HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Phạm Huyền Huyên

GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI

Chuyên nghành: Hệ thống thông tin
Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS. TS. Lê Hữu Lập

Phản biện 1: PGS. TS. Nguyễn Hà Nam

Phản biện 2: TS. Nguyễn Vĩnh An

Luận văn đã được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 9giờ 15 ngày 09 tháng 1 năm 2021

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỞ ĐẦU

1. Lý do chọn đề tài:

Cùng với sự phát triển mạnh mẽ của khoa học công nghệ, đặc biệt là công nghệ thông tin và điện tử viễn thông, nhu cầu trao đổi thông tin và dữ liệu của con người ngày càng cao. Mạng máy tính đóng vai trò quan trọng trong mọi lĩnh vực của cuộc sống. Bên cạnh nền tảng mạng máy tính có dây, mạng máy tính không dây ngay từ khi ra đời đã thể hiện những ưu điểm vượt trội về tính tiện dụng, linh hoạt và đơn giản. Mặc dù mạng máy tính không dây đã tồn tại từ lâu, nhưng chúng đã đạt được sự phát triển nổi bật trong thời đại công nghệ điện tử, và chịu ảnh hưởng sâu sắc của nền kinh tế và vật lý hiện đại. Ngày nay, mạng không dây đã trở nên thiết thực trong cuộc sống. Chúng ta chỉ cần các thiết bị như điện thoại thông minh, máy tính xách tay, PDA hoặc bất kỳ phương thức truy cập mạng không dây nào là có thể truy cập mạng tại nhà, cơ quan, trường học, văn phòng và những nơi khác.... Bất cứ nơi nào trong phạm vi phủ sóng của mạng. Do tính chất trao đổi thông tin trong không gian truyền dẫn nên khả năng rò rỉ thông tin là rất cao. Nếu chúng ta không khắc phục điểm yếu này, môi trường mạng không dây sẽ trở thành mục tiêu của các hacker xâm nhập, gây thất thoát thông tin và tiền bạc. Vì vậy, bảo mật thông tin là một vấn đề đang thu hút rất nhiều sự quan tâm. Với sự phát triển của mạng không dây, cần phát triển khả năng bảo mật để cung cấp cho người dùng thông tin hiệu quả và đáng tin cậy.

Vì vậy, việc kết nối mạng nội bộ của cơ quan tổ chức mình vào mạng Internet mà không có các biện pháp đảm bảo an ninh sẽ dẫn đến nguy cơ mất an toàn thông tin và dữ liệu cao. Để nâng cao tính bảo mật cho hệ thống mạng nội bộ phục vụ cho nhu cầu công việc, giảng dạy học tập của trường Đại học Hà Nội, học viên chọn đề tài: "**GIẢI PHÁP BẢO MẬT HỆ THỐNG WLAN, ÁP DỤNG CHO MẠNG TRƯỜNG ĐẠI HỌC HÀ NỘI**".

2. Tổng quan vấn đề nghiên cứu

Nội dung chính của luận văn này là quá trình nghiên cứu, tìm hiểu để từ đó đúc kết ra được những yếu tố đảm bảo tính bảo mật cho hệ thống mạng WLAN:

- Nắm bắt được một số phương pháp tấn công hệ thống mạng thường gặp và các giải pháp bảo mật để có được cách thức phòng chống, cách xử lý sự cố và khắc phục sau sự cố một cách nhanh nhất.

- Đề xuất giải pháp nâng cao tính bảo mật cho hệ thống mạng của Trường Đại học Hà Nội.

3. Mục tiêu nghiên cứu của đề tài

Mục tiêu nghiên cứu của luận văn là nghiên cứu kỹ thuật tấn công mạng WLAN, các giải pháp đảm bảo an toàn mạng WLAN và đề xuất giải pháp nâng cao độ bảo mật cho mạng WLAN tại trường Đại học Hà Nội.

4. Đối tượng và phạm vi nghiên cứu của đề tài

- Đối tượng nghiên cứu của luận văn là mạng WLAN và các vấn đề liên quan đến bảo mật mạng WLAN.

- Phạm vi nghiên cứu của luận văn là các giải pháp bảo mật mạng WLAN và ứng dụng cho mạng WLAN tại trường Đại học Hà Nội.

5. Phương pháp nghiên cứu của đề tài

- Về mặt lý thuyết: Thu thập, khảo sát, nghiên cứu các tài liệu và thông tin có liên quan đến bảo mật mạng WLAN.

- Về mặt thực nghiệm: Khảo sát hệ thống mạng WLAN nội bộ Trường Đại học Hà Nội và đề xuất giải pháp bảo mật cho hệ thống mạng.

6. Bố cục luận văn

Luận văn chia làm 3 chương chính:

Chương 1: Tổng quan về mạng không dây & Nguy cơ tấn công mạng.

1.1 Giới thiệu và WLAN

1.2 Các chuẩn mạng thông dụng của WLAN

1.3 Cơ sở hạ tầng mô hình mạng WLAN

1.4 Các nguy cơ tấn công mạng WLAN

1.5 Kết chương

Chương 2: Các giải pháp bảo mật trong mạng WLAN

2.1 Giới thiệu

2.2 Xác thực qua mã hóa Wifi: WEP; WPA; WPA2; WPA3

2.3 Xác thực Wifi bằng Radius Server

2.3 Kết chương

Chương 3: Bảo mật mạng WLAN của Hanu bằng chứng thực Radius Server

3.1 Khảo sát mạng WLAN Đại Học Hà Nội

3.2 Đề xuất các giải pháp bảo mật cho mạng WLAN tại trường Đại học Hà Nội

3.3 Cài đặt

3.4 Thử nghiệm và đánh giá kết quả

3.5 Kết chương

Trong quá trình thực hiện luận văn, mặc dù bản thân đã cố gắng thu thập tài liệu, củng cố kiến thức... nhưng luận văn vẫn còn những hạn chế nhất định. Học viên rất mong nhận được sự chỉ dạy, đóng góp tận tình của các thầy, cô để luận văn của học viên được hoàn thiện và có tính ứng dụng cao hơn trong thực tiễn.

CHƯƠNG I – TỔNG QUAN VỀ MẠNG WLAN & NGUY CƠ TẤN CÔNG MẠNG

1.1 – Giới thiệu về mạng WLAN

Công nghệ WLAN xuất hiện vào cuối những năm 1990, khi các nhà sản xuất giới thiệu các sản phẩm hoạt động ở dải tần 900MHz. Các giải pháp này cung cấp tốc độ truyền dữ liệu 1Mbps, thấp hơn nhiều so với tốc độ 10Mbps của hầu hết các mạng có dây hiện thời.

Năm 1997, IEEE (Viện Kỹ sư Điện và Điện tử) đã phê duyệt chuẩn 802.11, và nó còn được gọi là WIFI (Wireless Fidelity) của WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền dữ liệu, bao gồm một phương pháp truyền tín hiệu vô tuyến ở tần số 2.4 GHz.

Vào năm 1999, IEEE đã thông qua hai cách triển khai chuẩn 802.11, thông qua các phương thức truyền 8.2.11a và 802.11b. Các thiết bị 802.11b phát sóng với tốc độ 2.4GHz, cung cấp tốc độ truyền tải lên đến 11Mbps. So với mạng có dây, mục đích của việc tạo IEEE 802.11b là cung cấp hiệu quả, thông lượng và bảo mật.

Đầu năm 2003, IEEE công bố một tiêu chuẩn khác là 802.11g, có thể truyền thông tin ở dải tần 2.4GHz và 5GHz. Chuẩn 802.11g có thể tăng tốc độ truyền dữ liệu lên 54Mbps. Ngoài ra, các sản phẩm sử dụng chuẩn 802.11g cũng có thể tương thích với các thiết bị 802.11b. Ngày nay, chuẩn 802.11g đã đạt đến tốc độ 108Mbps-300Mbps.

Vào cuối năm 2009, chuẩn 802.11n đã được IEEE phê duyệt để sử dụng chính thức và là sản phẩm tiêu chuẩn được chứng nhận bởi Wi-Fi Alliance. Mục tiêu chính của công nghệ này là tăng tốc độ truyền tải và phạm vi hoạt động của thiết bị bằng cách kết hợp công nghệ tiên tiến.

Chuẩn 802.11ac được phát hành vào năm 2013 và được gọi là Wi-Fi 5. 802.11ac sử dụng công nghệ không dây băng tần kép để hỗ trợ kết nối đồng thời trên hai băng tần 2.4 GHz và 5 GHz. 802.11ac cung cấp khả năng tương thích ngược với các chuẩn 802.11b, 802.11g và 802.11n, đồng thời có băng thông lên tới 1300 Mbps trên băng tần 5 GHz và 450 Mbps trên băng tần 2.4 GHz.

Chuẩn 802.11ax được gọi là Wi-Fi 6, là phiên bản mới nhất được chính thức áp dụng vào ngày 16 tháng 9 năm 2019. Chuẩn kết nối không dây thế hệ thứ sáu cung cấp cho người dùng nền tảng kết

nối mới mang đến nhiều cải tiến đáng giá, trong đó quan trọng nhất là tốc độ truy cập nhanh, băng thông lớn và độ trễ thấp, so với sản phẩm thế hệ trước ưu việt hơn nhiều lần. Đối với một loạt các ứng dụng hiện đang yêu cầu tốc độ truyền ngày càng cao, điều này đã đạt được một bước tiến lớn: phát trực tuyến phim độ phân giải cực cao lên đến 4K, 8K; ứng dụng/phần mềm thương mại; chơi trò chơi trực tuyến, họp trực tuyến. .. có thể giúp người dùng nhận được nhiều lợi ích nhất từ cải tiến này.

1.2 - Các chuẩn mạng thông dụng của WLAN

Các chuẩn của WLAN được Học viện Kỹ nghệ Điện và Điện tử IEEE (Institute of Electrical and Electronics Engineers) qui chuẩn và thống nhất trên toàn thế giới.

1.2.1 - Chuẩn 802.11

Đây là tiêu chuẩn đầu tiên cho hệ thống mạng không dây. Tốc độ truyền từ 1 đến 2 Mbps và hoạt động ở dải tần 2.4GHz. Tiêu chuẩn bao gồm tất cả các công nghệ truyền dẫn hiện tại, bao gồm phổ chuỗi trực tiếp (DSS), trải phổ nhảy tần (FHSS) và tia hồng ngoại. Chuẩn 802.11 là một trong hai chuẩn mô tả hoạt động của sóng truyền (FHSS) trong mạng không dây. Chỉ phần cứng phù hợp với chuẩn 802.11 mới có thể sử dụng hệ thống bằng sóng mang này.

1.2.2 - Chuẩn 802.11a

IEEE đã bổ sung và phê duyệt tiêu chuẩn vào tháng 9 năm 1999 để cung cấp một tiêu chuẩn có thể hoạt động ở tốc độ cao hơn (từ 20 đến 54 Mbit/s) trên băng tần 5 GHz mới. Các hệ thống tuân thủ tiêu chuẩn này hoạt động ở băng tần 5.15 đến 5.25 GHz và 5.75 đến 5.825 GHz với tốc độ dữ liệu lên đến 54 Mbit/s. Tiêu chuẩn sử dụng công nghệ điều chế OFDM - Ghép kênh phân chia theo tần số trực giao) để đạt được tốc độ dữ liệu cao hơn và khả năng chống nhiễu đa đường tốt hơn.

1.2.3 - Chuẩn 802.11b

Giống như tiêu chuẩn IEEE 802.11a, lớp vật lý cũng đã thay đổi so với tiêu chuẩn IEEE.802.11. Các hệ thống tuân thủ tiêu chuẩn này hoạt động ở dải tần 2.400 đến 2.483 GHz và hỗ trợ các dịch vụ thoại, dữ liệu và hình ảnh với tốc độ tối đa 11 Mbit/s. Tiêu chuẩn xác định môi trường truyền DSSS với tốc độ dữ liệu 11 Mbit/s, 5,5 Mbit/s, 2Mbit/s và 1 Mbit/s.

WLAN tuân thủ IEEE 802.11b phù hợp với các môi trường đông đúc và các khu vực rộng lớn, chẳng hạn như các tòa nhà, nhà máy, nhà kho và trung tâm phân phối… Khoảng cách hoạt động của hệ thống khoảng 100 mét.

1.2.4 – Chuẩn 802.11g

Các hệ thống tuân theo tiêu chuẩn này hoạt động trên băng tần 2.4 GHz và có thể đạt tốc độ 54 Mbit/s. Giống như IEEE 802.11a, IEEE 802.11g cũng sử dụng công nghệ điều chế OFDM để đạt được tốc độ cao hơn. Ngoài ra, các hệ thống tuân thủ IEEE 802.11g tương thích ngược với các hệ thống IEEE 802.11b vì chúng thực hiện tất cả các chức năng IEEE 802.11b cần thiết và cho phép các máy khách của hệ thống tuân theo hệ thống IEEE 802.11b và chuẩn AP của IEEE 802.11g.

1.2.5 – Chuẩn 802.11n

Chuẩn 802.11n đã được viện IEEE phê duyệt để sử dụng chính thức, đồng thời cũng đã vượt qua thử nghiệm và chứng nhận của Liên minh Wi-Fi (Wi-Fi Alliance) cho các sản phẩm tiêu chuẩn. Chứng nhận Wi-Fi 802.11n là một bản cập nhật bổ sung một số tính năng tùy chọn cho bản dự thảo 802.11n 2.0 (bản nháp 2.0) do Wi-Fi Alliance đưa ra vào tháng 6 năm 2007.

Về lý thuyết, chuẩn 802.11n cho phép kết nối ở tốc độ 300 Mbps (lên đến 600 Mbps), nhanh hơn 6 lần và mở rộng vùng phủ sóng so với tốc độ đỉnh lý thuyết của các chuẩn trước đó như 802.11g/a. 802.11n (54 Mbps), là mạng Wi-Fi đầu tiên có thể cạnh tranh với mạng có dây 100Mbps về hiệu suất. Chuẩn 802.11n có thể hoạt động ở tần số 2.4GHz và 5GHz, người ta kỳ vọng rằng nó có thể giảm bớt tình trạng "quá tải" ở các chuẩn trước đây.

1.2.6 Chuẩn 802.11ac (tên gọi WiFi 5)

802.11ac là chuẩn WiFi mới nhất và phổ biến nhất hiện nay. 802.11ac sử dụng công nghệ không dây băng tần kép để hỗ trợ kết nối đồng thời trên băng tần 2.4 GHz và 5 GHz. 802.11ac cung cấp khả năng tương thích với các chuẩn 802.11b, 802.11g và 802.11n, băng thông của băng tần 5 GHz lên đến 1300 Mbps và băng thông của 2.4 GHz lên đến 450 Mbps.

Wi-Fi 802.11ac có thể gửi nhiều luồng không gian nhưng cho phép nhiều ăng-ten tiếp cận nhiều người dùng và nhiều thiết bị khác nhau trên cùng một dải tần cùng một lúc.

Tầm phủ sóng rộng hơn. Wi-Fi 802.11ac có phạm vi lớn hơn và tốc độ mạng nhanh hơn các chuẩn mạng khác. Nếu sử dụng trong các tòa nhà cao tầng, có thể giảm bớt các bộ lặp và bộ lặp lặp lại để giảm thiểu chi phí.

1.2.7 Chuẩn 802.11ax (Wi-Fi thế hệ thứ 6)

Wi-Fi thế hệ thứ sáu là bản cập nhật mới nhất của chuẩn mạng không dây, so với chuẩn Wi-Fi trước đây, chúng có tốc độ nhanh hơn, dung lượng lớn hơn và tiết kiệm năng lượng hơn.

Đặc điểm của Wifi 6: Tốc độ cực nhanh; Nâng cao hiệu quả; Điều chế cấp cao hơn 1024 – QAM; Symbol OFDM x 4; Độ rộng kênh 160MHz trên một luồng; OFDMA – Loại bỏ hoàn toàn độ trễ; 8x8 MU-MIMO: Chuẩn 802.11ax có thể hỗ trợ truyền đa người dùng MIMO đường lên và đường xuống bằng cách tạo nhiều luồng 802.11ax, do đó nhân hiệu suất của 802.11ac bằng cách tạo ra tối đa 8 luồng theo một hướng; Target Wake Time: Lập lịch kết nối để giảm thiểu điện năng tiêu thụ.

1.3 – Cơ sở hạ tầng mô hình mạng WLAN

1.3.1 - Cấu trúc cơ bản của mạng WLAN

Mạng sử dụng chuẩn 802.11 gồm có 4 thành phần chính:

- Hệ thống phân phối (DS)
- Điểm truy cập (AP)
- Tần liên lạc vô tuyến (Wireless Medium)
- Trạm (Stattions)

1.3.2 - Điểm truy cập: AP (Access Point)

AP là một thiết bị song công, và mức độ thông minh của nó tương đương với một bộ chuyển mạch Ethernet (Switch) phức tạp. Cung cấp điểm truy cập mạng cho máy khách (client).

Các chế độ hoạt động của AP: AP có thể giao tiếp với các máy không dây, với mạng có dây truyền thống và với các AP khác. Có 3 Mode hoạt động chính của AP: Chế độ gốc (Root mode); Chế độ cầu nối (Bridge mode); Chế độ lặp (Repeater mode).

1.3.3 – Các thiết bị máy khách trong mạng WLAN

a) Card PCI Wireless:
b) Card PCMCIA Wireless:
c) Card USB Wireless:

1.3.4 - Các mô hình mạng WLAN

Mạng WLAN gồm 3 mô hình cơ bản như sau: Mô hình mạng độc lập (IBSS) hay còn gọi là mạng Ad hoc; Mô hình mạng cơ sở (BSS); Mô hình mạng mở rộng (ESS).

1.4 – Các nguy cơ tấn công mạng WLAN

Hiện nay, có rất nhiều công nghệ có thể tấn công mạng WLAN, điển hình là các công nghệ sau:

1.4.1 – Phương thức bắt gói tin (Sniffing)

Đánh hơi là một khái niệm cụ thể của khái niệm chung "nghe trộm" được sử dụng trong mạng máy tính. Nó có thể là phương pháp đơn giản nhất, nhưng nó vẫn hiệu quả để chống lại các cuộc tấn công WLAN. Bắt gói có thể hiểu là phương thức lấy cắp thông tin khi đầu thu nằm trong hoặc gần vùng phủ sóng. Nếu thiết bị không thực sự được kết nối với AP để nhận gói dữ liệu, ngay cả khi thiết bị nằm trong hoặc gần vùng phủ sóng của mạng, thì cuộc tấn công bắt gói sẽ khó phát hiện ra sự hiện diện của thiết bị.

Các biện pháp ngăn chặn bắt gói tin: Vì “bắt gói tin” là phương thức tấn công thụ động nên rất khó phát hiện, đồng thời do đường truyền trên không phận nên không thể ngăn kẻ tấn công nghe trộm. Giải pháp ở đây là nâng cao khả năng mã hóa thông tin để kẻ tấn công không thể giải mã được, và khi đó thông tin thu được sẽ vô giá trị đối với kẻ tấn công. Cách tốt nhất để ngăn chặn việc đánh hơi là sử dụng IPSec để mã hóa thông lượng.

1.4.2 - Tấn công yêu cầu xác thực lại

Các cuộc tấn công chống xác thực là một cách để khai thác hiệu quả các lỗi trong chuẩn 802.11. Trong mạng 802.11, khi một nút mới muốn tham gia vào mạng, nó phải trải qua quá trình xác minh danh tính và liên kết. Khi các yêu cầu được đáp ứng, nút sẽ được cấp quyền truy cập vào mạng.

Rất dễ lấy địa chỉ AP trên mạng. Khi kẻ tấn công biết địa chỉ AP, nó sẽ sử dụng địa chỉ quảng bá để gửi thông báo khử xác thực đến tất cả các nút trong mạng. Nút sẽ chấp nhận thông báo xác minh

chắc chắn và thực hiện các biện pháp để xác minh xem thông báo hủy xác minh có được gửi từ AP hay không.

1.4.3 - Giả mạo AP

Giả mạo AP là một cuộc tấn công điển hình "người ở giữa". Đây là kiểu tấn công mà kẻ tấn công ở giữa và đánh cắp lưu lượng giữa hai nút. Loại tấn công này rất mạnh mẽ vì kẻ tấn công có thể tận dụng tất cả lưu lượng truy cập trong mạng. Rất khó để tạo ra một cuộc tấn công "man in the middle" trên mạng có dây vì kiểu tấn công này yêu cầu quyền truy cập thực tế vào liên kết. Trong mạng không dây, kiểu tấn công này rất dễ bị tấn công. Kẻ tấn công cần tạo ra một AP thu hút nhiều sự lựa chọn hơn các AP chính thống. Bạn có thể đặt AP giả này bằng cách sao chép tất cả các cấu hình của một AP hợp pháp: SSID, địa chỉ MAC, ...

Kiểu tấn công này tồn tại vì 802.11 không yêu cầu xác thực lẫn nhau giữa AP và nút. AP phát tới toàn bộ mạng. Điều này rất dễ bị kẻ tấn công nghe trộm, vì vậy kẻ tấn công có thể lấy được tất cả thông tin mà chúng cần.

1.4.4 - Tấn công dựa trên sự cảm nhận lớp vật lý

Kẻ tấn công đã sử dụng giao thức chống va chạm CSMA/CA, khiến tất cả người dùng luôn nghĩ rằng có một máy tính trong mạng. Điều này khiến các máy tính khác luôn phải đợi kẻ tấn công hoàn tất việc truyền dữ liệu, dẫn đến tình trạng nghẽn mạng.

Một phương pháp khác là sử dụng bộ tạo tín hiệu RF. Một cuộc tấn công tinh vi hơn là làm cho card mạng vào chế độ kiểm tra, trong đó card mạng liên tục truyền chế độ kiểm tra. Tất cả các nút trong phạm vi của nút giả đều rất nhạy cảm với sóng mang, và nếu có nút gửi thì không nút nào sẽ truyền.

1.4.5 - Tấn công ngắt kết nối

Quá trình tấn công như sau:

- Kẻ tấn công xác định mục tiêu (máy khách không dây) và mối quan hệ giữa AP và máy khách.
- Sau đó, kẻ tấn công gửi một khung ngắt kết nối bằng cách giả mạo MAC nguồn và MAC mục tiêu tới AP và máy khách tương ứng.

o Máy khách sẽ nhận được các khung này và nghĩ rằng khung bị ngắt kết nối đến từ AP. Đồng thời, kẻ tấn công cũng gửi một khung hủy liên kết đến AP.

o Sau khi ngắt kết nối một máy khách, kẻ tấn công tiếp tục thực hiện thao tác tương tự trên các máy khách còn lại, khiến máy khách tự động ngắt kết nối khỏi AP.

o Sau khi máy khách ngắt kết nối, họ sẽ ngay lập tức kết nối lại với AP. Kẻ tấn công tiếp tục gửi khung ngắt kết nối đến AP và máy khách.

1.5 – Kết luận chương 1

Mạng không dây có nhiều ưu điểm, tuy nhiên hacker có thể sẽ tấn công để lấy dữ liệu và làm hỏng hệ thống. Do điều kiện truy cập của mạng này, khả năng tiếp cận của các thiết bị bên ngoài trong không gian quảng bá là rất lớn. Đồng thời, khả năng bị nhiễu là không thể tránh khỏi. Để sử dụng mạng WLAN một cách an toàn, nghiên cứu sâu về các giải pháp bảo mật mạng WLAN là rất cần thiết. Trong chương II luận văn sẽ trình bày về vấn đề này.

CHƯƠNG II – CÁC GIẢI PHÁP BẢO MẬT TRONG MẠNG WLAN

2.1 – Giới thiệu

Trong hệ thống mạng, tính bảo mật và bí mật của hệ thống thông tin có vai trò rất quan trọng. Thông tin chỉ có giá trị nếu nó chính xác, và chỉ sau khi người có thẩm quyền lưu giữ thông tin biết được thông tin thì thông tin đó mới được bảo mật. Khi chúng ta không có thông tin hoặc việc sử dụng hệ thống thông tin không phải là phương tiện duy nhất để quản lý và vận hành, bảo mật đôi khi bị bỏ qua.

2.1.1 – Tại sao phải bảo mật

Mạng WLAN vốn dĩ không an toàn, nhưng dù sử dụng mạng LAN có dây hay WAN cũng không an toàn nếu không có phương pháp bảo mật hiệu quả.

Khi chi phí xây dựng mạng WLAN ngày càng giảm, ngày càng có nhiều tổ chức, công ty và cá nhân sử dụng nó. Điều này chắc chắn sẽ khiến tin tặc quay sang tấn công và khai thác lỗ hổng trên các nền tảng mạng sử dụng chuẩn 802.11. Sniffer có thể nắm bắt giao tiếp mạng, chúng có thể phân tích và đánh cắp thông tin quan trọng của

người dùng. Ngoài ra, tin tặc cũng có thể lấy đi dữ liệu bí mật của công ty; Can thiệp vào các giao dịch giữa tổ chức và khách hàng để lấy thông tin nhạy cảm; hoặc làm hỏng hệ thống. Những mất mát to lớn cho tổ chức, công ty không thể đo lường trước được. Do đó, cần thiết lập một mô hình và chiến lược bảo mật.

2.1.2 - Đánh giá vấn đề an toàn, bảo mật hệ thống

Để đảm bảo an ninh cho hệ thống mạng, cần thiết lập nhiều tiêu chuẩn để đánh giá mức độ an toàn và bảo mật của hệ thống mạng.

Trên phương diện logic, hệ thống bảo mật phải đảm bảo các yêu cầu sau: Tính bí mật (Confidentiality); Tính xác thực (Authentication); Tính toàn vẹn (Integrity); Tính không thể phủ nhận (Non repudiation); Tính không xác định đảm bảo rằng người gửi và người nhận không thể từ chối tin nhắn đã gửi; Tính khả dụng (Availability); Một hệ thống sẵn sàng đảm bảo có nghĩa là dữ liệu có thể được truy cập vào bất kỳ thời điểm nào mong muốn trong một thời gian nhất định; Khả năng điều khiển truy nhập (Access Control).

Trong bối cảnh an ninh mạng, kiểm soát truy cập là hạn chế khả năng truy cập máy chủ thông qua phương tiện truyền thông. Để đạt được sự kiểm soát này, cần phải xác định hoặc xác minh từng thực thể cố gắng có được quyền truy cập để quyền truy cập của mọi người có thể được thỏa mãn.

2.2 – Xác thực qua mã hóa Wifi

2.2.1 - Wired Equivalent Privacy (WEP)

WEP là một thuật toán đơn giản sử dụng PRNG (Pseudo Random Number Generator) và dòng mã RC4.

WEP sử dụng khóa mã hóa 64 bits hoặc 128 bits không đổi (nhưng trừ đi 24 bits được sử dụng cho vectơ khởi tạo khóa mã hóa, do đó độ dài khóa chỉ là 40 hoặc 104 bits cho phép truy cập vào mạng và cũng được sử dụng để mã hóa các thiết bị truyền dữ liệu.

Nhược điểm lớn nhất của WEP là nó sử dụng các khóa mã hóa tĩnh. Khi thiết lập cơ chế WEP cho bộ định tuyến, tất cả các thiết bị trên mạng sẽ sử dụng khóa để mã hóa tất cả các gói dữ liệu được truyền. Nhưng thực tế là, các gói dữ liệu mã hóa này không thể tránh khỏi việc bị đánh chặn. Do một số lỗi kỹ thuật "bí truyền", kẻ nghe trộm hoàn toàn có thể đánh chặn đủ số lượng gói tin mã hóa để tìm ra khóa giải mã là gì.

2.2.2 - WPA (Wi-Fi Protected Access)

Công nghệ mới mang tên WPA (Wi-Fi Protected Access) đã ra đời, khắc phục được nhiều khuyết điểm của WEP.

Một trong những cải tiến quan trọng nhất đối với WPA là việc sử dụng chức năng Giao thức toàn vẹn khóa tạm thời (TKIP). WPA cũng sử dụng thuật toán RC4 (chẳng hạn như WEP), nhưng sử dụng mã hóa 128-bit đầy đủ. Một chức năng khác của WPA là thay đổi khóa của mỗi gói.

Có hai tùy chọn cho WPA: WPA Personal và WPA Enterprise. Cả hai tùy chọn này đều sử dụng giao thức TKIP, sự khác biệt chỉ nằm ở khóa mã hóa ban đầu.

2.2.3 - WPA2 (Wi-Fi Protected Access II)

Sử dụng một thuật toán mã hóa mạnh và được gọi là tiêu chuẩn mã hóa nâng cao AES. AES sử dụng mật mã đối xứng khối Rijndael, sử dụng mã hóa 128 bits, 192 bits hoặc 256 bits.

Mặc dù AES được coi là tốt hơn nhiều so với 128-bit WEP hoặc 168-bit DES (Tiêu chuẩn mã hóa kỹ thuật số). Để đảm bảo hiệu suất, quá trình mã hóa cần được hoàn thành trong các thiết bị phần cứng như được tích hợp vào chip. Tuy nhiên, ít người dùng mạng không dây quan tâm đến vấn đề này. Ngoài ra, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch không tuân thủ 802.11i.

2.2.4 – WPA3 (Wi-Fi Protected Access III)

WPA3 ra đời nhằm khắc phục những điểm yếu mà thế hệ tiền nhiệm cần khắc phục.

Là phiên bản kế thừa cho thế hệ thứ ba của WPA2, phiên bản thứ ba này có ba mục tiêu chính: cải thiện khả năng mã hóa, đơn giản hóa việc sử dụng và tích hợp, đồng thời trở thành một giải pháp mạnh mẽ cho thiết bị IoT.

Đối mặt với các mối đe dọa đối với hơn 400 triệu mạng không dây, WPA3 phải được giới thiệu nhanh chóng. Tuy nhiên, hiện tại, không phải tất cả các bộ định tuyến hoặc thiết bị đều có thể sử dụng WPA3. Do đó, trong tương lai gần, WPA2 sẽ vẫn là một tiêu chuẩn mà các thiết bị được chứng nhận Wi-Fi phải hỗ trợ.

2.3 – Xác thực Wifi bằng RADIUS Server

2.3.1 Tổng quan về giao thức RADIUS

- Giao thức RADIUS: RADIUS thực chất là một giao thức mạng được sử dụng để xác thực và cho phép người dùng truy cập mạng từ xa.

- RADIUS cho phép xác thực tập trung, ủy quyền và kiểm tra quyền truy cập cho mạng.

Bảo mật WLAN kết hợp tiêu chuẩn 802.1x với xác thực người dùng trên điểm truy cập (AP). Máy chủ thực hiện xác thực trên nền tảng RADIUS có thể là một giải pháp tốt để cung cấp xác thực cho tiêu chuẩn 802.1x.

2.3.2 Tính chất của RADIUS

Nếu yêu cầu đến máy chủ xác thực chính không thành công, yêu cầu phải được gửi đến máy chủ phụ. Để thực hiện yêu cầu này, một bản sao của yêu cầu phải được lưu trữ trên lớp truyền tải để cho phép truyền thay thế. Điều này có nghĩa là phải có bộ đếm thời gian để truyền lại.

Trạng thái của RADIUS rất thoải mái, đơn giản hóa việc sử dụng UDP. Máy khách và máy chủ có thể thực hiện "truyền" dữ liệu UDP tức thì và cho phép chúng truyền các sự kiện có thể xảy ra một cách tự nhiên thông qua mạng.

UDP đơn giản hóa việc triển khai máy chủ. Quá trình xử lý độc lập sẽ được tạo ra trên máy chủ cho mỗi yêu cầu và các quá trình xử lý này sẽ phản hồi trực tiếp đến NAS của máy khách thông qua các gói dữ liệu UDP đến lớp truyền tải chính của máy khách.

2.3.3 Quá trình trao đổi gói tin

Khi máy khách được cấu hình để sử dụng RADIUS, một dấu nhắc lệnh để đăng ký mạng và yêu cầu người dùng nhập tên người dùng và mật khẩu.

Ứng dụng khách sẽ đưa ra một "yêu cầu truy cập" chứa các thuộc tính giống nhau: mật khẩu của người dùng, ID ứng dụng khách và ID cổng mà người dùng sẽ truy cập. "Yêu cầu truy cập" sẽ được gửi đến RADIUS qua mạng. Nếu không có phản hồi trong thời gian quy định, yêu cầu sẽ được gửi lại. Nếu máy chủ chính gặp sự cố hoặc chạy theo kiểu vòng tròn, máy khách có thể chuyển tiếp yêu cầu đến máy chủ dự phòng.

Mỗi khi máy chủ RADIUS nhận được yêu cầu, nó sẽ xác nhận việc gửi của máy khách.

Nếu máy khách hợp lệ, máy chủ RADIUS sẽ tìm kiếm người dùng có cùng tên trong yêu cầu trong cơ sở dữ liệu. RADIUS sẽ luôn xác minh mật khẩu của người dùng và cũng có thể xác minh ID ứng dụng khách và ID cổng mà người dùng được phép truy cập.

Máy chủ RADIUS có thể yêu cầu các máy chủ khác xác nhận yêu cầu. RADIUS sau đó hoạt động như một máy khách.

Nếu bất kỳ điều kiện nào không được đáp ứng, máy chủ RADIUS sẽ gửi phản hồi "Truy cập bị Từ chối", cho biết rằng yêu cầu của người dùng không hợp lệ.

Nếu tất cả các điều kiện được đáp ứng và máy chủ RADIUS muốn gửi yêu cầu phản hồi của người dùng, RADIUS sẽ gửi phản hồi "yêu cầu truy cập" (access-challenge). Client sẽ nhận access-challenge, và nếu nó được trang bị challenge/ response, nó sẽ hiển thị thông báo nhắc nhở user trả lời yêu cầu. Sau đó client sẽ gửi lại (re-submit) “yêu cầu truy cập” (original access-request) với một số hiệu yêu cầu (request ID) mới, nhưng thuộc tính usename-password được lấy từ thông tin vừa mới nhập vào, và kèm luôn cả thuộc tính trạng thái từ access-challenge. RADIUS server có thể trả lời một access-request bằng một access-accept, access-reject hoặc một access-challenge khác.

Nếu tất cả các điều kiện trên cuối cùng được đáp ứng, danh sách giá trị cấu hình của người dùng sẽ được đưa vào câu trả lời “chấp nhận truy cập".

2.3.4 - Xác thực, cấp phép và kiểm toán

Giao thức dịch vụ người dùng quay số xác thực từ xa (RADIUS) được định nghĩa trong RFC 2865 như sau: Nó có khả năng cung cấp xác thực tập trung, ủy quyền và kiểm soát truy cập (xác thực, ủy quyền và kế toán-AAA) cho các phiên. Được sử dụng kết hợp với SLIP và quay số PPP vì các nhà cung cấp dịch vụ xác thực Nhà cung cấp dịch vụ Internet (ISP) dựa vào giao thức này để xác thực người dùng với Internet.

Danh sách tên người dùng và mật khẩu phải được sử dụng để ủy quyền trong tất cả các máy chủ truy cập mạng (NAS). Một yêu cầu truy cập RADIUS sẽ chuyển thông tin đến máy chủ xác thực, thường

là máy chủ AAA. Trong cấu trúc hệ thống, dữ liệu người dùng, thông tin và các điều kiện truy cập có thể được tập trung vào một điểm (single point), nhà cung cấp giải pháp NAS có khả năng cung cấp các hệ thống quy mô lớn.

2.3.5 - Sự bảo mật và tính mở rộng

Tất cả các thông báo RADIUS được đóng gói bởi các biểu đồ dữ liệu UDP, bao gồm các thông tin như: loại thông báo, số thứ tự, độ dài, trình xác thực và các giá trị thuộc tính khác nhau.

Authenticator: Mục đích của Authenticator là cung cấp một chế độ an toàn.

Attribute-Value Pairs: Thông tin được mang bởi RADIUS được miêu tả trong một dạng Attribute-Value, hỗ trợ nhiều công nghệ khác nhau và nhiều phương pháp xác thực khác nhau. Một chuẩn được định nghĩa trong Attribute-Value pairs (cặp đôi), bao gồm User-Name, User-Password, NAS-IPAddress, NAS-Port, Service-Type.

2.3.6 - Áp dụng RADIUS cho WLAN

Cơ chế hoạt động:

RADIUS xác định quyền truy cập của người dùng mạng thông qua mô hình máy khách/máy chủ. Tuy nhiên, trên thực tế, yêu cầu truy cập mạng thường được gửi từ hệ thống máy khách và người dùng hoặc điểm truy cập WiFi tới hệ thống máy chủ RADIUS để xác thực.

Máy chủ RADIUS thường là sự kết hợp của các hệ thống tạo, duy trì và quản lý thông tin nhận dạng và cung cấp các dịch vụ xác thực riêng lẻ. Do đó, khi người dùng muốn truy cập mạng được bảo vệ bởi giao thức RADIUS từ xa, họ phải cung cấp thông tin xác thực phù hợp với dữ liệu trong chức năng thư mục liên kết.

Khi người dùng muốn truy cập để cung cấp thông tin đăng nhập đầy đủ, dữ liệu sẽ được truyền từ máy khách đến máy chủ RADIUS thông qua người yêu cầu. Nếu thông tin người dùng khớp với thông tin được lưu trữ trong cơ sở dữ liệu liên kết, một thông báo xác thực sẽ được gửi trở lại máy khách RADIUS để người dùng có thể truy cập để kết nối với mạng. Ngược lại, nếu dữ liệu không khớp, thông báo từ chối sẽ được hiển thị.

2.3.7 - Các tùy chọn bổ sung

Nếu chúng ta có một máy chủ AAA được gọi là RADIUS trên mạng, nó có thể hỗ trợ xác thực 802.1x và cho phép lựa chọn loại EAP.

Nếu có máy chủ RADIUS-AAA không hỗ trợ 802.1x hoặc không hỗ trợ loại EAP, chúng tôi có thể lựa chọn bằng cách cập nhật lên phiên bản phần mềm mới hơn của máy chủ hoặc cài đặt máy chủ mới.

Việc sử dụng RADIUS cho mạng WLAN mang lại sự tiện lợi rất cao, đó là xác thực toàn bộ hệ thống nhiều điểm truy cập, từ đó đưa ra giải pháp thông minh hơn.

2.3.8 - Lựa chọn máy chủ RADIUS như thế nào là hợp lý

Trong phần trước, chúng ta đã thấy rằng máy chủ RADIUS cung cấp xác thực cho kiểm soát truy cập cổng 802.1x. Chúng ta cần xem xét các lựa chọn triển khai cho các giải pháp sử dụng chuẩn 802.1x. Nếu việc triển khai phù hợp với doanh nghiệp thì chi phí quản lý ứng dụng này và chi phí máy chủ RADIUS sẽ là bao nhiêu?

Các doanh nghiệp muốn cải thiện tính bảo mật của hệ thống WLAN của họ, nhưng sử dụng tiêu chuẩn 802.1x - do đó, nên chọn triển khai RADIUS.

2.4 – Kết luận chương 2

Xác thực Wi-Fi bằng máy chủ Radius là một trong những công nghệ tiên tiến nhất hiện nay, là phương pháp bảo mật hiệu quả nhất dựa trên chuẩn 802.1x, được tối ưu hóa cao và được sử dụng rộng rãi ở nước ta cũng như nhiều nước khác trên thế giới. Tuy nhiên, chi phí lựa chọn máy chủ xác thực người dùng cũng cần được cân nhắc kỹ lưỡng để tránh thất thoát, lãng phí cho đơn vị và doanh nghiệp.

Chương III: BẢO MẬT CHO MẠNG WLAN CỦA TRƯỜNG ĐẠI HỌC HÀ NỘI BẰNG CHỨNG THỰC RADIUS SERVER

Chương 3 của luận văn sẽ nghiên cứu đề xuất một giải pháp bảo mật phù hợp cho mạng WLAN tại trường Đại học Hà Nội.

3.1 Khảo sát mạng WLAN Đại Học Hà Nội (sau khi đã xin phép và được sự đồng ý từ lãnh đạo nhà trường)

3.1.1 Mô hình kiến trúc, các chức năng và trang thiết bị mạng hiện có trong hệ thống mạng trường Đại học Hà nội

Trường Đại học Hà Nội có một môi trường sư phạm, môi trường văn hoá lành mạnh, cảnh quan xanh, sạch, đẹp, trường nằm trên trục giao thông chính vào trung tâm thành phố Hà Nội. Nhà trường có quần thể kiến trúc và không gian hiện đại và tiện ích, các khu hành chính, giảng đường, thư viện, ký túc xá... tất cả được bố trí trên diện tích tổng thể khoảng 8 ha.

Hệ thống mạng máy tính tại trường Đại học Hà nội được xây dựng theo mô hình client server, đồng thời với kiến trúc mạng hình sao ở các tầng, ta sẽ đạt được tốc độ nhanh nhất có thể và kiểm soát tốt khi xảy ra lỗi cũng như mở rộng tùy ý muốn. Hiện nay tại trường Đại học Hà nội đang sử dụng 3 máy chủ đặt tại 3 trung tâm là Nhà A, Nhà C, Thư viện của trường và 1100 máy trạm. Tại khu vực mạng nội bộ, ở mỗi tòa nhà trong trường Đại học Hà Nội đều có các Switch được kết nối thẳng tới Switch tổng để đi ra ngoài mạng cũng như đi vào khu vực máy chủ nội bộ, các máy chủ được kết nối với nhau thông qua switch Cisco 48 port đường 1000Base LX và 1000 Base TX, các máy trạm kết nối với máy chủ thông qua các Switch Cisco 24 port.

3.1.2. Ứng dụng mạng máy tính trong trường Đại học Hà nội.

- Tra cứu tài liệu phục vụ công việc học tập của sinh viên và công việc của cán bộ trong toàn trường.

- Sinh viên có thể theo dõi thông tin và tình hình học tập của mình trong thời gian học tại trường thông qua cổng thông tin của nhà trường (http://hanu.edu.vn).

- Việc trao đổi thông tin trong toàn trường dễ dàng hơn, khi có những thông báo, quyết định mới đều được phổ cập cho toàn bộ CB trong toàn trường thông qua trang tác nghiệp của trường (http://tacnghiep.hanu.vn)

3.1.3 Nhu cầu sử dụng mạng WLAN từ thực tiễn

- Mặc dù hệ thống mạng LAN đã tương đối đáp ứng được nhu cầu làm việc, giảng dạy của cán bộ và giảng viên trong toàn trường. Nhưng đây thời kỳ IoT (Internet of Things) nên chỉ dùng mạng LAN là chưa đủ phục vụ cho mọi đối tượng người dùng hiện nay. Nhu cầu sử dụng Internet là rất lớn, ngoài máy tính để bàn cần kết nối Internet còn cả trên Laptop, Ipad, Smart phone.... cần kết nối mạng ở mọi lúc mọi nơi trong khuôn viên nhà Trường để phục vụ học tập, làm việc và giải trí ngày càng nhiều, đòi hỏi Hệ thống phải luôn kết nối được Internet và phải ổn định, an toàn.

- Khi bùng phát dịch COVID - 19 đợt đầu năm lan ra toàn xã hội, yêu cầu giãn cách xã hội để tránh lây nhiễm bệnh, nhu cầu sử dụng mạng WLAN ở cả phòng ban, giảng đường và khu ký túc xá phục vụ cho việc làm việc, giảng dạy và học tập Online của cán bộ, giảng viên và sinh viên ngày càng cao.

- Khả năng cung ứng cao, đáp ứng được một lượng lớn kết nối vào trong hay ra ngoài mạng mà vẫn giữ được sự ổn định, an toàn là một yêu cầu bắt buộc.

- Có khả năng nâng cấp và cải tạo trong tương lai.

3.1.4 Hiện trạng các vấn đề liên quan đến bảo mật trong quá trình sử dụng thiết bị phát WLAN tại trường Đại học Hà Nội

Thực trạng:

- Các đơn vị trong trường (phòng ban, khoa) muốn sử dụng wifi cho mục đích của cán bộ đơn vị mình thì yêu cầu bên TT công nghệ thông tin lắp thêm thiết bị AP phát wifi riêng cho từng phòng ban (hoặc khoa). Các thiết bị này được cài đặt có thể là đặt mật khẩu bảo vệ riêng của đơn vị mình theo kiểu WPA/WPA2 personal (theo khuyến cáo của nhà sản xuất) hoặc thiết bị không đặt mật khẩu bảo vệ để thuận tiện cho việc truy cập vào mạng của người dùng, sau đó thiết bị được cắm vào đường mạng LAN nội bộ của trường.

Nguy cơ: Mất an toàn cho cả người dùng và cơ sở dữ liệu của nhà trường là rất lớn.

- Khi Wi-Fi không dùng mật khẩu để bảo vệ: Thiết bị truyền tải dữ liệu hoàn toàn mở và có thể bị lợi dụng, điểm phát không an toàn và nguy hiểm đối với dữ liệu cá nhân người dùng. Điều này có nghĩa

rằng mọi lưu lượng được chuyển tải từ những mạng này, bao gồm tin nhắn, mật khẩu, văn bản,…đều có thể bị những kẻ xấu lợi dụng.

- Khi đặt chế độ bảo mật là WPA/WPA2 Personal: Chức năng thay đổi khóa TKIP được sử dụng để tạo khóa mã hóa được phát hiện, nếu một tin tặc có thể đoán khóa khởi tạo hoặc một phần của mật khẩu, họ có thể xác định toàn bộ mật khẩu và do đó có thể giải mã dữ liệu.

Nỗ lực để hack những mạng này tùy thuộc vào cài đặt bao gồm độ mạnh của mật khẩu. Ví dụ, nếu mật khẩu yếu hoặc dễ đoán được (ví dụ như mật khẩu thường hay đặt một dãy số liên tiếp hay một dãy số lặp) thì tội phạm sẽ dễ dàng giải mã và bất kì thông tin nào được chuyển tải trên mạng này cũng đều không còn an toàn.

Như vậy biện pháp sử dụng Wifi hiện tại của các đơn vị trong trường (có mật khẩu và không có mật khẩu) đều mất an toàn rất cao: Đối tượng tấn công có thể nghe lén, giải mã giao thức mã hóa và đọc được nội dung của các gói tin mà trước đây được cho là an toàn. Dẫn đến, các thông tin cá nhân, thông tin nhạy cảm như tài khoản ngân hàng, thẻ tín dụng, tài khoản mạng xã hội, thông tin riêng, nội dung chat, thư điện tử, hình ảnh, video…của người dùng có thể bị đánh cắp nếu được truyền qua mạng không dây.

Vì những lý do trên, xây dựng hệ thống bảo mật mạng WLAN trường là hết sức cần thiết để bảo vệ người dùng mạng không dây và cơ sở dữ liệu của nhà trường.

3.2 Đề xuất các giải pháp bảo mật cho mạng WLAN tại trường Đại học Hà Nội

3.2.1 Các giải pháp bảo mật mạng WLAN hiện có tại Hanu

a. Thay đổi tên mạng (SSID):

b. Thay đổi tên người dùng và mật khẩu:

c. Sử dụng mã hóa mạnh để bảo mật wifi:

d. Chọn mật khẩu mạnh:

e. Thay đổi mật khẩu wifi:

f. Vô hiệu hóa mạng khách:

g. Bật tường lửa để bảo mật wifi:

h. Tắt WPS:

i. Quản lý firmware của bộ định tuyến:

k. Tắt quản lý từ xa/ dịch vụ không cần thiết:

Trên đây chính là các cách bảo mật WLAN cho mạng hiện tại của HANU. Trong số các cách này, nên chú ý tới cách mã hóa và đặt mật khẩu mạnh. Bởi đây chính là cách bảo mật mạng không dây đơn giản, an toàn và dễ thực hiện nhất.

3.2.2 Bảo mật mạng WLAN sử dụng chứng thực Radius Server tại Hanu

Xuất phát từ những lợi ích rất hữu ích như tính linh động, thuật tiện trong việc áp dụng mạng WLAN vào các nơi công cộng như công sở, trường học. Đặc biệt là trường Đại học Hà Nội với số lượng cán bộ, giảng viên khoảng 750 người, sinh viên nhà trường có khoảng 10.000 sinh viên các khóa, các sinh viên ở khu vực KTX có nhu cầu sử dụng mạng internet rất lớn. Học viên xin đề xuất áp dụng mô hình triển khai mạng WLAN với hình thức chứng thực RADIUS cho khu hành chính, giảng đường và ký túc xá trường với đối tượng sử dụng là cán bộ, giảng viên, và sinh viên của trường để quản lý tập trung và nâng cao tính báo mật cho người dùng và cơ sở dữ liệu của nhà trường.

Với đối tượng là Giảng viên, viên chức của trường, các dữ liệu truyền trong mạng cần có sự bảo mật trên đường truyền do đó sẽ tổ chức các đối tượng này vào các Group được phân quyền và áp dụng các chính sách thích hợp đáp ứng nhu cầu bảo mật dữ liệu truyền trên mạng cũng như vấn đề phân quyền.

Đối với đối tượng là Sinh viên, nhu cầu truy cập để sử dụng mạng internet là chính nên các đối tượng này sẽ được tổ chức vào các group thích hợp. Sinh viên có nhu cầu sử dụng mạng WLAN sẽ được cấp user và password. Cấp cho các user này khoảng thời gian truy cập cũng như các vấn đề về kiểm soát, thu phí…vv.

3.2.3 Giải pháp mạng

Xây dựng phòng máy chủ tập trung quản lý WLAN tại tầng 3 nhà A sử dụng chứng thực Radius Server để điều khiển và cấp quyền truy cập cho các user kết nối với các AP được lắp tại các khu làm việc, giảng đường và khu ký túc xá sinh viên cũng như khuôn viên nhà trường.

Để việc áp dụng giải pháp sử dụng Radius server được khả thi thì cần tính đến tính hiệu quả kinh tế phù hợp, ngoài các thiết bị ở phòng máy chủ, các switch chia cổng, đường cáp quang đi các tòa nhà,... là cần phải có, để giảm chi phí đầu tư các thiết bị Access Point lắp cho

các phòng ban và giảng đường, thư viện,... học viên đề xuất cách phân bổ lắp thiết bị tại các tòa nhà như sau:

Nhà A là khu hành chính có các phòng ban lắp 3 hoặc 4 chiếc thiết bị phù hợp ngoài hành lang (riêng khu vực phòng máy chủ không lắp thiết bị phát wifi để đảm bảo tính bảo mật cơ sở dữ liệu của nhà trường) phục vụ cho cán bộ sử mạng WLAN (ví dụ có thể dùng TP-Link Archer C50 đáp ứng 20-25 người dùng).

Các tòa nhà giảng đường như nhà B, nhà A1, nhà C, nhà E, D1, D2, D3, thư viện thì trang bị lắp 3 hoặc 4 thiết bị Access Point ở ngoài hành lang các tầng, các thiết bị này có khả năng đáp ứng số lượng lớn người dùng (ví dụ như dùng Wifi Ruckus ZoneFlex AccessPoint 7372 có khả năng đáp ứng được 200 người dùng cùng lúc).

Các khu KTX sinh viên nhà D4, D5, D6, D7, D8, D9, D10: Các nhà này ban quản lý bố trí có 6-8 bạn sinh viên ở 1 phòng, nên sẽ trang bị các thiết bị Access Point rẻ tiền hơn (như TP-Link 840N) vào từng phòng phục vụ đủ nhu cầu số người dùng cho mỗi phòng.

3.2.4 Mô tả hệ thống (thử nghiệm)

Mô tả yêu cầu:

+ 1 Access Point TP-Links (hoặc của các hãng khác có hỗ trợ WPA2-Enterprise).

+ 1 pc làm RADIUS server sử dụng hệ điều hành Windows Server 2012 Data center có RAM tối thiểu là 2GB, tạo user và password cho các client dự định tham gia vào mạng.

+ 1 Laptop có card wireless sử dụng hệ điều hành Windows 7 dùng làm client.

+ Kết nối network giữa access point và Window server 2012 phải thông suốt, không bị chặn bởi firewall.

3.3 – Cài đặt

Server phải được đặt IP và trỏ Prefer DNS về chính nó và đã được nâng cấp Active Director (AD) rồi.

3.3.1. Cài đặt + Cấu hình Active Directory Certificate Services (CA)

3.3.2. Cài đặt NAP và cấu hình NAP(Network Policy and Access Services)

3.3.3 Cấu trên access point và client

3.4 Thử nghiệm và đánh giá kết quả

3.4.1 Thử nghiệm

3.4.2 Đánh giá kết quả:

Khi bảo mật bằng phương pháp Radius server có sự khác biệt đáng kể với bảo mật khi sử dụng phương pháp khác là là ở hình thức có được khóa PMK (Pair-wise Master Key): Như với chế độ bảo mật WPA/WPA2 Personal, khóa PMK sinh ra từ khóa tĩnh được nhập vào thủ công trên AP và các Station. Còn sử dụng WPA/WPA2 Enterprise trong phương pháp Radius server, khóa PMK nhận được từ quá trình xác thực IEEE 802.1x/EAP. Việc cấp phát khóa này là hoàn toàn tự động và tương đối an toàn. Sau khi đã xác thực lẫn nhau rồi, station và máy chủ xác thực Radius xây dựng khóa PMK dựa trên các thông tin đã biết. Khóa này là giống nhau trên cả station và máy chủ xác thực Radius. Máy chủ xác thực Radius sẽ tiến hành sao chép một bản khóa PMK này rồi gửi về cho AP. Lúc này, cả AP và Station đều đã nhận được khóa PMK phù hợp và cho phép kết nối mạng. Bởi vậy, phương pháp Radius server sẽ an toàn hơn và thích hợp với triển khai hệ thống ở qui mô lớn như trường học, công ty.

Các máy client muốn vào được mạng wifi phải tiến hành cài đặt, phải được xác thực dựa vào thông tin cung cấp từ máy chủ Radius server. Điều này dẫn tới việc bảo mật cao hơn và an toàn hơn so với các hình thức bảo mật thông thường. Vì vậy sẽ bảo vệ người dùng tránh mất mát dữ liệu và các nguy cơ tấn công của các hacker xâm nhập.

3.5 Kết luận chương 3

Chương 3 của luận văn đã khảo sát mạng có dây và không dây tại trường Đại học Hà Nội, các vấn đề nảy sinh trong quá trình sử dụng và các yêu cầu bảo mật mạng nhằm đáp ứng nhu cầu đào tạo của nhà trường.

Luận văn cũng đề xuất một giải pháp bảo mật cho mạng WLAN của trường Đại học Hà Nội là phương pháp bảo mật dùng RADIUS SERVER. Các kết quả thử nghiệm cho thấy các giải pháp bảo mật đề xuất có thể triển khai trong thực tế và phù hợp với các yêu cầu đề ra.

KẾT LUẬN

Ngày nay, mạng không dây đã trở nên thiết thực trong cuộc sống, giúp người dùng có thể kết nối mạng ở mọi lúc, mọi nơi trong phạm vi phủ sóng của thiết bị, đáp ứng nhu cầu học tập, làm việc và giải trí của con người.

Đi đôi với tính tiện lợi, độ mất an toàn của mạng không dây cũng xuất hiện đồng thời tạo kẻ hở cho các Hacker xâm nhập lấy cắp thông tin, dữ liệu bằng các phương pháp khác nhau, đòi hỏi cần có sự phát triển các giải pháp bảo mật để cung cấp cho người dùng thông tin hiệu quả và đáng tin cậy.

Các chuẩn mạng và các phương pháp bảo mật mạng không dây được phát triển qua từng thời kỳ đáp ứng nhu cầu phát triển của kỹ thuật cũng như từ thực tế sử dụng. Hầu hết các thế hệ sau đều cải tiến công nghệ và khắc phục những hạn chế của thế hệ trước đó về tốc độ cũng như về bảo mật để nhằm mục đích phục vụ nhu cầu người dùng đạt hiệu quả tốt nhất có thể.

Trong các phương pháp bảo mật mạng không dây thì phương pháp bảo mật dùng máy chủ RADIUS được xem là hiệu quả tốt nhất ở thời điểm hiện nay. RADIUS cho phép xác thực tập trung, ủy quyền và kiểm tra quyền truy cập cho mạng nên mang đến cho người dùng độ an toàn bảo mật rất cao.

Với mục tiêu nghiên cứu giải pháp bảo mật cho mạng WLAN ứng dụng tại Trường Đại học Hà nội, luận văn đã đạt được một số kết quả sau đây:

- Nghiên cứu các yêu cầu bảo mật cho mạng WLAN.
- Nghiên cứu các giải pháp bảo mật cho mạng WLAN.
- Đề xuất các giải pháp bảo mật có thể triển khai cho mạng nội bộ tại Trường Đại học Hà nội: Sử dụng phương pháp RADIUS xác thực cho các user khi kết nối vào mạng WLAN. Luận văn này học viên đã giới thiệu chi tiết cách cài đặt và kết quả chạy thử nghiệm khi sử dụng RADIUS trên nền Windows Server 2012.

Hướng phát triển tiếp theo của luận văn:

- Tìm hiểu các yêu cầu, mô hình khi thiết kế, triển khai và bảo mật hệ thống Server RADIUS trong thực tế.
- Tìm hiểu, xây dựng hệ thống phát hiện xâm nhập cho mạng WLAN và thực hiện tấn công trên hệ thống này.