Nhóm 10

Báo cáo đồ án seminar - Mã hoá ứng dụng Wireless and Mobile Security

Version 3.0

GIẢNG VIÊN LÝ THUYẾT: PGS.TS Trần Minh Triết - TS. Trương Toàn Thịnh
GIẢNG VIÊN THỰC HÀNH: ThS. Lương Vĩ Minh

Thành viên trong nhóm

Mã số sinh viên	Họ tên sinh viên
20127261	Nguyễn Khôi Nguyên
20127262	Nguyễn Vũ Nhâm Nguyên
20127547	Phan Thành Lập

Lịch sử thay đổi

Ngày	Phiên bản	Miêu tả	Người thực hiện
20/02/23	1.0	Tham khảo tài liệu và phân chia công việc.	Nguyễn Khôi Nguyên
20/03/23	2.0	Giải thích các thông tin tìm hiểu.	Phan Thành Lập Nguyễn Khôi Nguyên Nguyễn Vũ Nhâm Nguyên
20/04/23	3.0	Hoàn thành cung cấp đầy đủ thông tin đề ra của bài báo cáo.	Phan Thành Lập Nguyễn Khôi Nguyên Nguyễn Vũ Nhâm Nguyên

Mục lục

1. Giới thiệu **5**

2. Sơ lược chủ đề **5**

3. Những thách thức trong giao tiếp không dây **5**

4. IEEE 802.11 Wireless LAN **7**

4.1. Wired Equivalent Privacy (WEP) **8**

4.2 INTRODUCTION TO 802.11i **14**

4.2.1 TKIP **14**

4.2.2 AES-CCMP **17**

Nguồn tham khảo **31**

Bảng kế hoạch đạt được **32**

Bảng kế hoạch sắp tới **33**

1. Giới thiệu

Tài liệu cung cấp kiến thức cơ bản về vấn đề **Wireless and Mobile Security** (sự an toàn bảo mật trên mạng không dây), nó sẽ giúp người đọc hình dung bao quát sự hình thành và phát triển của hệ thống truyền dẫn không dây và tính bảo mật của nó. Hơn thế nữa, tài liệu cũng sẽ giới thiệu những chuẩn bảo mật trên môi trường mạng không dây hiện nay đang được sử dụng. Kiến thức trong bài báo cáo này đã được các thành viên trong nhóm tìm hiểu, thảo luận và đưa ra một kết luận chung về mặt nội dung cho bài báo cáo. Bài báo cáo được cập nhật hàng tuần vì thế nội dung sẽ có một vài thay đổi so với bản trước đó. Tuy nhiên, mục đích cuối cùng của bài báo cáo này vẫn là cung cấp đầy đủ kiến thức về **Wireless and Mobile Security**.

2. Sơ lược chủ đề

Với sự phát triển không ngừng nghỉ của mạng không dây như 3G, 4G hay 5G… sự bảo mật của hệ thông mạng không dây này đóng một vai quan trọng, nó quyết định sự định hình và phát triển của mạng lưới không dây trong tương lai. Bên cạnh những thành tựu và lợi ích của hệ thống mạng không dây mang lại, thì nó cũng tồn tại một vài lỗ hỏng về bảo mật và đây là cơ hội cho những tin tặc tấn công những hệ thống mạng cục bộ và khai thác dữ liệu người dùng, doanh nghiệp hay tổ chức. Để tăng cường tính báo mật cho mạng không dây thì có nhiều cá nhân và tổ chức đã và đang phát triển những hệ thống bảo để đảm bảo sự an toàn thông tin cho người dùng mạng không dây. Và bài báo cáo này chúng tôi sẽ giới thiệu một vài phương pháp bảo mật mạng cục bộ đã được phát triển để giải quyết vấn đề của mạng không dây.

Một số chủ đề tìm hiểu:

- Challenges in Wireless Communications.
- Introduction to IEEE 802.11 Wireless LAN.
- The Insecurity of WEP.
- Introduction to IEEE 802.11i (WPA, WPA2)
- Introduction to WPA3
- More about AES-CCMP.
- Access Control: 802.1X, EAP, RADIUS

3. Những thách thức trong giao tiếp không dây

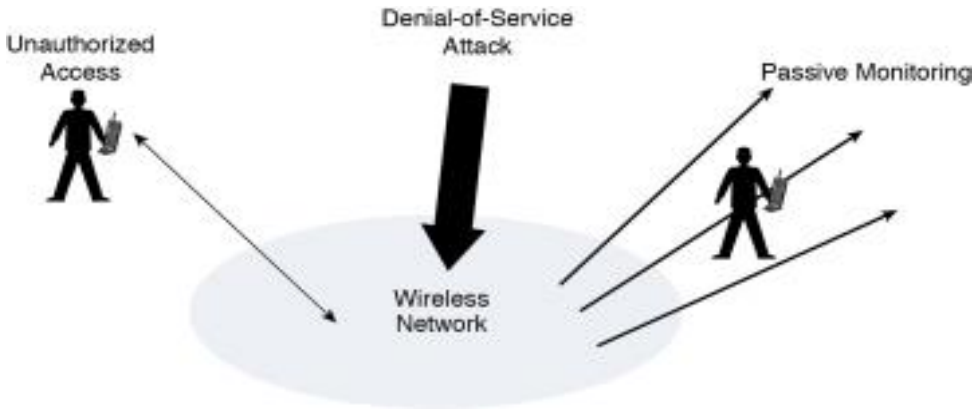
Giao tiếp không dây là phương pháp truyền tải thông tin giữa các thiết bị mà không cần sử dụng dây cáp. Thay vì sử dụng dây để kết nối các thiết bị với nhau, giao tiếp không dây sử dụng sóng điện từ như sóng vô tuyến, Bluetooth, Wi-Fi, NFC, GPS, v.v. để truyền tải thông tin. Nó giải quyết được vấn đề của mạng LAN, WLAN truyền thống.

Giao tiếp không dây đang ngày càng trở nên phổ biến và quan trọng trong cuộc sống hiện đại. Các thiết bị như điện thoại thông minh, máy tính bảng, máy tính xách tay, đồng hồ thông minh, loa thông minh, v.v. đều sử dụng giao tiếp không dây để kết nối với mạng internet, truyền tải dữ liệu và âm thanh.

Tuy nhiên, giao tiếp không dây cũng có những hạn chế nhất định, chẳng hạn như tầm phủ sóng hạn chế và tốc độ truyền tải thấp hơn so với giao tiếp có dây. Ngoài ra mạng không dây, các tín hiệu là công khai và ai cũng có thể bắt được tín hiệu dữ liệu.

Vì thế, bảo mật mạng không dây ra đời để ngăn chặn các người dùng không được cho phép truy cập vào mạng không dây của một cá nhân hay tổ chức. Kẻ xấu có thể lợi dụng việc truy cập trái phép đó để làm điều xấu (đánh cắp thông tin cá nhân; tuyên truyền những thứ cực đoan; v.v). Chúng có thể thông qua đường truyền mạng, tính cơ động, khả năng truy cập hay tài nguyên để tấn công hệ thống mạng. Một số mối hiểm hoạ có thể xảy ra nếu bảo mật không tốt:

- *Malicious Association:* khi một hệ thống mạng của công ty được truy cập bởi thiết bị lạ mặt một cách dễ dàng, từ đó người dùng thiết bị ấy có thể đánh cắp thông tin của công ty, cấy virus để tống tiền, v.v.
- *Ad-hoc network:* vì không có *AP* như một lớp phòng thủ nên các *station* rất dễ bị tấn công nến bảo mật của mỗi chúng không được cài đặt tốt từ đầu.
- *Identity theft (MAC spoofing):* kẻ xấu sẽ thay đổi địa chỉ MAC trên *network interface* (card mạng, v.v) thông qua các *driver*, từ đó có thể truy cập để đánh cắp dữ liệu hay quấy phá hệ thống.
- *Network Injection:* những hệ thống mạng không có các bộ lọc (*non-filtering network)* thường sẽ gây ra những lỗ hỏng lớn khiến người xấu có thể xâm nhập trái phép và gây hại đến hệ thống.

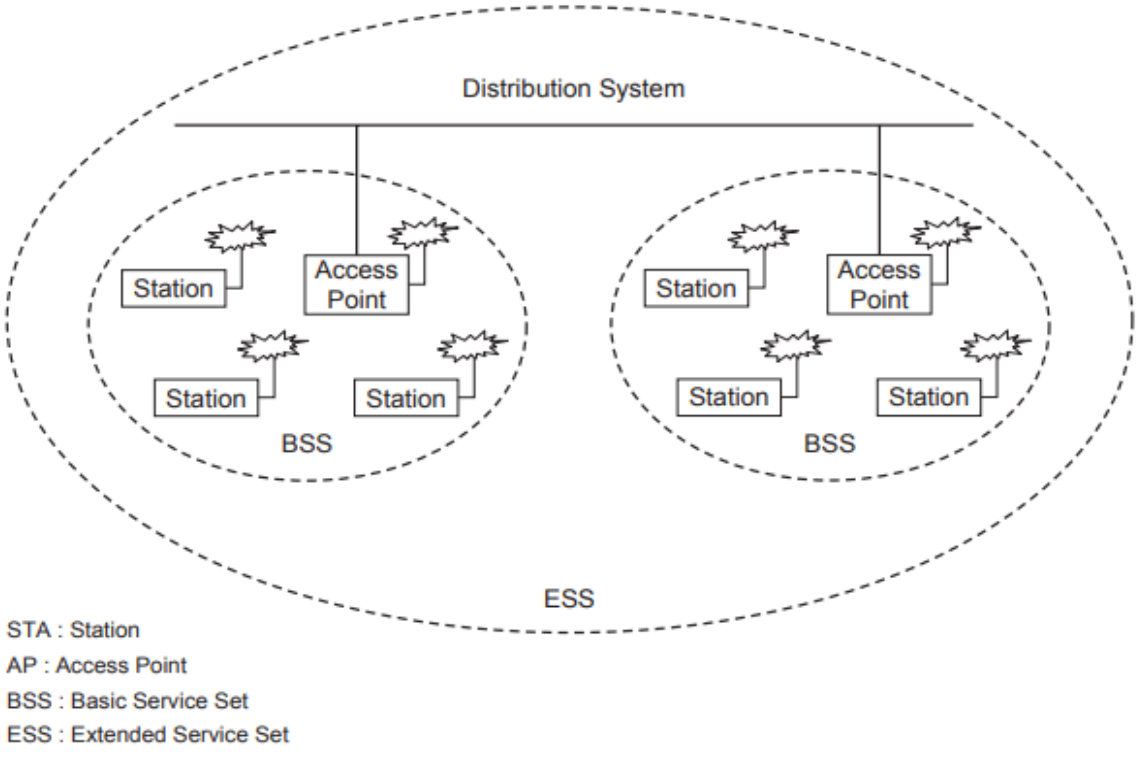


Nguồn: Cisco Press

4. IEEE 802.11 Wireless LAN

IEEE 802.11 Wireless LAN (còn được gọi là WLAN hay Wi-Fi) là một chuẩn giao tiếp không dây được sử dụng để kết nối các thiết bị với mạng internet hoặc với nhau. Chuẩn này đã trở thành một phương tiện truyền tải thông tin quan trọng và phổ biến trong cuộc sống hiện đại và được sử dụng rộng rãi trong các tòa nhà, quán cà phê, sân bay, khách sạn, v.v. Lợi ích lớn nhất từ WLAN chính là nâng cao tính cơ động, không còn bị hạn chế nơi truy cập như mạng có dây. Như mọi chuẩn IEEE 802 khác, 802.11 cũng tập trung vào 2 tầng cuối ISO (PHYS layer và Link layer) và để hiểu rõ hơn về những thứ liên quan đến chủ đề này ta cần hiểu những cụm từ sau đây:

- *Wireless station (station)*: thiết bị sẽ được kết nối với mạng không dây (wireless network), có thể là laptop, smartphone, v.v.
- *Access point (AP hay base station):* thiết bị tạo kết nối giữa *wireless station* và *distribution system* bằng mạng không dây và có dây, có thể là router hoặc modem, v.v.
- *Distribution system (DS):* hệ thống phân phối gói dữ liệu giữa *wireless station* và mạng có dây (*wired network*).
- *BSS:* khi có 2 hay nhiều *wireless station* kết nối với nhau, chúng tạo nên một *Basic Service Set.*
- *IBSS:* là *BSS* đứng một mình, không kết nối với *base station*.
- *ESS:* là tập hợp các *BSS* và *DS.*
- *Portal:* là một "cây cầu" giữa *wireless network* và *wired network.*



Nguồn: Internet

IEEE 802.11 Wireless LAN có 2 loại cấu trúc:

- *Ad-hoc network:* là hệ thống mạng mà các *station* giao tiếp peer-to-peer với nhau.
- *Infrastructure network:* chính là *ESS*

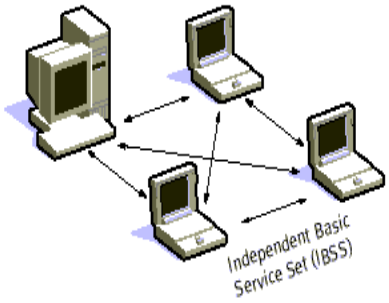


Fig 1: "Adhoc Mode"

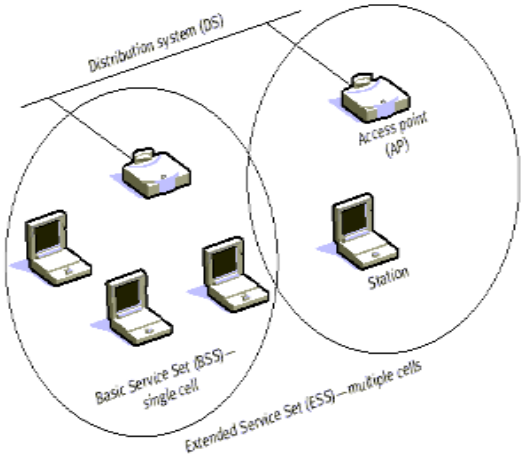


Fig 2: Infrastructure Mode

Nguồn: Tutorial-Reports

Bên cạnh đó, 802.11 có tập hợp các giao thức để dữ liệu được trao đổi trong hệ thống mạng không dây. Đầu tiền, MAC Layer có nhiệm vụ điều khiển quyền truy cập vào *wireless network* và ngăn va chạm (collision) giữa các gói tin. Lớp MAC sử dụng nhiều kỹ thuật để quản lý quyền truy cập vào phương tiện không dây, bao gồm sử dụng multiple access với tránh va chạm (*carrier sense multiple access with collision avoidance - CSMA/CA*). Trong kỹ thuật này, *wireless station* lắng nghe các truyền tải khác trước khi gửi các gói dữ liệu của riêng mình, để tránh va chạm với các trạm khác.

Một giao thức quan trọng khác trong kiến trúc hệ thống IEEE 802.11 Wireless LAN là lớp vật lý (Physical Layer), xác định các đặc tính của tín hiệu không dây và cách nó được truyền tải qua không khí. Lớp vật lý bao gồm các thông số về phương pháp điều chế, băng tần tần số và tốc độ truyền tối đa.

4.1. Wired Equivalent Privacy (WEP)

WEP là một giao thức bảo mật được giới thiệu trong chuẩn 802.11, nó không chỉ dùng để bảo mật end-to-end mà còn bảo vệ dữ liệu truyền qua lại giữa thiết bị client và access point. WEP được sử dụng rộng rãi trong mạng LAN. Giao thức WEP được gắn vào thiết bị phần cứng với các tính năng sau:

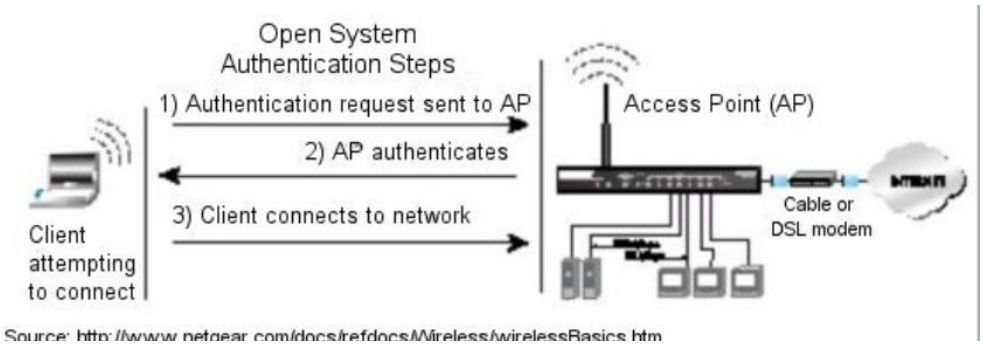
- *Tính bảo mật(confidentiality)*: ngăn chặn tin tặc nghe trộm dữ liệu trong đường mạng.
- *Kiểm soát quyền truy cập (access control)*: ngăn chặn tin tặc sử dụng cơ sở hạ tầng mạng không dây.
- *Toàn vẹn dữ liệu (data integrity)*: ngăn chặn kẻ xấu thay đổi dữ liệu trên đường vận chuyển.

Để tiếp tục tìm hiểu sâu vào thuật toán bên trong chúng ta cần quan tâm đến những thuật ngữ liên quan:

- SSID (The service set ID): đây là một con số định danh một mạng không dây. Các thiết bị kết nối một AP thì cùng một SSID. Nó giúp định danh thiết bị user trên network. Nó là một đoạn text không được mã hóa vì vậy tính bảo mật rất thấp
- MAC address filter: đây là một danh sách các MAC address cho card mạng không dây được cho phép kết nối đến AP. Nó giống như SSID đều là một cleartext nên tính bảo mật thấp.

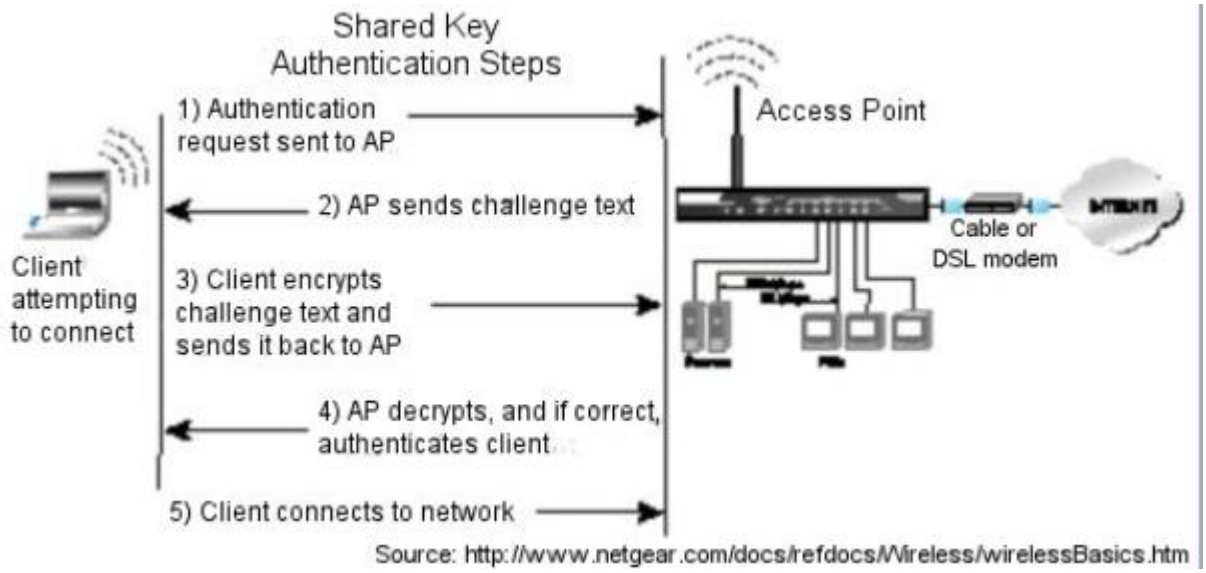
WEP có hai phương pháp xác thực: OSA (Open System authentication) và SKA (Shared Key authentication) được giới thiệu trong 802.11b.

- *Open System authentication: client* không cần phải đưa thông tin đăng nhập cho *AP* trong quá trình xác thực. Nó cho phép các thiết bị kết nối vào chung một network hay một SSID.như một AP. Ví dụ cụ thể là những wifi công cộng. Tuy nhiên hệ thống này vẫn có thể xác thực ở level application.Và đây là chế độ mặc định.



Nguồn: Internet

- *Share key authentication:* ở mode này WEP key được dùng cho chứng thực và mã hóa. quá trình chứng thực được thực hiện bởi "bắt tay bốn bước" (*four-step challenge-response handshake)*
    1. *Client* gửi một lời mời chứng thực (*authentication request)* cho *AP.*
    2. *AP* trả lời lại với một *clear-text challenge* cho *client* để mã hoá.
    3. *Client* sẽ mã hoá *challenge* đó bằng *WEP key* và gửi lại kết quả đó qua *request* khác.
    4. *AP* nhận và giải mã, nếu kết quả trùng với *challenge* thì *AP* sẽ trả kết quả đúng.



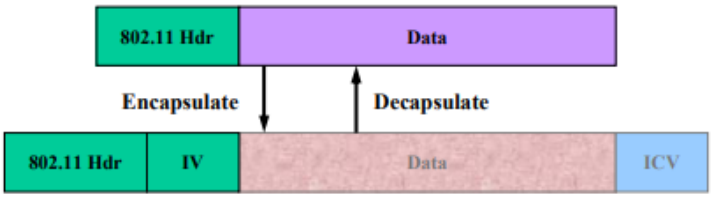
Nguồn: Internet

WEP là giao thức dùng thuật toán stream cipher RC4 để mã hóa và CRC-32 để checksum. Để kết nối được đến AP thì client sẽ Request đến AP để nhận được một challenge 128-bit ngẫu nhiên được sinh bởi AP. Sau đó client thực hiện mã hóa challenge đó bằng khóa xác thực được trao đổi trước đó qua kênh truyền out-of-band và gửi lại cho AP nếu AP giải mã đúng thì client được cho phép kết nối vào network.

Tuy nhiên, một vài vấn đề về xác thực của WEP làm cho giao thức này kém về mặt xác thực:

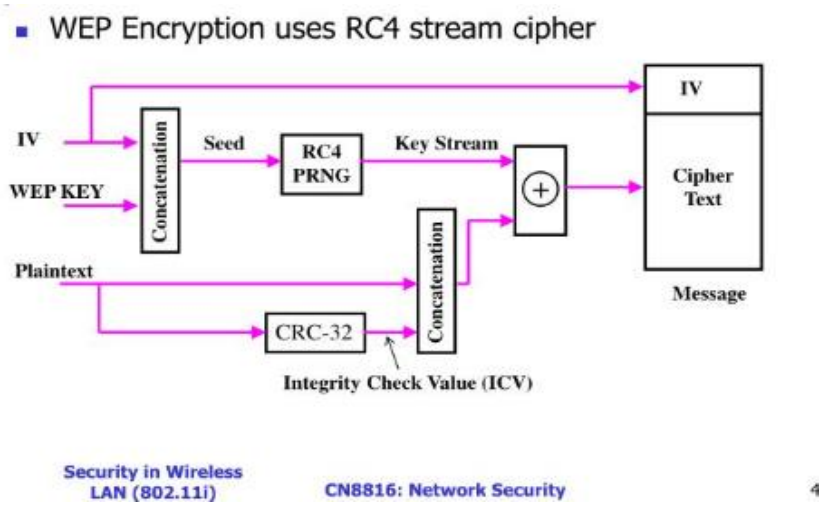
- Không cho phép user xác thực mà xác thực dựa trên thiết bị kết nối, nó dễ dàng bị đánh cắp dữ liệu nếu thiết bị kiểm soát bởi người khác.
- Client dễ dàng bị lừa nếu có người giả mạo AP để tấn công DoS.

WEP dùng chuẩn 64-bit, trong đó 40-bit key được shared giữa client và AP, và nối với 24-bit ngẫu nhiên dùng IV (initialization vector) để tạo khóa RC4 stream cipher. Trong 40-bit thì chúng ta có thể chọn 10 số hexa(hệ 16) để biểu diễn mỗi số 4-bit, tuy nhiên phần lớp thiết bị yêu cầu nhập 5 kí tự ASCII. Ngoài phiên bản 64-bit key thì WEP cũng có phiên bản 128-bit key cũng tương tự như 64-bit cũng dùng 24-bit IV để nói với 26 số hexa hoặc 13 kí tự ASCII. Hay 152-bit, 256-bit. ICV được đóng ở cuối gói tin để kiểm tra tính toàn vẹn dữ liệu. Nó dựa trên thuật toán CRC (Cyclic Redundancy Check) 32-bit block.



Nguồn: Internet

Về thuật toán RC4, đây là một *stream cipher* được sử dụng để sinh ra *keystream* trong WEP. Cách hoạt động của RC4 trong giao thức WEP như sau:



Nguồn: Internet

- Khởi tạo *key-scheduling algorithm (KSA)* nhằm tạo một hoán vị trong mảng *S* gồm 256 byte (tạo S-box). Đầu tiền, mảng *S* sẽ được khởi tạo giá trị từ 0 đến 255. Với mỗi phần tử trong mảng *S*, ta tính *j = (j + S[i] + key[i mod keylength]) mod 256* và thay đổi giá trị phần tử đó với *j* vừa được tính.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

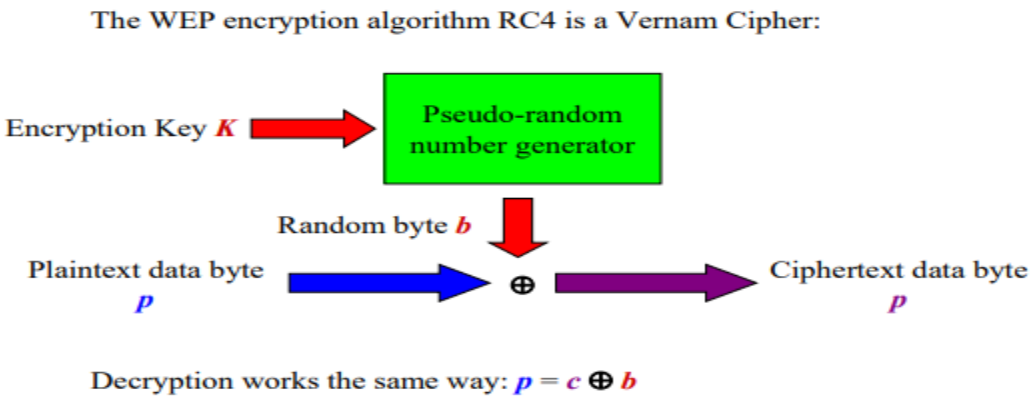
Nguồn: Internet

- Sau khi có S-box, ta khởi tạo *keystream* bằng *pseudorandom generation algorithm (PRGA).* Đầu tiên, ta khởi tạo *i = 0 và j = 0,* sau đó ta tính *i* và *j* rồi đổi vị trí của *S[i]* và *S[j]* và tính modulo của tổng 2 giá trị vừa đổi cho 256 để tìm ra *K.* Với mỗi *K[0], K[1]…* sẽ tạo thành *keystream.*

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

Nguồn: Internet

Tuy nhiên thuật toán RC4 dùng cho WEP vẫn chưa tối ưu và WEP đã bị phá. Đặt điểm của RC4 (là một stream cipher) là khóa không được dùng lại. Trong WEP, *IV* được sử dụng chỉ có độ dài 24-bit nên sẽ có không gian sử dụng nhỏ (2^{24} key stream), dẫn đến việc bị sử dụng lại với tỷ lệ 50% sau 4832 gói tin, tạo cơ hội cho kẻ xấu tấn công dựa vào sự trùng lặp IV. RC4 dùng Vernam Cipher để mã hóa vì vậy IV bị lặp lại dẫn đến hacker có thể phá hệ mã dễ dàng.



Nguồn: Internet

Một ví dụ là sẽ như thế nào nếu chúng ta mã hai data với cùng một khóa.

$$c_1 = p_1 \oplus b \qquad c_2 = p_2 \oplus b$$

Then:

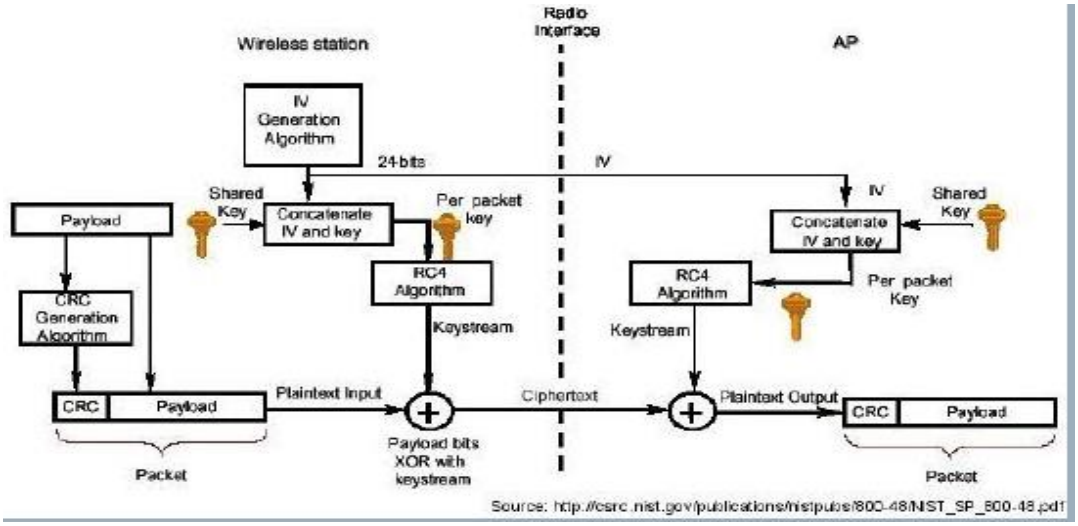
$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

Nguồn: Internet

Nếu hai đoạn plaintext dùng chung khóa b để mã thì dễ dạng chúng ta có thể suy ra plaintext từ cipher text.

Ngoài ra, *Access Control* (chỉ có *Authentication*) không đủ an toàn cho xác thực người dùng. Nó chỉ tin tưởng vào địa chỉa MAC vật lý, tuy nhiên địa chỉ đó dễ dàng được giả mạo. Khóa được chia sẽ cho tất cả client và ít thay đổi thường xuyên, dễ bị replay attack.

Thuật toán sử dụng cho ICV quá đơn giản không đủ phức tạp, nó có thể dễ dàng bị kẻ tấn công thay đổi nội dung của gói tin mà hệ thống không thể phát hiện được.

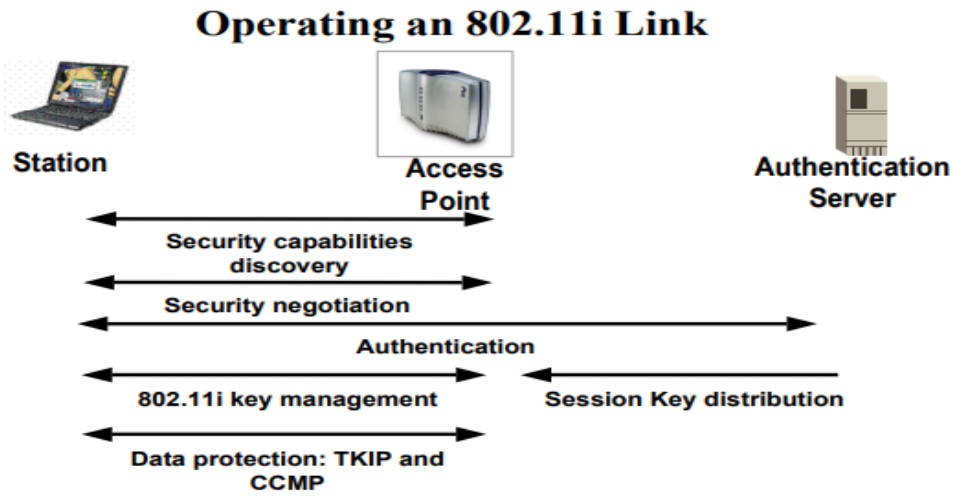


Nguồn: Internet

Kết luận bộ các thuật toán sử dụng cho giao thức WEP không đủ độ tin cậy cho hệ thông mạng truyền dẫn không dây, để đáp ứng sự phát triển nhanh chóng của mạng không dây thì nó đòi hỏi mức độ tinh cậy của các thuật toán phải phức tạp hơn và khó phá giải. Tuy nhiên, việc nghiên cứu một thuật toán mới thì tốn thời gian vì vậy một chuẩn khác được nâng cấp từ WEP thay thế cho đến khi thuật toán phức tạp hơn ra đời là WPA(TKIP), nó là một phần của 802.11i và chúng ta sẽ tiếp tục tìm hieeure nó ở mục tiếp theo.

4.2 INTRODUCTION TO 802.11i

WPA, WPA2, WPA3 là ba chuẩn mà WiFi Alliance phát triển sau năm 2000 để phản ứng lại điểm yếu của WEP trước đó.



Nguồn: Internet

Ở IEEE 802.11i sẽ cung cấp một bộ những tính năng mà cung cấp tính bảo mật cao hơn (RSNA). Nó bao gồm:

- Tăng cường độ phức tạp cho đóng gói dữ liệu CCMP, TKIP (thay thế tạm thời cho WEP)
- Kết nối và quản lý khóa 4-way handshake
- Tăng mức độ an toàn xác thực, sử dụng lại pre-shared key, 802.1X/EAP và RADIUS database
- Quản lý khóa và thay đổi khóa thường xuyên

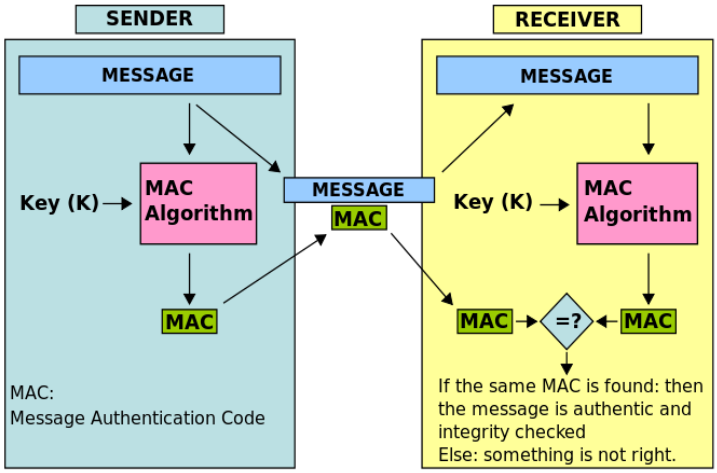
WPA là phiên bản nâng cấp của WEP, nó được coi như là phương án tạm thời cho sự nghiên cứu một hệ thống bảo mật hoàn toàn mới. WPA(TKIP) được đưa vào sử dụng năm 2003 để chờ chuẩn WPA2 phức tạp và bảo mật hơn được phát triển hoàn thiện vào năm 2004. Do là một phiên bản nâng cấp nên WPA dễ dàng được cài đặt trên phần cứng, chúng ta có thể dễ dàng thay đổi WEP bằng WPA thông qua thiết bị phần cứng.

4.2.1 TKIP

TKIP (Temporal Key Integrity Protocol) là một giao thức bảo mật được sử dụng trong chuẩn 802.11, cụ thể nó được thiết kế bởi 802.11i. Nó cải thiện độ tin cậy cho WEP khi cung cấp thêm.

- 64-bit MIC (Message Integrity Code) đây là một phương thức xác thực chống giả mạo. Nó đảm bảo tính toàn vẹn của dữ liệu. Và được thiết lập để thay thế CRC-32 được dùng cho WEP trước đó.
- STA và AP dùng khác khóa cho truyền tin

- Tăng kích thước IV lên 48-bit và trộn với key thay vì chỉ nối đơn giản như ở WEP, nó làm khả năng lặp lại của IV thấp hơn.
- Cung cấp tính xác thực mạnh mẽ hơn dựa trên EAP/802.1X/RADIUS thay thế hai phương pháp OSA và SKA. Và chúng ta sẽ bàn về EAP/802.1X/RADIUS ở chương sau



Nguồn: Internet

IEEE 802.11i sử dụng 2 phương thức xác thực là WPA-Persional(Pre-Shared Key) và WPA-Enterprise. Để thực hiện một kết nối WPA-PSK thì một khóa tĩnh hay Pairwise Master Key phải được chia sẽ trước khi thực hiện giao tiếp giữa AP và STA. Vì WPA-PSK chỉ dùng cho một khu vực nhỏ như văn phòng hay cà phê, vì vậy không cần một server để xác thức. Ngược lại ở WPA-Enterprise sử dụng authentication server để xác thực người dùng trong một network.

TKIP sẽ dùng 128-bit key động cho mỗi lần mã hóa và giải mã một gói tin thay vì 64-bit ở WEP việc tăng kích thước như vậy sẽ hạn chế được sự lặp lại của key và tất nhiên IV sẽ được tăng kích thước. AP và STA sẽ không còn dùng chung một key để mã hóa và xác thực. Ở phiên bản này ICV vẫn còn sử dụng tuy nhiên nó không còn được sử dụng để kiểm tra toàn vẹn dữ liệu. MIC sẽ được TKIP đóng gói vào dữ liệu trước khi chuyển đi để đảm bảo tính toàn vẹn dữ liệu thay vì ICV.

MIC(Micheal) 64-bit key được thiết kế đặc biệt cho TKIP. Nó chỉ thực hiện các phép tính XOR, ADD, SHIFT để tính toán. Nó tính toán dựa trên DA, SA, MSDU và plaintext sau đó dùng khóa xác thực để mã hóa. Tuy nhiên, thuật toán Micheal được thiết kế để phù hợp với TKIP và phần cứng nên nó chỉ có 20-bit an toàn, có nghĩa trong kẻ tấn công chỉ thành công trong một trên một triệu lần nên dễ bị tấn công vét cạn. Vì vậy countermeasure ra đời để chống lại vét cạn.

64-bit Micheal được chia thành hai phần 32-bit (k0, k1), đoạn dữ liệu sẽ được chia thành nhiều phần mỗi phần 32-bit block nếu không đủ 32-bit thì block đó sẽ được đệm thêm vào một giá trị 0x5a và 0x0 sau đó được gắn vào gói tin ở sau MSDUs. Ở chiều nhận thì họ sẽ tính toán MIC và so sánh gói tin được nhận.

Countermeasure sẽ thực hiện kiểm tra CRC, ICV và IV trước khi xác thực MIC. Việc này nhằm giảm tối thiểu khả nâng bị tấn công. Nếu mà phát hiện tấn công hệ thống sẽ loại bỏ seasion key và sinh key sau 1 phút. Hệ thống sẽ unlink kết nối đó 1 phút để giới hạn số lần thử của kẻ tấn công. IV ở phiên bản này được ví như một sequence counter (bộ đếm) việc này sẽ làm cho hệ thống không bị replay attack.

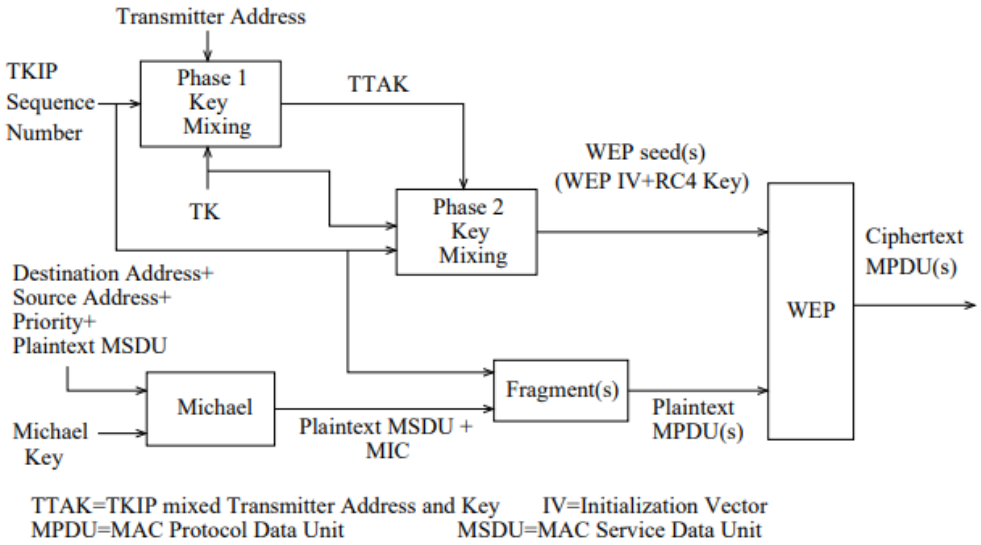
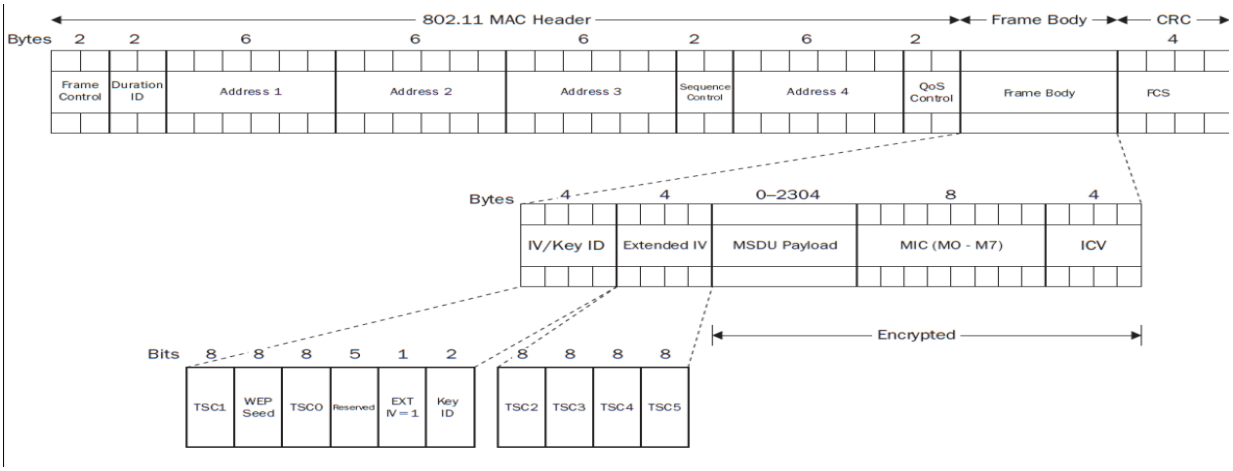


Fig. 1. *TKIP Encryption Diagram*

TKIP sẽ sử dụng 2 phase để mã hóa:

- Ở phase I, 128-bit khóa (session key) sẽ trộn với địa chỉ 48-bit MAC và 32-bit đầu sequence couter (IV) để tạo thành 80-bit key (intermediate key).
- Ở phase II, 16-bit ở sau của IV, 128-bit output của phase I và 128-bit khóa (session key) để tạo ra 128-bit khóa cuối cùng cho mã hóa RC4. Ở chiều nhận có thể tính ngược lại khóa.



Hình trên mô tả gói tin của TKIP, MSDU + MIC +ICV được mã hóa, FCS (frame check sequence) tính trên mỗi header và chứa CRC32.

4.2.2 AES-CCMP

Chuẩn 802.11i còn giới thiệu thêm giao thức AES-CCMP (128-bit AES-counter mode with CBC-MAC), đây là giao thức sử dụng thuật toán mã hóa block cipher AES 128-bit với mode CCM, phức tạp và an toàn hơn được phát triển để thay thế phương phương RC4 stream cipher ở WEP và WPA và đụng áp dụng ở chuẩn WP2.

AES-CCMP là một giải pháp lâu dài dựa trên kỹ thuật mã hóa, ở phiên bản này thuật toán giải quyết được hết tất cả các vấn đề bảo mật ở WEP hay WPA như ngăn chặn được giả mạo gói tin, ngăn được replay tấn công, ...

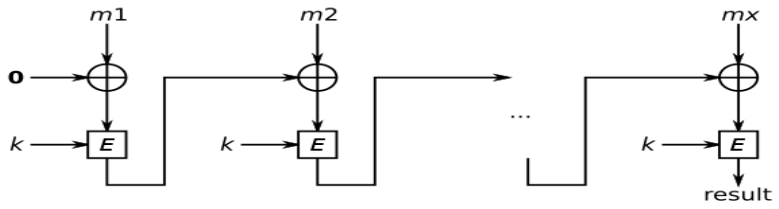
Để hiểu được giao thức bảo mật này hoạt động chúng ta sẽ tìm hiểu ba phần của giao thức:

- Thuật toán mã hóa block cipher AES
- CBC-MAC phương thức mã hóa chuỗi khóa các block cipher
- CTR mode dùng cho thuật toán mã hóa các block cipher

AES là một thuật toán mã hóa block cipher, nó được dùng rộng rãi cho đến hiện bởi tính phức tạp và ổn định của nó. AES thích hợp cả về phần cứng và phần mềm, nó là phương pháp mã hóa block cipher được chọn để mã khóa dữ liệu trong chuẩn WPA2 thay thế cho RC4 stream cipher. So với thuận toán RC4 dùng Vernam cipher thì AES trội hơn về độ phức tạp. AES gồm phải qua nhiều bước để mã hóa một plaintext.

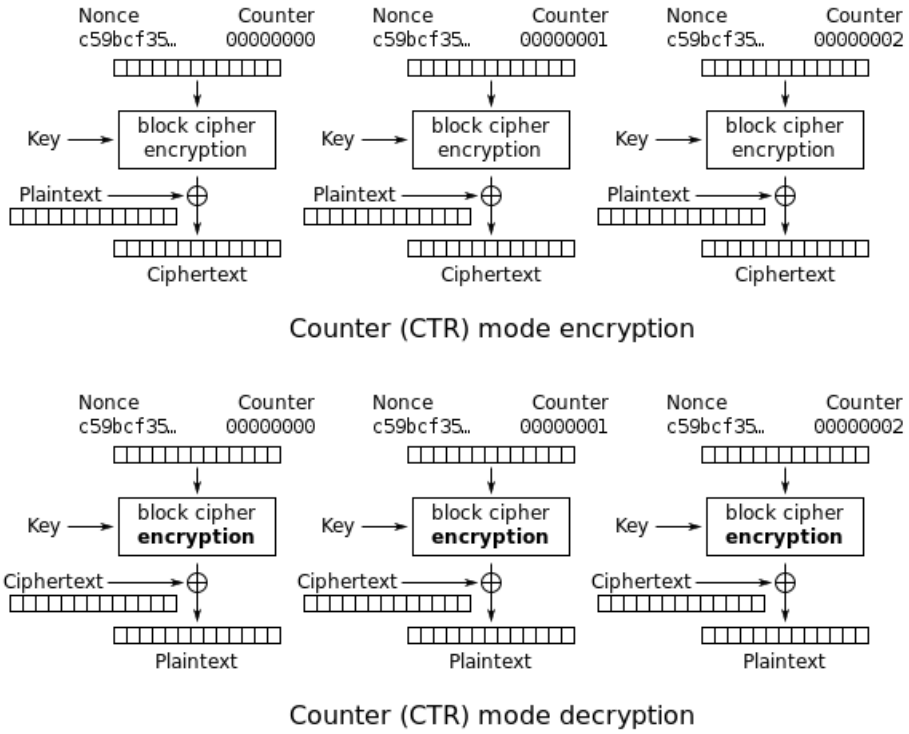
AES sẽ thực hiện mã hóa 128-bit dữ liệu đầu vào với 128-bit key. Ở bước đầu tiên, thuật toán sẽ lấy 128-bit key đầu vào để sinh ra 10 RoundKey, tùy vào 128, 192 hay 256 thì số lượng RoundKey sẽ thay đổi theo, ở bước này được gọi là Key Expansion. Ở bước thứ 2, thuật toán sẽ lấy RoundKey thứ i XOR với block dữ liệu. Tiếp đến bước 3, thuật toán thực hiện Byte Substitution, ở bước này chúng ta sẽ có một định nghĩa mới là S-Box. S-Box là một bảng giá trị mà một byte của block sẽ được thay thế bằng một giá trị mới khi đi qua S-Box. Ở chiều ngược lại ta có một bảng S-Box-inv ở bảng này, giá trị trước đó đã qua S-Box sẽ trở lại giá trị đầu tiên, nó được dùng ở chiều giải mã. Ở bước 4, thuật toán sẽ dịch qua trái mỗi 4-byte được gọi là Shift Rows. Ở bước tiếp 5, tưởng tượng rằng 16-byte sẽ được biểu diễn theo chiều từ trái qua phải từ trên xuống dưới sẽ tạo thành một ma trận 4x4 và thực hiện nhân với một ma trận khả nghịch tạo thành một ma trận mới, bước này gọi là Mix columns, tuy nhiên ở RoundKey cuối cùng chúng ta sẽ không thực hiện Mix columns. Ở bước 6, thuật toán sẽ AddRoundKey tiếp theo, và lặp lại bước một. Ở chiều giải mã thuật toán sẽ thực hiện ngược lại với bước mã.

CBC-MAC (cipher block chaining message authentication code) là một phương thức xây dựng một MAC từ block cipher. MAC sẽ được mã hóa với một block cipher (AES) với CBC mode để tạo thành một chuỗi các khối mà khối phía sau sẽ dựa trên khối phía trước, nó đảm bảo kẻ tấn công sẽ không thể đoán được dữ liệu nếu không có khóa. Thuật toán cũng sử dụng IV để tạo ra sự ngẫu nhiên và phức tạp.



Nguồn: Internet

AES nó chỉ là một block cipher mã hóa trong một block, vì vậy cần một phương thức khác để mã hóa các block lại với nhau đảm bảo tính bảo mật là toàn vẹn của toàn bộ dữ liệu. Ngoài CBC mode mà được giới thiệu ở trên, thì CTR sẽ là mode tiếp theo chúng ta sẽ tìm hiểu.



Nguồn: Internet

Ở mode này, AES-CTR sẽ chuyển một block cipher thành như một stream cipher. Nó đòi hỏi mỗi gói tin mã hóa sinh ra phải duy nhất và được truyền đi cho giải mã. Nó có thể hiểu như một IV và Nonce, tuy nhiên IV này với key kết hợp phải là duy nhất để tránh kẻ tấn công tìm ra sự trùng lặp. Và cách đơn giản để sinh IV là tăng một mỗi gói tin. Nonce không yêu cầu bảo mật tuy nhiên nó phải sinh một cách ngẫu nhiên và duy nhất để đảm bảo không bị tấn công precomputation. Điểm đặt biệt của AES-CTR là nó có thể chạy song song, nó phù hợp máy có thể chạy nhiều tiến trình một lúc. Người nhận sẽ không thể giải mã gói tin nếu gói tin chưa đến, bởi vì người nhận chỉ có thể giải mã khi và chỉ khi gói tin đã đến về nonce nó được gắn vào gói tin. Vì vậy AES-CTR cung cấp tinh bảo mật rất cao nếu dùng đúng cách, ngược lại nó sẽ là thảm họa nếu IV bị trùng, thì lập tức thông tin của plaintext bị lộ. Vì vậy AES-CTR không nên được sử dụng với khóa tĩnh, nó nên được trao đổi khóa giữa hai bên liên tục. Một điểm yếu dễ bị khai thác đó là, kẻ tấn công có thể gửi những nội dung giả mạo. Vì vậy việc sử dụng AES-CTR kết hợp với một thuật toán xác thực là cần thiết ví dụ: HMAC-SHA-1-96.

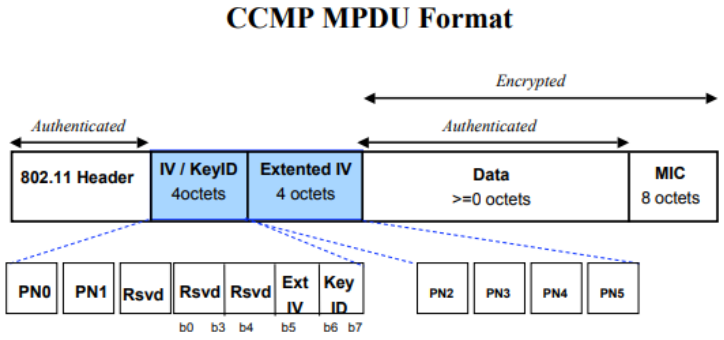
AES-CTR sẽ thực hiện mã hóa bằng cách XOR 128-bit của block phaintext với 128-bit CTR bao gồm: NONCE 32-bit đầu, 64-bit tiếp theo là IV và 32-bit cuối cùng sẽ được bật hết lên 1. Sau mỗi block thì 128-bit này sẽ cộng 1. Ở khối cuối cùng, hàm TRUNC() sẽ làm cho khối luôn là 128-bit.

```
PT = PT[1] PT[2] ... PT[n]

CTRBLK := NONCE || IV || ONE
FOR i := 1 to n-1 DO
  CT[i] := PT[i] XOR AES(CTRBLK)
  CTRBLK := CTRBLK + 1
END
CT[n] := PT[n] XOR TRUNC(AES(CTRBLK))
```

Nguồn: Internet

Đặt biệt ở AES-CTR, chúng ta không cần padding độ dài block vì 128-bit được sinh từ NONCE, IV và ONE luôn là 128. Và có nghĩa giới hạn chỉ là 2^31-1 blocks=4,294,967,295 blocks.



Nguồn: Internet

Tổng quát thì WPA2 được cài đặt giao thức CCMP, sử dụng CBC-MAC để tính toán MIC trên header gồm chiều dài và dữ liệu. CRT được sử dụng để mã hóa dữ liệu và MIC.

Mặc dù TKIP và CCMP đều được giới thiệu trong 802.11i như những giao thức bảo mật mạnh mẽ hơn thay cho WEP trong bảo mật không dây, tuy nhiên CCMP trội hơn nhiều so với TKIP về mặt an toàn.

Data Protection Protocol Comparison

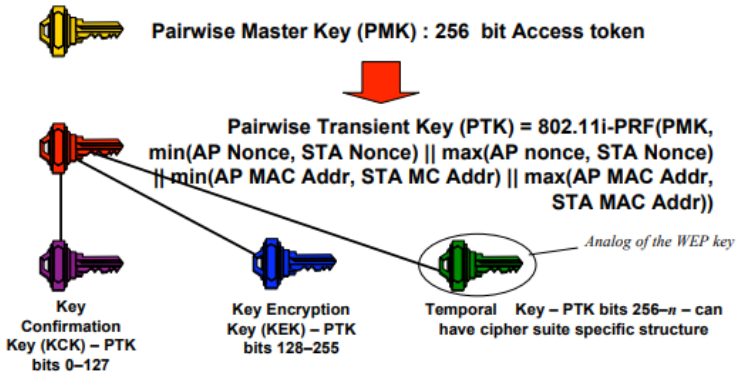
	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits encryption, 64 bit auth	128 bits
Key Life	24-bit IV, wrap	48-bit IV 48-bit IV	
Packet Key	Concat.	Mixing Fnc	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt	None	802.11i 4-Way Handshake	802.11i 4-Way Handshake

Nguồn: Internet

Trước khi bắt đầu tìm hiểu các 4-Way handshake vận hành, chúng ta sẽ tìm hiểu một vài khái niệm.

- Key Managements: đảm bảo cho việc khóa được làm mới theo một chu kỳ, quản lý được trạng thái của peer kết nối tới AP, tránh được tấn công Downgrade, đảm bảo kết nối là duy nhất.
- Pairwise Transient Key: đây là một khóa được kế thừa từ những khóa ở phiên bản trước đó. Nó là sự kết hợp của Temporal key, Key Encrypt Key, và Key Confirmation Key.

802.11i Pairwise Key Hierarchy



Nguồn: Internet

802.11i-PRF dùng hàm HMAC-SHA1 để băm khóa.

802.11i-PRF(*K*, *A*, *B*, *Len*)
R ← ""
for *i* ← 0 **to** ((*Len*+159)/160) – 1) **do**
R ← *R* || HMAC-SHA1(*K*, *A* || *B* || *i*)
return Truncate-to-len(*R*, *Len*)

Ví dụ ở AES-CCMP

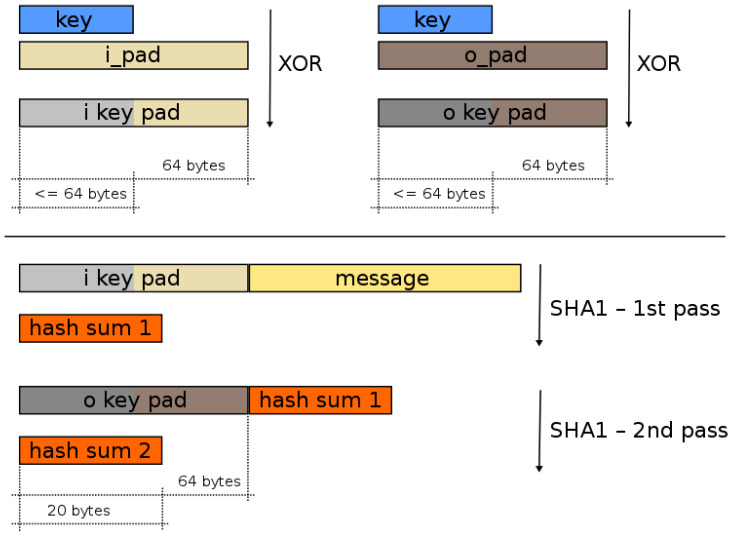
Example for AES-CCMP:
PTK ← 802.11i-PRF(PMK, "Pairwise key expansion", min(AP-Addr, STA-Addr) || max(AP-Addr, STA-Addr) || min(ANonce, SNonce) || max(ANonce, SNonce), 384)

HMAC tương tự như MAC là hàm dùng để xác thực tính toàn vẹn của dữ liệu. HMAC kèm theo hàm băm (hash) và một khóa bí mật. Như vậy HMAC đòi hỏi quá trình trao đổi khóa phải thật phức tạp để tạo kết nối.

$$\mathrm{HMAC}(K, m) = \mathrm{H}\left(\left(K' \oplus opad\right) \parallel \mathrm{H}\left(\left(K' \oplus ipad\right) \parallel m\right)\right)$$

$$K' = \begin{cases} \mathrm{H}(K) & \text{if } K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases}$$

HMAC sử dụng hai lần hash, đầu hiên K được truyền vào sẽ tạo ra hai khóa con gọi là inner và outer khóa. Ở hash đầu tiên, khóa inner được dùng để hash với m (message). Tiếp theo, lần hash thứ hai sẽ dùng khóa outer và giá trị được hash trước đó để hash lần hai. HMAC đảm bảo luôn sinh ra độ dài khóa cố định.



Nguồn: Internet

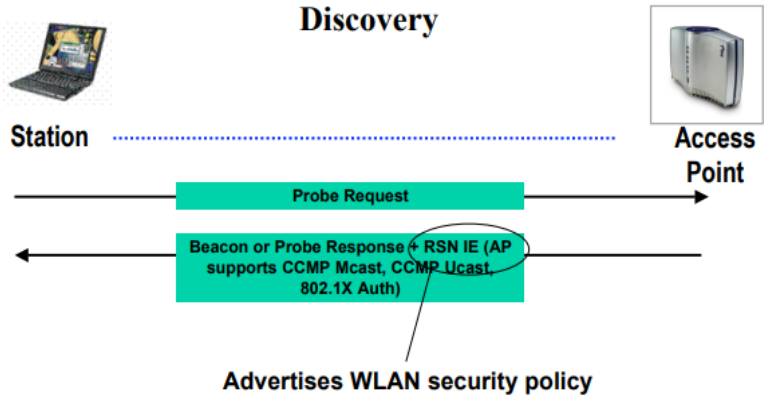
Để tạo một kết nối trên mạng không dây giữa AP và STA thì sẽ có hai bước.

- Discovery (khám phá): tìm chính sách bảo mật của WLANs.
- Negotiation (dàn xếp): cho phép để sử dụng kết nối.

Mục đích của việc có hai giai đoạn là:

1. Tạo ra khả năng tương tác giữa các thiết bị đã được triển khai và chưa triển khai trên 802.11i
2. Tối hiểu chi phí mới trên Beacons (thiết bị vô tuyến)
3. Tạo cơ chế mở rộng trên 802.11i để cho phép AKMs, Ciphersuites (một bộ các thuật toán và giao thức để bảo mật kết nối) không có sẵn trên 802.11i

Discovery cho phép STA và AP khởi tạo kết nối với nhau bằng cách STA request lên AP và AP trả về response. Ở gói response chứa gói RSN IE, đây là gói được AP dùng để quảng bá chính sách bảo mật.



RSN Information Element

Element ID	Length	Version
Group Key Ciphersuite Selector		
Pairwise Ciphersuite Count		Pairwise Ciphersuite List
Pairwise Ciphersuite List		AKM Count
AKM List		
Capabilities		PMK ID Count
PMK ID List		

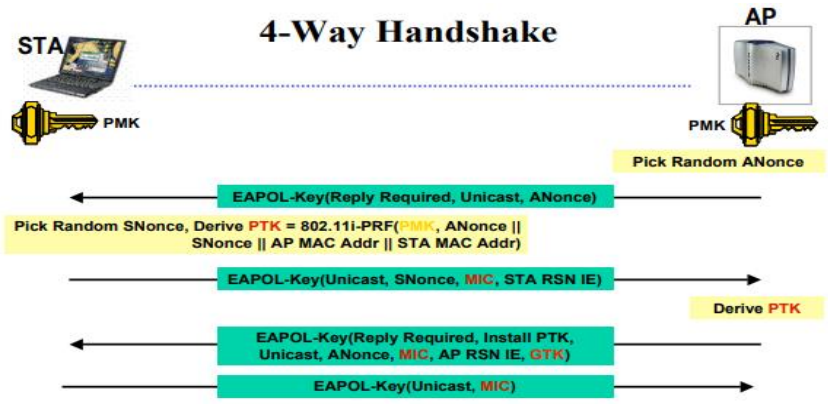
Nguồn: Internet

Dưới đây là bảng định nghĩa các AKMs, Ciphersuites

Defined Ciphersuites	Defined AKMs
• 00-0F-AC:1 WEP-40 • 00-0F-AC:2 TKIP • 00-0F-AC:4 AES-CCMP (default) • 00-0F-AC:5 WEP-104 • Vendor OUI:Any Vendor specific • Other Reserved	• 00-0F-AC:1 802.1X Authentication + 4-Way Handshake • 00-0F-AC:2 PSK + 4-Way Handshake • Vendor OUI:Any Vendor specific • Other Reserved

Nguồn: Internet

Khi STA chọn được Ciphersuites và AKMs phù hợp thì nó tiến hành gửi về AP gói tin kèm RSN IE để thông báo chọn giao thức phù hợp, và khi thành công AP sẽ gửi lại response cho STA. Ở những thiết bị WEP-only thì STAs sẽ không nhận biết được gói RSN IE.



Nguồn: Internet

EAPOL (extensible authentication protocol over lan) được giới thiệu ở 802.1X là một giao thức gói tin cho STA và AP trao đổi gói tin với nhau. Chúng ta sẽ tìm hiểu sâu về EAP ở sau.

EAPOL Key Message

Descriptor Type – 1 octet	
Key Information – 2 octets	Key Length – 2 octets
Replay Counter – 8 octets	
Nonce – 32 octets	
IV – 16 octets	
RSC – 8 octets	
Key ID – 8 octets	
MIC – 16 octets	
Data Length – 2 octets	Data – n octets

Nguồn: Internet

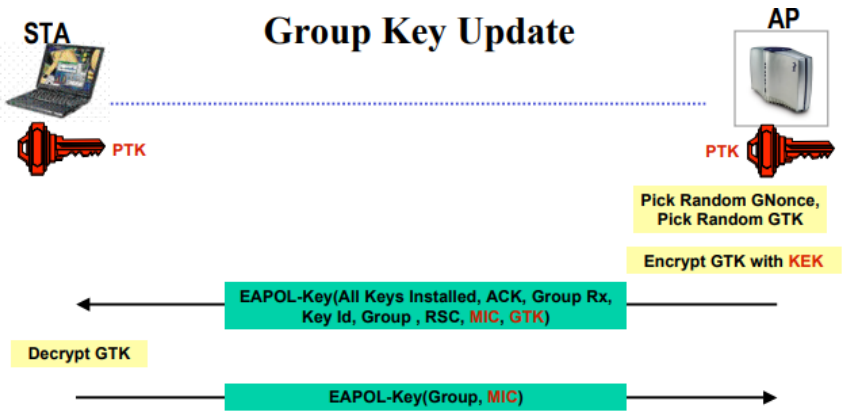
Đầu tiên AP sẽ gửi EAPQL-key cho STA để trả lời yêu cầu từ STA trước đó với một ANonce là một dữ liệu được sinh ngẫu nhiên từ AP.

Tiếp theo STA cũng sẽ chọn một SNonce ngẫu nhiên kèm theo MIC và STA RSN IE và gửi về AP. Sau khi có đủ thông tin để tạo khóa, AP sẽ sinh ra nhóm khóa từ ANonce và SNonce (256-bit ngẫu nhiên) trao đổi giữa STA và AP trước đó. Sau đó AP sẽ gửi về cho STA thiết lập kết nối kèm theo nhóm khóa (GTK). Sau khi STA cài đặt xong thì sẽ báo lại cho AP. Trong quá trình bắt tay của STA và AP thì MIC luôn được gửi kèm để kiểm tra tính xác thực của gói tin.

GTK cần được cập nhật khi thiết bị ngắt kết nối, như vậy sẽ tránh được sẽ ngăn chặn được thiết bị nhận gói tin không mong muốn từ AP.

IEEE 802.11i giới thiệt two-way handshake:

1. AP gửi GTK mới đến STA, GTK được mã hóa với KEK (key encrypt key) được đăng kí đến STA đó để tránh giả mạo MIC.
2. Sau thi nhận được STA gửi xác nhận với AP.



Nguồn: Internet

IEEE 802.11i giới thiệu hai phương thức xác thực là WPA-Personal và WPA-Enterprise. Ở trên chúng ta đã đi qua phương thức xác thực Personal với 4-way handshake, tuy nhiên ở mực độ doanh nghiệp thì tính bảo mật phải được đảm bảo tập trung vì vậy ở WPA-Enterprise server authentication được sử dụng để xác thực.

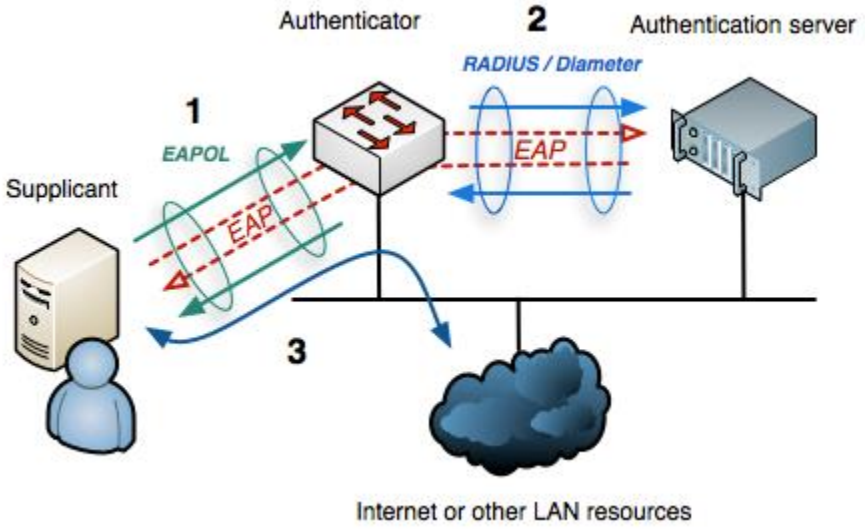
Tuy nhiên ở 802.11i không hổ trợ tính xác thực tập trung, phương thức EAP và RADIUS database ở 802.1X được chọn như một phương thức xác thực cho 802.11.

Chúng ta sẽ đi nhìn qua 802.1X để hiểu rõ hơn phương thức xác thực sắp được giới thiệu tiếp theo.

802.1X là một IEEE Standard cho PNAC (port-based network access control), nó cung cấp cơ chế xác thực đến mạng LAN, WLAN. 802.1X sử dụng đóng gói EAP trên mạng có dây và EAPOL trên mạng không dây và PORT ảo (logical PORT) thay vì PORT vật lý.

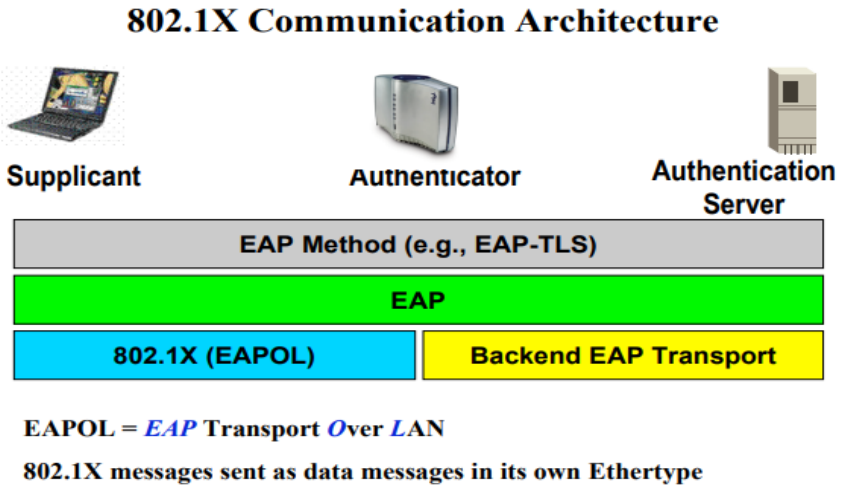
802.1X gồm một vài đinh nghĩa thành phần:

- Port entity: đây là một firewall thô, nó có thể đóng vai trò như supplicant hoặc authenticator, nó quản lý luồng của dữ liệu. Bao gồm Controlled Port và Uncontrol Port.
- Controlled Port: dùng cho data thông thường
- Uncontrolled Port: dùng cho 802.1X truyền nhận frames
- Supplicant: người dùng (STA ở 802.11i)
- Authenticator: switch, AP, NAS(AP ở 802.11i)
- Authentication server (AS): máy chủ xác thực (tập trung)

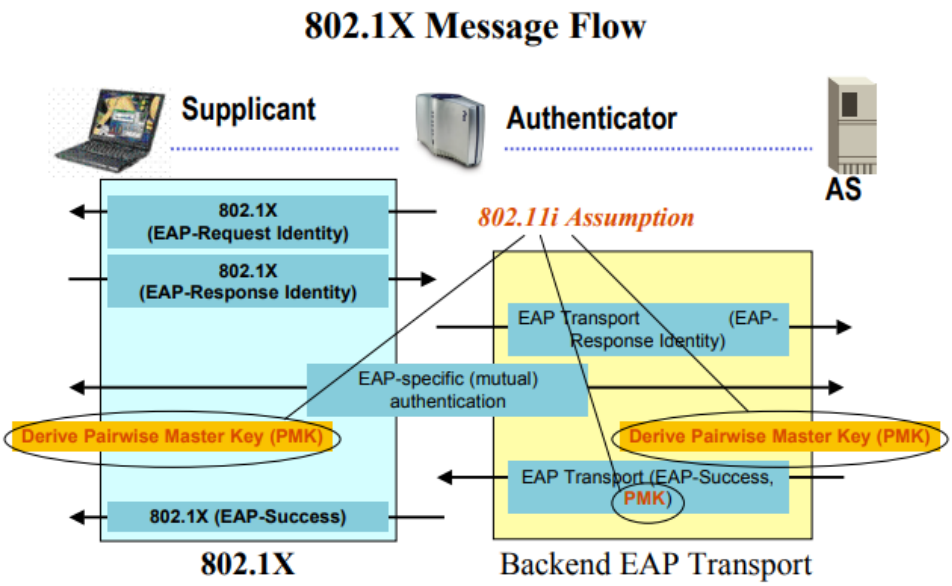


Nguồn: Internet

Ở kết nối giữa người dùng và NAS thì sẽ dùng EAPOL và ở \AS và server dùng RADIUS. Authenticator bảo vệ server khỏi những supplicant không được thực. Supplicant phải được xác thực và cho phép của server để truy cập tài nguyên trên network.



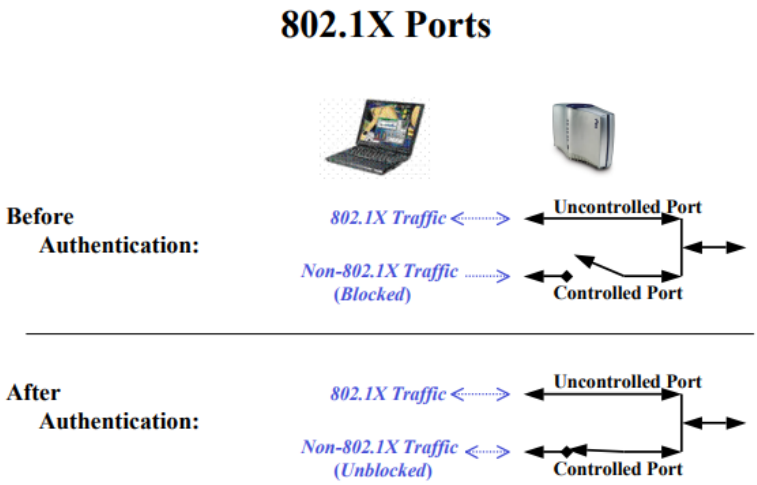
Nguồn: Internet



Hình ảnh mô tả 802.1X hoạt động (nguồn: Internet)

Gồm 4 bước:

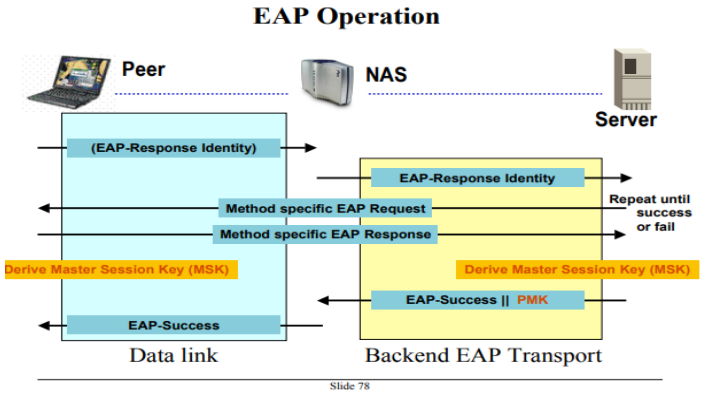
1. Khởi tạo kết nối, ở bước này authenticator cho phép những supplicant chưa xác thực gửi nhận dữ liệu, lưu ý chỉ có những 802.1X được gửi và nhận (TCP, UDP, … không được cho phép).
2. Authenicator sẽ gửi những EAP-request đến những supplicant muốn connect, và sau khi nhận được các supplicant đó sẽ response lại cho authenticator thông tin định danh, ví dụ như ID User. Authenticator sẽ đóng gói dữ liệu đó với gói RADIUS Access-Request và chuyển tiếp lên server. Supplicant có thể làm mới thông tin xác thực bằng cách gửi EAPOL-Start.
3. Ở bước này, server sẽ trả lời bằng gói RADIUS Access-Challenge đến authenticator. Trong đó bao gồm gói EAP Request chỉ rõ EAP method (kiểu phương thức xác thực supplicant muốn). Sau đó supplicant có thể sử dụng EAP method hoặc EAP NAK để phản hồi về server.
4. Khi mà cả hai supplicant và server xác định được phương thức thì những EAP request và response có thể truyền giữa supplicant và server cho đến khi server gửi về EAP-Success hoặc EAP-Failure đóng gói trong gói tin RADIUS. Nếu thành công thì authenticator sẽ thêm gắn cho PORT của supplicant là xác thực và chia sẽ khóa (MSK) truyền dữ liệu bình thường. Ngược lại, PORT vẫn là không xác thực và không thể sử dụng luồng. Khi mà supplicant ngắt kết nối thì nó sẽ gửi gói EAPOL -logoff đến authenticator và authenticator sẽ coi như là port đó chưa được xác thực.



Nguồn: Internet

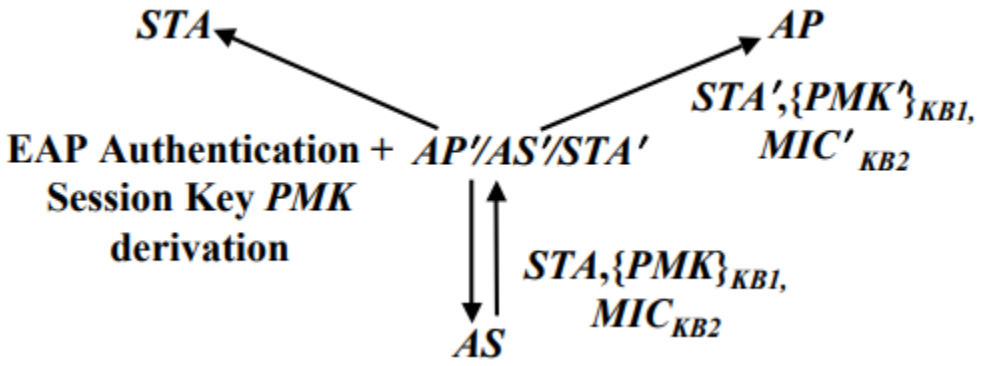
EAP sử dụng MSK (Master Session Key), một key được thiết lập bởi EAP Method dùng để thiết lập kết nối giữa peer (supplicant) và server. Ngoài ra một key được tạo bởi server và peer là AAA key, PMK trong 802.11i =1st trong 32 octets của AAA key. AAA sau đó được server đưa ra cho NAS như một key tạm thời cho NAS với peer giao tiếp với nhau.

EAP là một giao thức stop-and-wait, ngoại trừ message đầu tiền và cuối cùng vì vậy nó tránh được tấn công DoS. EAP phù hợp với 802.11i ở tính tập trung (dùng RADIUS), và giảm được chi phí cho các doanh nghiệp khi sử dụng.



Nguồn: Internet

Tuy nhiên, do có bên thứ bat rung gian và data end-to-end không được mã hóa nên STA và AS có thể bị tấn công MITM. Hơn nữa, key không được mã hóa end-to-end dẫn đến PMK bị đánh cắp.



Nguồn: Internet

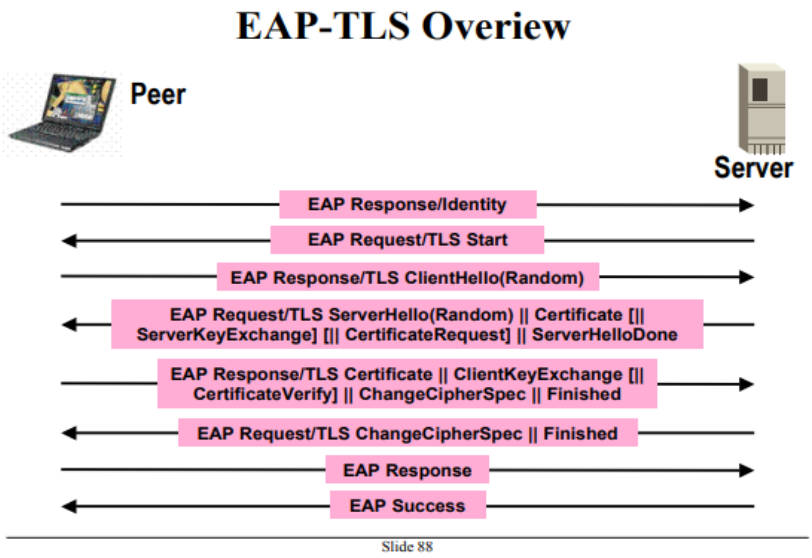
Vì vậy để được triển khai trên 802.11i thì EAP cần cung chấp xác thực lẫn nhau. AAA key được giữa dũng giữa AS và AP cần được mã hóa end-to-end.

Để chọn được EAP method phù hợp thì chúng ta cần quan tấm đến 3 yếu tố:

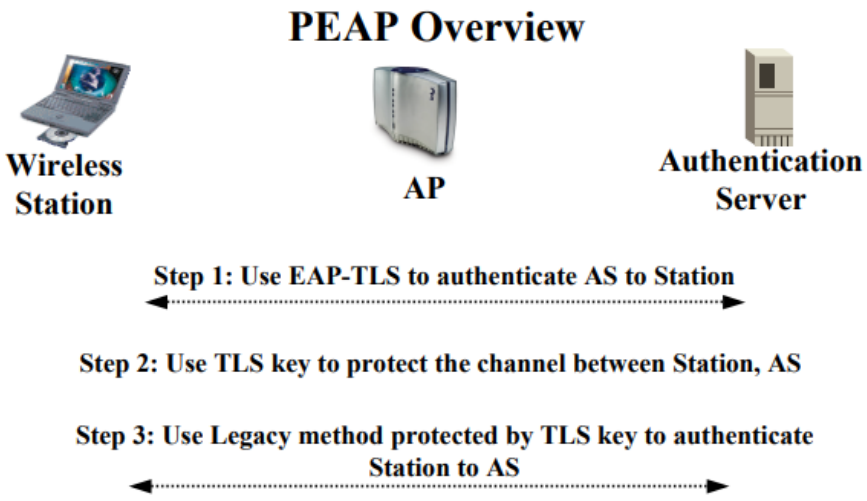
- Tính bảo mật thông tin người dùng cao
- Xác thực lẫn nhau
- Và tạo khóa

Có 3 phương thức xác thực dựa trên EAP:

- EAP-MD5: ở phương thức này, nó không cung cấp mã hóa động, xác thực bằng mật khẩu và không xác thực lẫn nhau (netwok không xác thực user). Phương pháp này không đáp ứng được tiêu chí một giao thức EAP mạnh.
- EAP-TLS: cung cấp mã hóa động, xác thực lẫn nhau (server certificate). Phương pháp này đáp ứng được tiêu chí. Nó cũng giải quyết được MITM ở STA và AS.



- EAP-PEAP: đặt biệt ở phương thức này, nó sử dụng EAP-TSL để xác thực AS và STA. và sử dụng TLS key để bảo vệ kênh truyền giữa AS và STA.



Nguồn: Internet

Nguồn tham khảo

1. https://www.ieee802.org/16/liaison/docs/80211-05_0123r1.pdf
2. https://www.rfc-editor.org/rfc/rfc3686#section-2.2
3. https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Bảng kế hoạch đạt được

STT	Miêu tả	Thời hạn	Thành viên phụ trách	%Complete
1	Chốt đề tài và sơ lược đề tài: • Giới thiệu • Sơ lược chủ đề • Mục tiêu tìm hiểu	20/02/2023	NKNguyen	100%
2	IEEE 802.11 Wireless LAN	20/03/2023	NKNguyen	100%
3	Challenges in Wireless Communications. Wireless security	20/03/2023	PTLap	100%
4	Wired Equivalent Privacy	20/03/2023	NVNNguyen	100%
5	Thiết kế Powerpoint	20/04/2023	NVNNguyen	100%

Bảng kế hoạch sắp tới

STT	Miêu tả	Thời hạn	Thành viên phụ trách
1	Tìm hiểu về AES-CCMP	Báo cáo tiếp theo	PTLap
2	Tìm hiểu về Access Control: 802.1X, EAP, and Access Control: 802.1X, EAP, and RADIUS	Báo cáo tiếp theo	NVNNguyen