ sở hữu không thể thay đổi mật khẩu ngay lập tức, hãy khóa tài khoản. Ngoài ra, thu hồi bất kỳ mã token xác thực tồn tại lâu dài nào, vì kẻ tấn công cũng có thể có một trong những mã đó. Nếu đó là phần mềm độc hại, phần mềm chống phần mềm độc hại có thể cách ly không? Hoặc loại bỏ các mã độc không? Nếu không, máy bị nhiễm cần phải được gỡ bỏ khỏi mạng càng sớm càng tốt để ngăn chặn chuyển động ngang xung quanh mạng. Để làm điều này, chúng ta có thể điều chỉnh các quy tắc tường lửa mạng để cách ly máy một cách hiệu quả. Chúng ta cũng có thể di chuyển máy sang một VLAN riêng biệt được sử dụng cho mục đích cách ly bảo mật. Đây sẽ là một VLAN với các hạn chế và bộ lọc nghiêm ngặt được áp dụng để ngăn chặn việc lây nhiễm thêm các hệ thống và mạng khác. Trong giai đoạn này, điều quan trọng là phải nỗ lực để tránh việc phá hủy bất kỳ nhật ký hoặc bằng chứng nào. Những kẻ tấn công thường cố gắng che giấu dấu vết của chúng bằng cách sửa đổi nhật ký và xóa tệp, đặc biệt khi chúng nghi ngờ mình đã bị phát hiện. Chúng sẽ thực hiện các biện pháp để đảm bảo rằng chúng vẫn giữ quyền truy cập vào các hệ thống bị xâm phạm. Điều này có thể liên quan đến việc cài đặt một backdoor hoặc một số loại phần mềm độc hại truy cập từ xa. Một bước khác cần chú ý là tạo một tài khoản người dùng mới mà họ có thể sử dụng để xác thực trong tương lai. Với các cấu hình và hệ thống ghi nhật ký hiệu quả, các hoạt động này sẽ hiển thị trong nhật ký đánh giá. Vì vậy, loại truy cập này nên được phát hiện trong quá trình điều tra sự cố, sau đó có thể thực hiện các hành động để loại bỏ quyền truy cập.



Xác định mức độ nghiêm trọng

Một phần khác của phân tích sự cố là xác định mức độ nghiêm trọng, tác động và khả năng phục hồi của sự cố. Mức độ nghiêm trọng bao gồm các yếu tố như cái gì và bao nhiêu hệ thống đã bị xâm phạm và vi phạm ảnh hưởng như thế nào đến các chức năng kinh doanh. Ví dụ, một sự cố làm ảnh hưởng đến một loạt các máy trong mạng sẽ nghiêm trọng hơn một sự cố trong đó một máy chủ web duy nhất bị tấn công. Bạn có thể tưởng tượng rằng nỗ lực cần thiết để sửa chữa một tấn công quy mô lớn sẽ ảnh hưởng tiêu cực đến khả năng thực hiện công việc bình thường. Vì vậy, ảnh hưởng của sự cố cũng là một vấn đề quan trọng cần quan tâm. Nếu tổ chức chỉ có một máy chủ web và nó đã bị xâm phạm, nó có thể được coi là một vi phạm có mức độ nghiêm trọng cao hơn nhiều. Nó có thể có tác động trực tiếp từ bên ngoài có thể nhìn thấy được đối với doanh nghiệp.

Vấn đề đánh cắp dữ liệu

Đánh cắp dữ liệu (data exfiltration) là việc chuyển dữ liệu trái phép từ máy tính. Nó cũng là một mối quan tâm rất quan trọng khi một sự cố bảo mật xảy ra. Tin tặc có thể cố gắng đánh cắp dữ liệu vì một số lý do. Chúng có thể muốn đánh cắp thông tin tài khoản để cung cấp quyền truy cập sau này. Chúng có

thể nhằm mục tiêu dữ liệu kinh doanh để công khai trực tuyến nhằm gây tổn thất tài chính hoặc tổn hại đến danh tiếng của tổ chức. Trong một số trường hợp, kẻ tấn công có thể chỉ muốn gây ra thiệt hại và phá hủy, có thể liên quan đến việc xóa hoặc làm hỏng dữ liệu. Một sự cố có thể được khôi phục bằng cách khôi phục đơn giản từ bản sao lưu bằng cách làm theo các quy trình được coi là cách dễ dàng. Tuy nhiên, một sự cố trong đó kẻ tấn công đã xóa một lượng lớn thông tin khách hàng và tàn phá rất nhiều hệ thống cơ sở hạ tầng quan trọng sẽ khó khôi phục hơn. Có thể hoàn toàn không thể khôi phục được. Trong một số trường hợp, tùy thuộc vào cấu hình và hệ thống sao lưu, một số dữ liệu có thể bị mất vĩnh viễn và không thể khôi phục được. Bản sao lưu sẽ không chứa bất kỳ thay đổi hoặc dữ liệu mới nào được thực hiện sau lần chạy sao lưu cuối cùng.

Khôi phục hệ thống

Một khi mối đe dọa đã được phát hiện và ngăn chặn, nó phải được loại bỏ hoặc khắc phục. Khi nói đến việc lây nhiễm phần mềm độc hại, điều này có nghĩa là xóa phần mềm độc hại khỏi các hệ thống bị ảnh hưởng. Nhưng trong một số trường hợp, điều này có thể không thực hiện được, vì vậy các hệ thống bị ảnh hưởng phải được khôi phục về cấu hình tốt đã biết. Điều này có thể được thực hiện bằng cách xây dựng lại máy hoặc khôi phục từ bản sao lưu. Hãy cẩn thận khi xóa phần mềm độc hại khỏi hệ thống vì một số phần mềm độc hại được thiết kế để hoạt động rất bền bỉ, có nghĩa là nó chống lại việc bị xóa.

Nhưng trước khi chúng ta có thể bắt đầu khôi phục, chúng ta phải ngăn chặn sự cố. Điều này có thể liên quan đến việc tắt các hệ thống bị ảnh hưởng để ngăn ngừa thiệt hại thêm hoặc lây lan phần mềm độc hại. Mặt khác, các hệ thống bị ảnh hưởng có thể bị xóa quyền truy cập mạng để cắt bất kỳ liên lạc nào với hệ thống bị xâm phạm. Một lần nữa, yếu tố thúc đẩy ở đây sẽ là ngăn chặn sự lây lan của bất kỳ sự lây nhiễm nào hoặc loại bỏ quyền truy cập từ xa vào hệ thống. Chiến lược ngăn chặn khác nhau tùy thuộc vào bản chất của hệ thống bị ảnh hưởng. Giả sử một phần cơ sở hạ tầng mạng quan trọng đã bị xâm phạm. Việc tắt nhanh có thể không hoạt động vì nó sẽ ảnh hưởng đến các hoạt động kinh doanh khác. Trên hết, việc xóa quyền truy cập mạng có thể kích hoạt một số hành động trong phần mềm tấn công hoặc phần mềm độc hại. Giả sử một phần mềm độc hại được thiết kế để kiểm tra định kỳ vào máy chủ lệnh và

điều khiển. Việc cắt đứt liên lạc mạng với máy tính bị nhiễm có thể khiến phần mềm độc hại kích hoạt chức năng tự hủy trong nỗ lực tiêu hủy bằng chứng.

Phân tích pháp y có thể cần được thực hiện để phân tích vụ tấn công. Điều này đặc biệt đúng khi nói đến nhiễm phần mềm độc hại. Trong trường hợp phân tích pháp y, các máy bị ảnh hưởng có thể được điều tra rất kỹ để xác định chính xác những gì kẻ tấn công đã làm. Điều này thường được thực hiện bằng cách chụp ảnh đĩa, về cơ bản là tạo một bản sao ảo của ổ cứng. Điều này cho phép người điều tra phân tích nội dung của đĩa mà không có nguy cơ sửa đổi hoặc thay đổi các tập tin gốc. Nếu điều đó xảy ra, nó sẽ ảnh hưởng đến tính toàn vẹn của bất kỳ bằng chứng pháp y nào. Thông thường, thu thập bằng chứng cũng là một phần của quy trình ứng phó sự cố. Điều này cung cấp bằng chứng cho cơ quan thực thi pháp luật nếu tổ chức muốn theo đuổi hành động pháp lý chống lại những kẻ tấn công. Bằng chứng pháp y rất hữu ích để cung cấp thông tin chi tiết về vụ tấn công cho cộng đồng an ninh. Nó cho phép các nhóm bảo mật khác nhận thức được các xử lý mới và cho phép họ tự bảo vệ mình tốt hơn. Điều rất quan trọng là chúng ta phải mời các thành viên từ nhóm pháp lý tham gia vào bất kỳ kế hoạch xử lý sự cố nào. Bởi vì một sự cố có thể có ảnh hưởng pháp lý đối với công ty, nên có luật sư để tư vấn về các khía cạnh pháp lý của cuộc điều tra. Điều quan trọng là để tránh những phức tạp hoặc các vấn đề về trách nhiệm pháp lý. Các thành viên của nhóm quan hệ công chúng cũng nên tham gia vì những sự cố này có thể ảnh hưởng đến danh tiếng của công ty.



Đầu tiên, chúng ta cần xác định lỗ hổng mà phần mềm độc hại đã khai thác. Việc này cần được thực hiện cùng lúc với việc dọn dẹp. Nếu chúng ta xóa phần mềm độc hại lây nhiễm mà không giải quyết lỗ hổng cơ bản, hệ thống có thể bị tái nhiễm ngay sau khi dọn dẹp chúng. Nếu một hệ thống quan trọng đã bị xâm

phạm, việc khắc phục có thể phức tạp do thời gian ngừng hoạt động trong quá trình khắc phục và phục hồi. Nhật ký phải được kiểm tra để xác định chính xác những gì kẻ tấn công đã làm trong khi chúng có quyền truy cập vào hệ thống. Nó cũng sẽ cho chúng ta biết những dữ liệu mà kẻ tấn công đã truy cập. Hệ thống phải được xem xét kỹ lưỡng để đảm bảo không có backdoor nào được cài đặt hoặc phần mềm độc hại được cài đặt trên hệ thống. Tùy thuộc vào mức độ nghiêm trọng của sự xâm nhập hoặc lây nhiễm, có thể cần phải xây dựng lại hệ thống từ đầu.

Khi tất cả các dấu vết của cuộc tấn công đã được và các lỗ hổng đã biết đã được đóng lại, chúng ta có thể chuyển sang bước cuối cùng. Đó là lúc các hệ thống cần được kiểm tra kỹ lưỡng để đảm bảo rằng chức năng thích hợp đã được khôi phục. Thông thường, các hệ thống bị ảnh hưởng cũng sẽ được theo dõi chặt chẽ, đôi khi có bật tính năng theo dõi và ghi nhật ký chi tiết bổ sung. Điều này là để theo dõi bất kỳ dấu hiệu xâm nhập bổ sung nào trong trường hợp có thứ gì đó bị bỏ sót trong quá trình dọn dẹp. Cũng có thể kẻ tấn công sẽ cố gắng tấn công lại cùng một mục tiêu. Có khả năng rất cao là chúng sử dụng phương pháp tấn công tương tự vào các mục tiêu khác trong mạng. Cảnh giác và chuẩn bị để bảo vệ hệ thống của chúng ta khỏi các cuộc tấn công mới.

6. Bảo mật điện thoại

Giữ an toàn cho thiết bị di động là điều cực kỳ quan trọng. Hãy nghĩ về loại dữ liệu mà thiết bị di động có thể có. Email, tập tin cá nhân, ảnh, dữ liệu sức khỏe, dữ liệu vị trí, v.v. Các thiết bị di động đi cùng chúng ta và chúng không được bảo vệ bởi mức độ bảo mật vật lý tương tự như một máy tính trong trung tâm dữ liệu. Các thiết bị di động rất dễ bị thất lạc hoặc bị đánh cắp. Vì vậy chúng ta cần đảm bảo bảo mật các thiết bị này. Một trong những biện pháp bảo vệ cơ bản nhất mà bạn có thể bật trên điện thoại thông minh hoặc máy tính bảng là khóa màn hình. Khóa màn hình đưa ra một số loại thử thách mà chúng ta phải đáp ứng để mở khóa thiết bị. Chúng ta có thể nhập mã pin hoặc mật khẩu, chúng ta có thể vẽ hình trên màn hình hoặc có thể sử dụng dữ liệu sinh trắc học như vân tay hoặc thậm chí là khuôn mặt của mình để mở khóa thiết bị.

Không có biện pháp bảo vệ nào là hoàn hảo. Vì vậy, chúng ta nên sử dụng phòng thủ một cách chuyên sâu để bảo vệ dữ liệu trên thiết bị di động. Điều gì sẽ xảy ra nếu ai đó đánh cắp thiết bị và khởi động lại thiết bị hoặc tháo rời thiết

bị để lấy trực tiếp tại vùng nhớ? Để giúp bảo vệ khỏi điều này, hãy bật mã hóa bộ nhớ trên thiết bị di động. Trên một số thiết bị, điều này được thực hiện theo mặc định. Nhưng nếu không, chúng ta nên bật tính năng đó.

Chúng ta đã nói một chút về việc bảo vệ thiết bị của bạn khỏi kẻ tấn công bên ngoài. Nhưng còn việc bảo vệ dữ liệu trên thiết bị khỏi một ứng dụng được cài đặt trên thiết bị thì sao? Người dùng cuối sẽ có thể kiểm soát ứng dụng nào trên thiết bị di động của họ có quyền truy cập vào dữ liệu nào. Hệ điều hành di động có các quyền được xác định để kiểm soát ứng dụng nào có quyền truy cập vào hệ thống hoặc dữ liệu. Mỗi hệ điều hành có một danh sách các quyền và ứng dụng yêu cầu quyền truy cập vào các quyền cụ thể mà nó cần. Ứng dụng dành cho thiết bị di động sẽ yêu cầu quyền khi chúng được cài đặt lần đầu tiên hoặc khi chúng cố gắng sử dụng quyền lần đầu tiên.

Phần 2

HƯỚNG DẪN

TRẢ LỜI CÂU HỎI

Các mối đe dọa

1. Trong bộ ba CIA, "Confidentiality" (Bảo mật) có nghĩa là đảm bảo rằng dữ liệu:

- A. có sẵn và mọi người có thể truy cập nó
- B. không thể truy cập bởi các bên không mong muốn
- C. chính xác và không bị giả mạo
- D. có thể truy cập ẩn danh

Đáp án: B

2. Trong bộ ba CIA, "Integrity" (tính toàn vẹn) có nghĩa là đảm bảo rằng dữ liệu:

- A. có sẵn và mọi người có thể truy cập nó
- B. không thể truy cập bởi các bên không mong muốn
- C. chính xác và không bị giả mạo
- D. trung thực và đáng tin

Đáp án: C

3. Trong bộ ba CIA, "Availability" (tính khả dụng) có nghĩa là đảm bảo rằng dữ liệu:

- A. có sẵn và mọi người có thể truy cập nó
- B. không thể truy cập bởi các bên không mong muốn
- C. chính xác và không bị giả mạo
- D. có sẵn cho bất kỳ ai từ bất cứ đâu

Đáp án: A

4. Mối quan hệ giữa lỗ hổng và khai thác là gì?

- A. Chúng không liên quan.
- B. Kẻ khai thác lợi dụng lỗ hổng để chạy mã tùy ý hoặc giành quyền truy cập
- C. Một lỗ hổng bảo mật lợi dụng việc khai thác để chạy mã tùy ý hoặc giành quyền truy cập
- D. Việc khai thác tạo ra lỗ hổng trong hệ thống

Đáp án: B

5. Câu nào đúng cho cả sâu máy tính và vi-rút máy tính?

- A. Chúng tự tái tạo và tự lây lan
- B. Chúng lây nhiễm các tập tin khác bằng mã độc hại
- C. Chúng không thể phát hiện được bởi phần mềm chống phần mềm độc hại
- D. Chúng không gây hại cho hệ thống đích

Đáp án: A

6. Chọn tất cả các ví dụ về các loại phần mềm độc hại:

- A. Vi-rút máy tính
- B. Bộ phát sinh khóa
- C. Sâu máy tính
- D. Phần mềm quảng cáo

Đáp án: A, C, D

7. Đặc điểm của rootkit là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Cung cấp thông tin xác thực nâng cao
- B. Rất khó phát hiện
- C. Chúng vô hại
- D. Có tính phá hoại

Đáp án: A, B

8. Những mối nguy hiểm của một cuộc tấn công xen giữa là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Kẻ tấn công có thể nghe trộm các trao đổi không được mã hóa
- B. Kẻ tấn công có thể sửa đổi các trao đổi trong quá trình chuyển tiếp
- C. Kẻ tấn công có thể chặn hoặc chuyển hướng trao đổi
- D. Kẻ tấn công có thể phá hủy dữ liệu ở trạng thái còn lại

Đáp án: A, B, C

9. Tại sao một cuộc tấn công giả mạo DNS lại nguy hiểm? Đánh dấu vào tất cả các câu phù hợp.

- A. Ờ thì ... nó không thực sự nguy hiểm.
- B. Nó ảnh hưởng đến bất kỳ máy khách nào truy vấn máy chủ DNS bị nhiễm
- C. Nó cho phép kẻ tấn công điều khiển máy tính của bạn từ xa
- D. Nó cho phép kẻ tấn công chuyển hướng mục tiêu đến các máy chủ web độc hại

Đáp án: B, D

10. Điều nào sau đây là đúng với một cuộc tấn công DDoS?

- A. Kẻ tấn công gửi tấn công trực tiếp đến mục tiêu
- B. Luồng tấn công đến từ nhiều máy chủ khác nhau
- C. Luồng tấn công được mã hóa
- D. Kiểu tấn công này gây ra mất mát dữ liệu đáng kể

Đáp án: A

11. Hậu quả nào sau đây xuất phát từ một cuộc tấn công từ chối dịch vụ?
Đánh dấu vào tất cả các câu phù hợp.

- A. Hiệu suất mạng chậm
- B. Nhiễm phần mềm độc hại
- C. Phá hủy dữ liệu
- D. Gián đoạn dịch vụ

Đáp án: A, D

12. Làm cách nào để bạn có thể bảo vệ khỏi các cuộc tấn công tiêm mã độc từ phía máy khách? Đánh dấu vào tất cả các câu phù hợp.

- A. Sử dụng kiểm tra đầu vào
- B. Sử dụng một cơ sở dữ liệu SQL
- C. Sử dụng mật khẩu mạnh
- D. Sử dụng tính năng làm sạch dữ liệu

Đáp án: A, D

13. Đúng hay sai: Một cuộc tấn công brute-force hiệu quả hơn một cuộc tấn công từ điển.

- A. Đúng
- B. Sai

Đáp án: B

14. Tình huống nào sau đây là các cuộc tấn công phi kỹ thuật (social engineering attack)? Đánh dấu vào tất cả các câu phù hợp.

- A. Bạn nhận được một email có tệp đính kèm chứa vi-rút
- B. Ai đó sử dụng ID giả để truy cập vào một khu vực hạn chế
- C. Kẻ tấn công thực hiện một cuộc tấn công xen giữa
- D. Kẻ tấn công thực hiện một cuộc tấn công giảm mạo DNS

Đáp án: A, B

15. Lừa đảo, nhử mồi và trà trộn là những ví dụ về các cuộc tấn công _____.

- A. Mật khẩu (password)
- B. Mạng (network)
- C. Mã độc (malware)
- D. Phi kỹ thuật (social engineering)

Đáp án: D

16. Khi dọn dẹp hệ thống sau khi bị xâm nhập, bạn nên xem xét kỹ bất kỳ _____ nào có thể đã được kẻ tấn công cài đặt.

- A. AP giả mạo
- B. DNS bị giả mạo
- C. Tấn công tiêm mã độc
- D. Cửa hậu

Đáp án: D

17. Một cuộc tấn công _____ nhằm ngăn chặn lưu lượng truy cập hợp pháp đến một dịch vụ.

- A. Mật khẩu
- B. Giả mạo DNS
- C. Từ chối dịch vụ
- D. Tiêm mã độc

Đáp án: C

18. Điều gì làm cho một cuộc tấn công DDoS khác với một cuộc tấn công DoS? Đánh dấu vào tất cả các câu phù hợp.

- A. Một cuộc tấn công DoS có lưu lượng tấn công đến từ nhiều nguồn khác nhau
- B. Một cuộc tấn công DoS có lưu lượng tấn công đến từ một nguồn
- C. Một cuộc tấn công DDoS có lưu lượng tấn công đến từ một nguồn
- D. Một cuộc tấn công DDoS có lưu lượng tấn công đến từ nhiều nguồn khác nhau

Đáp án: B, D

19. Điều nào trong số này là một ví dụ về nguyên tắc toàn vẹn có thể đảm bảo dữ liệu của bạn chính xác và không bị can thiệp?

- A. Sử dụng MAC (Mã xác thực thông điệp)
- B. Sử dụng đóng gói thông tin bảo mật
- C. Thực hiện bảo vệ khỏi nghẽn mạng
- D. Giữ bí mật khóa đối xứng

Đáp án: A, B

20. Điều gì có thể làm giảm tính khả dụng của bảo mật và khả năng sẵn sàng do việc mất dữ liệu?

- A. Phần mềm quảng cáo (adware)
- B. Phần mềm tống tiền (ransomware)
- C. Phần mềm theo dõi thao tác bàn phím (keylogger)
- D. Phần mềm gián điệp (spyware)

Đáp án: B

21. Điều nào trong số này đúng với hacker mũ đen và mũ trắng?

- A. Hacker mũ đen gây hại. Hacker mũ trắng khai thác điểm yếu để giúp giảm thiểu các mối đe dọa.
- B. Hacker mũ đen cố gắng tìm ra điểm yếu, nhưng mũ trắng thì không.
- C. Hacker mũ đen làm việc với chủ sở hữu để khắc phục sự cố. Hacker mũ trắng chỉ đang cố gắng xâm nhập vào một hệ thống.
- D. Hacker mũ đen và mũ trắng không nên được tin cậy.

Đáp án: A

22. Nếu tin tặc muốn đánh cắp mật khẩu của bạn bằng cách cài đặt phần mềm độc hại ghi lại tất cả thông điệp bạn gõ, thì tin tặc cần cài đặt loại phần mềm độc hại nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Phần mềm gián điệp (spyware)
- B. Phần mềm theo dõi thao tác bàn phím (keylogger)
- C. Rootkit
- D. Bom logic (logic bomb)

Đáp án: A, B

23. Một quản trị viên hệ thống bí quan đã viết một chương trình phần mềm độc hại để phá hủy các dịch vụ của công ty sau khi một sự kiện nhất định xảy ra. Điều này mô tả loại phần mềm độc hại nào?

- A. Ransomware
- B. Logic bomb
- C. Spyware
- D. Rootkit

Đáp án: B

24. Điều gì có thể xảy ra trong một cuộc tấn công PoD (Ping of Death)? Đánh dấu vào tất cả các câu phù hợp.

- A. Tràn vùng đệm
- B. Thực thi mã từ xa
- C. Từ chối dịch vụ
- D. Mồi nhử

Đáp án: A, B, C

25. Nó được gọi là gì nếu một hacker hạ gục nhiều dịch vụ rất nhanh với sự trợ giúp của botnet?

- A. Tấn công XSS (Cross-site scripting)
- B. Tấn công mật khẩu
- C. Tiêm mã độc SQL
- D. Từ chối dịch vụ phân tán (DDoS)

Đáp án: D

26. Làm thế nào bạn có thể tăng cường độ mạnh cho mật khẩu của mình? Đánh dấu vào tất cả các câu phù hợp.

- A. Loại trừ các từ trong từ điển.
- B. Sử dụng mật khẩu từ danh sách được chuẩn bị trước.
- C. Kết hợp các ký hiệu và số.
- D. Sử dụng kết hợp chữ viết hoa và viết thường.

Đáp án: A, C, D

27. Một kẻ tấn công, đóng vai một nhân viên bưu điện, đã sử dụng các chiến thuật phi kỹ thuật để lừa một nhân viên nghĩ rằng cô ấy đang giao các gói hàng một cách hợp pháp. Kẻ tấn công sau đó có thể truy cập vật lý vào một khu vực hạn chế bằng cách theo sau nhân viên vào tòa nhà. Kẻ tấn công đã thực hiện kiểu tấn công nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Tấn công phi kỹ thuật (social engineering)
- B. Lừa đảo (phishing)

- C. Trà trộn (tailgating)
- D. Giả mạo (spoofing)

Đáp án: A, C

Mật mã học

1. Các thành phần tạo nên một hệ thống mật mã là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Thuật toán phát sinh khóa
- B. Thuật toán mã hóa
- C. Thuật toán giải mã
- D. Thuật toán truyền nhận

Đáp án: A, B, C

2. Steganography là gì?

- A. Nghiên cứu về stegosauruses
- B. Thực hành mã hóa thông điệp
- C. Thực hành ẩn thông điệp
- D. Nghiên cứu ngôn ngữ

Đáp án: C

3. Điều gì làm nên một thuật toán mã hóa đối xứng?

- A. Tốc độ cao
- B. Các khóa khác nhau được sử dụng để mã hóa và giải mã

- C. Kích thước khóa rất lớn
- D. Các khóa giống nhau được sử dụng để mã hóa và giải mã

Đáp án: D

4. Sự khác biệt giữa mã hóa dòng và mã hóa khối là gì?

- A. Mã hóa dòng không thể lưu dữ liệu đã mã hóa xuống đĩa.
- B. Mã hóa khối chỉ được sử dụng để mã hóa thiết bị khối.
- C. Mã hóa dòng mã hóa dữ liệu dưới dạng một dòng liên tục, trong khi mã hóa khối hoạt động trên nhiều đoạn dữ liệu.
- D. Không có sự khác biệt.

Đáp án: C

5. Đúng hay sai: Khóa mã hóa càng nhỏ thì dữ liệu mã hóa càng an toàn.

- A. Đúng
- B. Sai

Đáp án: B

6. Hệ thống mã hóa bất đối xứng cung cấp những yếu tố nào sau đây? Đánh dấu vào tất cả các câu phù hợp.

- A. Tính bảo mật (confidentiality)
- B. Tính sẵn sàng (availability)
- C. Tính xác thực (authenticity)
- D. Chống thoái thác (non-repudiation)

Đáp án: A, C, D

7. Các thuật toán bất đối xứng có những ưu điểm gì so với các thuật toán đối xứng?

- A. Chúng cho phép giao tiếp an toàn qua các kênh không an toàn.
- B. Chúng có hiệu suất rất nhanh.
- C. Chúng an toàn hơn.
- D. Chúng dễ thực hiện hơn.

Đáp án: A

8. Ứng dụng phổ biến cho thuật toán bất đối xứng là gì?

- A. Mã hóa toàn bộ ổ đĩa
- B. Lưu trữ mật khẩu an toàn
- C. Trao đổi khóa an toàn
- D. Tạo số ngẫu nhiên

Đáp án: C

9. Băm khác với mã hóa như thế nào?

- A. Nó kém an toàn hơn.
- B. Nó nhanh hơn.
- C. Băm có nghĩa là cho một lượng lớn dữ liệu, trong khi mã hóa dành cho một lượng nhỏ dữ liệu.
- D. Thực thi băm là hàm một chiều.

Đáp án: D

10. Độ băm là gì?

- A. Khi hai thuật toán băm khác nhau tạo ra cùng một giá trị băm
- B. Khi hai tập tin giống nhau tạo ra các bản băm khác nhau
- C. Khi bản băm được đảo ngược để khôi phục bản gốc
- D. Khi hai tập tin khác nhau tạo ra cùng một bản băm

Đáp án: D

11. Kiểm tra tính toàn vẹn thông điệp (MIC) khác với mã xác thực thông điệp (MAC) như thế nào?

- A. Chúng giống nhau.
- B. MIC chỉ băm thông điệp, trong khi MAC kết hợp một khóa bí mật.
- C. MAC yêu cầu mật khẩu, trong khi MIC thì không.
- D. MIC đáng tin cậy hơn MAC.

Đáp án: B

12. Làm thế nào bạn có thể bảo vệ chống lại các cuộc tấn công mật khẩu vét cạn (brute-force)? Đánh dấu vào tất cả các câu phù hợp.

- A. Bắt buộc sử dụng mật khẩu mạnh.
- B. Thêm các giá trị muối vào băm mật khẩu.
- C. Chạy mật khẩu qua hàm băm nhiều lần.
- D. Lưu trữ mật khẩu trong một bảng cầu vồng

Đáp án: A, B, C

13. Chứng thư số chứa thông tin gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Dữ liệu khóa cá nhân
- B. Dữ liệu khóa công khai
- C. Thông tin nhận dạng của chủ sở hữu chứng chỉ
- D. Chữ ký điện tử

Đáp án: B, C, D

14. SSL/TLS sử dụng loại mã hóa nào?

- A. Mã hóa bất đối xứng
- B. Mã hóa đối xứng
- C. Cả hai
- D. Không

Đáp án: C

15. Một số chức năng mà TPM có thể thực hiện là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Xác thực người dùng an toàn
- B. Phát hiện phần mềm độc hại
- C. Ràng buộc và niêm phong dữ liệu
- D. Chứng thực từ xa

Đáp án: C, D

16. Bản rõ (plaintext) là thông điệp gốc, trong khi ____ là thông điệp được mã hóa.

- A. Bản mã (ciphertext)
- B. Mật mã (cipher)
- C. Chuỗi tiêu thụ (digest)
- D. Thuật toán (algorithm)

Đáp án: A

17. Chức năng cụ thể của việc chuyển đổi bản rõ thành bản mã được gọi là một ____.

- A. Hoán vị
- B. Thuật toán mã hóa
- C. Chuẩn bảo vệ dữ liệu
- D. Kiểm tra tính toàn vẹn

Đáp án: B

18. Nghiên cứu tần suất các chữ cái và các cặp chữ cái xảy ra trong một ngôn ngữ được gọi là ____.

- A. Phân tích tần số
- B. Gián điệp
- C. Phá mã
- D. Mật mã học

Đáp án: A

19. Đúng hay sai: Cùng một bản rõ được mã hóa bằng cùng một thuật toán và cùng một khóa mã hóa sẽ dẫn đến kết quả đầu ra bản mã khác nhau.

- A. Đúng
- B. Sai

Đáp án: B

20. Thực hành ẩn tin nhằm thay vì mã hóa chúng được gọi là _____.

- A. Steganography
- B. Mã hóa
- C. Làm xáo trộn
- D. Băm

Đáp án: A

21. ROT13 và mã hóa Caesar là ví dụ của _____.

- A. Mã hóa thay thế
- B. Chữ ký điện tử
- C. Mã hóa bất đối xứng
- D. Steganography

Đáp án: A

22. DES, RC4 và AES là các ví dụ về thuật toán mã hóa _____.

- A. Đối xứng
- B. Bất đối xứng

- C. Yếu
- D. Mạnh

Đáp án: A

23. Hai thành phần của hệ thống mã hóa bất đối xứng, cần thiết cho các hoạt động mã hóa và giải mã là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Khóa công khai
- B. Khóa bí mật
- C. Chuỗi tiêu thụ
- D. Bộ phát sinh số ngẫu nhiên

Đáp án: A, B

24. Để tạo chữ ký khóa công khai, bạn sẽ sử dụng khóa _____.

- A. Bí mật
- B. Đối xứng
- C. Công khai
- D. Giải mã

Đáp án: A

25. Sử dụng hệ thống mật mã bất đối xứng mang lại lợi ích nào sau đây? Đánh dấu vào tất cả các câu phù hợp.

- A. Tính bảo mật
- B. Tính xác thực

C. Chống thoái thác

D. Băm

Đáp án: A, B, C

26. Nếu hai tập tin khác nhau dẫn đến cùng một hàm băm, thì điều này được gọi là _____.

A. Đụng độ băm

B. Trùng hợp ngẫu nhiên

C. Sai sót

D. Đụng độ khóa

Đáp án: A

27. Khi xác thực mật khẩu của người dùng, mật khẩu do người dùng cung cấp sẽ được xác thực bằng cách so sánh ____ của mật khẩu vừa mới nhập với giá trị băm của mật khẩu đã được lưu trữ trên hệ thống.

A. Bản băm

B. Bản rõ

C. Bản mã

D. Chiều dài

Đáp án: A

28. Nếu một bảng cầu vồng được sử dụng thay vì các băm vét cạn (brute-force), sự đánh đổi tài nguyên là gì?

- A. Bảng cầu vồng sử dụng ít tài nguyên tính toán hơn và nhiều không gian lưu trữ hơn
- B. Bảng cầu vồng sử dụng ít không gian lưu trữ hơn và nhiều tài nguyên tính toán hơn
- C. Bảng cầu vồng sử dụng ít tài nguyên RAM hơn và nhiều tài nguyên tính toán hơn
- D. Bảng cầu vồng sử dụng ít dung lượng lưu trữ hơn và nhiều tài nguyên RAM hơn

Đáp án: A

29. Trong hệ thống PKI, thực thể nào chịu trách nhiệm cấp, lưu trữ và ký chứng chỉ?

- A. Tổ chức phát hành chứng chỉ
- B. Cơ quan trung gian
- C. Cơ quan đăng ký
- D. Chính phủ

Đáp án: A

Bảo mật AAA

1. Xác thực khác với ủy quyền như thế nào?

- A. Xác thực là xác minh quyền truy cập vào một tài nguyên; ủy quyền là xác minh danh tính.
- B. Xác thực là xác minh danh tính; ủy quyền là xác minh quyền truy cập vào một tài nguyên.
- C. Xác thực là xác định một tài nguyên; ủy quyền là xác minh quyền truy cập vào tài khoản.

D. Chúng giống nhau.

Đáp án: B

2. Một số đặc điểm của một mật khẩu mạnh là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Chứa các từ trong từ điển
- B. Bao gồm số và ký tự đặc biệt
- C. Dài ít nhất 8 ký tự
- D. Được sử dụng trên nhiều tài khoản và hệ thống

Đáp án: B, C

3. Trong sơ đồ xác thực đa yếu tố, mật khẩu có thể được coi là:

- A. Cái gì đó bạn có.
- B. Cái gì đó bạn là.
- C. Cái gì đó bạn biết.
- D. Cái gì đó bạn sử dụng.

Đáp án: C

4. Một số hạn chế khi sử dụng sinh trắc học để xác thực là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Xác thực sinh trắc học rất khó hoặc không thể thay đổi nếu bị xâm phạm.
- B. Xác thực sinh trắc học chậm hơn nhiều so với các lựa chọn thay thế.
- C. Có những lo ngại về quyền riêng tư tiềm ẩn.

D. Sinh trắc học rất dễ chia sẻ.

Đáp án: A, C

5. Bằng cách nào các thiết bị U2F an toàn hơn các trình tạo OTP?

A. Chúng rẻ hơn.

B. Chúng có khả năng chống lại các cuộc tấn công lừa đảo.

C. Chúng được bảo vệ bằng mật khẩu.

D. Chúng không thể được nhân bản.

Đáp án: B

6. Những yếu tố nào của chứng chỉ cần được kiểm tra khi chứng chỉ đã được xác nhận? Đánh dấu vào tất cả các câu phù hợp.

A. Kích thước khóa chứng chỉ

B. Sự tin cậy của CA ký

C. Thông tin ngày trong trường “Not valid before” (không hợp lệ trước ngày)

D. Thông tin ngày trong trường “Not valid after” (không hợp lệ sau ngày)

Đáp án: B, C, D

7. CRL là gì?

A. Caramel Raspberry Lemon

B. Certified Recursive Listener

C. Certificate Recording Language

D. Certificate Revocation List

Đáp án: D

8. Tên của các phần tử tương tự nhau mà máy chủ thư mục tổ chức các phần tử bên trong là gì?

A. Đơn vị tổ chức (organizational units)

B. Nhóm (groups)

C. Cụm (clusters)

D. Cây (trees)

Đáp án: A

9. Đúng hay sai: Máy chủ truy cập mạng (network access server, NAS) xử lý xác thực trong lược đồ RADIUS.

A. Đúng

B. Sai

Đáp án: B

10. Đúng hay sai: Máy khách xác thực trực tiếp trên máy chủ RADIUS.

A. Đúng

B. Sai

Đáp án: B

11. Máy chủ xác thực Kerberos gây ra sự cố gì cho một máy khách mà đã xác thực thành công?

- A. Mật khẩu chính
- B. Khóa mã hóa
- C. Phiếu cấp vé
- D. Chứng chỉ số

Đáp án: C

12. Đăng nhập một lần mang lại lợi ích gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó cung cấp xác thực được mã hóa.
- B. Nó thực thi xác thực đa yếu tố.
- C. Nó làm giảm thời gian xác thực.
- D. Nó làm giảm tổng số thông tin đăng nhập.

Đáp án: C, D

13. OpenID cung cấp những gì?

- A. Ủy quyền xác thực
- B. Chữ ký điện tử
- C. Ký chứng chỉ
- D. Băm mã hóa

Đáp án: A

14. Ủy quyền có vai trò gì?

- A. Nó xác định xem một thực thể có quyền truy cập vào tài nguyên hay không.
- B. Nó xác minh danh tính của một thực thể.
- C. Nó xác minh mật khẩu.
- D. Nó cung cấp mã hóa mạnh mẽ.

Đáp án: A

15. OAuth cung cấp những gì?

- A. Tính bảo mật
- B. Tính toàn vẹn
- C. Ủy quyền truy cập
- D. Giao tiếp bảo mật

Đáp án: C

16. Kiểm toán liên quan đến kế toán như thế nào?

- A. Chúng không liên quan.
- B. Chúng giống nhau.
- C. Kế toán xem xét bản ghi, trong khi kiểm toán ghi lại việc truy xuất và sử dụng.
- D. Kế toán ghi lại việc truy xuất và sử dụng, trong khi kiểm toán xem xét các bản ghi này.

Đáp án: D

17. Authn viết tắt của từ _____.

- A. Authoritarian
- B. Authored
- C. Authentication
- D. Authorization

Đáp án: C

18. Hai loại mã mật khẩu dùng một lần là _____ và _____. Đánh dấu vào tất cả các câu phù hợp.

- A. Dựa trên mật khẩu
- B. Dựa trên danh tính
- C. Dựa trên bộ đếm
- D. Dựa trên thời gian

Đáp án: C, D

19. Chìa khóa bảo mật (security key) lý tưởng hơn trình tạo OTP vì chúng có khả năng chống lại các cuộc tấn công _____.

- A. Lừa đảo
- B. Vết cặn
- C. DDoS
- D. Mật khẩu

Đáp án: A

20. Kerberos sử dụng _____ làm mã xác thực.

- A. Vé
- B. Mật khẩu
- C. Khóa mã hóa
- D. Chứng chỉ

Đáp án: A

21. Mật khẩu nào sau đây là mật khẩu mạnh nhất để xác thực hệ thống?

- A. P@55wOrd!
- B. P@ssword!
- C. Password!
- D. P@w04d!\$\$L0N6

Đáp án: D

22. Giao thức LDAP sử dụng cấu trúc _____ để giữ các phần tử thư mục.

- A. Tên phân biệt (distinguished name)
- B. Cây thông tin dữ liệu (data information tree)
- C. Đơn vị tổ chức (organization unit)
- D. Liên kết (bind)

Đáp án: B

23. Cái nào được sử dụng để yêu cầu quyền truy cập vào các dịch vụ trong tiến trình Kerberos?

- A. ID máy khách

- B. Khóa phiên TGS
- C. Vé máy khách-đến-máy chủ
- D. Phiếu cấp vé

Đáp án: D

24. Nhiều thiết bị chuyển mạch khách và bộ định tuyến đã được thiết lập tại một căn cứ quân sự nhỏ. Nhóm mạng quyết định triển khai TACACS +, cùng với Kerberos và dịch vụ LDAP bên ngoài. Lý do chính TACACS + được chọn cho việc này là gì?

- A. Đăng nhập một lần
- B. NIPRNet
- C. Quản trị thiết bị
- D. Truy cập mạng

Đáp án: C

25. Những cái nào là ví dụ của dịch vụ đăng nhập một lần (SSO)? Đánh dấu vào tất cả các câu phù hợp.

- A. Mã thông báo (tokens)
- B. Các bên phụ thuộc (relying parties)
- C. OpenID
- D. Kerberos

Đáp án: C, D

26. Một công ty đang sử dụng các ứng dụng Google Business cho bộ phận tiếp thị. Các ứng dụng này có thể tạm thời truy cập vào tài khoản email của người dùng để gửi các liên kết cho việc đánh giá. Tại sao công ty nên sử dụng ủy quyền mở (OAuth) trong tình huống này?

- A. Sử dụng máy chủ trung tâm phân phối khóa
- B. Có được quyền truy xuất thông qua một điểm truy cập không dây
- C. Quản lý nhiều thiết bị mạng
- D. Khả năng tương thích với các ứng dụng của bên thứ ba

Đáp án: D

27. Một quản trị viên mạng đã triển khai hệ thống TACACS + để các quản trị viên khác có thể quản lý đúng cách nhiều thiết bị chuyển mạch và bộ định tuyến trên mạng cục bộ (LAN). Hệ thống sẽ theo dõi và ghi lại các truy xuất của quản trị viên vào từng thiết bị và các thay đổi được thực hiện. Việc "ghi nhật ký" này thỏa mãn phần nào của bảo mật AAA?

- A. Ủy quyền (authorization)
- B. Xác thực (authentication)
- C. Quản trị (administration)
- D. Kế toán (accounting)

Đáp án: D

Bảo mật mạng

1. Tại sao việc chuẩn hóa dữ liệu nhật ký lại quan trọng trong cấu hình ghi nhật ký tập trung?

- A. Rất khó để phân tích nhật ký bất thường.

- B. Chuẩn hóa nhật ký phát hiện các cuộc tấn công tiềm ẩn.
- C. Nhật ký được định dạng thống nhất sẽ dễ lưu trữ và phân tích hơn.
- D. Dữ liệu phải được giải mã trước khi gửi đến máy chủ nhật ký.

Đáp án: C

2. Những loại tấn công nào mà một người flood guard cần chống lại? Đánh dấu vào tất cả các câu phù hợp.

- A. Tấn công xen giữa
- B. Nhiễm mã độc
- C. Tấn công DDoS
- D. Tấn công SYN flood

Đáp án: C, D

3. DHCP Snooping bảo vệ chống lại điều gì?

- A. Tấn công giả mạo máy chủ DHCP
- B. Đánh cắp dữ liệu
- C. Tấn công vét cạn
- D. Tấn công DDoS

Đáp án: A

4. Dynamic ARP Inspection bảo vệ chống lại điều gì?

- A. Tấn công giả mạo máy chủ DHCP
- B. Tấn công DDoS

- C. Tấn công đầu độc ARP
- D. Nhiễm mã độc

Đáp án: C

5. IP Source Guard bảo vệ chống lại những gì?

- A. Tấn công DDoS
- B. Tấn công giả mạo máy chủ DHCP
- C. Tấn công vét cạn
- D. Tấn công giả mạo IP

Đáp án: D

6. EAP-TLS sử dụng gì để xác thực lẫn nhau của cả máy chủ và máy khách?

- A. Chứng chỉ kỹ thuật số
- B. Tên người dùng và mật khẩu
- C. Sinh trắc học
- D. Mật khẩu dùng một lần

Đáp án: A

7. Tại sao nên sử dụng cả tường lửa trên mạng và trên máy tính? Đánh dấu vào tất cả các câu phù hợp.

- A. Để bảo vệ các máy tính khỏi bị xâm nhập trên cùng một mạng
- B. Để bảo vệ khỏi các cuộc tấn công DDoS
- C. Để bảo vệ bản thân các thiết bị di động, như máy tính xách tay

D. Để bảo vệ khỏi các cuộc tấn công xen giữa

Đáp án: A, C

8. Một số điểm yếu của WEP là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Sử dụng mã hóa dòng RC4
- B. Sử dụng các ký tự ASCII cho cụm mật khẩu
- C. Kích thước hồ giá trị IV nhỏ
- D. Phương pháp phát sinh khóa kém

Đáp án: A, C, D

9. WPA2 sử dụng thuật toán mã hóa đối xứng nào?

- A. DES
- B. AES
- C. DSA
- D. RSA

Đáp án: B

10. Làm thế nào bạn có thể giảm khả năng xảy ra các cuộc tấn công vét cạn WPS? Đánh dấu vào tất cả các câu phù hợp.

- A. Tắt WPS.
- B. Cập nhật các quy tắc tường lửa.
- C. Thực hiện khóa hệ thống một lúc sau những lần thử không chính xác.
- D. Sử dụng một cụm mật khẩu rất dài và phức tạp.

Đáp án: A, C

11. Chọn cấu hình bảo mật WiFi an toàn nhất từ bên dưới:

- A. WPA cá nhân (WPA-Personal)
- B. WPA doanh nghiệp (WPA-Enterprise)
- C. WPA2 cá nhân (WPA3-Personal)
- D. WEP 128 bit
- E. WPA2 doanh nghiệp (WPA2-Enterprise)
- F. Không có

Đáp án: E

12. Tcpdump làm gì? Chọn tất cả những câu phù hợp.

- A. Bắt các gói tin
- B. Phát sinh gói tin
- C. Phân tích gói tin và cung cấp một phân tích dưới dạng văn bản
- D. Mã hóa gói tin

Đáp án: A, C

13. Wireshark làm gì khác với tcpdump? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó có giao diện đồ họa.
- B. Nó hiểu nhiều giao thức ở tầng ứng dụng hơn.
- C. Nó có thể nắm bắt các gói tin và phân tích chúng.

D. Nó có thể ghi gói tin vào một tập tin.

Đáp án: A, B

14. Bạn nên xem xét những yếu tố nào khi thiết kế cài đặt IDS? Đánh dấu vào tất cả các câu phù hợp.

- A. Bảng thông lưu lượng
- B. Dung lượng lưu trữ
- C. Loại hệ điều hành đang sử dụng
- D. Tốc độ kết nối Internet

Đáp án: A, B

15. Sự khác biệt giữa Hệ thống phát hiện xâm nhập (IDS) và Hệ thống ngăn chặn xâm nhập (IPS) là gì?

- A. IDS có thể chủ động chặn luồng tấn công, trong khi IPS chỉ có thể cảnh báo về luồng tấn công được phát hiện.
- B. IDS có thể phát hiện hoạt động phần mềm độc hại trên mạng, nhưng IPS thì không
- C. Một IDS có thể cảnh báo về luồng tấn công được phát hiện, nhưng IPS có thể chủ động chặn luồng tấn công.
- D. Chúng giống nhau

Đáp án: C

16. Những yếu tố nào sẽ hạn chế khả năng bắt các gói tin của bạn? Đánh dấu vào tất cả các câu phù hợp.

- A. Card mạng không ở chế độ giám sát (monitor mode) hoặc hỗn tạp (promiscuous mode)
- B. Phần mềm chống phần mềm độc hại
- C. Mã hóa
- D. Khả năng truy xuất đến luồng nghi vấn

Đáp án: A, D

17. Luồng truy cập nào mà quy tắc tường lửa từ chối ngầm?

- A. Mọi thứ không được phép
- B. Luồng đến
- C. Luồng đi
- D. Không có trừ khi bị chặn

Đáp án: A

18. Quá trình chuyển đổi các trường nhật ký thành định dạng chuẩn được gọi là _____.

- A. Chuẩn hóa nhật ký
- B. Kiểm tra nhật ký
- C. Phân tích nhật ký
- D. Mã hóa nhật ký

Đáp án: A

19. _____ có thể bảo vệ mạng của bạn khỏi các cuộc tấn công DoS.

- A. Flood Guard
- B. DHCP Snooping
- C. Dynamic ARP Inspection
- D. IP Source Guard

Đáp án: A

20. Việc sử dụng các VLAN khác nhau cho các thiết bị mạng khác nhau là một ví dụ về _____.

- A. Tách mạng
- B. Từ chối ngầm
- C. Truy cập từ xa
- D. Mã hóa mạng

Đáp án: A

21. Làm cách nào để bạn bảo vệ khỏi các cuộc tấn công giả mạo máy chủ DHCP?

- A. DHCP Snooping
- B. Flood Guard
- C. Dynamic ARP Inspection
- D. IP Source Guard

Đáp án: A

22. Dynamic ARP Inspection bảo vệ chống lại điều gì?

- A. Tấn công xen giữa ARP
- B. Tấn công giả mạo máy chủ ARP
- C. Tấn công DoS
- D. Tấn công giả mạo IP

Đáp án: A

23. IP Source Guard bảo vệ chống lại loại tấn công nào?

- A. Tấn công giả mạo IP
- B. Tấn công xen giữa ARP
- C. Tấn công DoS
- D. Tấn công giả mạo máy chủ DHCP

Đáp án: A

24. Một reverse proxy khác với proxy vì reverse proxy cung cấp _____.

- A. Truy cập từ xa
- B. Quyền riêng tư
- C. Bảo vệ DoS
- D. Xác thực

Đáp án: A

25. WEP sử dụng mã hóa đối xứng cơ bản nào?

- A. RC4
- B. AES

C. DES

D. RSA

Đáp án: A

26. Mã hóa WEP hỗ trợ độ dài khóa nào? Đánh dấu vào tất cả các câu phù hợp.

A. 40-bit

B. 64-bit

C. 128-bit

D. 256-bit

Đáp án: B, C

27. Cách được đề xuất để bảo vệ mạng WPA2 là gì? Đánh dấu vào tất cả các câu phù hợp.

A. Sử dụng một SSID duy nhất

B. Sử dụng cụm mật khẩu dài và phức tạp

C. Sử dụng WEP64

D. Ẩn SSID

Đáp án: A, B

28. Nếu bạn đang kết nối với một switch và card mạng của bạn đang ở chế độ hỗn tạp (promiscuous mode), bạn sẽ có thể bắt được luồng truy cập nào? Đánh dấu vào tất cả các câu phù hợp.

A. Luồng truy cập đến và đi từ máy của bạn

- B. Luồng broadcast
- C. Tất cả luồng trên switch
- D. Không có luồng nào

Đáp án: A, B

29. Bạn có thể sử dụng gì để bắt gói tin trên một switch?

- A. Port Mirroring
- B. Network hub
- C. DHCP Snooping
- D. Promiscuous Mode

Đáp án: A

30. Tcpdump làm gì?

- A. Thực hiện thu thập và phân tích gói tin
- B. Cơ sở dữ liệu mật khẩu vét cạn
- C. Phát sinh luồng tấn công DDoS
- D. Xử lý việc tiêm gói

Đáp án: A

31. So với tcpdump, Wireshark có _____ được hỗ trợ ở phạm vi rộng hơn nhiều.

- A. Giao thức
- B. Kích thước gói
- C. Loại gói

D. Ngôn ngữ

Đáp án: A

32. Hệ thống phát hiện xâm nhập mạng theo dõi luồng truy cập độc hại tiềm ẩn và _____ khi phát hiện một cuộc tấn công.

A. Kích hoạt cảnh báo

B. Chặn luồng

C. Tắt nguồn

D. Tắt quyền truy cập mạng

Đáp án: A

33. Hệ thống ngăn chặn xâm nhập mạng làm gì khi phát hiện một cuộc tấn công?

A. Nó kích hoạt một cảnh báo.

B. Nó chặn luồng truy cập mạng.

C. Nó không làm gì cả.

D. Nó tấn công trở lại.

Đáp án: B

Phòng thủ theo chiều sâu

1. Vectơ tấn công là gì?

A. Hướng tấn công đang diễn ra.

B. Một cơ chế mà kẻ tấn công có thể tương tác với mạng hoặc hệ thống của bạn.

C. Phân loại kiểu tấn công.

D. Mức độ nghiêm trọng của cuộc tấn công.

Đáp án: B

2. Việc vô hiệu hóa các thành phần không cần thiết phục vụ cho những mục đích nào? Đánh dấu vào tất cả các câu phù hợp.

A. Làm cho một hệ thống khó sử dụng hơn

B. Tăng hiệu suất

C. Giảm bề mặt tấn công

D. Đóng vectơ tấn công

Đáp án: C, D

3. Bề mặt tấn công là gì?

A. Tổng phạm vi của một cuộc tấn công

B. Mục tiêu hoặc nạn nhân của một cuộc tấn công

C. Dữ liệu của cuộc tấn công

D. Tổ hợp tất cả các vectơ tấn công trong một hệ thống hoặc mạng

Đáp án: D

4. Một chiến lược phòng thủ theo chiều sâu tốt sẽ liên quan đến việc triển khai tường lửa nào?

A. Không có tường lửa

- B. Chỉ tường lửa trên mạng
- C. Chỉ tường lửa trên máy tính
- D. Cả tường lửa trên máy tính và trên mạng

Đáp án: D

5. Sử dụng máy tính pháo đài (bastion host) cho phép điều nào sau đây?
Chọn tất cả những câu phù hợp.

- A. Thực thi các biện pháp an ninh chặt chẽ hơn
- B. Áp dụng các quy tắc tường lửa hạn chế hơn
- C. Có giám sát và ghi nhật ký chi tiết hơn
- D. Chạy nhiều phần mềm một cách an toàn

Đáp án: A, B, C

6. Ghi nhật ký tập trung mang lại những lợi ích gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó cho phép phân tích nhật ký dễ dàng hơn.
- B. Nó ngăn chặn việc đánh cắp cơ sở dữ liệu.
- C. Nó chặn sự lây nhiễm phần mềm độc hại.
- D. Nó giúp bảo mật nhật ký khỏi giả mạo hoặc phá hủy.

Đáp án: A, D

7. Một số thiếu sót của phần mềm diệt virus hiện nay là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó không thể bảo vệ khỏi các mối đe dọa chưa biết.

- B. Nó rất đắt.
- C. Nó chỉ bảo vệ chống lại virus.
- D. Nó chỉ phát hiện phần mềm độc hại, nhưng không bảo vệ chống lại nó.

Đáp án: A

8. Bằng cách nào danh sách trắng nhị phân là một lựa chọn tốt hơn phần mềm chống virus?

- A. Nó có thể chặn các mối đe dọa không xác định hoặc mới xuất hiện.
- B. Nó có ít tác động đến hiệu suất hơn.
- C. Nó rẻ hơn.
- D. Nó không tốt hơn. Nó thực sự khủng khiếp.

Đáp án: A

9. Mã hóa toàn đĩa bảo vệ chống lại điều gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Nhiễm phần mềm độc hại
- B. Đánh cắp dữ liệu
- C. Giả mạo tập tin hệ thống
- D. Các cuộc tấn công giả mạo IP

Đáp án: B, C

10. Mục đích của việc ký quỹ khóa mã hóa đĩa là gì?

- A. Ngăn chặn đánh cắp dữ liệu

- B. Cung cấp tính toàn vẹn của dữ liệu
- C. Thực hiện khôi phục dữ liệu
- D. Bảo vệ chống lại sự truy cập trái phép

Đáp án: C

11. Tại sao điều quan trọng là phải cập nhật phần mềm?

- A. Nó không quan trọng. Nó chỉ gây phiền phức.
- B. Để đảm bảo quyền truy cập vào các tính năng mới nhất.
- C. Để đảm bảo khả năng tương thích với các hệ thống khác.
- D. Để giải quyết bất kỳ lỗ hổng bảo mật nào được phát hiện.

Đáp án: D

12. Một số loại phần mềm mà bạn muốn có chính sách ứng dụng rõ ràng là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Trò chơi điện tử
- B. Bộ xử lý văn bản
- C. Phần mềm chia sẻ tập tin
- D. Bộ công cụ phát triển phần mềm

Đáp án: A, C

13. Đặc điểm chính của chiến lược bảo vệ chuyên sâu đối với bảo mật CNTT là gì?

- A. Bảo mật

- B. Mã hóa
- C. Mật khẩu mạnh
- D. Nhiều lớp phòng thủ đan xen nhau

Đáp án: D

14. Ghi nhật ký chi tiết phục vụ mục đích nào sau đây? Đánh dấu vào tất cả các câu phù hợp.

- A. Tái tạo sự kiện
- B. Bảo vệ dữ liệu
- C. Kiểm toán
- D. Phát hiện lỗ hổng bảo mật

Đáp án: A, C

15. Mọi loại lỗ hổng bảo mật chưa được biết đến trước khi chúng được khai thác là gì?

- A. Vectơ tấn công
- B. ACL
- C. Bề mặt tấn công
- D. 0-day

Đáp án: D

16. Một nhà phân tích an ninh mạng đã nhận được cảnh báo về mối đe dọa phần mềm độc hại tiềm ẩn trên máy tính của người dùng. Nhà phân tích có thể

xem xét những gì để có thông tin chi tiết về ý kiến này? Đánh dấu vào tất cả các câu phù hợp.

- A. Phần mềm danh sách trắng nhị phân
- B. Nhật ký
- C. Hệ thống quản lý sự kiện và thông tin bảo mật (SIEM)
- D. Mã hóa toàn bộ đĩa (FDE)

Đáp án: B, C

17. Nếu quên mật khẩu mã hóa toàn đĩa (FDE), thì điều gì có thể được kết hợp để lưu trữ an toàn khóa mã hóa để mở khóa đĩa?

- A. Chính sách ứng dụng
- B. Gia cố ứng dụng
- C. Ký quỹ khóa
- D. Khởi động an toàn

Đáp án: C

18. Mục đích của việc cài đặt các bản cập nhật trên máy tính của bạn là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Cập nhật giúp chặn tất cả luồng truy cập không mong muốn.
- B. Cập nhật thêm các tính năng mới.
- C. Cập nhật cải thiện hiệu suất và độ ổn định.
- D. Cập nhật các lỗ hổng bảo mật địa chỉ.

Đáp án: B, C, D

19. Một máy chủ xác thực lỗi được kết nối với internet và các dịch vụ nhạy cảm. Làm cách nào bạn có thể hạn chế các kết nối để bảo vệ máy chủ khỏi bị tin tặc xâm nhập? Đánh dấu vào tất cả các câu phù hợp.

- A. Tường lửa an toàn
- B. Danh sách kiểm soát truy cập (ACL)
- C. Quản lý bản vá
- D. Máy chủ pháo đài (bastion host)

Đáp án: A, B, D

Bảo mật trong công ty

1. Một số ví dụ về các mục tiêu bảo mật mà bạn có thể có cho một tổ chức là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Để bảo vệ dữ liệu của khách hàng khỏi bị truy cập trái phép.
- B. Để triển khai chính sách mật khẩu mạnh.
- C. Để ngăn chặn truy cập trái phép vào thông tin đăng nhập của khách hàng.
- D. Để triển khai hệ thống ngăn chặn xâm nhập.

Đáp án: A, C

2. Bạn sẽ coi mục tiêu nào có giá trị cao đối với kẻ tấn công tiềm năng? Đánh dấu vào tất cả các câu phù hợp.

- A. Thông tin thẻ tín dụng của khách hàng
- B. Cơ sở dữ liệu xác thực
- C. Máy in nối mạng

D. Máy chủ ghi nhật ký

Đáp án: A, B

3. Mục đích của máy quét lỗ hổng bảo mật là gì?

- A. Nó sửa chữa các lỗ hổng trên hệ thống.
- B. Nó phát hiện các lỗ hổng trên mạng và hệ thống của bạn.
- C. Nó bảo vệ mạng của bạn khỏi phần mềm độc hại.
- D. Nó chặn luồng độc hại xâm nhập vào mạng của bạn.

Đáp án: B

4. Một số bảo mật sẽ áp dụng cho dữ liệu nhạy cảm và bí mật là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó có thể được lưu trữ trên phương tiện di động.
- B. Nó chỉ có thể được lưu trữ trên phương tiện được mã hóa.
- C. Nó có thể được truy cập và lưu trữ trên các thiết bị cá nhân.
- D. Nó có thể được chuyển qua email.

Đáp án: B

5. Chính sách bảo mật được thiết kế để bảo vệ chống lại điều gì?

- A. Những kẻ tấn công đánh cắp dữ liệu khách hàng
- B. Nghe trộm thông tin liên lạc
- C. Tấn công từ chối dịch vụ
- D. Lạm dụng dữ liệu nhạy cảm

Đáp án: D

6. Bạn quan tâm đến việc sử dụng các dịch vụ của một công ty cung cấp. Bạn đánh giá khả năng bảo mật của họ như thế nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Giả sử rằng họ đang sử dụng các giải pháp tiêu chuẩn công nghiệp
- B. Yêu cầu toàn quyền truy cập vào hệ thống của họ để thực hiện đánh giá
- C. Yêu cầu họ hoàn thành bảng câu hỏi
- D. Yêu cầu họ cung cấp bất kỳ báo cáo kiểm tra thâm nhập hoặc đánh giá bảo mật nào

Đáp án: C, D

7. Mục tiêu của đào tạo bảo mật CNTT bắt buộc cho một tổ chức là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Để trừng phạt nhân viên có các biện pháp bảo mật kém
- B. Để huấn luyện nhân viên về cách giữ an toàn
- C. Để xây dựng một nền văn hóa ưu tiên bảo mật
- D. Để tránh sự cần thiết của một đội bảo vệ

Đáp án: B, C

8. Bước đầu tiên trong việc xử lý một sự cố là gì?

- A. Phát hiện sự cố
- B. Ngăn chặn sự cố

- C. Xóa hoặc diệt tận gốc sự cố
- D. Phục hồi sau sự cố

Đáp án: A

9. Làm thế nào để bạn bảo vệ khỏi một sự cố tương tự xảy ra trong tương lai?

- A. Cập nhật bản định nghĩa chống vi-rút của bạn.
- B. Thay đổi tất cả mật khẩu tài khoản.
- C. Tiến hành phân tích hậu sự cố.
- D. Hãy khoan tay và hy vọng những điều tốt đẹp nhất!

Đáp án: C

10. Những đặc điểm nào được sử dụng để đánh giá mức độ nghiêm trọng của các lỗ hổng được tìm thấy? Đánh dấu vào tất cả các câu phù hợp.

- A. Cơ hội của khai thác
- B. Sử dụng mã hóa hay không
- C. Loại quyền truy cập đã đạt được
- D. Có thể khai thác từ xa hay không

Đáp án: A, C, D

11. Mật khẩu mạnh là một bước tốt để bảo mật tốt, nhưng bạn nên làm gì khác để xác thực an toàn?

- A. Thay đổi mật khẩu định kỳ
- B. Xác thực 2 yếu tố

- C. Quét lỗ hổng bảo mật
- D. Thuật toán mã hóa mạnh

Đáp án: B

12. Hai bước xử lý và ứng phó sự cố đầu tiên là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Phát hiện sự cố
- B. Ngăn chặn sự cố
- C. Loại bỏ sự cố
- D. Phục hồi sau sự cố

Đáp án: A, B

13. Ngoài việc khôi phục các hoạt động và dữ liệu thông thường, bạn nên làm gì khác trong giai đoạn khôi phục?

- A. Sửa chữa nguyên nhân gốc rễ bên dưới
- B. Cập nhật tài liệu
- C. Đưa hệ thống vào ngoại tuyến
- D. Đổ lỗi cho sự cố

Đáp án: A

14. Đánh giá rủi ro bảo mật bắt đầu bằng _____.

- A. Xử lý thanh toán
- B. Những kẻ tấn công bên ngoài

- C. Tác động của tấn công
- D. Mô hình hóa mối đe dọa

Đáp án: D

15. Công ty của bạn muốn thiết lập các thực thi tốt về quyền riêng tư tại nơi làm việc để dữ liệu của nhân viên và khách hàng được bảo vệ đúng cách. Các chính sách bảo mật được thiết lập và xác định rõ ràng đã được áp dụng, nhưng chúng cũng cần phải được thực thi. Một số cách để thực thi các chính sách bảo mật này là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Ít đặc quyền
- B. Kiểm tra nhật ký truy cập
- C. In thông tin khách hàng
- D. Kết nối VPN

Đáp án: A, B

16. Các chính sách xử lý dữ liệu thường cấm lưu trữ thông tin bí mật trên thiết bị nào trong số các thiết bị này? Đánh dấu vào tất cả các câu phù hợp.

- A. Các chia sẻ tập tin truy xuất bị giới hạn
- B. Ổ đĩa cứng portal được mã hóa
- C. Thẻ USB
- D. Đĩa CD

Đáp án: C, D

17. Đồng nghiệp cần chia sẻ tập tin nhạy cảm với bạn nhưng tập tin này quá lớn để gửi qua email được mã hóa. Đồng nghiệp làm việc tại một văn phòng từ

xa. Bạn làm việc tại trụ sở chính. Tùy chọn nào trong số các tùy chọn sau có nhiều khả năng được các chính sách bảo mật của công ty chấp thuận nhất? Đánh dấu vào tất cả các câu phù hợp.

- A. Chia sẻ trực tiếp qua VPN
- B. Tải lên ổ đĩa Google cá nhân
- C. Tải lên OneDrive cá nhân
- D. Tải lên bộ nhớ đám mây an toàn của công ty.

Đáp án: A, D

18. Ban lãnh đạo muốn xây dựng một nền văn hóa nơi nhân viên luôn lưu ý đến vấn đề bảo mật. Nhân viên có thể truy cập thông tin một cách tự do và cung cấp phản hồi hoặc đề xuất mà không phải lo lắng. Ý tưởng nào trong số này là những ý tưởng tuyệt vời cho loại hình văn hóa này? Đánh dấu vào tất cả các câu phù hợp.

- A. Phần mềm giám sát máy tính để bàn
- B. Mang thiết bị của riêng bạn
- C. Áp phích tuyên truyền hành xử bảo mật tốt
- D. Hộp thư góp ý

Đáp án: C, D

19. Bước đầu tiên của việc xử lý một sự cố là _____ sự cố.

- A. hiểu
- B. dò tìm
- C. đổ lỗi
- D. làm ngơ

Đáp án: B

20. Sau khi một bản sao lưu tốt được khôi phục và các lỗ hổng bảo mật được đóng lại, các hệ thống nên được _____ hoàn toàn.

- A. chuyển nền tảng
- B. kiểm tra
- C. hỗ trợ
- D. loại bỏ

Đáp án: B

21. Tình huống áp dụng

Nhiệm vụ: Trong một dự án, bạn sẽ tạo một tài liệu thiết kế cơ sở hạ tầng bảo mật cho một tổ chức hư cấu. Các dịch vụ và công cụ bảo mật mà bạn mô tả trong tài liệu phải có khả năng đáp ứng nhu cầu của tổ chức. Công việc của bạn sẽ được đánh giá dựa trên mức độ bạn đáp ứng các yêu cầu của tổ chức.

Về tổ chức : Tổ chức hư cấu này có một cơ sở nhân viên nhỏ, nhưng đang phát triển, với 50 nhân viên trong một văn phòng nhỏ. Công ty là nhà bán lẻ trực tuyến các vật dụng thủ công, thủ công tốt nhất thế giới. Họ đã thuê bạn làm cố vấn bảo mật để giúp đưa hoạt động của họ vào hoạt động tốt hơn.

Yêu cầu của tổ chức: Với tư cách là nhà tư vấn bảo mật, công ty cần bạn bổ sung các biện pháp bảo mật cho các hệ thống sau:

- Trang web bên ngoài cho phép người dùng duyệt và mua các vật dụng
- Trang web mạng nội bộ cho nhân viên sử dụng
- Bảo mật quyền truy cập từ xa cho nhân viên kỹ thuật
- Các quy tắc tường lửa cơ bản, hợp lý
- Phủ sóng không dây trong văn phòng

- Cấu hình an toàn hợp lý cho máy tính xách tay

Vì đây là một công ty bán lẻ sẽ xử lý dữ liệu thanh toán của khách hàng, tổ chức này muốn hết sức thận trọng về quyền riêng tư. Họ không muốn thông tin khách hàng rơi vào tay kẻ tấn công do nhiễm phần mềm độc hại hoặc thiết bị bị mất.

Các kỹ sư sẽ yêu cầu quyền truy cập vào các trang web nội bộ, cùng với quyền truy cập từ xa, chạy dòng lệnh vào các máy trạm của họ.

Những gì bạn sẽ làm: Bạn sẽ tạo một tài liệu thiết kế cơ sở hạ tầng bảo mật cho tổ chức hư cấu này. Kế hoạch của bạn cần đáp ứng các yêu cầu của tổ chức và các yếu tố sau phải được kết hợp vào kế hoạch của bạn:

- Hệ thống xác thực
- Bảo mật trang web bên ngoài
- Bảo mật trang web nội bộ
- Giải pháp truy cập từ xa
- Các đề xuất về tường lửa và các quy tắc cơ bản
- Bảo mật không dây
- Đề xuất cấu hình VLAN
- Cấu hình bảo mật máy tính xách tay
- Đề xuất chính sách ứng dụng
- Các khuyến nghị về chính sách bảo mật và quyền riêng tư
- Phát hiện hoặc ngăn chặn xâm nhập đối với hệ thống chứa dữ liệu khách hàng

Đáp án:

Một bài nộp tuyệt vời nên bao gồm:

- Hai yêu cầu hệ thống xác thực, chẳng hạn như đa yếu tố dựa trên Khóa bảo mật hoặc đa yếu tố dựa trên OTP và một số loại hệ thống xác thực tập trung (ví dụ: LDAP hoặc Active Directory).

- Mô tả về HTTPS.

- Đề xuất cho cả dịch vụ VPN và giải pháp reverse proxy.

- Mô tả về hai hoặc nhiều loại dịch vụ tường lửa (ví dụ: quy tắc từ chối ngầm, truy cập từ xa, trang web).

- Yêu cầu đối với 802.1X.

- Mô tả về bốn yêu cầu của VLAN, bao gồm VLAN kỹ thuật, VLAN bán hàng, VLAN cơ sở hạ tầng và VLAN khách.

- Ba yêu cầu bảo mật máy tính xách tay, bao gồm khuyến nghị FDE, đề xuất chống vi-rút và đề xuất danh sách trắng nhị phân.

- Yêu cầu đối với chính sách yêu cầu cập nhật phần mềm và yêu cầu về các hạn chế đối với các loại ứng dụng được phép.

- Đề xuất cho các quy tắc bảo vệ quyền truy cập vào dữ liệu người dùng và các quy tắc bảo vệ việc lưu trữ dữ liệu người dùng.

- Mô tả bốn trong số các khuyến nghị về chính sách bảo mật sau: mật khẩu yêu cầu tối thiểu 8 ký tự; mật khẩu yêu cầu các ký tự đặc biệt; yêu cầu thay đổi mật khẩu định kỳ > 6 tháng; và một số hình thức đào tạo bảo mật bắt buộc cho người dùng.

- Yêu cầu đối với NIPS / NIDS trên mạng đối với dữ liệu khách hàng và yêu cầu đối với HIPS / HIDS trên hệ thống chứa dữ liệu khách hàng.