BẢO MẬT WI-FI: LỰA CHỌN GIẢI PHÁP NÀO?

Bảo mật là vấn đề rất quan trọng và đặc biệt rất được sự quan tâm của những doanh nghiệp. Không những thế, bảo mật cũng là nguyên nhân khiến doanh nghiệp e ngại khi cài đặt mạng cục bộ không dây (wireless LAN). Họ lo ngại về bảo mật trong WEP(Wired Equivalent Privacy), và quan t

Bảo mật là vấn đề rất quan trọng và đặc biệt rất được sự quan tâm của những doanh nghiệp. Không những thế, bảo mật cũng là nguyên nhân khiến doanh nghiệp e ngại khi cài đặt mạng cục bộ không dây (wireless LAN). Họ lo ngại về bảo mật trong WEP(Wired Equivalent Privacy), và quan tâm tới những giải pháp bảo mật mới thay thế an toàn hơn. IEEE và Wi-Fi Alliance đã phát triển một giải pháp bảo mật hơn là: Bảo vệ truy cập Wi-Fi WPA (Wi-Fi Protected Access) và IEEE 802.11i (cũng được gọi là "WPA2 Certified" theo Wi-Fi Alliance) và một giải pháp khác mang tên VPN Fix cũng giúp tăng cường bảo mật mạng không dây. Theo như Webtorial, WPA và 802.11i được sử dụng tương ứng là 29% và 22%. Mặt khác, 42% được sử dụng cho các "giải pháp tình thế" khác như: bảo mật hệ thống mạng riêng ảo VPN (Vitual Private Network) qua mạng cục bộ không dây. Vậy, chúng ta nên lựa chọn giải pháp bảo mật nào cho mạng không dây? WEP: Bảo mật quá tồi WEP (Wired Equivalent Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn. WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy cập vào trong mạng, và cũng được sử dụng để mã hoá truyền dữ liệu. Rất đơn giản, các khoá mã hoá này dễ dàng bị "bẻ gãy" bởi thuật toán brute-force và kiểu tấn công thử lỗi (trial-and-error). Các phần mềm miễn phí như Airsnort hoặc WEPCrack sẽ cho phép hacker có thể phá vỡ khoá mã hoá nếu họ thu thập đủ từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khoá mã hoá 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hoá nên chỉ có 104 bit được sử dụng để mã hoá, và cách thức cũng giống như mã hoá có độ dài 64 bit nên mã hoá 128 bit cũng dễ dàng bị bẻ khoá. Ngoài ra, những điểm yếu trong những vector khởi tạo khoá mã hoá giúp cho hacker có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều. Không dự đoán được những lỗi trong khoá mã hoá, WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khoá mã hoá mới cho mỗi phiên làm việc. Khoá mã hoá sẽ thay đổi trên mỗi phiên làm việc. Điều này sẽ gây khó khăn hơn cho hacker thu thập đủ các gói dữ liệu cần thiết để có thể bẽ gãy khoá bảo mật. Giải pháp tình thế: VPN (Vitual Private Network) Fix Nhận ra sự yếu kém của WEP, những người sử dụng doanh nghiệp đã khám phá ra một cách hiệu quả để bảo vệ mạng không dây WLAN của mình, được gọi là VPN Fix. Ý tưởng cơ bản của phương pháp này là coi những người sử dụng WLAN như những người sử dụng dịch vụ truy cập từ xa. Trong cách cấu hình này, tất các những điểm truy cập WLAN, và cũng như các máy tính được kết nối vào các điểm truy cập này, đều được định nghĩa trong một mạng LAN ảo (Vitual LAN). Trong cơ sở hạ tầng bảo mật, các thiết bị này được đối xử như là "không tin tưởng". Trước khi bất cứ các thiết bị WLAN được kết nối, chúng sẽ phải được sự cho phép từ thành phần bảo mật của mạng LAN. Dữ liệu cũng như kết nối của các thiết bị sẽ phải chạy qua một máy chủ xác thực như RADIUS chẳng hạn... Tiếp đó, kết nối sẽ được thiết lập thành một tuyến kết nối bảo mật đã được mã hoá bởi một giao thức bảo mật ví dụ như IPSec, giống như khi sử dụng các dịch vụ truy cập từ xa qua Internet. Tuy nhiên, giải pháp này cũng không phải là hoàn hảo, VPN Fix cần lưu lượng VPN lớn hơn cho

tường lửa, và cần phải tạo các thủ tục khởi tạo cho từng người sử dụng. Hơn nữa, IPSec lại không hỗ những thiết bị có nhiều chức năng riêng như thiết bị cầm tay, máy quét mã vạch... Cuối cùng, về quan điểm kiến trúc mạng, cấu hình theo VPN chỉ là một giải pháp tình thế chứ không phải là sự kết hợp với WLAN. Giải pháp bảo mật bằng xác thực Một sự thật là khi đã khám phá ra những lỗi về bảo mật trong mạng LAN không dây, ngành công nghiệp đã phải tốn rất nhiều công sức để giải quyết bài toán này. Một điều cần ghi nhớ là chúng ta cần phải đối diện với 2 vấn đề: xác thực và bảo mật thông tin. Xác thực nhằm đảm bảo chắc chắn người sử dụng hợp pháp có thể truy cập vào mạng. Bảo mật giữ cho truyền dữ liệu an toàn và không bị lấy trộm trên đường truyền. Một trong những ưu điểm của xác thực là IEEE 802.1x sử dụng giao thức xác thực mở rộng EAP (Extensible Authentication Protocol). EAP thực sự là một cơ sở tốt cho xác thực, và có thể được sử dụng với một vài các giao thức xác thực khác. Những giao thức đó bao gồm MD5, Transport Layer Security (TLS), Tunneled TLS (TTLS), Protected EAP (PEAP) và Cisco's Lightweight EAP (LEAP). Thật may mắn, sự lựa chọn giao thức xác thực chỉ cần vài yếu tố cơ bản. Trước hết, một cơ chế chỉ cần cung cấp một hoặc 2 cách xác thực, có thể gọi là sự xác thực qua lại (mutual authentication), có nghĩa là mạng sẽ xác thực người sử dụng và người sử dụng cũng sẽ xác thực lại mạng. Điều này rất quan trọng với mạng WLAN, bởi hacker có thể thêm điểm truy cập trái phép nào đó vào giữa các thiết bị mạng và các điểm truy cập hợp pháp (kiểu tấn công man-in-the-middle), để chặn và thay đổi các gói tin trên đường truyền dữ liệu. Và phương thức mã hoá MD5 không cung cấp xác thực qua lại nên cũng không được khuyến khích sử dụng WLAN. Chuẩn mã hoá 802.11i hay WPA2 Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mĩ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này. Và chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mĩ để bảo vệ các thông tin nhạy cảm. Nếu muốn biết chi tiết về cách làm việc của thuật toán Rijndael, bạn có thể ghé thăm http://en.wikipedia.org/wiki/Rijndael Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít card mạng WLAN hoặc các điểm truy cập có hỗ trợ mã hoá bằng phần cứng tại thời điểm hiện tại. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i. WPA (Wi-Fi Protected Access) Nhận thấy được những khó khăn khi nâng cấp lên 802.11i, Wi-Fi Alliance đã đưa ra giải pháp khác gọi là Wi-Fi Protected Access (WPA). Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol). WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. Một trong những điểm hấp dẫn nhất của WPA là không yêu cầu nâng cấp phần cứng. Các nâng cấp miễn phí về phần mềm cho hầu hết các card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn. Tuy nhiên, WPA cũng không hỗ trợ các thiết bị cầm tay và máy quét mã vạch. Theo Wi-Fi Alliance, có khoảng 200

thiết bị đã được cấp chứng nhận tương thích WPA. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn này đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc. Trong khi Wi-Fi Alliance đã đưa ra WPA, và được coi là loại trừ mọi lỗ hổng dễ bị tấn công của WEP, nhưng người sử dụng vẫn không thực sự tin tưởng vào WPA. Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "PASSWORD" để làm mật khẩu). Điều này cũng có nghĩa rằng kĩ thuật TKIP của WPA chỉ là giải pháp tạm thời , chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ. Kết luận Trong khi sử dụng VPN Fix qua các kết nối WLAN có thể là một ý tưởng hay và cũng sẽ là một hướng đi đúng. Nhưng sự không thuận tiện cũng như giá cả và tăng lưu lượng mạng cũng là rào cản cần vượt qua. Sự chuyển đổi sang 802.11i và mã hoá AES đem lại khả năng bảo mật cao nhất. Nhưng các tổ chức, cơ quan vẫn đang sử dụng hàng nghìn những card mạng WLAN không hỗ trợ chuẩn này. Hơn nữa AES không hỗ các thiết bị cầm tay và máy quét mã vạch hoặc các thiết bị khác... Đó là những giới hạn khi lựa chọn 802.11i. Sự chuyển hướng sang WPA vẫn còn là những thử thách. Mặc dù, vẫn còn những lỗ hổng về bảo mật và có thể những lỗ hổng mới sẽ được phát hiện. Nhưng tại thời điểm này, WPA là lựa chọn tốt. Minh Phúc