GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG QUA NGƯỜI TRUNG GIAN VÀO MẠNG CỤC BỘ KHÔNG DÂY

Trần Ngọc Bảo, Nguyễn Công Phú
Trường Đại học Sư phạm Tp,HCM

TÓM TẮT: *Ngày nay, mạng cục bộ không dây ngày càng trở nên phổ biến, người dùng có xu hướng sử dụng mạng không dây, nhất là những người làm kinh doanh, với chiếc máy tính xách tay hoặc các thiết bị hỗ trợ không dây khác như PDA, Mobile phone,..họ có thể ở bất kỳ nơi nào có cung cấp dịch vụ truy cập không dây để truy cập Internet hoặc truy cập vào hệ thống mạng riêng của công ty để trao đổi thông tin giữa các máy tính trong hệ thống mạng nội bộ. Tuy nhiên, bên cạnh những thuận lợi trên, hệ thống mạng không dây cũng chứa đựng rất nhiều rủi ro và nguy cơ tấn công của hacker. Báo cáo nhằm trình bày giải pháp phòng chống tấn công qua trung gian vào mạng không dây. Giải pháp có tên gọi AMIMA – Against Man-In-Middle Attack. Hệ thống AMIMA cung cấp 3 dịch vụ đảm bảo an ninh cơ bản cho mạng không dây bao gồm dịch vụ xác nhận truy cập dựa trên nghi thức xác nhận mở rộng EAP, dịch vụ đảm bảo bí mật và toàn vẹn thông điệp thông qua hai lớp kỹ thuật là WEP (Wired Equivalent Protocol) và IPSec.*

Từ khóa: *An ninh mạng không dây, Mạng riêng ảo, Tấn công qua người trung gian.*

1. GIỚI THIỆU

Từ khoảng đầu năm 2000 nhiều chuyên gia nghiên cứu về an toàn thông tin mạng không dây cho thấy giao thức WEP có nhiều yếu điểm không đảm bảo được tính an toàn của hệ thống trước nguy cơ tấn công của hacker [1], [2], [7], [9], [10], [11], [13], [14] . Ngày 24 tháng 06 năm 2004, Viện Kỹ thuật Điện - Điện tử Hoa Kỳ (IEEE) đã chính thức thông qua chuẩn IEEE 802.11i, đặc tả về công nghệ và giao thức bảo vệ an toàn thông tin trong hệ thống mạng không dây. Chuẩn 802.11i được xây dựng trên cơ sở sử dụng phương pháp mã hóa AES thay thế phương pháp mã hóa RC4 sử dụng trong WEP [3], [4], [5].Theo dự kiến ban đầu thì khoảng cuối năm 2004 trên thị trường sẽ bắt đầu xuất hiện thiết bị WLAN (Wireless Local Area Networks) hỗ trợ chuẩn 802.11i.

Trong bài báo này chúng tôi trình bày một giải pháp phần mềm phòng chống tấn công qua người trung gian nhằm khắc phục một số yếu điểm trong giao thức WEP. Giải pháp có tên gọi là AMIMA - Against Man-In-Middle Attack. Phần còn lại của bài báo được tổ chức như sau: Phần 2 trình bày mô hình hệ thống AMIMA và qui trình hoạt động của hệ thống. Phần 3 trình bày chi tiết giao thức xác nhận và trao đổi khóa. Phần 4 trình bày qui trình mã hóa và đảm bảo tính toán vẹn của thông điệp. Phần 5 là phần kết luận.

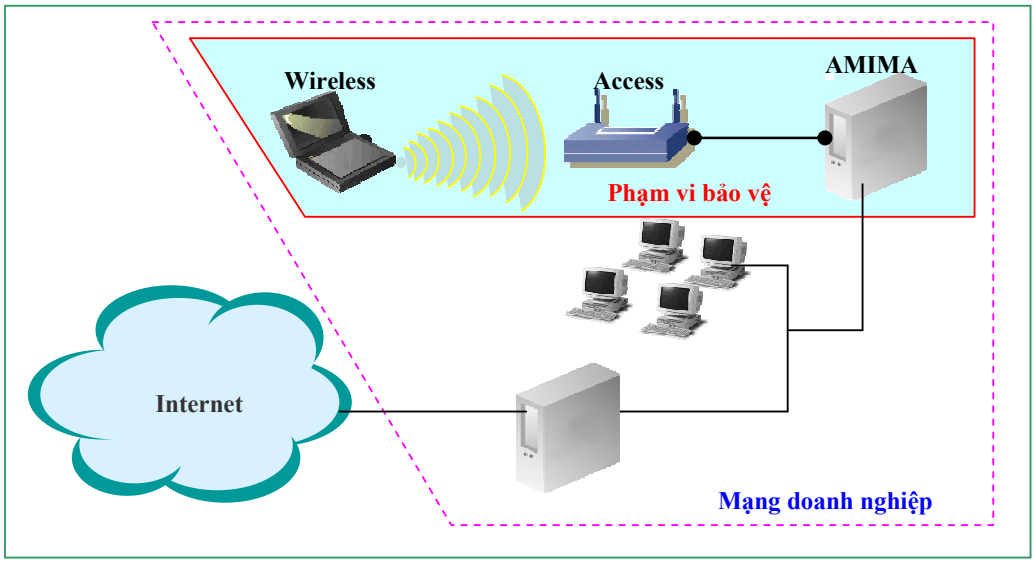
2. MÔ HÌNH HỆ THỐNG VÀ QUI TRÌNH HOẠT ĐỘNG

2.1. Mô hình hệ thống

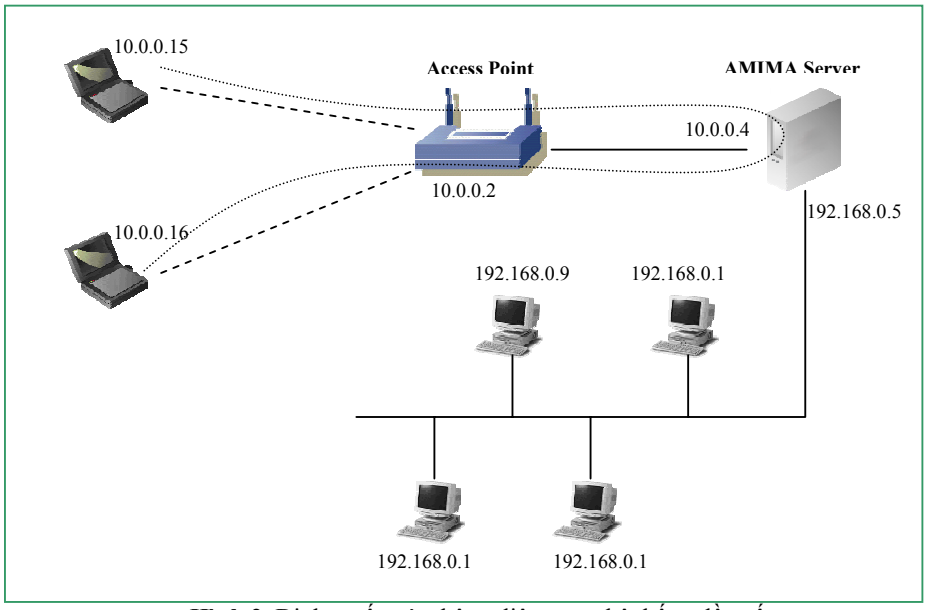
Hệ thống mạng của doanh nghiệp bao gồm các máy tính cá nhân (PC), máy chủ và các thiết bị khác… kết nối với nhau qua hệ thống dây cáp truyền thống và các máy tính (hay thiết bị) không dây kết nối vào hệ thống có dây thông qua Access Point (hình 1).

Hệ thống mạng không dây (Wireless LAN) - WLAN sẽ bao gồm các máy tính không dây kết nối vào hệ thống mạng có dây (hoặc kết nối với nhau) thông qua Access Point và AMIMA (Againts Man-In-Middle Attack) server.

Access Point nhận dữ liệu truyền từ máy tính không dây và chuyển qua AMIMA server để xử lý, đồng thời nó cũng chuyển dữ liệu từ AMIMA server đến các máy tính không dây (hình 2).



Hình 1. Mô hình mạng doanh nghiệp của hệ thống đề xuất



Hình 2. Định tuyến các thông điệp trong hệ thống đề xuất.

AMIMA server cung cấp các dịch vụ cơ bản sau:

- Đóng vai trò như một RADIUS server cung cấp dịch vụ xác nhận quyền truy cập và trao đổi khoá cho các thiết bị không dây dựa trên nền nghi thức EAP [12].

- Đóng vai trò như một VPN Gateway [8] dùng để đảm bảo an toàn cho thông điệp truyền từ thiết bị không dây vào hệ thống mạng có dây của doanh nghiệp.

2.2.Cơ chế bảo vệ mạng WLAN

WLAN được bảo vệ qua 2 lớp: 802.11 và IPSec.

Access Point sẽ được cấu hình cho phép dùng AMIMA server cho quá trình xác nhận truy cập thông qua nền nghi thức EAP và WEP key dùng cho mã hóa dữ liệu của 802.11.

Wireless Client sẽ cài đặt một phần mềm AMIMA Client và cấu hình 2 hệ thống tham số: một cho Access Point (SSID, WEP key, kiểu Authentication…) và một cho AMIMA server (địa chỉ AMIMA server, khóa mã hóa, thuật toán mã hóa…).

AMIMA server cài đặt phần mềm AMIMA server cung cấp dịch vụ Xác nhận truy cập hệ thống và bảo vệ thông điệp truyền thông giữa các Wireless Client với hệ thống mạng có dây.

2.3.Quy trình hoạt động của hệ thống

Đầu tiên, những Wireless Client không hợp lệ (chưa đăng nhập hệ thống) có nhu cầu truy cập vào hệ thống, nó sẽ gởi tín hiệu cần truy cập hệ thống đến Access Point.

Access Point thấy Wireless Client không hợp lệ, sẽ cản không cho Wireless Client truy cập hệ thống và gởi yêu cầu Xác nhận truy cập đến AMIMA server. Lúc này, Wireless Client và AMIMA server sẽ tiến hành quá trình xác nhận lẫn nhau. Và AMIMA server sẽ thông báo kết quả Xác nhận cho Access Point.

Nếu quá trình xác nhận thất bại, Access Point sẽ đóng port (cổng), không cho Wireless Client truy cập hệ thống.

Nếu Xác nhận thành công, Wireless Client và AMIMA server sẽ tiến hành trao đổi khóa dùng cho mã hóa dữ liệu truyền thông. Đến đây, Wireless Client đã có quyền truy cập hệ thống và sẵn sàng cho việc truyền nhận dữ liệu.

Quy trình truyền dữ liệu của Wireless Client như sau:

- Dữ liệu sẽ được đóng gói thông qua các tầng của giao thức TCP/IP.
- Tại tầng IP, các packet sẽ được mã hóa thông qua cơ chế IPSec và chuyển hướng packet đến AMIMA server.
- Packet đã mã hóa sẽ được chuyển xuống lớp 802.11 và tiếp tục được mã hóa thông qua WEP tạo thành các frame. Các frame này sẽ được truyền đến Access Point.
- Access Point nhận các frames và dùng WEP giải mã để lấy được các packet được mã hóa bởi AMIMA client. Access Point sẽ gởi các packet này đến AMIMA server.
- AMIMA server nhận các packet (được mã hóa dùng cơ chế IPSec) do Access Point gởi đến, giải mã và gởi các packet này đến địa chỉ đích thực sự.

Quá trình truyền dữ liệu từ AMIMA server đến Wireless Client cũng được thực hiện tương tự như vậy: AMIMA dùng IPSec mã hóa các packet và gởi đến Access Point, Access Point dùng WEP mã hóa tiếp packet và gởi đến Wireless Client. Wireless Client nhận các data frame, dùng WEP giải mã và dùng IPSec giải mã tiếp để cuối cùng lấy được dữ liệu cần.

3. DỊCH VỤ XÁC NHẬN

Hệ thống xác nhận thông qua một RADIUS server và trao đổi thông điệp xác nhận dựa trên nền EAP (Extensible Authentication Protocol).

RADIUS cung cấp cho mỗi người dùng một account bao gồm ít nhất 2 thông tin (bắt buộc) username và password.

Hệ thống sẽ chuyển password của mỗi user từ dạng chuỗi sang dạng số dùng thuật toán tạo bản tóm tắt cho thông điệp (Message Digest) như MD5 [1] hay các thuật toán SHA [1] và xem giá trị này như là một giá trị bí mật quy ước chung giữa 2 thực thể. Trong luận văn này, chúng tôi sử dụng SHA-256.

Quy trình xác nhận tương tự như quy trình xác nhận của 802.1X nhưng nội dung các bước xác nhận lẫn nhau giữa station và authentication server do chúng tôi đề xuất khác với WPA. Chi tiết như sau:

Bước 1: Username sẽ được chuyển đổi thành bản tóm tắt thông điệp thông qua hàm băm một chiều H (SHA-256). Station gởi thông tin về H(username) đến Authentication Server dưới dạng thông điệp EAPoL-Packet.

Bước 2: Authentication Server gởi cho Station một certificate xác nhận đã nhận ra station với username tương ứng. Cách tạo Certificate như sau:

- Authentication Server nhận được H(username), tìm giá trị password trong database tài khoản của hệ thống tương ứng với H(username) đã cho.
- Authentication tạo một mặt nạ tương ứng với password như sau:
  - Tạo ma trận mặt nạ (2, n) với n là độ dài bit của khóa.
  - Nếu bit đầu tiên của password là 0 thì chọn cột đầu tiên của dòng đầu tiên trong ma trận mặt nạ. Nếu giá trị này là 1 thì chọn cột đầu tiên của dòng thứ hai trong ma trận mặt nạ. Cách tạo ma trận mặt nạ tương tự như vậy cho các bit 2, 3…n.

Khóa	1	0	1	1	0
Hàng 1		x			x
Hàng 2	X		x	X	

  - Tạo dãy số ngẫu nhiên n giá trị sao cho tổng các giá trị của dãy số này bằng 0. Ghi tuần tự các giá trị của dãy số này vào các vị trí được đánh dấu trên mặt nạ (đã được thực hiện ở bước trên).

    Ví dụ dãy: 5, 8, -9, 2, -6. Ta có: 5 + 8 + (-9) + 2 + (-6) = 0

Khóa	1	0	1	1	0
Hàng 1		**8**			**-6**
Hàng 2	**5**		**-9**	**2**	

  - Tạo tiếp một dãy ngẫu nhiên n giá trị sao cho tổng các giá trị của dãy số này khác 0. Ghi tuần tự các giá trị của dãy số vào các vị trí còn lại trên mặt nạ. Dãy này được gọi là dãy **Ks**.

    Ví dụ dãy: 10, -15, -5, 9, -8. Ta có: 10 + (-15) + (-5) + 9 + (-8) ≠ 0

Khóa	1	0	1	1	0
Hàng 1	10	**8**	-5	9	**-6**
Hàng 2	**5**	-15	**-9**	**2**	-8

  - Ma trận được tạo ra ở trên chính là Certificate ở dạng bản rõ.
- Authentication Server sẽ mã hóa Certificate này bằng thuật toán AES [6] với khóa là password: $C_{Certificate}$ = AES(Certificate)[password].
- Authentication Server gởi giá trị $C_{Certificate}$ đến Station.

Lưu ý: ngay cả khi mã hóa bằng AES Certificate mà gởi bản rõ của Certificate thì kẻ nghe lén cũng khó lấy ra được đúng dãy số có tổng bằng 0 tương ứng với password của username. Dãy Certificate này có thể có nhiều dãy số có tổng bằng 0, nhưng nếu là chủ nhân của khóa thì chỉ chọn ra đúng những vị trí tương ứng với password. Vì thế, đối với chủ nhân của khóa, thao tác này là tuyến tính, nhưng với người khác, cần cộng thử m x 2^n lần để có được khóa đúng, với m là số dòng có tổng bằng 0 trong mặt nạ và n là chiều dài khóa.

Bước 3: Station kiểm tra giá trị $C_{Certificate}$ nhận được

- Station dùng password của mình để giải mã $C_{Certificate}$, nhận được giá trị Certificate.
- Station đọc các giá trị ở mặt nạ tương ứng với password (được đánh dấu x như nêu ở bước trên). Cộng các giá trị này lại.
- Nếu tổng này bằng 0, Station sẽ đọc tiếp các vị trí còn lại để lấy dãy Ks. Ngược lại, tiến trình xác nhận thất bại.
- Tiếp đến, Station mã hóa dãy Ks bằng thuật toán AES với khóa là password: C_{Ks} = AES(Ks)[Password]
- Station gởi giá trị C_{Ks} đến Authentication Server.

Bước 4: Authentication Server nhận C_{Ks}, xác nhận C_{Ks} và thành lập khóa mã hóa dữ liệu cho phiên làm việc này.

- Authentication Server giải mã C_{Ks} lấy được Ks'.
- Authentication Server so sánh Ks' với Ks do Authentication Server tạo ở bước 2. Nếu 2 giá trị này bằng nhau, quy trình xác nhận thành công và khóa mã hóa cho phiên làm việc hiện tại là f(Ks) với hàm f là một hàm quy ước trước của hệ thống. Ngược lại, quy trình xác nhận thất bại.
- Authentication Server thông báo kết quả xác nhận cho Access Point. Dựa vào kết quả này, Access Point sẽ quyết định cho phép Station truy cập vào hệ thống hay không.
- Kết thúc quá trình xác nhận lẫn nhau giữa Station và Authentication Server.

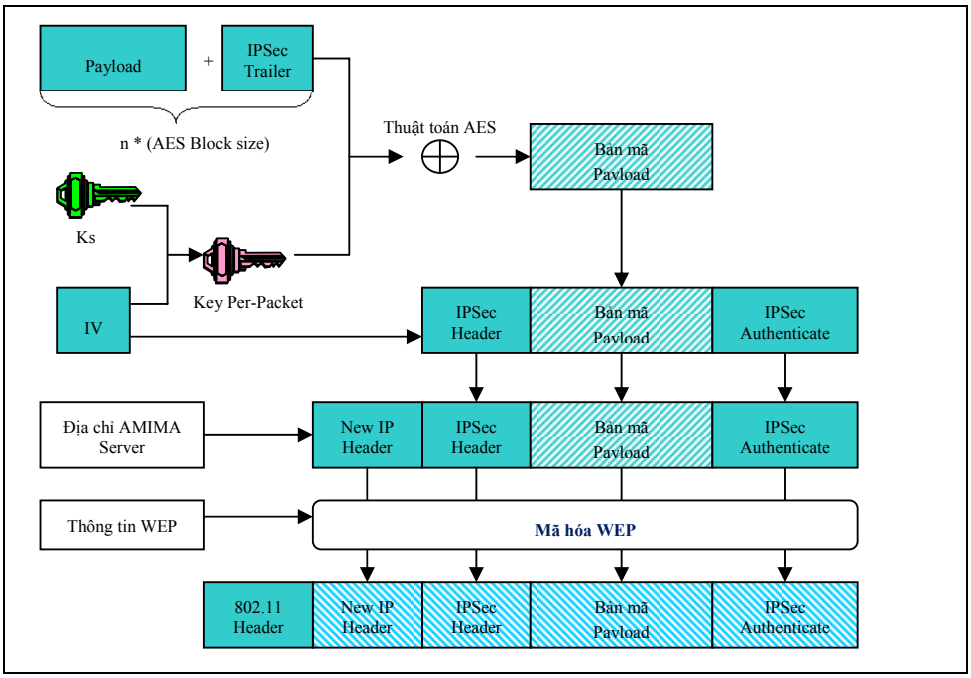
4. MÃ HÓA VÀ ĐẢM BẢO TÍNH TOÀN VẸN CỦA THÔNG ĐIỆP

Quy trình trao đổi và thiết lập khóa, như đã trình bày ở mục 3, đã được thực hiện ngay trong quy trình Xác nhận (authentication). Giá trị khoá bí mật quy ước giữa AS và Station sẽ là giá trị Ks được mô tả trong mục 3.

Chúng tôi đề xuất sẽ dùng kỹ thuật IPSec để mã hóa và truyền thông điệp: thông điệp nguồn sẽ được hệ thống mã hóa ở lớp IP, sau đó chuyển xuống cho lớp 802.11 mã hóa tiếp (dùng WEP hoặc WPA tùy theo sự hỗ trợ của thiết bị). Như vậy, hệ thống được cài đặt như một phần mềm cài vào máy tính mà không cần phải nâng cấp phần cứng.

Đầu vào của quy trình mã hóa này là gói tin ở tầng IP trong mô hình TCP/IP gọi là Payload. Quy trình mã hóa và giải mã thông điệp như sau:

4.1 Mã hóa thông điệp



Hình 3. Mã hóa thông điệp.

Bước 1: chèn IPSec Trailer và tạo khóa mã hóa cho payload

- Payload sẽ được chèn thông tin IPSec Trailer vào cuối sao cho tổng kích thước sau khi thêm sẽ là bội số của kích thước khối theo thuật toán mã hóa được chọn.
- Hệ thống phát sinh số IV (có thể được tạo ngẫu nhiên hoặc tăng tuần tự).
- Khóa mã hóa của IPSec cho payload (Key Per-Packet) sẽ là sự kết hợp giữa IV và khóa của phiên làm việc (Ks).

Bước 2: mã hóa payload (đã chèn IPSec Trailer).

- Hệ thống chia payload thành các khối có kích thước bằng kích thước khối của thuật toán mã hóa quy định (ở đây ta chọn thuật toán mã hóa là AES).
- Dùng thuật toán AES để mã hóa các khối dữ liệu của payload.

Bước 3: chèn IPSec Header và IPSec Authenticate

- Hệ thống chèn IPSec Header vào đầu khối payload đã được mã hóa.
- Dùng thuật toán băm HMAC để băm thông điệp trên (Payload đã chèn IPSec Header, IPSec Trailer và chưa được mã hóa) thành giá trị MAC dùng để kiểm tra tính toàn vẹn của payload.
- Chèn giá trị MAC vào IPSec Authenticate và nối vào cuối payload.
- Đến bước này, payload đã được đóng gói xong. Xem như payload đã được đảm bảo tính bí mật và toàn vẹn dữ liệu.

Bước 4: chèn IP Header mới

- Bước này sẽ là bước định tuyến lại payload. Hệ thống sẽ thêm một IP Header mới vào đầu packet chỉ ra Destination IP mới chính là địa chỉ của AMIMA server.
- Bước này xem như ta đã tạo được 1 gói IP mới cho payload.

Bước 5: đưa packet xuống tầng Physical (802.11) và giao cho lớp 802.11 mã hóa tiếp tạo thành các frames dữ liệu.

Bước 6: các frame dữ liệu sẽ được truyền qua sóng Radio đến Access Point. Kết thúc quá trình mã hóa và truyền dữ liệu

4.2 Giải mã thông điệp

Việc giải mã sẽ bao gồm 2 phần, một phần được xử lý ở Access Point và một phần được xử lý ở AMIMA server.

Bước 1: Access Point nhận được các frame và giải mã các frame này thành packet đã được IPSec đóng gói.

Bước 2: Access Point sẽ gởi packet này đến AMIMA server.

Bước 3: giải mã packet để lấy nội dung payload

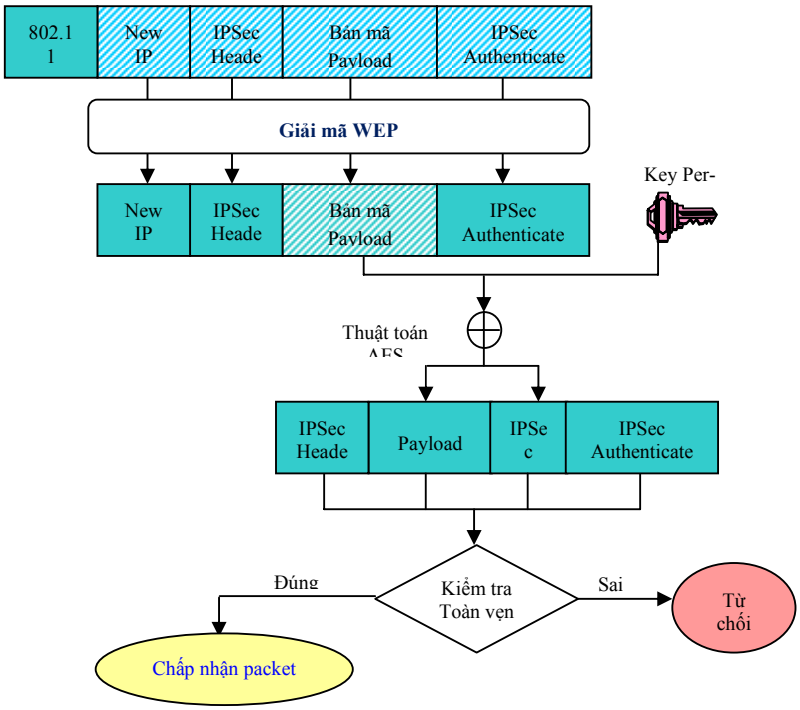
- Hệ thống sẽ lấy giá trị IV từ IPSec Header.
- Kết hợp IV với khóa của phiên làm việc (Ks) để tạo thành khóa giải mã packet (Key Per-Packet).
- Dùng thuật toán AES để giải mã packet và lấy được nội dung payload cùng với IPSec Trailer.

Bước 4: kiểm tra tính hợp lệ của packet, xác nhận packet không bị thay đổi trên đường truyền

- AMIMA server nhận packet, sẽ dùng hàm băm để băm IPSec Header và Payload đã giải mã thành một giá trị MAC1.
- AMIMA server sẽ so sánh giá trị MAC1 này với giá trị MAC trong IPSec Authenticate. Nếu 2 giá trị này trùng khớp, xem như packet là hợp lệ. Ngược lại, nó sẽ từ chối packet.

Bước 5: chuyển payload đến máy đích thực sự

- Payload này chính là gói tin IP gốc của thông điệp.
- AMIMA sẽ kiểm tra xem địa chỉ đích của payload thuộc vùng bên trong hay ngoài hệ thống (bên WLAN hay hệ thống bên trong doanh nghiệp). Nếu địa chỉ đích nằm bên WLAN thì nó sẽ dùng IPSec để đóng gói packet lại (giống như quy trình đóng gói packet ở mục 4.1) và chuyển sang mạng WLAN (đến Access Point).
- Nếu địa chỉ đích của payload nằm bên hệ thống mạng doanh nghiệp, nó sẽ chuyển trực tiếp payload này xuống tầng Physical để truyền payload đến máy tính bên trong doanh nghiệp (hoặc ngoài Internet theo đường mạng có dây của doanh nghiệp).
- Kết thúc quá trình giải mã lấy nội dung payload.



Hình 4. Giải mã thông điệp.

5. KẾT LUẬN

Phương pháp tấn công qua người trung gian vào mạng không dây là một phương pháp tấn công vào điểm yếu của WEP, phương pháp tấn công này cho phép hacker có thể hiểu được nội dung thông điệp truyền trên mạng không dây và họ cũng có thể giả mạo thay đổi nội dung thông điệp đó trước khi truyền đến người nhận thực sự. Nhóm tác giả đã tập trung nghiên cứu về các điểm yếu của WEP và đề xuất hệ thống cho phép bảo vệ tính bí mật của thông điệp qua các hình thức tấn công (kể cả hình thức tấn công qua người trung gian) cho các thiết bị phổ biến mà WEP là công cụ chính dùng để bảo vệ tính bí mật của thông điệp.

Hệ thống đề xuất, AMIMA, dựa trên nền phần cứng có sẵn, tăng cường thêm khả năng xác nhận truy cập và bảo vệ thông điệp trên đường truyền thông qua kỹ thuật IPSec. Hệ thống được cài đặt như một phần mềm, do đó, dễ dàng cài đặt cho các thiết bị đang được sử dụng mà không cần phải nâng cấp phần cứng. Hệ thống AMIMA cung cấp 3 dịch vụ đảm bảo an ninh cơ bản cho mạng không dây bao gồm dịch vụ xác nhận truy cập dựa trên nghi thức xác nhận mở rộng EAP, dịch vụ đảm bảo bí mật và toàn vẹn thông điệp thông qua hai lớp kỹ thuật là WEP và IPSec.

AMIMA – A SOFTWARE SOLUTION FOR SECURITY IN WLAN

Tran Ngoc Bao, Nguyen Cong Phu
HCM City University of Pedagogy

ABSTRAC: *Wireless local area networks have become more and more popular. They had been installed by businesses of all types. The IEEE 802.11 standards were developed for WLAN. However, sources have shown that even the new standards are flawed, allowing attackers to perpetrate attacks. Our works focus on man-in-the-middle attacks, a type of attacks that can be used to steal passwords and to disrupt key exchange operations. This paper presents a software solution – called AMIMA (Against Man-in-the-Middle Attacks), to defend against this type of attacks. In this solution, the "delayed password disclosure" technique is used for authentication phase, IPSec and VPN technique will be used for data exchange phase.*

Keywords: *Wireless Network Security, VPN, Man-in-the-middle attack.*

TÀI LIỆU THAM KHẢO

[1]. William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, *Your 802.11 Wireless Network has No Clothes*, Department of Computer Science, University of Maryland, College Park, Maryland 20742 (March 2001).

[2]. Binoy A. George, *Securing IEEE 802.11 Protocol Wireless Networks Using Java Secure Proxy Server*, Master thesis of Science, Department of Computer Sicence, University of Cape Town (February 2004).

[3]. Wi-Fi Alliance, *Wi-Fi Protectd Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*, (April 2004).

[4]. Wi-Fi Alliance, *WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks*, (Oct 2004).

[5]. Wi-Fi Alliance, *Deploying Wi-Fi Protected Access WPA™ and WPA2™ in the Enterprise*, (March 2005).

[6]. FIPS-197, *Specification for the Advanced Encryption Standard*, (Nov 2001)

[7]. Seth Fogie, *Cracking Wi-Fi Protected Access (WPA), Part 2*, (Mar 2005)

[8]. Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W.Richey, Steven R.Sharma, *Guide to IPSec VPN*, Computer Security Division, Information Technology Laboratory, NIST, (January 2005).

[9]. J. Lundberg. *Routing Security in Ad-Hoc Networks*. http://www.tml.hut.fi/~jlu, 2000.

[10]. M. Jakobsson, S. Wetzl and B. Yener. *Stealth Attacks*. http://www.informatics.indiana,edu/markus/stealth-attacks.htm (2005).

[11]. F. Stajano and R. Anderson. *The Resurrrecting Duckling: Security Issues for Ad-Hoc Wireless Networks*. Proceedings of International Workshop on Security Protocols, (1999).

[12]. Jesse Walker, *802.11 Security Series. Part II: The Temporal Key Integrity Protocol (TKIP)*, Network Security Architect, Platform Networking Group, Intel Corporation, (2002).

[13]. C. D. J. Welch, M. S. D.Lathrop. *A Survey of 802.11a Wireless Security Threats and Security Mechanisms*. Information Technology and Operations Center, Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, New York, (2003).

[14]. L. Zhou and Z. J. Haas. *Securing Ad-Hoc Networks*, (1999).