## Các công cụ bảo mật Wi-Fi miễn phí

**Bài viết giới thiệu đến bạn một số công cụ sử dụng trong mạng Wi-Fi: công cụ tìm kiếm và bảo mật chuyển vùng (roaming security)…**

Bảo mật Wi-Fi trải qua một chặng đường dài từ lúc bộ định tuyến không dây (wireless router) không hỗ trợ mã hóa hay hỗ trợ không đầy đủ, và đôi khi người dùng bỏ qua thao tác thay đổi mật khẩu mặc định cho việc truy cập vào cổng thông tin này.

This image has been resized. Click this bar to view the full image. The original image is sized 640x307px.

Vấn đề ở trên là do các sản phẩm được thiết kế khá nghèo nàn, hãng sản xuất không quan tâm đến công nghệ bảo mật then chốt, và một phần cũng do sự thiếu hiểu biết của người dùng dẫn đến việc phát tán thông tin lên web, e-mail thông qua tầm phủ sóng vô tuyến vốn mạnh mẽ.

Trải qua một quá trình phát triển, hầu hết các router Wi-Fi thế hệ mới nhất (802.11n) đều yêu cầu nhập tên và mật khẩu truy cập trong quá trình cài đặt, mã hóa WPA2 hiện khá an toàn, hacker khó bẻ khóa hơn.

Tuy nhiên, vấn đề bảo mật không dây luôn "nóng" vì người dùng thường kết nối thông qua các điểm truy cập công cộng, đôi khi ngoài máy tính, người dùng còn sử dụng các thiết bị khác để kết nối, chẳng hạn điện thoại, máy tính bảng…

Thông thường, WPA2 sử dụng mã hóa 128bit hay cao hơn. Nhưng không phải tất cả người dùng đều sử dụng chế độ mã hóa này, đây chính là lớp mã hóa cơ bản nhất của bảo mật mạng không dây. Lỗ hỏng này luôn ở máy tính, đặc biệt khi chuyển vùng (roaming) từ nhà, các mối đe dọa tấn

công kỹ thuật mạng xã hội bằng tin tặc (hijacking) hay dò tim (sniffing) qua kết nối không dây.

## Các công cụ bảo mật cơ bản

Gõ cụm từ **“wireless tool**s” vào thanh công cụ tìm kiếm, bạn sẽ nhận được rất nhiều kết quả trả về, từ các công cụ tấn công cho đến bẻ khóa máy người dùng kết nối qua mạng Wi-Fi. Đây là những nhu cầu có thật cho dù để trở thành tin tặc (black hat) hay nắm rõ thông tin để dập tắt các nguy cơ tiềm ẩn. Tuy vậy, nhìn chung đây chỉ là tiện ích cơ bản dành cho máy tính xách tay để quan sát các điểm truy cập xung quanh bạn. Sau đây là các tiện ích Wi-Fi, bạn có thể tải về miễn phí.

### InSSIDer

**InSSIDer** là tiện ích khá tốt của hãng *MetaGeek* (tải về miễn phí tại đây), chủ yếu được sử dụng để khắc phục sự cố về tín hiệu không dây, nhiễu từ phía các điểm truy cập khác. Tuy nhiên, công cụ này cũng sẽ thông báo đến tất cả các thiết bị Wi-Fi đang sử dụng các SSID trong khu vực. Từ công cụ này, bạn có thể "thấy" cường độ tín hiệu (thể hiện bằng số – càng nhỏ càng tốt), độ tin cậy và xem các điểm truy cập có sử dụng mã hóa hay không. Công cụ này chạy trên hệ điều hành (HĐH) Windows. Bạn có thể gặp rắc rối nếu không có bất kỳ công cụ nào để phân biệt đâu là "kẻ xấu", "người tốt". Liệu có nên kết nối đến điểm truy cập (Access Point – AP) ở nơi công cộng không? Hãy thử dùng

InSSIDer vì là tiện ích được đánh giá khá tốt từ người dùng am hiểu về kỹ thuật cho đến người dùng thông thường.

Sau khi được cài đặt trên máy tính xách tay, chọn lựa thông tin card không dây, **InSSIDer** sẽ quét và hiển thị các mạng không dây hiện hữu, phân tích thông tin tín hiệu mạng đang kết nối. Phần thông tin hiển thị hữu ích với những số liệu về tín hiệu mạng không dây ở những vị trí khác nhau trong phạm vi phủ sóng. Bạn sẽ biết được đặt máy tại vị trí nào thì thu được tín hiệu mạnh nhất. Do đó, InSSIDer thường dùng để phân tích mạng Wi-Fi, tìm ra nơi sóng mạnh/yếu. Hơn nữa, những thông tin như điểm truy cập nào đó đang sử dụng chế độ bảo mật nào, địa chỉ MAC của bộ định tuyến (router)… cũng hiển thị song song với tín hiệu mạng.

**Wi-Fi Inspector**


**Wi-Fi Inspecto**r là công cụ của Xirrius (tải về miễn phí tại đây). Đây là công cụ có chức năng tương tự InSSIDer nhưng chi tiết hơn. Một tính năng hữu ích là có thể vẽ biểu đồ hướng và

khoảng cách của các điểm truy cập. Công cụ này hoàn tất công việc nhanh hơn tiếng "bíp" của dụng cụ dò và đo bức xạ Geiger. Đây có thể là một công cụ hữu ích trong việc xác định điểm truy cập lừa đảo.

**Wi-Fi Inspector** cũng là công cụ tuyệt vời trong việc khắc phục sự cố kết nối. Ngoài ra, công cụ này cũng giúp đánh giá tốc độ kết nối và chất lượng dịch vụ của các điểm truy cập nội bộ. Wi-Fi Inspector có thể sử dụng trong quản lý môi trường sóng vô tuyến nội bộ.

## Công cụ bảo vệ chuyển vùng

Một bước tiến xa hơn nữa là các công cụ được thiết kế để quản lý bảo mật ở nơi công cộng, những rủi ro hay gặp nhất khi truy cập Wi-Fi công cộng. Một điều lạ là đa số người dùng bỏ qua nguy cơ này và không sử dụng thường xuyên tính năng hữu ích của công cụ.


**WeFi** (tải về tại đây) là công cụ định hướng cộng đồng để định vị miễn phí và là "*bạn đồng hành*" với các điểm truy cập không dây phát triển trên nhiều nền tảng khác nhau như

Windows, Mac, Android, Symbian và Windows Mobile. Tính năng bảo mật đầu tiên cho phép người dùng truy cập vào thư mục bản đồ miễn phí để tìm các điểm truy cập đáng tin cậy tại khu vực đó, xem thông tin về giá dịch vụ Wi-Fi để có thể chọn dịch vụ có giá thấp.

Trình quản lý kết nối của WeFi cho phép tùy biến dễ dàng để thiết lập máy tính xách tay kết nối đến điểm truy cập mong muốn ở nhiều vị trí khác nhau, bất kể ở nhà hay nơi công cộng. Tiện ích này cho phép đăng nhập tự động vào trang web quản lý của một số điểm truy cập đã biết. Tuy nhiên, việc đăng nhập tự động bao giờ cũng tiềm ẩn nhiều nguy cơ, nhất là ở nơi công cộng. Ngoài ra, bạn có thể đăng nhập vào trang WeFi thông qua tài khoản Facebook. WeFi Basic là phiên bản miễn phí có thể đáp ứng đầy đủ nhu cầu của hầu hết người dùng. Ngoài ra, nếu có nhu cầu cao hơn, bạn có thể mua phiên bản
WeFi Premium.

**Easy WiFi** (tải về tại đây) cung cấp một số tính năng tương tự WeFi, bao gồm

chế độ tự động đăng nhập vào các cổng thông tin (captive portals) và dữ liệu mã hóa nhạy cảm chuyển đến/đi từ các máy chủ Easy WiFi. Phần mềm miễn phí này cho phép chống evil twin (tạo trang web giả) bằng cách chứng thực chứng nhận bảo mật trên điểm truy cập Wi-Fi. Nếu chứng thực trên điểm truy cập Wi-Fi thất bại, ứng dụng sẽ khóa kết nối.Tính năng bảo mật này khá hữu ích cho lớp phòng thủ. Ngoài hỗ trợ cho HĐH Windows, Mac, Easy WiFi còn có phiên bản dành cho điện thoại di động dùng HĐH Android, iPhone/iPad, Nokia S60, HĐH Windows Mobile dùng trên các thiết bị di động.

**Avanquest Connection Manager** (tải về tại đây) là phần mềm miễn phí hữu ích cho người dùng doanh nghiệp và gia đình. Về nguyên tắc, đây là công cụ quản lý kết nối trong văn phòng (máy in, ánh xạ ổ đĩa, e-mail), tại nhà (thiết lập truy cập Wi-Fi) và đôi khi có cả thiết lập chuyển vùng (roaming), nhưng khả năng quản lý các thiết lập bảo mật VPN và di chuyển giữa các tên miền còn khá sơ sài.

**Xác thực không dây**

Người dùng Wi-Fi truy cập qua VPN sẽ nhận được mã hóa miễn phí, bất kể AP hỗ trợ trình mã hóa Wi-Fi nào. Bên cạnh đó, người dùng cũng có thể truy cập vào máy chủ xác thực RADIUS, trong đó sẽ kiểm tra bằng loạt giao thức mạnh hơn mã truy cập vào AP thông thường.

Các chuyên gia cho rằng, không lâu nữa dịch vụ xác thực **SecureMyWiFi** của Witopia sẽ sẵn sàng, hiện tại công ty này đang tập trung vào dịch vụ di động thay vì VPN. Điều này có nghĩa là RADIUS sẽ phổ biến hơn, kể cả những router Wi-Fi gia đình.

> **¼ mạng không dùng bảo mật**
>
> Người dùng kết nối đến bất kỳ nơi nào có thể, không quan tâm đến an toàn dữ liệu cá nhân. Đó là một thực tế cần sớm khắc phục.
>
> Từ khi bảo mật mạng Wi-Fi được coi là vấn đề quan trọng, trong một khảo sát gần đây tại Anh có đến ¼ AP "thả cửa". Tệ hơn nữa, phần lớn người dùng rất sung sướng khi được "xài chùa" tại một số điểm truy cập tại trung tâm thành

phố, không yêu cầu bất cứ điều gì, “cửa mở tự do” dẫn đến nguy cơ đánh cắp dữ liệu rất lớn. Tại London, theo khảo sát có đến 4.746/ 4.908 người không thiết lập mã hóa cho AP của họ, ở Birmingham có 910/ 3.753, còn Manchester là 870/ 2.894.

Hành vi “vô tư” của người dùng tại nơi công cộng có lẽ là vấn đề đáng lo ngại nhất, nhiều người dùng sẵn sàng kết nối để kiểm tra điểm truy cập đang được thiết lập ở trạng thái “mở”. Một hacker mũ trắng cho rằng mọi người hay nghĩ tội phạm mạng phải sử dụng các kỹ thuật tinh vi để đăng nhập vào mạng. Tuy nhiên, để làm được điều này, hacker chỉ cần có một máy tính xách tay và phần mềm được phổ biến rộng rãi trên mạng.

Giải pháp đề nghị cho những người dùng hay kết nối đến các điểm truy cập công cộng là nên sử dụng mạng mở thông qua kết nối VPN. VPN cung cấp kênh mã hóa giúp khắc phục

tình trạng an ninh kém của các điểm truy cập. Ngoài ra, còn rất nhiều tiện ích bảo vệ máy tính nơi công cộng, ngay bây giờ bạn có thể chọn cho mình một công cụ bảo mật mạng Wi-Fi miễn phí riêng để đảm bảo dữ liệu của bạn an toàn.

# 8 công cụ bảo mật Wi-Fi miễn phí tốt nhất

Dưới đây là một số công cụ hữu ích, đa phần có thể sử dụng trên các hệ điều hành phổ biến hiện nay như Windows, MacOS X hay Linux, với chúng bạn có thể nhìn thấy tất cả các Access Point (AP - điểm truy cập mạng không dây) ở gần kèm theo các thông tin chi tiết như kênh, tần số tín hiệu, địa chỉ MAC.

Ngay cả khi bạn đã có một bộ phân tích phổ sóng Wi-Fi chuyên nghiệp như Wi-Spy hay AirMagnet, các công cụ bảo mật Wi-Fi miễn phí vẫn rất hữu dụng. Những công cụ này có thể được dùng để thiết kế hoặc cài đặt mạng không dây, khắc phục sự cố hay bảo trì.

1. NetStumbler

NetStumbler là một trong những công cụ lâu đời nhất và nổi tiếng nhất hiện nay. NetStumbler chạy trên hệ điều hành Windows và Windows CE/Mobile, giúp liệt kê các AP ở gần và các thông tin cơ bản như: SSID, kênh, tốc độ, địa chỉ MAC, hãng sản xuất và chuẩn mã hóa.

Không giống như các công cụ khác, NetStumbler không chỉ hiển thị tín hiệu, nhiễu và tỉ lệ nhiễu, mà còn hỗ trợ định vị GPS nhằm xác định vị trí của các AP này. Tuy nhiên công cụ này đã không được cập nhật thêm kể từ năm 2004 và có thể không chạy ổn định trên các hệ điều hành Windows Vista/Windows 7 và các thậm chí là Windows XP 64 bit., chúng không hiển

thị thực sự chính xác chuẩn mã hóa của AP, ví dụ chúng luôn hiển thị AP được mã hóa với chuẩn WEP trong khi thực tế có thể là WPA hay WPA2.

2. Vistumbler

Vistumbler là chương trình phân tích sóng Wi-Fi mã nguồn mở đầu tiên được phát hành vào năm 2007 và được cập nhật mới nhất vào năm 2010. Vistumbler hiển thị thông tin cơ bản về AP, bao gồm chính xác cách mã hóa và xác thực, cả SSID và RSSI của AP.

Tương tự như NetStumbler, bạn có thể xem danh sách tất cả các AP hay theo phân loại kiểu xác thực, mã hóa, kênh, kiểu mạng và SSID. Thay vì chỉ hiển thị dạng văn bản, Vistumbler cho phép bạn có thể xem cả biểu đồ tín hiệu của AP. Ngoài ra, Vistumbler rất dễ tùy biến và có các tùy chọn cấu hình rất linh hoạt. Vistumbler hỗ trợ GPS, giúp định vị chính xác vị trí của các AP theo thời gian thực thông qua Google Earth.

Tuy nhiên, không giống như NetStumbler, Vistumbler chỉ cho bạn thông tin về mức độ tín hiện mà không hiển thị nhiễu. Ứng dụng này cũng chỉ hỗ trợ cho 2 hệ điều hành Windows Vista và Windows 7.

3. InSSIDer

InSSIDer là phần mềm phân tích sóng Wi-Fi nguồn mở khá mới hiện nay, cho phép hiển thị thông tin chi tiết về danh sách các AP, tuy nhiên InSSIDer chỉ hiển thị được RSSI mà không hiển thị chính xác phương thức xác thực của AP, không hiển thị được nhiễu và tỉ lệ nhiễu trên tín hiệu (SNR).

Song tiện ích này lại có chức năng hiển thị biểu đồ rất tốt. Mức tín hiệu được hiển thị trên biểu đồ theo thời gian quãng 5 phút. Sau đó có một đồ thị cho mỗi kênh 2.4GHz và 5GHz, hiển thị mức tín hiệu hiện tại và chiều rộng kênh của mỗi AP. Bạn có thể lọc các AP dựa theo dải tần, kênh, tín hiệu, mức độ bảo mật. InSSIDer cũng hỗ trợ chức năng GPS và cho phép truy cập kèm Google Earth.

4. NetSurveyor


NetSurveyor là công cụ miễn phí nhưng ở dạng nguồn đóng, được cập nhật lần cuối vào năm 2009, khi thực thi sẽ hiển thị các thông tin cơ bản của các AP, nhưng các thông tin về phương thức xác thực và mã hóa lại không được hiển thị chi tiết (chỉ cho biết có hay không có mã hóa) và không cho phép người dùng tùy biến bất cứ điều gì.

Tuy không hỗ trợ hiển thị mức độ nhiễu, NetSurveyor lại là ứng dụng cung cấp thông tin dạng biểu đồ chi tiết nhất trong những phần mềm miễn phí hiện nay, bao gồm Timecourse AP, AP Differential, Channel Usage, Channel Timecourse, Channel Heatmap, và Channel Spectrogram. Phần mềm này có thể ghi lại dữ liệu trong một khoảng thời gian dài để xem lại sau đó, bạn cũng có thể tạo các báo cáo rất hữu dụng theo định dạng PDF, bao gồm bản sao thông tin chi tiết và các biểu đồ của AP.

5. Kismet

Kismet là phần mềm mã nguồn mở rất nổi tiếng, chuyên phân tích, bắt gói tin và phát hiện xâm nhập, chạy trên các hệ điều hành Windows, MacOS X, Linux và BSD. Kismet hiển thị thông tin chi tiết về các AP, bao gồm cả SSID của các mạng ẩn, báo cáo mức độ nhiễu, mức độ nhiễu trên tín hiệu. Bạn có thể bắt các gói tin được truyền đi qua mạng không dây ở dạng thô và lưu lại thành file PCAP, từ đó bạn có thể dùng các công cụ khác như Wireshark, TCPdump để phân tích tiếp.

Trên Windows, Kismet chỉ hoạt động với bộ điều hợp AirPcap của CACE do sự hạn chế trong các trình điều khiển của Windows, tuy nhiên trên MacOS và Linux, Kismet hỗ trợ hầu hết các bộ điều hợp mạng không dây.

6. Xirrus Wi-Fi Inspector

Là phần mềm nguồn đóng miễn phí, cùng với việc hiển thị thông tin chi tiết về các AP, Xirrus Wi-Fi Inspector cung cấp bộ Radar và hiển thị một biểu đồ theo từng quãng 8 phút. Xirrus Wi-Fi Inspector cũng hiển thị tín hiệu, địa chỉ của các kết nối hiện tại. Ngoài ra, Xirrus Wi-Fi Inspector cung cấp một

công cụ đơn giản cho phép bạn kiểm tra các thành phần chính trong kết nối mạng và liên kết đến trang kiểm tra tốc độ và chất lượng kết nối.

Chức năng xuất báo cáo hỗ trợ tạo bản sao các thông tin chi tiết của AP thành tập tin định dạng CSV. Tuy Xirrus Wi-Fi Inspector không cho phép lưu tên AP, nhưng bạn có thể tùy chỉnh một số cấu hình, chẳng hạn: đơn vị tín hiện (dBm hay %), phương thức RSSI, và tần số quét.

7. Meraki Wi-Fi Stumbler

Là phần mềm dạng Web-based (giao diện web), có thể sử dụng miễn phí trên trang của Meraki tại địa chỉ: http://tools.meraki.com/stumbler. Meraki Wi-Fi Stumbler hỗ trợ hầu hết tất cả các loại trình duyệt trên các máy tính Mac, PC và có thể chạy ở chế độ ngoại tuyến (offline). Meraki Wi-Fi Stumbler cung cấp những thông tin cơ bản của AP như: mức tín hiệu, biểu đồ dạng cột cho mỗi kênh.

Một điểm đáng tiếc là Meraki Wi-Fi Stumbler không cho phép người dùng tùy biến và chỉ hỗ trợ những chức năng cơ bản như thông tin mạng, tìm kiếm dữ liệu. Tuy nhiên, đây vẫn là một công cụ rất hữu ích cho những ai muốn kiểm tra mạng Wi-Fi mà không muốn cài đặt bất kỳ một công cụ nào.

8. KisMAC

Nếu bạn là người dùng Mac, có thể KisMAC sẽ hữu ích cho bạn, đây là công cụ an ninh và phân tích rất tốt. Gần tương tự như Kismet, KisMAC có thể tìm được những mạng Wi-Fi ẩn. Ngoại trừ chạy trên hệ điều hành MAC OS, các chức năng của KisMAC giống như Kismet.

# Bảo mật Wi-Fi bằng các kỹ thuật nâng cao

**Nếu tiến hành thực hiện một tìm kiếm về bảo mật Wi-Fi trên Google thì chắc chắn những gì bạn nhận được sẽ là: Không nên sử dụng WEP mà sử dụng WPA hoặc WPA2, vô hiệu hóa SSID broadcasting, thay đổi các thiết lập mặc định,… Đây là những vấn đề rất cơ bản, trong bảo mật Wi-Fi. Tuy nhiên trong bài này chúng tôi sẽ bỏ qua những cánh thức cơ bản đó và giới thiệu cho các bạn những kỹ thuật nâng cao nhằm tăng độ bảo mật cho mạng không dây của mình.**

## 1. Chuyển sang mã hóa doanh nghiệp - Enterprise

Nếu bạn đã tạo một khóa mã hóa WPA hoặc WPA2 ở bất cứ kiểu nào và phải nhập vào khóa này khi kết nối với mạng không dây thì bạn cũng mới chỉ sử dụng chế độ Personal hay Pre-shared key (PSK) của Wi-Fi Protected Access (WPA). Các mạng doanh nghiệp – dù to hoặc nhỏ - vẫn cần phải được bảo vệ với chế độ Enterprise, đây là chế độ có bổ sung thêm tính năng thẩm định 802.1X/EAP cho quá trình kết nối không dây. Thay vì nhập vào khóa mã hóa trên tất cả các máy tính, người dùng sẽ đăng nhập bằng tên và mật khẩu. Các khóa mã hóa được cung cấp một cách an toàn trong chế độ background và duy nhất cho mỗi người dùng cũng như mỗi session.

Phương pháp này cho phép quản lý tập trung và toàn diện đối với sự an toàn của mạng Wi-Fi. Thay vì load các khóa mã hóa vào các máy tính nơi các nhân viên và những người dùng khác có thể phát hiện ra chúng, mỗi người dùng sẽ đăng nhập vào mạng bằng tài khoản riêng của mình khi sử dụng chế độ Enterprise. Bạn có thể dễ dàng thay đổi hoặc thu hồi truy cập nếu cần. Cách thức này đặc biệt hữu dụng khi có các nhân viên rời công ty hoặc laptop bị đánh cắp. Nếu sử dụng chế độ Personal, bạn sẽ phải tự thay đổi các khóa mã hóa trên tất cả các máy tính và các điểm truy cập (AP).

Một thành phần đặc biệt của chế độ Enterprise là máy chủ RADIUS/AAA. Máy chủ này sẽ truyền thông với các AP trên mạng và tra cứu cơ sở dữ liệu người dùng. Cân nhắc đến việc sử dụng Internet Authentication Service (IAS) của Windows Server 2003 hay Network Policy Server (NPS) của Windows Sever 2008.

## 2. Thẩm định bảo mật vật lý

Bảo mật cho một hệ thống không dây không phải chỉ đơn thuần là các công việc kỹ thuật. Bạn có thể có được kỹ thuật mã hóa Wi-Fi tốt nhất nhưng vẫn có ai đó có thể truy cập vào mạng của bạn bằng cách sử dụng cổng ethernet. Hoặc người nào đó có thể vào công ty hay nhà bạn và ấn nút reset của điểm truy cập và khôi phục lại các thiết lập mặc định nhà máy và để mở hoàn toàn mạng không dây của bạn.

Hãy bảo đảm rằng tất cả các AP của bạn phải nằm ngoài tầm với của những người không cần thiết và ngoài tầm nhìn của nhân viên trong công ty. Thay vì đặt các AP trên bàn, hãy gắn nó lên tường hoặc trần nhà là cách làm tốt nhất.

Bạn có thể cân nhắc đến việc gắn các AP ngoài tầm nhìn và lắp đặt thêm các anten mở rộng để tăng tín hiệu thu phát của AP. Cách thức này cho phép bạn bảo mật được AP trong khi vẫn cung cấp tín hiệu không dây tốt thông qua các anten có độ khuyếch đại cao.

Tuy nhiên không chỉ các AP là thành phần mà bạn cần quan tâm. Tất cả các thành phần mạng cũng cần được bảo vệ đúng cách, thậm chí ngay cả cáp ethernet. Các hacker có thể cắt đứt cáp ethernet của bạn và truy cập vào mạng của bạn bằng cách đó.

Cùng với việc gắn và bảo vệ các AP, bạn cũng cần kiểm tra chặt chẽ các AP của mình. Tạo một trang

bảng tính để ghi chép các model AP được sử dụng cùng với các địa chỉ IP và MAC. Thêm vào đó là nơi đặt chúng. Cách này giúp bạn biết chính xác nơi đặt AP khi thực hiện các hành động kiểm tra hoặc kiểm tra một AP nào đó có vấn đề.

### 3. Cài đặt hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)

Các hệ thống này thường có một chương trình phần mềm để sử dụng adapter không dây của bạn nhằm phát hiện xem các tín hiệu Wi-Fi xem có vấn đề nào hay không. Chúng có thể phát hiện các AP giả mạo, một AP mới xuất hiện trong mạng hoặc một AP đang tồn tại được reset về các thiết lập mặc định hay không hợp kiểu với một tập các chuẩn mà bạn đã định nghĩa.

Các hệ thống này cũng có thể phân tích các gói mạng để xem có ai đó có thể đang sử dụng kỹ thuật *hacking* hay *jamming* hay không.

Có nhiều hệ thống phát hiện và ngăn chặn xâm nhập khác nhau và sử dụng nhiều kỹ thuật khác nhau. Bạn có thể sử dụng các tùy chọn mã nguồn mở hoặc miễn phí phải nói đến nhưKismet và Snort. Bên cạnh đó là các sản phẩm thương mại của nhiều hãng khác nhưAirMagnet, AirDefense và AirTight.

### 4. Tạo các chính sách sử dụng mạng không dây

Cùng với các hướng dẫn sử dụng máy tính, bạn cần phải có một tập các chính sách đặc biệt cho việc truy cập mạng Wi-Fi, tối thiểu các chính sách đó phải như những gì được liệt kê dưới đây:

- **Danh sách các thiết bị được thẩm định có quyền truy cập mạng không dây**: Đây là cách tốt nhất để từ chối tất cả các thiết bị và cho phép các thiết bị mong muốn bằng cách sử dụng lọc địa chỉ MAC trên router mạng của bạn. Mặc dù các địa chỉ MAC có thể bị giả mạo, nhưng cách thức này vẫn cung cấp sự điều khiển ở một mức độ nào đó trên các thiết bị mà nhân viên của bạn đang sử dụng trên mạng. Bạn cần giữ một copy chứa tất cả các thiết bị được phép và các chi tiết của chúng để so sánh đối chiếu khi kiểm tra mạng và nhập vào các hệ thống phát hiện xâm nhập.

- **Danh sách các cá nhân có thẩm quyền truy cập vào mạng Wi-Fi**. Danh sách này này có thể được điều chỉnh lại khi sử dụng thẩm định 802.1X (WPA/WPA2-Enterprise) bằng cách tạo các tài khoản trong máy chủ RADIUS cho những ai cần truy cập Wi-Fi. Nếu thẩm định 802.1X cũng đang được sử dụng trên mạng chạy dây thì bạn có thể chỉ định người dùng nhận truy cập chạy dây hoặc không dây bằng cách thay đổi Active Directory hoặc sử dụng các chính sách thẩm định trên bản thân máy chủ RADIUS.

- **Các rule trong thiết lập router không dây hoặc AP**: Cho ví dụ, chỉ phòng CNTT mới có quyền thiết lập thêm các AP để các nhân viên không thể mang AP từ nhà của mình đến và cắm vào mạng để mở rộng phạm vi tín hiệu. Một rule bên trong cho phòng CNTT là có thể định nghĩa các model và cấu hình thiết bị có thể được sử dụng.

- **Các Rule đang sử dụng trên các hotspot Wi-Fi hoặc kết nối đến các mạng gia đình với các thiết bị công ty.** Vì dữ liệu trên một thiết bị hoặc laptop có thể bị thỏa hiệp và hành động Internet có thể bị kiểm tra trên các mạng không dây không an toàn nên bạn có thể hạn chế các kết nối Wi-Fi chỉ cho mạng công ty. Vấn đề này có thể được điều khiển bằng cách đặt thêm các bộ lọc mạng với tiện ích Network Shell (netsh) trong Windows. Cách khác có thể thực hiện là bạn có thể yêu cầu một kết nối VPN cho mạng công ty để bảo vệ hoạt động Internet và các file truy cập từ xa.

### 5. Sử dụng SSL hoặc IPsec phía trên mã hóa Wi-Fi

Mặc dù có thể đang sử dụng mã hóa Wi-Fi mới nhất (trên lớp 2 của mô trình OSI) nhưng bạn vẫn cần

xem xét đến việc thực thi một cơ chế bảo mật khác, chẳng hạn như IPSec (trên lớp 3 của mô trình OSI). Ngoài việc cung cấp sự mã hóa hai lần trên các hệ thống không dây, nó cũng có thể bảo vệ kết nối chạy dây. Cách thức này sẽ ngăn chặn được hành vi nghe trộm từ phía các nhân viên hoặc những kẻ xấu bên ngoài thâm nhập vào cổng ethernet.

- **Khả năng di động**: Với sự phát triển của các mạng không dây công cộng, *người dùng có thể truy cập Internet ở bất cứ đâu*. Chẳng hạn ở các quán Cafe, người dùng có thể truy cập Internet không dây miễn phí.
- **Hiệu quả**: Người dùng có thể *duy trì kết nối mạng* khi họ đi từ nơi này đến nơi khác.
- **Triển khai**: Việc thiết lập hệ thống mạng không dây ban đầu *chỉ cần ít nhất 1 access point*. Với mạng dùng cáp, phải tốn thêm chi phí và có thể gặp khó khăn trong việc triển khai hệ thống cáp ở nhiều nơi trong tòa nhà.
- **Khả năng mở rộng**: Mạng không dây có thể *đáp ứng tức thì khi gia tăng số lượng người dùng*. Với hệ thống mạng dùng cáp cần phải gắn thêm cáp.

### 1.1.3 Nhược điểm của WLAN

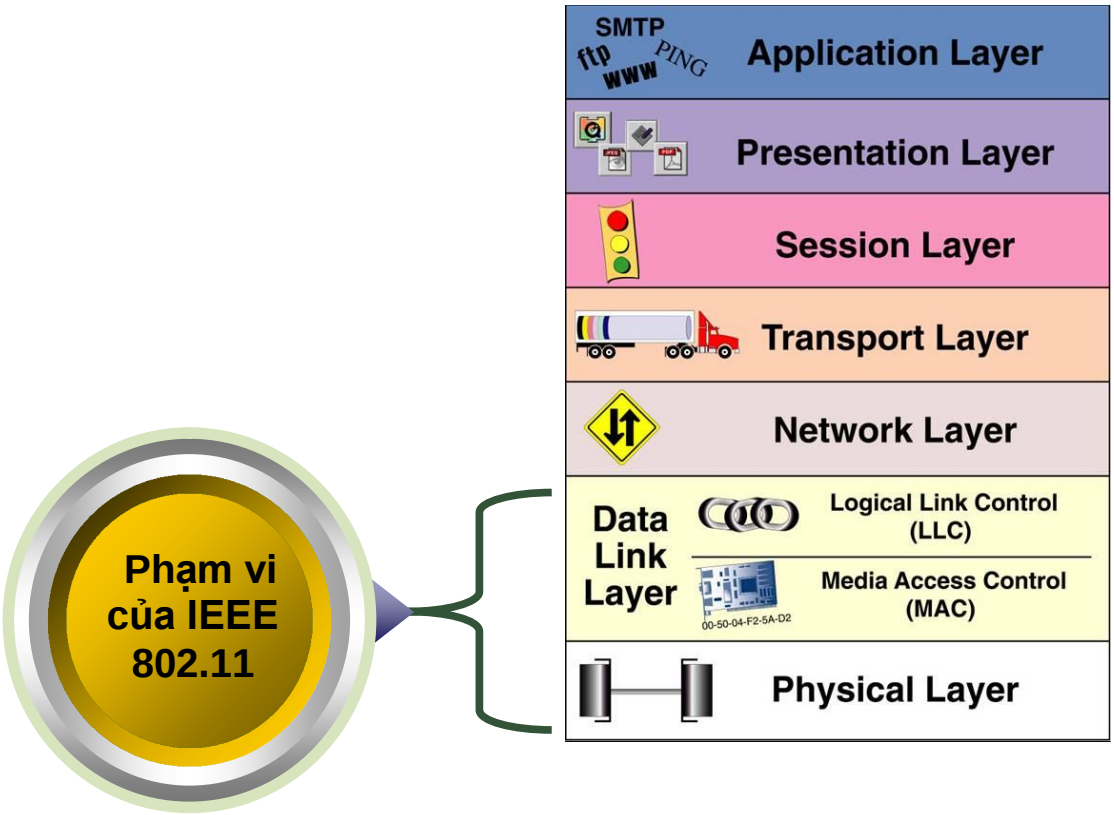
Công nghệ mạng LAN không dây, ngoài rất nhiều sự tiện lợi và những ưu điểm được đề cập ở trên thì cũng có các nhược điểm. Trong một số trường hợp mạng LAN không dây có thể không như mong muốn vì một số lý do. Hầu hết chúng phải làm việc với những giới hạn vốn có của công nghệ.

- **Bảo mật:** Môi trường kết nối không dây là không khí nên *khả năng bị tấn công của người dùng là rất cao*.
- **Phạm vi:** Một mạng chuẩn 802.11g với các thiết bị chuẩn *chỉ có thể hoạt động tốt trong phạm vi vài chục mét.* Nó phù hợp trong 1 căn nhà, nhưngvới một tòa nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.

- **Độ tin cậy:** Vì sử dụng sóng vô tuyến để truyền thông nên *việc bị nhiễu, tín hiệu bị giảm* do tác động của các thiết bị khác (lò vi sóng,…) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng.
- **Tốc độ:** Tốc độ của mạng không dây (1- 125 Mbps) *rất chậm so với mạng sử dụng cáp* (100 Mbps đến hàng Gbps).

## 1.2 CÁC CHUẨN THÔNG DỤNG CỦA WLAN

Hiện nay tiêu chuẩn chính cho Wireless là một họ giao thức truyền tin qua mạng không dây IEEE 802.11. Do việc nghiên cứu và đưa ra ứng dụng rất gần nhau nên có một số giao thức đã thành chuẩn của thế giới, một số khác vẫn còn đang tranh cãi và một số còn đang dự thảo. Một số chuẩn thông dụng như: 802.11b (cải tiến từ 802.11), 802.11a, 802.11g, 802.11n.




**Hình 1.1** Phạm vi của WLAN trong mô hình OSI

### 1.2.1 Chuẩn IEEE 802.11b

Chuẩn này được đưa ra vào năm 1999, nó cải tiến từ chuẩn 802.11.

- ✓ Cũng hoạt động ở dải tần 2,4 Ghz nhưng chỉ sử dụng trải phổ trực tiếp DSSS.
- ✓ Tốc độ tại Access Point có thể lên tới 11Mbps (802.11b), 22Mbps (802.11b+).
- ✓ Các sản phẩm theo chuẩn 802.11b được kiểm tra và thử nghiệm bởi hiệp hội các công ty Ethernet không dây (WECA) và được biết đến như là hiệp hội Wi-Fi, những sản phẩm Wireless được WiFi kiểm tra nếu đạt thì sẽ mang nhãn hiệu này.
- ✓ Hiện nay IEEE 802.11b là một chuẩn được sử dụng rộng rãi nhất cho Wireless LAN. Vì dải tần số 2,4Ghz là dải tần số ISM (Industrial, Scientific and Medical: dải tần vô tuyến dành cho công nghiệp, khoa học và y học, không cần xin phép) cũng được sử dụng cho các chuẩn mạng không dây khác như là: Bluetooth và HomeRF, hai chuẩn này không được phổ biến như là 801.11. Bluetooth được thiết kế sử dụng cho thiết bị không dây mà không phải là Wireless LAN, nó được dùng cho mạng cá nhân PAN(Personal Area Network). Như vậy Wireless LAN sử dụng chuẩn 802.11b và các thiết bị Bluetooth hoạt động trong cùng một dải băng tần.

**Bảng 1.1** Một số thông số kỹ thuật của chuẩn IEEE 802.11b

| Release Date | Op. Frequency | Data Rate (Typ) | Data Rate (Max) | Range (Indoor) |
|---|---|---|---|---|
| October 1999 | 2.4 GHz | 4.5 Mbit/s | 11 Mbit/s | ~35 m |

### 1.2.2 Chuẩn IEEE 802.11a

- ✓ Đây là một chuẩn được cấp phép ở dải băng tần mới. Nó hoạt động ở dải tần số 5 Ghz sử dụng phương thức điều chế ghép kênh theo vùng tần số vuông góc (OFDM). Phương thức điều chế này làm tăng tốc độ trên mỗi kênh (từ 11Mbps/1kênh lên 54 Mbps/1 kênh).
- ✓ Có thể sử dụng đến 8 Access Point (truyền trên 8 kênh Non-overlapping,kênh không chồng lấn phổ), đặc điểm này ở dải tần 2,4Ghz chỉ có thể sử dụng 3 Access Point (truyền trên 3 kênh Non – overlapping).
- ✓ Hỗ trợ đồng thời nhiều người sử dụng với tốc độ cao mà ít bị xung đột.
- ✓ Các sản phẩm của theo chuẩn IEEE 802.11a không tương thích với các sản phẩm theo chuẩn IEEE 802.11 và 802.11b vì chúng hoạt động ở các dải tần số khác nhau. Tuy nhiên các nhà sản xuất chipset đang cố gắng đưa loại chipset hoạt động ở cả 2 chế độ theo hai chuẩn 802.11a và 802.11b. Sự phối hợp này được biết đến với tên WiFi5 ( WiFi cho công nghệ 5Gbps).

**Bảng 1.2** Một số thông số kỹ thuật của chuẩn IEEE 802.11a

| Release Date | Op. Frequency | Data Rate (Typ) | Data Rate (Max) | Range (Indoor) |
|---|---|---|---|---|
| October 1999 | 5 GHz | 23 Mbit/s | 54 Mbit/s | ~35 m |

### 1.2.3 IEEE 802.11g

- ➢ Bản dự thảo của tiêu chuẩn này được đưa ra vào tháng 10 – 2002.

- Sử dụng dải tần 2,4 Ghz, tốc độ truyền lên đến 54Mbps.
- Phương thức điều chế: Có thể dùng một trong 2 phương thức
  - Dùng OFDM (giống với 802.11a) tốc độ truyền lên tới 54Mbps.
  - Dùng trải phổ trực tiếp DSSS tốc độ bị giới hạn ở 11 Mbps.
- Tương thích ngược với chuẩn 802.11b.
- Bị hạn chế về số kênh truyền.

**Bảng 1.3** Một số thông số kỹ thuật của chuẩn IEEE 802.11g

| Release Date | Op. Frequency | Data Rate (Typ) | Data Rate (Max) | Range (Indoor) |
|---|---|---|---|---|
| June 2003 | 2.4 GHz | 23 Mbit/s | 54 Mbit/s | ~35 m |

### 1.2.4 Chuẩn IEEE 802.11n


**Hình 1.2** Logo Wi-fi

Chuẩn 802.11n đang được xúc tiến để đạt tốc độ 100 Mb/giây, nhanh gấp 5 lần chuẩn 802.11g và cho phép thiết bị kết nối hoạt động với khoảng cách xa hơn các mạng Wi-Fi hiện hành.

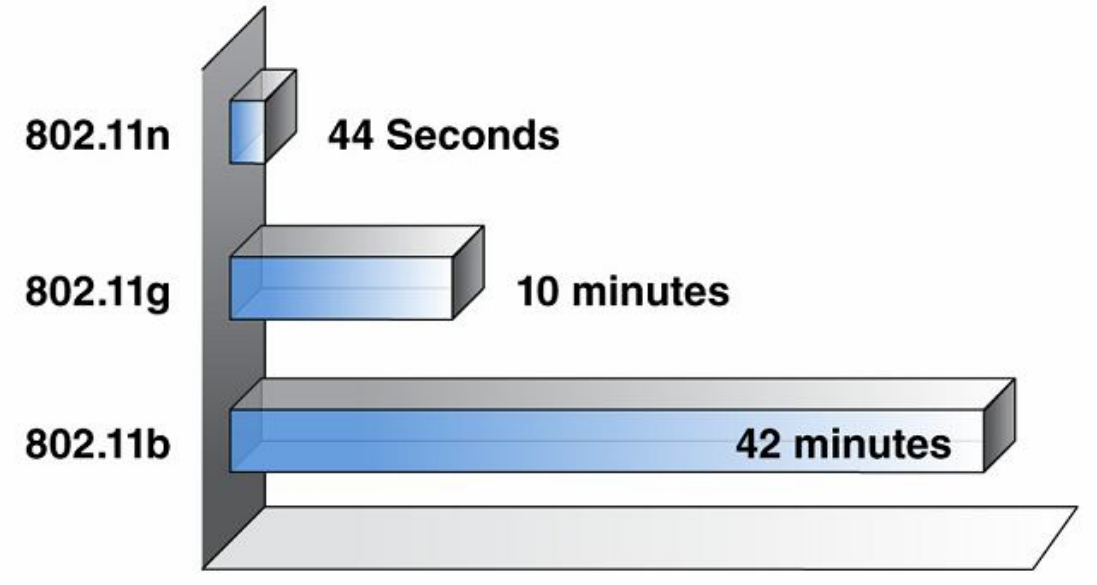
Winston Sun, giám đốc công nghệ của công ty không dây Atheros Communications, nhận xét, một thiết bị tương thích 802.11n có thể truy cập các điểm hotspot với tốc độ 150 MB/giây với khoảng cách lý tưởng dưới 6m, khả năng liên kết càng giảm khi người dùng ở cách xa điểm truy cập đó.

802.11n chưa thể sớm trở thành chuẩn Wi-Fi thế hệ mới vì một số mạng Wi-Fi không thuộc thông số 802.11n cũng được giới thiệu. Theo Sun, các chuẩn Wi-Fi mới được ra mắt có thể tự động dò tần sóng thích hợp để kết nối Internet. Chính vì thế, thiết bị hỗ trợ 802.11n không thể "độc chiếm" phổ Wi-Fi và phải "nhường" sóng cho các mạng kết nối khác.

Ông Sun cho biết, tốc độ truy cập Wi-Fi giảm tỷ lệ nghịch với khoảng cách từ thiết bị tới hotspot vẫn cho phép các máy cầm tay, như iTV của Apple stream được các đoạn video clip nhưng không thể stream video nén có độ nét cao .

**Bảng 1.4** Một số thông số kỹ thuật của chuẩn IEEE 802.11n

| **Release Date** | **Op. Frequency** | **Data Rate (Typ)** | **Data Rate (Max)** | **Range (Indoor)** |
|---|---|---|---|---|
| June 2009 (est.) | 5 GHz and/or 2.4 GHz | 74 Mbit/s | 300 Mbit/s (2 streams) | ~70 m |




**Hình 1.3** Tốc độ truyền tải so với các chuẩn khác

### 1.2.5 So sánh các chuẩn IEEE 802.11x

Wi-Fi còn có tên gọi khác là IEEE 802.11 (hay ngắn gọn là 802.11) cũng chính là nhóm các tiêu chuẩn kỹ thuật của công nghệ kết nối này do liên minh Wi-Fi (Wi-Fi Alliance: www.wi-fi.org) quy định. Hiện tồn tại các xác thực sau được đưa ra bởi Wi-Fi Alliance:

**Bảng 1.5** So sánh các chuẩn IEEE 802.11x

| **Chuẩn** | **Phân loại** | **Tính năng chính**<br>**Định nghĩa** | **Chú thích** |
|---|---|---|---|
| IEEE 802.11 | Kết nối | Tần số: 2,4 GHz<br>Tốc độ tối đa: 2 mbps<br>Tầm hoạt động: không xác | Chuẩn lý thuyết |

| | | | |
|---|---|---|---|
| | | định | |
| IEEE 802.11a | Kết nối | Tần số: 5 GHz<br>Tốc độ tối đa: 54 mbps<br>Tầm hoạt động: 25-75 m | Xem thêm 802.11d và 802.11h |
| IEEE 801.11b | Kết nối | Tần số: 2,4 GHz<br>Tốc độ tối đa: 11 mbps<br>Tầm hoạt động: 35-100 m | Tương thích với 802.11g |
| IEEE 802.11g | Kết nối | Tần số: 2,4 GHz<br>Tốc độ tối đa: 54 mbps<br>Tầm hoạt động: 25-75 m | Tương thích ngược với 802.11b, xem thêm 802.11d và 802.11h |
| IEEE 8021.11n | Kết nối | Tần số: 2,4 GHz<br>Tốc độ tối đa: 540 mbps<br>Tầm hoạt động: 50-125 m | Tương thích ngược với 802.11b/g<br>Dự kiến sẽ được thông qua vào tháng 11/2008 |
| IEEE 802.11d | Tính | Bật tính năng thay đổi tầng | Hỗ trợ bởi một |

## Các phương thức bảo mật mạng WLAN

Với giá thành xây dựng một hệ thống mạng WLAN giảm,ngày càng có nhiều công ty sử dụng.

Điều này sẽ không thể tránh khỏi việc Hacker chuyển sang tấn công và khai thác các điểm yếu trên nền tảng mạng sử dụng chuẩn 802.11. Những công cụ Sniffers cho phép tóm được các gói tin giao tiếp trên mạng, họ có thể phân tích và lấy đi những thông tin quan trọng của bạn. Vậy bạn đã biết gì về các phương thức bảo mật mạng WLAN.

Những phần mềm scan có thể được cài đặt trên các thiết bị như Smart Phone hay trên một chiếc Laptop hỗ trợ chuẩn kết nối Wi-Fi.

- Wide availability and low cost of IEEE 802.11 wireless equipment
- 802.11 standard ease of use and deployment
- Availability of sniffers
- Statistics on WLAN security
- Media hype about hot spots, WLAN hacking, war driving
- Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption
- Authentication vulnerability


Điều này dẫn tới những thông tin nhạy cảm trong hệ thống mạng, như thông tin cá nhân của người dùng…

**Những nguy cơ bảo mật trong WLAN bao gồm**:

| "War Drivers" | Hackers | Employees |
|---|---|---|
| Find "Open" networks; use them to gain free internet access | Exploit weak privacy measures to view sensitive WLAN info and even break into WLANs | Plug consumer-grade APs/Gateways into company ethernet ports to create own WLANs |
|  |   |  |

- Các thiết bị có thể kết nối tới những Access Point đang broadcast SSID.
- Hacker sẽ cố gắng tìm kiếm các phương thức mã hoá đang được sử dụng trong quá trình truyền thông tin trên mạng, sau đó có phương thức giải mã riêng và lấy các thông tin nhạy cảm.
- Người dụng sử dụng Access Point tại gia đình sẽ không đảm bảo tính bảo mật như khi sử dụng tại doanh nghiệp.

**Để bảo mật mạng WLAN, bạn cần thực hiện qua các bước sau**:

| Control and Integrity | Privacy and Confidentiality | Protection and Availability |
|---|---|---|
| Authentication | Encryption | Intrusion Detection System (IDS) |
| Ensure that legitimate clients associate with trusted APs. | Protect data as it is transmitted and received. | Track and mitigate unauthorized access and network attacks. |

- Chỉ có những người dùng được xác thực mới có khả năng truy cập vào mạng thông qua các Access Point.
- Các phương thức mã hoá được áp dụng trong quá trình truyền các thông tin quan trọng.
- Bảo mật các thông tin và cảnh báo nguy cơ bảo mật bằng hệ thống IDS và IPS.

Xác thực và bảo mật dữ liệu bằng cách mã hoá thông tin truyền trên mạng.

IDS như một thiết bị giám sát mạng Wireless và mạng Wire để tìm kiếm và cảnh báo khi có các dấu hiệu tấn công.

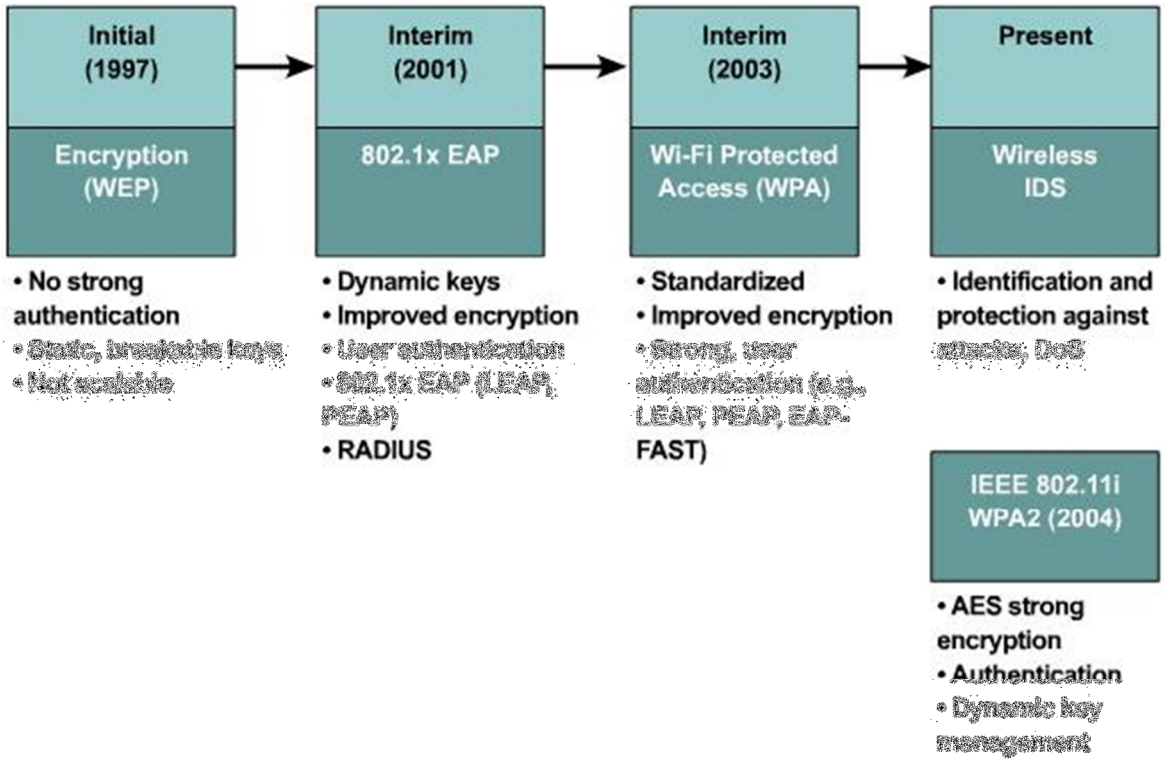
Ban đầu, IEEE 802.11 sử dụng giải pháp bảo mật bằng những khoá tĩnh (static keys) cho cả quá trình mã hoá và xác thực. Phương thức xác thực như vậy là không đủ mạnh, cuối cùng có thể bị tấn công. Bởi vì các khoá được quản lý và không thay đổi, điều này không thể áp dụng trong một giải pháp doanh nghiệp lớn được.

Cisco giới thiệu và cho phép sử dụng IEEE 802.1x là giao thức xác thực và sử dụng khoá động (dynamic keys), bao gồm 802.1x Extensible Authentication Protocol (EAP). Cisco cũng giới thiệu phương thức để chống lại việc tấn công bằng cách sử dụng quá trình băm

(hashing) (Per Packet Key – PPK) và Message Integrity Check (MIC). Phương thức này được biết đến như Cisco Key Integrity Protocol (CKIP) và Cisco Message Integrity Check (CMIC).

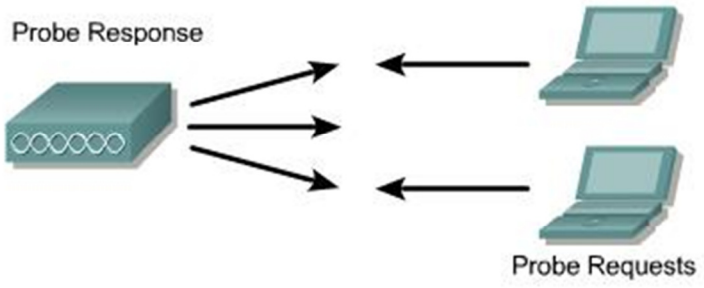
Các tổ chức chuẩn 802.11 bắt đầu tiến hành việc nâng cấp bảo mật cho mạng WLAN. Wi-Fi Alliance giới thiệu giải pháp WPA (Wi-Fi Protected Access). Một chuẩn nằm trong chuẩn 802.11i là chuẩn bảo mật của WLAN và sử dụng chuẩn 802.1x làm phương thức xác thực và mã hoá dữ liệu. WPA được sử dụng cho việc xác thực người dung, MIC, Temporal Key Integrity Protocol (TKIP), và Dynamic Keys. Nó tương tự như phương thức của Cisco nhưng cách thực hiện có khác đôi chút. WPA cũng bao gồm một passphrase hay preshared key cho người dung để họ xác thực trong giải pháp bảo mật trong gia đình, nhưng không được sử dụng cho giải pháp doanh nghiệp.

Ngày nay , IEEE 802.11i đã nâng cấp và Advanced Encryption Standard (AES) đã thay thế cho WEP và là phương thức bảo mật mới nhất và bảo mật nhất trong mã hoá dữ liệu. Wireless IDS hiện nay đã có với vai trò nhận diện và bảo vệ hệ thống WLAN trước những tấn công. Wi-Fi Alliance 802.11i làm việc và sử dụng như WPA2

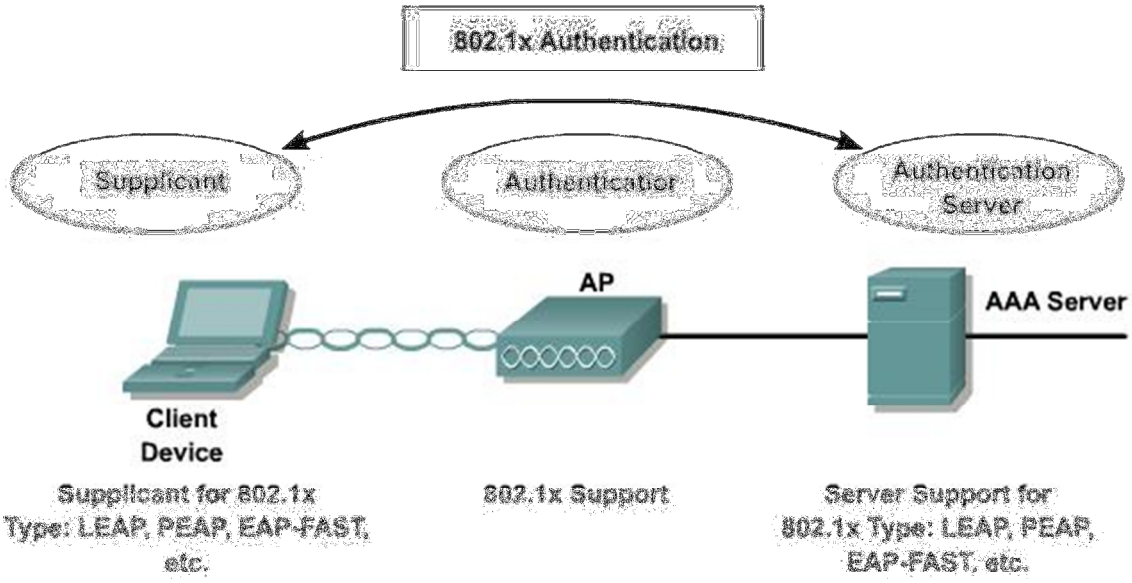



Các Access Point gửi broadcast một hoặc nhiều SSIDs, hay data rates, và một số thông tin. Các thiết bị Wi-Fi có thể scan tất cả các kênh và tìm truy cập vào bất kỳ mạng nào mà họ scan ra được từ những Access Point. Client sẽ thường kết nối tới những Access Point mà tín hiệu mạnh nhất. Nếu tín hiệu yếu, client tiếp tục scan tới một Access Point khác (trong trường hợp Roaming). Trong quá trình kết nối, SSID, địa chỉ MAC và các thiết lập bảo mật được gửi từ client tới Access Point và kiểm tra bởi Access Point.

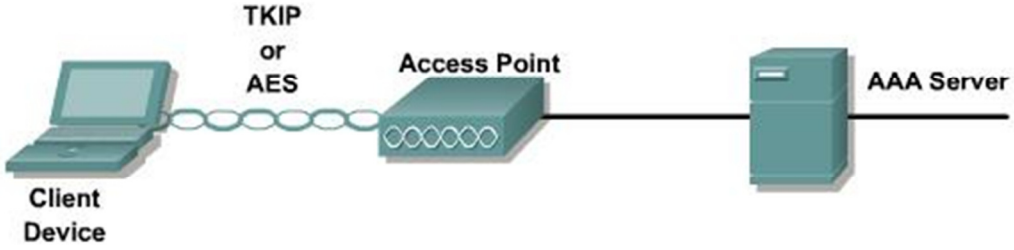
- Access points send out beacons announcing SSID, data rates, and other information.
- Client scans all channels.
- Client listens for beacons and responses from access points.
- Client associates to access point with strongest signal.
- Client will repeat scan if signal becomes low to reassociate to another access point (roaming).
- During association, SSID, MAC address, and security settings are sent from the client to the AP and checked by the AP.




Người dung được xác thực thong qua giao thức 802.1x. Với chuẩn 802.1x hay EAP cần thiết trên WLAN client. Access Point cũng có thể như một máy chủ đáp ứng việc xác thực cho người dùng, hoặc có thể lien kết tới máy chủ RADIUS nhờ xác thực hộ, hoặc có thể làm việc với Cisco Secure ACS. Lightweight Access Poínt sẽ giao tiếp với WLAN controller, và nó làm việc như một máy chủ xác cung cấp xác thực cho các users.
Client và máy chủ cung cấp xác thực triển khai với hai phiên bản EAP khác nhau. Thông tin EAP sẽ được truyền từ Access point tới máy chủ xác thực




Sau khi xác thực song WLAN client, dữ liệu sẽ được mã hoá trước khi truyền đi. Về cơ bản phương thức mã hoá dựa vào thuật toán RC4 được sử dụng bắt đầu từ WEP. TKIP sử dụng mã hoá RC4 được tăng cường bảo mật hơn và với nhiều bít mã hoá hơn và có khoá tích hợp cho mỗi packet (key per packet –PPK). AES được thay thế cho RC4 với thuật toán bảo mật cao cấp hơn. WPA sử dụng TKIP, trong khi WPA2 sử dụng AES hay TKIP.


**Sự khác nhau giữa các dạng WLANs**.

- Cho các điểm truy cập tự động (hotspots), việc mã hoá không cần thiết, chỉ cần người dung xác thực mà thôi.
- Với người dùng sử dụng mạng WLAN cho gia đình, một phương thức bảo mật với WPA passphare hay preshared key được khuyến cáo sử dụng.
- Với giải pháp doanh nghiệp, để tối ưu quá trình bảo mật với 802.1x EAP làm phương thức xác thực và TKIP hay AES làm phương thức mã hoá. Được dựa theo chuẩn WPA

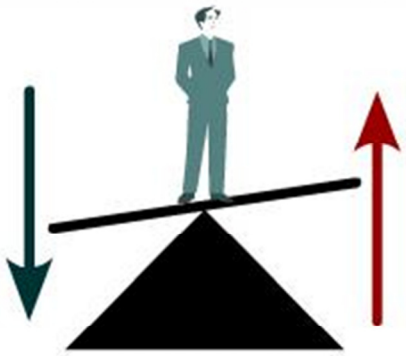
hay WPA2 và 802.11i security.

| Open Access | Basic Security | Enhanced Security | Remote Access |
|---|---|---|---|
| • No encryption<br>• Basic Authentication<br>• Public "Hotspots" | • WPA Passphrase<br>• WEP Encryption<br>• Home Use | • 802.1x EAP<br>• Mutual Authentication<br>• TKIP Encryption<br>• WPA / WPA 2<br>• 802.11i Security<br>• Enterprise | • Virtual Private Network (VPN)<br>• Business Traveler<br>• Telecommuter |

Bảo mật mạng WLAN cũng tương tự như bảo mật cho các hệ thống mạng khác. Bảo mật hệ thống phải được áp dụng cho nhiều tầng, các thiết bị nhận dạng phát hiện tấn công phải được triển khai. Giới hạn các quyền truy cập tối thiểu cho những người dùng cần thiết. Dữ liệu được chia sẻ và yêu cầu xác thực mới cho phép truy cập. Dữ liệu truyền phải được mã hoá.

Kẻ tấn công có thể tấn công mạng WLAN không bảo mật bất cứ lúc nào. Bạn cần có một phương án triển khai hợp lý.

- Evaluate effectiveness of encrypted WLAN statistics.
- Focus on proper planning and implementation.
- Estimate potential security threats and the level of security needed.
- Evaluate amount of WLAN traffic being sent when selecting security methods.
- Evaluate tools and options applicable to WLAN design.



WLAN Security Options

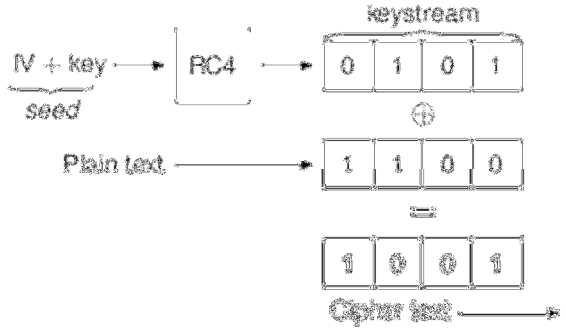
- Phải ước lượng được các nguy cơ bảo mật và các mức độ bảo mật cần thiết để áp dụng.
- Đánh giá được toàn bộ các giao tiếp qua WLAN và các phương thức bảo mật cần được áp dụng.
- Đánh giá được các công cụ và các lựa chọn khi thiết kế về triển khai mạng WLAN.

***Theo VNE Research Deparment***

**So sánh các phương thức bảo mật dựa trên việc chứng thực (sưu tầm)**

## I Bảo mật bằng WEP (Wired Equivalent Privacy)

WEP là một thuật toán bảo nhằm bảo vệ sự trao đổi thông tin chống lại sự nghe trộm, chống lại những nối kết mạng không được cho phép cũng như chống lại việc thay đổi hoặc làm nhiễu thông tin truyền. WEP sử dụng stream cipher RC4 cùng với một mã 40 bit và một số ngẫu nhiên 24 bit (initialization vector – IV) để mã hóa thông tin. Thông tin mã hóa được tạo ra bằng cách thực hiện operation XOR giữa keystream và plain text. Thông tin mã hóa và IV sẽ được gửi đến người nhận. Người nhận sẽ giải mã thông tin dựa vào IV và khóa WEP đã biết trước. Sơ đồ mã hóa được miêu tả bởi hình 1.




Hình 1: Sơ đồ mã hóa bằng WEP

**Những điểm yếu về bảo mật của WEP**

+ WEP sử dụng khóa cố định được chia sẻ giữa một Access Point (AP) và nhiều người dùng (users) cùng với một IV ngẫu nhiên 24 bit. Do đó, cùng một IV sẽ được sử dụng lại nhiều lần. Bằng cách thu thập thông tin truyền đi, kẻ tấn công có thể có đủ thông tin cần thiết để có thể bẻ khóa WEP đang dùng.

+ Một khi khóa WEP đã được biết, kẻ tấn công có thể giải mã thông tin truyền đi và có thể thay đổi nội dung của thông tin truyền. Do vậy WEP không đảm bảo được *confidentiality* và *integrity*.

+ Việc sử dụng một khóa cố định được chọn bởi người sử dụng và ít khi được thay đổi (tức có nghĩa là khóa WEP không được tự động thay đổi) làm cho WEP rất dễ bị tấn công.

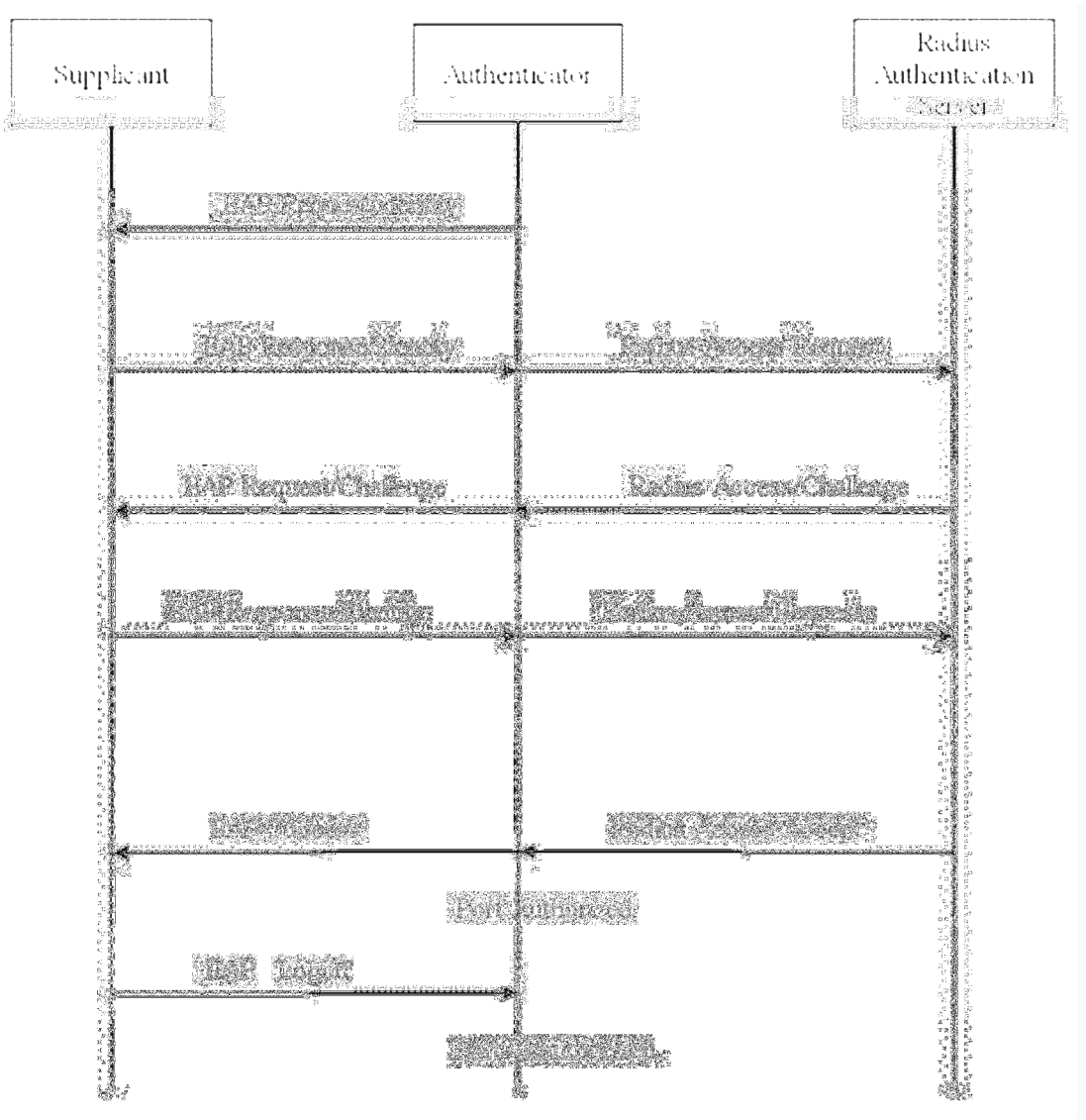
+ WEP cho phép người dùng (supplicant) xác minh (authenticate) AP trong khi AP không thể xác minh tính xác thực của người dùng. Nói một cách khác, WEP không cung ứng *mutual authentication*.

## II. Bảo mật bằng WPA (Wifi Protected Access )

WPA là một giải pháp bảo mật được đề nghị bởi WiFi Alliance nhằm khắc phục những hạn chế của WEP. WPA được nâng cấp chỉ bằng một update phần mềm SP2 của microsoft.

**WPA cải tiến 3 điểm yếu nổi bật của WEP :**

+ WPA cũng mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128 bit và IV có chiều dài là 48 bit. Một cải tiến của WPA đối với WEP là WPA sử dụng giao thức TKIP (Temporal Key Integrity Protocol) nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình trao đổi thông tin. Cụ thể là TKIP dùng một khóa nhất thời 128 bit kết hợp với địa chỉ MAC của user host và IV để tạo ra mã khóa. Mã khóa này sẽ được thay đổi sau khi 10 000 gói thông tin được trao đổi.
+ WPA sử dụng 802.1x/EAP để đảm bảo mutual authentication nhằm chống lại man-in-middle attack. Quá trình authentication của WPA dựa trên một authentication server, còn được biết đến với tên gọi RADIUS/ DIAMETER. Server RADIUS cho phép xác thực user trong mạng cũng như định nghĩa những quyền nối kết của user. Tuy nhiên trong một mạng WiFi nhỏ (của công ty hoăc trường học), đôi khi không cần thiết phải cài đặt một server mà có thể dùng một phiên bản WPA-PSK (pre-shared key). Ý tưởng của WPA-PSK là sẽ dùng một password (Master Key) chung cho AP và client devices. Thông tin authentication giữa user và server sẽ được trao đổi thông qua giao thức EAP (Extensible Authentication Protocol). EAP session sẽ được tạo ra giữa user và server đêr chuyển đổi thông tin liên quan đến identity của user cũng như của mạng. Trong quá trình này AP đóng vai trò là một EAP proxy, làm nhiệm vụ chuyển giao thông tin giữa server và user. Những authentication messages chuyển đổi được miêu tả trong hình 2.




*Hình 2: Messages trao đổi trong quá trình authentication.*

+ WPA sử dụng MIC (Michael Message Integrity Check ) để tăng cường integrity của thông tin truyền. MIC là một message 64 bit được tính dựa trên thuật tóan Michael. MIC sẽ được gửi trong gói TKIP và giúp người nhận kiểm tra xem thông tin nhận được có bị lỗi trên đường truyền hoặc bị thay đổi bởi kẻ phá hoại hay không.

Tóm lại, WPA được xây dựng nhằm cải thiện những hạn chế của WEP nên nó chứa đựng những đặc điểm vượt trội so với WEP. Đầu tiên, nó sử dụng một khóa động mà được thay đổi một cách tự động nhờ vào giao thức TKIP. Khóa sẽ thay đổi dựa trên người dùng, session trao đổi nhất thời và số lượng gói thông tin đã truyền. Đặc điểm thứ 2 là WPA cho phép kiểm tra xem thông tin có bị thay đổi trên đường truyền hay không nhờ vào MIC message. Và đăc điểm nối bật thứ cuối là nó cho phép multual authentication bằng cách sử dụng giao thức 802.1x

**Những điểm yếu của WPA.**

- Điểm yếu đầu tiên của WPA là nó vẫn không giải quyết được denial-of-service (DoS) attack [5]. Kẻ phá hoại có thể làm nhiễu mạng WPA WiFi bằng cách gửi ít nhất 2 gói thông tin với một khóa sai (wrong encryption key) mỗi giây. Trong trường hợp đó, AP sẽ cho rằng một kẻ phá hoại đang tấn công mạng và AP sẽ cắt tất cả các nối kết trong vòng một phút để trách hao tổn tài nguyên mạng. Do đó, sự tiếp diễn của thông tin không được phép sẽ làm xáo trộn hoạt động của mạng và ngăn cản sự nối kết của những người dùng được cho phép (authorized users).
- Ngoài ra WPA vẫn sử dụng thuật tóan RC4 mà có thể dễ dàng bị bẻ vỡ bởi FMS attack đề nghị bởi những nhà nghiên cứu ở trường đại học Berkeley [6]. Hệ thống mã hóa RC4 chứa đựng những khóa yếu (weak keys). Những khóa yếu này cho phép truy ra khóa encryption. Để có thể tìm ra khóa yếu của RC4, chỉ cần thu thập một số lượng đủ thông tin truyền trên kênh truyền không dây.
- WPA-PSK là một biên bản yếu của WPA mà ở đó nó gặp vấn đề về quản lý password hoặc shared secret giữa nhiều người dùng. Khi một người trong nhóm (trong công ty) rời nhóm, một password/secret mới cần phải được thiết lập.

## III. Tăng cường bảo mật với chuẩn 802.11i (WPA2)

Chuẩn 802.11i được phê chuẩn vào ngày 24 tháng 6 năm 2004 nhằm tăng cường tính mật cho mạng WiFi. 802.11i mang đầy đủ các đặc điểm của WPA. Tập hợp những giao thức của 802.11i còn được biết đến với tên gọi WPA 2. Tuy nhiên, 802.11i sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) thay vì RC4 như trong WPA. Mã khóa của AES có kích thước là 128, 192 hoặc 256 bit. Tuy nhiên thuật toán này đổi hỏi một khả năng tính toán cao (high computation power). Do đó, 802.11i không thể update đơn giản bằng software mà phải có một dedicated chip. Tuy nhiên điều này đã được ước tính trước bởi nhiều nhà sản xuất nên hầu như các chip cho card mạng Wifi từ đầu năm 2004 đều thích ứng với tính năng của 802.11i.

# Các tài liệu hướng dẫn bảo mật hệ thống mạng máy tính

**Ngày nay vấn đề bảo mật đã trở thành những chủ đề nóng nhất trên Internet. Với tốc độ phát triển cực nhanh của mạng toàn cầu đã đem lại những lợi ích về mặt kinh tế và xã hội không thể phủ nhận. Chính những lợi thế đó đã là nơi lý tưởng để tội phạm, hacker sử dụng khai thác với nhiều mục đích khác nhau.**

Để giúp các bạn có thêm thông tin và kiến thức Quản Trị Mạng xin trân trọng giới thiệu các giải pháp, hướng dẫn bảo mật của Trung tâm bảo mật và cứu hộ toàn cầu - Cert.org. Bài viết gồm rất nhiều nội dung do đó chúng tôi không thể tiến hành biên dịch ra tiếng Việt được mong các bạn thông cảm

## CERT® Security Improvement Modules

Each CERT Security Improvement module addresses an important but narrowly defined problem in network security. It provides guidance to help organizations improve the security of their networked computer systems.

The CERT security practices have been compiled in *The CERT® Guide to System and Network Security Practices*, published by Addison-Wesley and available at walk-in and online bookstores. Using a practical, phased approach, the book shows administrators how to protect systems and

networks against malicious and inadvertent compromise based on security incidents reported to the CERT/CC.

Each module page links to a series of practices and implementations. Practices describe the choices and issues that must be addressed to solve a network security problem. Implementations describe tasks that implement recommendations described in the practices. Please note that these implementations should be considered examples; they have not been updated to reflect current versions of operating systems or current vulnerabilities. For more information about modules, read the section about module structure.

- Available formats

**Modules**

1. Outsourcing Managed Security Services
2. Securing Desktop Workstations
3. Responding to Intrusions
4. Securing Network Servers
5. Deploying Firewalls
6. Securing Public Web Servers
7. Detecting Signs of Intrusion

HTML versions of the modules are available from the CERT web site. PDF and Postscript versions of the modules are available from the SEI web site. For the PDF and Postscript versions, click on the icons next to the module names. The currently available modules are:

**Practices**

1. **Harden and secure your systems by establishing secure configurations Considerations for Vulnerability Assessment as a Managed Security Service**

2. **Prepare for intrusions by getting ready for detection and response**
3. **Detect intrusions quickly**
4. **Respond to intrusions to minimize damage**
5. **Improve your security to help protect against future attacks**

**We also have practices relating to outsourcing managed security services. They are listed under the heading**

**Practices related to outsourcing managed security services**

**Practices about hardening and securing systems**

1. **Develop a computer deployment plan that includes security issues**
2. **Include explicit security requirements when selecting servers**
3. **Keep operating systems and applications software up to date**
4. **Offer only essential network services and operating system services on the server host machine**
5. **Configure computers for user authentication**
6. **Configure computer operating systems with appropriate object, device, and file access controls**
7. **Configure computers for file backups**

8. Protect computers from viruses and similar programmed threats
9. Configure computers for secure remote administration
10. Allow only appropriate physical access to computers
11. Configure network service clients to enhance security
12. Configure multiple computers using a tested model configuration and a secure replication procedure
13. Develop and promulgate an acceptable use policy for workstations
14. Configure computers to provide only selected network services
15. Isolate the Web server from public networks and your organization's internal networks
16. Configure the Web server with appropriate object, device and file access controls
17. Identify and enable Web-server-specific logging mechanisms
18. Consider security implications before selecting programs, scripts, and plug-ins for your web server
19. Configure the web server to minimize the functionality of programs, scripts, and plug-ins

20. Configure the Web server to use authentication and encryption technologies, where required
21. Maintain the authoritative copy of your Web site content on a secure host
22. Protect your Web server against common attacks
23. Design the firewall system
24. Acquire firewall hardware and software
25. Acquire firewall documentation, training, and support
26. Install firewall hardware and software
27. Configure IP routing
28. Configure firewall packet filtering
29. Configure firewall logging and alert mechanisms
30. Test the firewall system
31. Install the firewall system
32. Phase the firewall system into operation

**Practices about preparing to detect and respond to intrusions**

1. Establish a policy and procedures that prepare your organization to detect signs of intrusion
2. Identify data that characterize systems and aid in detecting signs of suspicious behavior
3. Manage logging and other data collection mechanisms
4. Establish policies and procedures for responding to intrusions
5. Prepare to respond to intrusions

**Practices about detecting intrusions**

1. Ensure that the software used to examine systems has not been compromised
2. Monitor and inspect network activities for unexpected behavior
3. Monitor and inspect system activities for unexpected behavior
4. Inspect files and directories for unexpected changes
5. Investigate unauthorized hardware attached to your organization's network
6. Inspect physical resources for signs of unauthorized access
7. Review reports by users and external contacts about suspicious and unexpected behavior

8. Take appropriate actions upon discovering unauthorized, unexpected, or suspicious activity

**Practices about responding to intrusions**

1. Analyze all available information to characterize an intrusion
2. Communicate with all parties that need to be made aware of an intrusion and its progress
3. Collect and protect information associated with an intrusion
4. Apply short-term solutions to contain an intrusion
5. Eliminate all means of intruder access
6. Return systems to normal operation
7. Identify and implement security lessons learned

**Practices about improving system security**

1. Take appropriate actions upon discovering unauthorized, unexpected, or suspicious activity
2. Identify and implement security lessons learned

**Practices related to outsourcing managed security services**

1. **Content Guidance for an MSS Request for Proposal**
2. **Guidance for Evaluating an MSS Proposal**
3. **Content Guidance for an MSS Service Level Agreement**
4. **Transitioning to MSS**
5. **Managing an Ongoing MSS Provider Relationship**
6. **Terminating an MSS Provider Relationship**
7. **Considerations for Network Boundary Protection as Managed Security Services**
8.

The practices are grouped into five general steps, listed below. They are illustrated in the diagram "Security Knowledge in Practice." Please note that the implementations referenced in these practices should be considered examples; they have not been updated to reflect current versions of operating systems or current vulnerabilities.

**Implementations (archive)**

We developed these implementations to provide details for how users could complete steps discussed in CERT security practices for specific operating systems. However, these implementations should be considered examples;

they have not been updated to reflect current versions of operating systems or current vulnerabilities. We recommend that you visit vendor web sites for current information and guidance about securing your operating system.

**General**

1. Process analysis checklist
2. Examples of contract language for terms and conditions or statements of work
3. Maintaining currency by periodically reviewing public and vendor information sources
4. Identifying tools that aid in detecting signs of intrusion
5. Establishing and maintaining a physical inventory of your computing equipment

**UNIX**

1. Using MD5 to verify the integrity of file contents
2. Using Tripwire to verify the integrity of directories and files on systems running Solaris 2.x

3. Inspecting your Solaris system and network logs for evidence of intrusions
4. Inspecting the logs produced by the TCP wrapper program on a Solaris 2.x system
5. Using the ps program to examine processes for signs of intrusive activity
6. Configuring Sun Solaris as a Web server
7. Configuring NCSA httpd and Web-server content directories on a Sun Solaris 2.5.1 host
8. Enabling process accounting on systems running Solaris 2.x
9. Installing, configuring, and using tcp wrapper to log unauthorized connection attempts on systems running Solaris 2.x
10. Configuring and using syslogd to collect logging messages on systems running Solaris 2.x
11. Using newsyslog to rotate files containing logging messages on systems running Solaris 2.x
12. Installing, configuring, and using logdaemon to log unauthorized login attempts on systems running Solaris 2.x

13. Installing, configuring, and using logdaemon to log unauthorized connection attempts to rshd and rlogind on systems running Solaris 2.x
14. Understanding system log files on a Solaris 2.x operating system
15. Installing, configuring, and using swatch to analyze log messages on systems running Solaris 2.x
16. Installing, configuring, and using logsurfer on systems running Solaris 2.x
17. Configuring and installing lsof 4.50 on systems running Solaris 2.x
18. Configuring and installing top 3.5 on systems running Solaris 2.x
19. Installing, Configuring, and using npasswd to improve password quality on systems running Solaris 2.x
20. Installing and configuring sps to examine processes on systems running Solaris 2.x
21. Installing and securing Solaris 2.6 servers
22. Installing, configuring, and operating the secure shell (SSH) on systems running Solaris 2.x
23. Characterizing files and directories with native tools on Solaris 2.X

24. Detecting changes in files and directories with native tools on Solaris 2.X
25. Installing and operating lastcomm on systems running Solaris 2.x
26. Installing, configuring, and using spar 1.3 on systems running Solaris 2.x
27. Installing and operating tcpdump 3.5.x on systems running Solaris 2.x
28. Installing, configuring, and using argus to monitor systems running Solaris 2.x
29. Using newarguslog to rotate log files on systems running Solaris 2.x
30. Installing libpcap to support network packet tools on systems sunning Solaris 2.x
31. Writing rules and understanding alerts for Snort, a network intrusion detection system
32. Disabling network services on systems running Solaris 2.x
33. Installing noshell to support the detection of access to disabled accounts on systems running Solaris 2.x.
34. Disabling user accounts on systems running Solaris 2.x

35. Installing OpenSSL to ensure availability of cryptographic libraries on systems running Solaris 2.x.
36. Installing and Operating ssldump 0.9 Beta 1 on systems running Solaris 2.x.
37. Installing The Coroner's Toolkit and using the mactime utility.
38. Using The Coroner's Toolkit: Harvesting information with grave-robber.
39. Using The Coroner's Toolkit: Rescuing files with lazarus.

**NT**

1. Using RDISK /S to create an Emergency Repair Disk for Windows NT 4.0
2. Using SYSKEY to protect the password data for Windows NT 4.0
3. Selecting audit events for directories and files on Windows NT 4.0 systems
4. Selecting audit events for Windows NT 4.0 registry keys
5. Restricting access to the %SYSTEMROOT%\repair directory for Windows NT 4.0
6. Setting up a logon banner on Windows NT 4.0

7. Configuring a Windows NT 4.0 system to shut down automatically when writing to an event log fails
8. Enabling auditing of Windows NT 4.0 printer events
9. Selecting Windows NT 4.0 event log settings
10. Selecting Audit Policy Settings on Windows NT 4.0 Workstations
11. Selecting Audit Policy Settings on Windows NT 4.0 Servers

**Basic Windows NT 4.0 Security Implementations**

12. Preparing for the initial installation of Windows NT 4.0 systems
13. Securing Windows NT 4.0 workstation during initial installation
14. Securing a stand-alone Windows NT 4.0 Server during initial installation
15. Securing a Windows NT 4.0 Server as Primary Domain Controller during initial installation
16. Securing a Windows NT 4.0 Server as Backup Domain Controller during initial installation

**Other technologies**

1. Inspecting the logs produced by the Apache Web server
2. Inspecting the logs produced by the NCSA Web server

**Intended audience**

The modules are written for system and network administrators. These are the people whose day-to-day activities include installation, configuration, and maintenance of the computers and networks.

**Module structure**

Each module has three kinds of components:

The **executive summary** describes the problem and outlines a general approach to its solution.

**CERT security practices** present the problem solution in detail. Each practice includes a brief description (*what* to do), the specific security problem or vulnerability that the practice addresses (*why* do it), and one or more methods (steps) for executing the practice (*where*, *when*, and *how* to do it). Each executive summary contains links to all the relevant practices.

**Implementation details** provide additional information on how to perform a practice for a specific technology; for example, Sun, Solaris, UNIX, Windows, and NT. In most cases, practices are independent of particular technologies and are applicable to all organizations. How an organization adopts and implements the practices, however, often depends on the specific networking and computing technologies it uses. The practices contain links to available technology-specific implementation details. Please note that these implementations should be considered examples; they have not been updated to reflect current versions of operating systems or current vulnerabilities.

**Formats**

Modules are published in three formats:

Title: **World Wide Web** (HTML), suitable for online reading with a Web browser

**Portable Document Format** (PDF), suitable for printing or online viewing with an appropriate viewer or Web browser plug-in

**PostScript**, suitable for printing

The PDF and PostScript icons will appear after the module title in the list above when these formats become available.

**Kiến thức bảo mật mạng máy tính**

Trong phần này chúng tôi muốn giới thiệu với các bạn các kiến thức bảo mật mạng máy tính cơ bản bằng Tiếng Anh. Tài liệu được lấy từ tổ chức bảo mật CERT

This document gives home users an overview of the security risks and countermeasures associated with Internet connectivity, especially in the context of “always-on” or broadband access services (such as cable modems and DSL). However, much of the content is also relevant to traditional dial-up users (users who connect to the Internet using a modem).

Introduction

I. Computer security
   A. What is computer security?
   B. Why should I care about computer security?
   C. Who would want to break into my computer at home?
   D. How easy is it to break into my computer?
II. Technology
   A. What does "broadband" mean?
   B. What is cable modem access?
   C. What is DSL access?
   D. How are broadband services different from traditional dial-up services?
   E. How is broadband access different from the network I use at work?
   F. What is a protocol?
   G. What is IP?
   H. What is an IP address?
   I. What are static and dynamic addressing?
   J. What is NAT?
   K. What are TCP and UDP ports?
   L. What is a firewall?
   M. What does antivirus software do?
III. Computer security risks to home users
   A. What is at risk?
   B. Intentional misuse of your computer
      1. Trojan horse programs
      2. Back door and remote administration programs
      3. Denial of service
      4. Being an intermediary for another attack
      5. Unprotected Windows shares

I. Computer security

*A. What is computer security?*

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

*B. Why should I care about computer security?*

We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements).

*C. Who would want to break into my computer at home?*

Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.

Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

*D. How easy is it to break into my computer?*

Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely. Most of the incident reports of computer break-ins received at the CERT/CC could have been prevented if system administrators and users kept their computers up-to-date with patches and security fixes.

Also, some software applications have default settings that allow other users to access your computer unless you change the settings

to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

## II. Technology

This section provides a basic introduction to the technologies that underlie the Internet. It was written with the novice end-user in mind and is not intended to be a comprehensive survey of all Internet-based technologies. Subsections provide a short overview of each topic. This section is a basic primer on the relevant technologies. For those who desire a deeper understanding of the concepts covered here, we include links to additional information.

### *A. What does broadband mean?*

"Broadband" is the general term used to refer to high-speed network connections. In this context, Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently referred to as broadband Internet connections. "Bandwidth" is the term used to describe the relative speed of a network connection -- for example, most current dial-up modems can support a bandwidth of 56 kbps (thousand bits per second). There is no set bandwidth threshold required for a connection to be referred to as "broadband", but it is typical for connections in excess of 1 Megabit per second (Mbps) to be so named.

### *B. What is cable modem access?*

A cable modem allows a single computer (or network of computers) to connect to the Internet via the cable TV network. The cable modem usually has an Ethernet LAN (Local Area Network) connection to the computer, and is capable of speeds in excess of 5 Mbps.

Typical speeds tend to be lower than the maximum, however, since cable providers turn entire neighborhoods into LANs which share the same bandwidth. Because of this "shared-medium" topology, cable modem users may experience somewhat slower network access during periods of peak demand, and may be more susceptible to risks such as packet sniffing and unprotected windows shares than

users with other types of connectivity. (See the "Computer security risks to home users" section of this document.)

C. *What is DSL access?*

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is only dedicated between your home and the DSL provider's central office -- the providers offer little or no guarantee of bandwidth all the way across the Internet.

DSL access is not as susceptible to packet sniffing as cable modem access, but many of the other security risks we'll cover apply to both DSL and cable modem access. (See the "Computer security risks to home users" section of this document.)

D. *How are broadband services different from traditional dial-up services?*

Traditional dial-up Internet services are sometimes referred to as "dial-on-demand" services. That is, your computer only connects to the Internet when it has something to send, such as email or a request to load a web page. Once there is no more data to be sent, or after a certain amount of idle time, the computer disconnects the call. Also, in most cases each call connects to a pool of modems at the ISP, and since the modem IP addresses are dynamically assigned, your computer is usually assigned a different IP address on each call. As a result, it is more difficult (not impossible, just difficult) for an attacker to take advantage of vulnerable network services to take control of your computer.

Broadband services are referred to as "always-on" services because there is no call setup when your computer has something to send. The computer is always on the network, ready to send or receive data through its network interface card (NIC). Since the connection is always up, your computer’s IP address will change less frequently (if at all), thus making it more of a fixed target for attack.

What’s more, many broadband service providers use well-known IP addresses for home users. So while an attacker may not be able to

single out your specific computer as belonging to you, they may at least be able to know that your service providers' broadband customers are within a certain address range, thereby making your computer a more likely target than it might have been otherwise.

The table below shows a brief comparison of traditional dial-up and broadband services.

| | Dial-up | Broadband |
|---|---|---|
| Connection type | Dial on demand | Always on |
| IP address | Changes on each call | Static or infrequently changing |
| Relative connection speed | Low | High |
| Remote control potential | Computer must be dialed in to control remotely | Computer is always connected, so remote control can occur anytime |
| ISP-provided security | Little or none | Little or none |

*Table 1: Comparison of Dial-up and Broadband Services*

*E. How is broadband access different from the network I use at work?*

Corporate and government networks are typically protected by many layers of security, ranging from network firewalls to encryption. In addition, they usually have support staff who maintain the security and availability of these network connections.

Although your ISP is responsible for maintaining the services they provide to you, you probably won't have dedicated staff on hand to manage and operate your home network. You are ultimately responsible for your own computers. As a result, it is up to you to take reasonable precautions to secure your computers from accidental or intentional misuse.

*F. What is a protocol?*

A protocol is a well-defined specification that allows computers to communicate across a network. In a way, protocols define the "grammar" that computers can use to "talk" to each other.

*G. What is IP?*

IP stands for "Internet Protocol". It can be thought of as the common language of computers on the Internet. There are a number of detailed descriptions of IP given elsewhere, so we won't cover it in detail in this document. However, it is important to know a few things about IP in order to understand how to secure your computer. Here we'll cover IP addresses, static vs. dynamic addressing, NAT, and TCP and UDP Ports.

An overview of TCP/IP can be found in the TCP/IP Frequently Asked Questions (FAQ) at

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/

and

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/

*H. What is an IP address?*

IP addresses are analogous to telephone numbers – when you want to call someone on the telephone, you must first know their telephone number. Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address. IP addresses are typically shown as four numbers separated by decimal points, or "dots". For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

If you need to make a telephone call but you only know the person's name, you can look them up in the telephone directory (or call directory services) to get their telephone number. On the Internet, that directory is called the Domain Name System, or DNS for short. If you know the name of a server, say www.cert.org, and you type this into your web browser, your computer will then go ask its DNS server what the numeric IP address is that is associated with that name.

Every computer on the Internet has an IP address associated with it that uniquely identifies it. However, that address may change over time, especially if the computer is

- dialing into an Internet Service Provider (ISP)
- connected behind a network firewall
- connected to a broadband service using dynamic IP addressing.

*I. What are static and dynamic addressing?*

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Since ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

*J. What is NAT?*

Network Address Translation (NAT) provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet. NAT can be used in many different ways, but one method frequently used by home users is called "masquerading".

Using NAT masquerading, one or more devices on a LAN can be made to appear as a single IP address to the outside Internet. This allows for multiple computers in a home network to use a single

cable modem or DSL connection without requiring the ISP to provide more than one IP address to the user. Using this method, the ISP-assigned IP address can be either static or dynamic. Most network firewalls support NAT masquerading.

*K. What are TCP and UDP Ports?*

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP. Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications (also known as "services") on those computers to talk to each other.

In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications (e.g. email, file services, web services) running on the same IP address. Ports allow a computer to differentiate services such as email data from web data. A port is simply a number associated with each application that uniquely identifies that service on that computer. Both TCP and UDP use ports to identify services. Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Domain Name System (DNS).

*L. What is a firewall?*

The Firewalls FAQ (http://www.faqs.org/faqs/firewalls-faq/) defines a firewall as "a system or group of systems that enforces an access control policy between two networks." In the context of home networks, a firewall typically takes one of two forms:

- *Software firewall* - specialized software running on an individual computer, or
- *Network firewall* - a dedicated device designed to protect one or more computers.

Both types of firewall allow the user to define access policies for inbound connections to the computers they are protecting. Many also provide the ability to control what services (ports) the protected computers are able to access on the Internet (outbound access). Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some allow the user to customize these policies for their specific needs.

More information on firewalls can be found in the Additional resources section of this document.

*M. What does antivirus software do?*

There are a variety of antivirus software packages that operate in many different ways, depending on how the vendor chose to implement their software. What they have in common, though, is that they all look for patterns in the files or memory of your computer that indicate the possible presence of a known virus. Antivirus packages know what to look for through the use of virus profiles (sometimes called "signatures") provided by the vendor.

New viruses are discovered daily. The effectiveness of antivirus software is dependent on having the latest virus profiles installed on your computer so that it can look for recently discovered viruses. It is important to keep these profiles up to date.

More information about viruses and antivirus software can be found on the CERT Computer Virus Resource page

http://www.cert.org/other_sources/viruses.html

III. Computer security risks to home users

*A. What is at risk?*

Information security is concerned with three main areas:

- Confidentiality - information should be available only to those who rightfully have access to it
- Integrity -- information should be modified only by those who are authorized to do so
- Availability -- information should be accessible to those who need it when they need it

These concepts apply to home Internet users just as much as they would to any corporate or government network. You probably wouldn't let a stranger look through your important documents. In the same way, you may want to keep the tasks you perform on your computer confidential, whether it's tracking your investments or sending email messages to family and friends. Also, you should have some assurance that the information you enter into your computer remains intact and is available when you need it.

Some security risks arise from the possibility of intentional misuse of your computer by intruders via the Internet. Others are risks that you would face even if you weren't connected to the Internet (e.g. hard disk failures, theft, power outages). The bad news is that you probably cannot plan for every possible risk. The good news is that you can take some simple steps to reduce the chance that you'll be affected by the most common threats -- and some of those steps help with both the intentional and accidental risks you're likely to face.

Before we get to what you can do to protect your computer or home network, let's take a closer look at some of these risks.

*B. Intentional misuse of your computer*

The most common methods used by intruders to gain control of home computers are briefly described below. More detailed information is available by reviewing the URLs listed in the References section below.

1. Trojan horse programs
2. Back door and remote administration programs
3. Denial of service
4. Being an intermediary for another attack
5. Unprotected Windows shares
6. Mobile code (Java, JavaScript, and ActiveX)
7. Cross-site scripting
8. Email spoofing
9. Email-borne viruses
10. Hidden file extensions
11. Chat clients
12. Packet sniffing
13. Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus. More information about Trojan horses can be found in the following document.

http://www.cert.org/advisories/CA-1999-02.html

14. Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer. We recommend that you review the CERT vulnerability note about Back Orifice. This document describes how it works, how to detect it, and how to protect your computers from it:

http://www.cert.org/vul_notes/VN-98.07.backorifice.html

15. Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack. The following documents describe denial-of-service attacks in greater detail.

http://www.cert.org/advisories/CA-2000-01.html

http://www.cert.org/archive/pdf/DoS_trends.pdf

It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

16. Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not your own computer, but someone else’s -- your computer is just a convenient tool in a larger attack.

17. Unprotected Windows shares

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools such as those described in

http://www.cert.org/incident_notes/IN-2000-01.html

Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm described in

http://www.cert.org/incident_notes/IN-2000-03.html

There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

18. Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser. We recommend that you do so if you are browsing web sites that you are not familiar with or do not trust.

Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to display HTML. Thus, vulnerabilities

that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

More information on malicious code is available in http://www.cert.org/tech_tips/malicious_code_FAQ.html

More information on ActiveX security is available in http://www.cert.org/archive/pdf/activeX_report.pdf

19. Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

You can potentially expose your web browser to malicious scripts by

- following links in web pages, email messages, or newsgroup postings without knowing what they link to
- using interactive forms on an untrustworthy site
- viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags

More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

20. Email spoofing

Email “spoofing” is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering ploys. Examples of the latter include

- email claiming to be from a system administrator requesting users to change their passwords to a

specified string and threatening to suspend their account if they do not comply
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

Note that while service providers may occasionally request that you change your password, they usually will not specify what you should change it to. Also, most legitimate service providers would never ask you to send them any password information via email. If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately.

21. Email borne viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus (see References) spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs.

Many recent viruses use these social engineering techniques to spread. Examples include

- W32/Sircam -- http://www.cert.org/advisories/CA-2001-22.html
- W32/Goner -- http://www.cert.org/incident_notes/IN-2001-15.html

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

22. Hidden file extensions

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows. Multiple email-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". Other malicious programs have since incorporated similar naming schemes. Examples include

- Downloader (MySis.avi.exe or QuickFlick.mpg.exe)
- VBS/Timofonica (TIMOFONICA.TXT.vbs)
- VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)
- VBS/OnTheFly (AnnaKournikova.jpg.vbs)

The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example). For further information about these and other viruses, please visit the sites listed on our Computer Virus Resource page:

http://www.cert.org/other_sources/viruses.html

23. Chat clients

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type.

Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat client's ability to execute downloaded files. As always, you should be wary of exchanging files with unknown parties.

24. Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access.

Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighborhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

*Accidents and other risks*

In addition to the risks associated with connecting your computer to the Internet, there are a number of risks that apply even if the computer has no network connections at all. Most of these risks are well-known, so we won't go into much detail in this document, but it is important to note that the common practices associated with reducing these risks may also help reduce susceptibility to the network-based risks discussed above.

0. Disk failure

Recall that availability is one of the three key elements of information security. Although all stored data can become unavailable -- if the media it's stored on is physically damaged, destroyed, or lost -- data stored on hard disks is at higher risk due to the mechanical nature of the device. Hard disk crashes are a common cause of data loss on personal computers. Regular system backups are the only effective remedy.

1. Power failure and surges

Power problems (surges, blackouts, and brown-outs) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the

computer. Common mitigation methods include using surge suppressors and uninterruptible power supplies (UPS).

2. Physical Theft

Physical theft of a computer, of course, results in the loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect. Regular system backups (with the backups stored somewhere away from the computer) allow for recovery of the data, but backups alone cannot address confidentiality. Cryptographic tools are available that can encrypt data stored on a computer's hard disk. The CERT/CC encourages the use of these tools if the computer contains sensitive data or is at high risk of theft (e.g. laptops or other portable computers).

Actions home users can take to protect their computer systems

The CERT/CC recommends the following practices to home users:

0. Consult your system support personnel if you work from home
    1. Use virus protection software
    2. Use a firewall
    3. Don't open unknown email attachments
    4. Don't run programs of unknown origin
    5. Disable hidden filename extensions
    6. Keep all applications (including your operating system) patched
    7. Turn off your computer or disconnect from the network when not in use
    8. Disable Java, JavaScript, and ActiveX if possible
    9. Disable scripting features in email programs
    10. Make regular backups of critical data
    11. Make a boot disk in case your computer is damaged or compromised

Further discussion on each of these points is given below.

*Recommendations*

12. Consult your system support personnel if you work from home

If you use your broadband access to connect to your employer's network via a Virtual Private Network (VPN) or other means, your

employer may have policies or procedures relating to the security of your home network. Be sure to consult with your employer's support personnel, as appropriate, before following any of the steps outlined in this document.

13. Use virus protection software

The CERT/CC recommends the use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available.

See http://www.cert.org/other_sources/viruses.html#VI for more information.

14. Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it’s not sufficient to install a firewall and then ignore all other security measures.

15. Don't open unknown email attachments

Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

0. be sure your virus definitions are up-to-date (see "Use virus protection software" above)
    1. save the file to your hard disk
    2. scan the file using your antivirus software
    3. open the file

For additional protection, you can disconnect your computer's network connection before opening the file.

Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

16. Don't run programs of unknown origin

    Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

17. Disable hidden filename extensions

    Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows. After disabling this option, there are still some file extensions that, by default, will continue to remain hidden.

    There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

    Specific instructions for disabling hidden file name extensions are given in http://www.cert.org/incident_notes/IN-2000-07.html

18. Keep all applications, including your operating system, patched

    Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

    Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a

mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates.

19. Turn off your computer or disconnect from the network when not in use

    Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

20. Disable Java, JavaScript, and ActiveX if possible

    Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

    The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites.

    Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

    Detailed instructions for disabling browser scripting languages are available in http://www.cert.org/tech_tips/malicious_code_FAQ.html

    More information on ActiveX security, including recommendations for users who administer their own computers, is available in http://www.cert.org/archive/pdf/activeX_report.pdf

    More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

21. Disable scripting features in email programs

    Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages.

Therefore, in addition to disabling scripting features in web browsers (see "Disable Java, JavaScript, and ActiveX if possible", above), we recommend that users also disable these features in their email programs.

22. Make regular backups of critical data

    Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer.

23. Make a boot disk in case your computer is damaged or compromised

    To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help when recovering a computer after such an event has occurred. Remember, however, you must create this disk before you have a security event.

## Appendix

### References and additional information

This section contains links to references and additional resources related to this document.

### References

The following documents were used in compiling portions of this document:

- CERT Advisories
- CERT Incident Notes
- CERT Vulnerability Notes
- CERT Tech Tips
- Other CERT documents

CERT Advisories

CA-1999-02: Trojan Horses
http://www.cert.org/advisories/CA-1999-02.html
CA-1999-04: Melissa Macro Virus
http://www.cert.org/advisories/CA-1999-04.html
CA-2000-01: Denial-of-Service Developments
http://www.cert.org/advisories/CA-2000-01.html
CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests
http://www.cert.org/advisories/CA-2000-02.html
CA-2001-22: W32/Sircam Malicious Code
http://www.cert.org/advisories/CA-2001-22.html

CERT Incident Notes

IN-2000-01: Windows Based DDOS Agents
http://www.cert.org/incident_notes/IN-2000-01.html
IN-2000-02: Exploitation of Unprotected Windows Networking Shares
http://www.cert.org/incident_notes/IN-2000-02.html
IN-2000-03: 911 Worm
http://www.cert.org/incident_notes/IN-2000-03.html
IN-2000-07: Exploitation of Hidden File Extensions
http://www.cert.org/incident_notes/IN-2000-07.html
IN-2000-08: Chat Clients and Network Security
http://www.cert.org/incident_notes/IN-2000-08.html
IN-2001-15: W32/Goner Worm
http://www.cert.org/incident_notes/IN-2001-15.html

### CERT Vulnerability Notes

VN-98.07: Back Orifice
http://www.cert.org/vul_notes/VN-98.07.backorifice.html

### CERT Tech Tips

Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites
http://www.cert.org/tech_tips/malicious_code_FAQ.html
Protecting Yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond
http://www.cert.org/tech_tips/virusprotection.html
Spoofed/Forged Email
http://www.cert.org/tech_tips/email_spoofing.html
Windows 95/98 Computer Security Information
http://www.cert.org/tech_tips/win-95-info.html

### Other CERT documents

Other Computer Virus Resources
http://www.cert.org/other_sources/viruses.html
Securing Desktop Workstations
http://www.cert.org/security-improvement/modules/m04.html
Results of the Security in ActiveX Workshop
http://www.cert.org/archive/pdf/activeX_report.pdf
Security of the Internet
http://www.cert.org/encyc_article/tocencyc.html#PackSnif
Trends in Denial of Service Attack Technology
http://www.cert.org/archive/pdf/DoS_trends.pdf

## Additional resources

Additional information is available from the following sources.
TCP/IP Frequently Asked Questions
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/
Computer Virus Frequently Asked Questions for New Users
http://www.faqs.org/faqs/computer-virus/new-users/
alt.comp.virus Frequently Asked Questions
http://www.faqs.org/faqs/computer-virus/alt-faq/part1/
http://www.faqs.org/faqs/computer-virus/alt-faq/part2/
http://www.faqs.org/faqs/computer-virus/alt-faq/part3/
http://www.faqs.org/faqs/computer-virus/alt-faq/part4/
VIRUS-L/comp.virus Frequently Asked Questions
http://www.faqs.org/faqs/computer-virus/faq/
Firewalls Frequently Asked Questions
http://www.faqs.org/faqs/firewalls-faq/

## CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

### *Using encryption*

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

### *Getting security information*

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```



## Revision History

| | |
|---|---|
| June 22, 2001 | Initial Release |
| June 26, 2001 | Added SubSeven to Remote Administration Programs section |
| August 6, 2001 | Clarification of IP addressing for ISP dial-up modem pools |
| December 5, 2001 | Fixed broken link to CA-1999-02, added links for Sircam, Goner, and DDoS Trends |