CHƯƠNG X

AN NINH MẠNG CỤC BỘ KHÔNG DÂY

ThS. Nguyễn Cao Đạt

E-mail: dat@hcmut.edu.vn

Tham khảo

[2]. Network Security – A Beginner's Guide: module 18

http://www.wifi.org

http://standards.ieee.org/wireless

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf

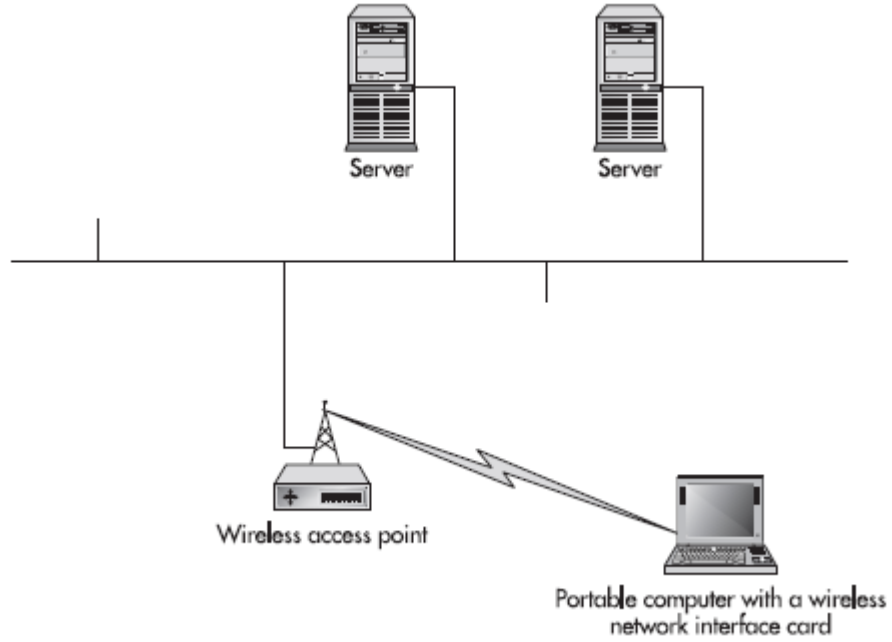
https://quantrimang.com/cac-chuan-wireless-802-11b-802-11a-802-11g-va-802-11n-47723

Nội dung trình bày

- Công nghệ WLAN hiện nay
- Lịch sử phát triển an ninh WLAN
- Các tính năng an ninh cơ bản của 802.11
- Các tính năng an ninh cải tiến
- So sánh các chuẩn an ninh WLAN
- Kết luận và các khuyến cáo

Công nghệ WLAN hiện nay

- Các chuẩn 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax
- Cho phép các máy trạm thiết lập kết nối với Access Point lên đến 11Mbps/54Mbps/450Mbps/1300Mbps



Công nghệ WLAN hiện nay

CÁC CHUẨN WIFI 802.11					
Chuẩn IEEE	802.11a	802.11b	802.11g	802.11n	802.11ac
Năm phát hành	1999	1999	2003	2009	2013
Tần số	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Tốc độ tối đa	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Phạm vi trong nhà	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Phạm vi ngoài trời	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

mesh, point2point of building

Công nghệ WLAN hiện nay

- **Các chuẩn khác**
  - *802.11e – QoS*
    - Được liên minh WiFi đặt tên là "Wireless MultiMedia (WMM)"
  - *802.11i*
    - Thêm thuật toán mã hóa AES
    - Đòi hỏi bộ xử lý tốc độ cao for access point
    - TKIP là giải pháp tạm thời

Công nghệ WLAN hiện nay

- **Vấn đề an ninh**
  - WLAN dùng không khí như là phương tiện truyền thông cho việc gửi và nhận thông tin.
  - Tín hiệu có thể thu được khi ở trong phạm vi hoạt động.
  - WLAN có một số lỗ hổng về bảo mật mà không tồn tại trong mạng cục bộ có dây.

Công nghệ WLAN hiện nay

- **Môt số mối đe dọa**
  - War driver: Kẻ tấn công muốn truy cập Internet miễn phí nên cố gắng để tìm và tấn công các điểm truy cập WLAN không có an ninh hay an ninh yếu.
  - Tin tặc: Sử dụng mạng không dây như một cách để truy cập vào mạng doanh nghiệp mà không cần phải đi qua các kết nối Internet do có bức tường lửa.
  - Nhân viên: Nhân viên vô tình có thể giúp tin tặc truy cập vào mạng doanh nghiệp bằng nhiều cách.
  - Điểm truy cập giả mạo: kẻ tấn công thiết lập AP của riêng mình, với các thiết lập tương tự các AP hiện có. Khi người dùng sử dụng các AP giả mạo này sẽ bị lộ thông tin.

Công nghệ WLAN hiện nay

- **Các hình thức giảm nguy cơ**
  - Xác thực lẫn nhau
  - Mã hóa dữ liệu
  - Phát hiện thâm nhập bất hợp pháp

Lịch sử phát triển an ninh WLAN

- **1997, chuẩn 802.11 chỉ cung cấp**
  - SSID (Service Set Identifier)
  - Lọc trên địa chỉ MAC private / home
  - WEP (Wired Equivalent Privacy)
- **2001**
  - Fluhrer, Mantin và Shamir đã chỉ ra một số điểm yếu trong WEP
  - IEEE bắt đầu khởi động nhóm i (802.11i)

Lịch sử phát triển an ninh WLAN

- **2003**
  - Wi-Fi Protected Access(WPA) được giới thiệu
  - Là một giải pháp tạm thời cho WEP
  - Một phần của IEEE 802.11i
- **2004**
  - WPA2 được giới thiệu
  - Nó dựa trên chuẩn IEEE 802.11i
  - Được phê chuẩn vào 25/06/2004

Các tính năng an ninh cơ bản của 802.11

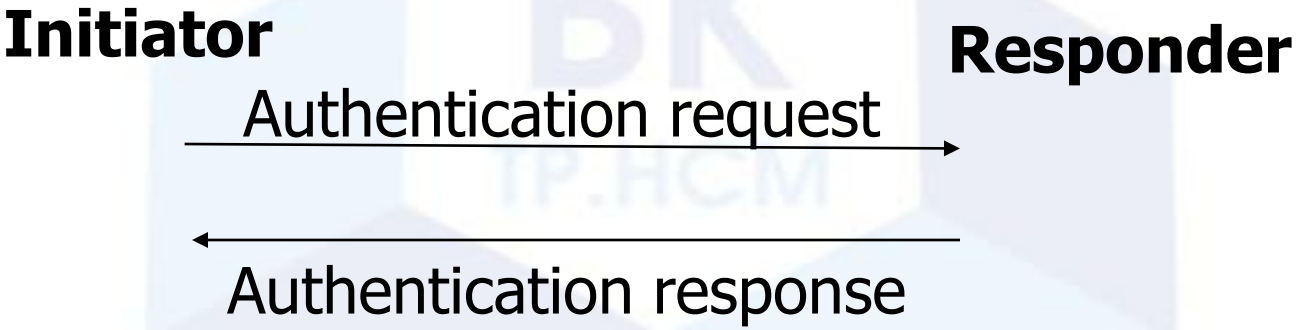
- **Kiểm soát truy cập dùng SSID**
  - Service Set Identifier.
  - SSID là định danh của mạng cục bộ không dây.
  - Người dùng được yêu cầu phải cung cấp SSID khi kết nối đến các Access Point.
  - Khi thay đổi SSID cần phải thông báo đến mọi người.
  - SSID được các máy trạm gửi dạng bản rõ nên dể dàng bị đánh cắp.

Các tính năng an ninh cơ bản của 802.11

- **Lọc địa chỉ MAC**
  - Kiểm soát truy cập bằng cách chỉ cho phép các máy tính có các địa chỉ MAC khai báo trước được kết nối đến mạng.
  - Địa chỉ MAC có thể bị giả mạo.
  - Phải duy trì và phân phối một danh sách các địa chỉ MAC đến tất cả các Access Point.
  - Không phải là giải pháp khả thi cho các ứng dụng công cộng.

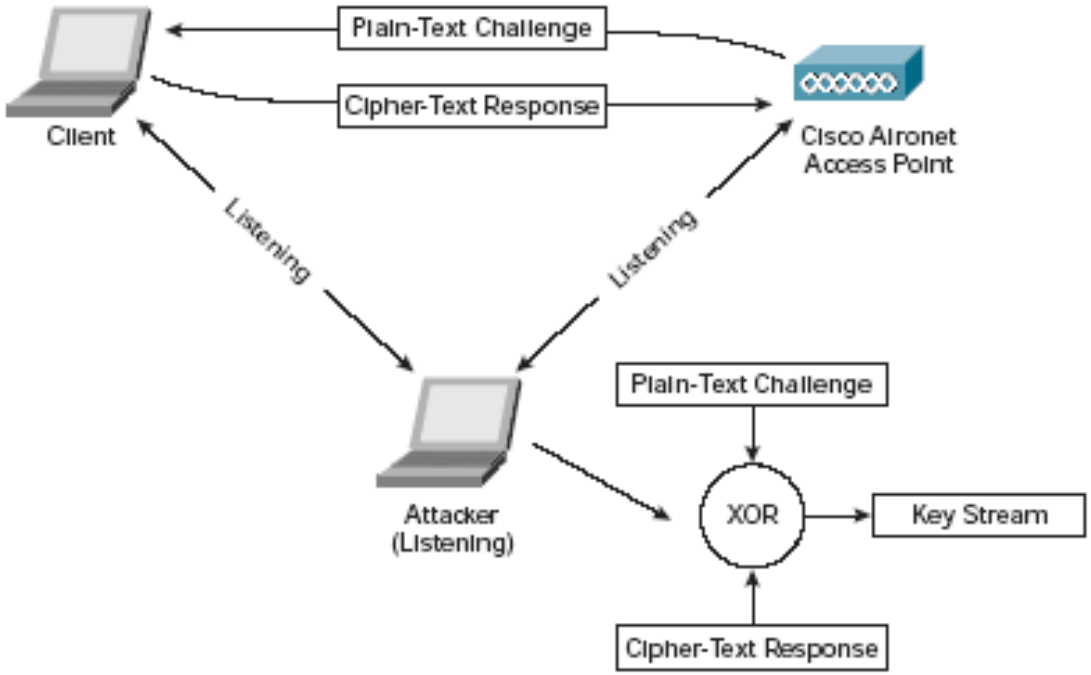
Các tính năng an ninh cơ bản của 802.11

- **Xác thực người dùng**
  - Có hai loại xác thực người dùng
  - Xác thực hệ thống mở
    - Xác thực bất cứ ai yêu cầu xác thực
    - Cung cấp dạng xác thực NULL



Các tính năng an ninh cơ bản của 802.11

- **Xác thực người dùng**
  - Xác thực dùng khóa chung
    - Dễ dàng sniff khóa chung



Các tính năng an ninh cơ bản của 802.11

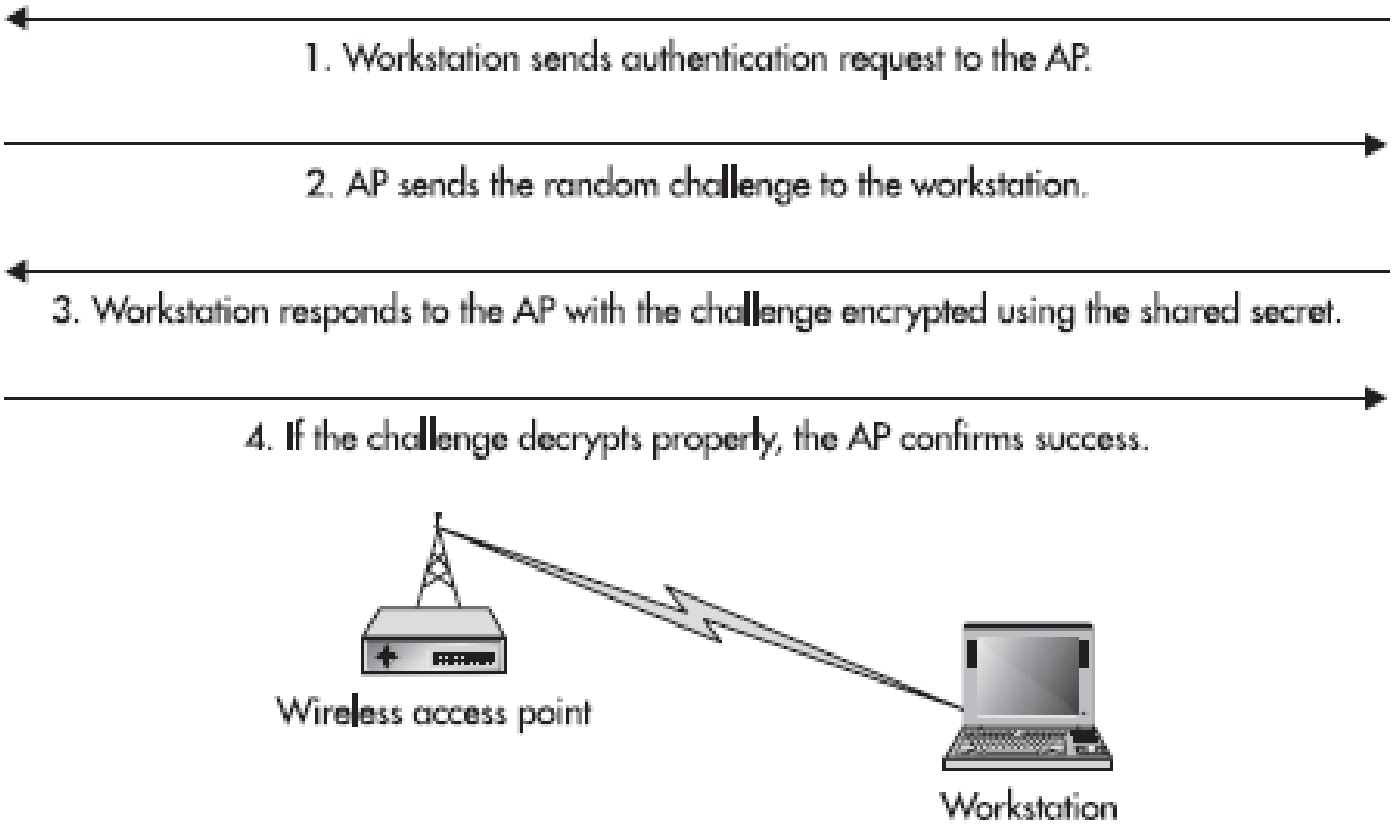
- Ngoài vấn đề kiểm soát truy cập cũng cần phải đảm bảo bí mật và toàn vẹn thông tin giữa các máy trạm và Access Point.
- Chuẩn 802.11x định nghĩa WEP(Wired Equivalent Privacy) để kiểm soát truy cập và bảo vệ thông tin khi nó đi qua mạng cục bộ không dây.
- WEP cung cấp 3 dịch vụ cơ bản: xác thực, bí mật, toàn vẹn.

WEP

- **Dịch vụ xác thực**
  - Được dùng để xác thực các máy trạm khi kết nối đến các Access Point
  - Trong hệ thống xác thực mở, máy trạm được xác thực nếu nó đáp ứng một địa chỉ MAC khi trao đổi ban đầu với Access Point -> không cung cấp danh tính của máy trạm.
  - WEP cũng sử dụng một cơ chế xác thực dựa trên mật mã. Cơ chế này dựa trên một khóa bí mật dùng chung và thuật toán mã hóa RC4.
  - Trao đổi xác thực dùng một hệ thống challenge – response.

WEP

- **Dịch vụ xác thực**



WEP

- **Dịch vụ xác thực**
  - Hệ thống challenge – response không xác thực Access Point.
  - Vì vậy nó dể dàng bị tấn công như dùng Access Point giả mạo, "man in the midle"
- **Dịch vụ bí mật**
  - Cũng dựa trên RC4.
  - Tạo ra dòng khóa giả ngẫu nhiên để mã hóa dữ liệu.
  - Tuy nhiên WEP không chỉ định một cơ chế quản lý khóa. Điều này có nghĩa là WEP dựa trên các khóa tĩnh. Trong thực tế, các khóa tương tự được sử dụng cho tất cả các máy trạm trên mạng.

WEP

- **Cách thức xử lý**

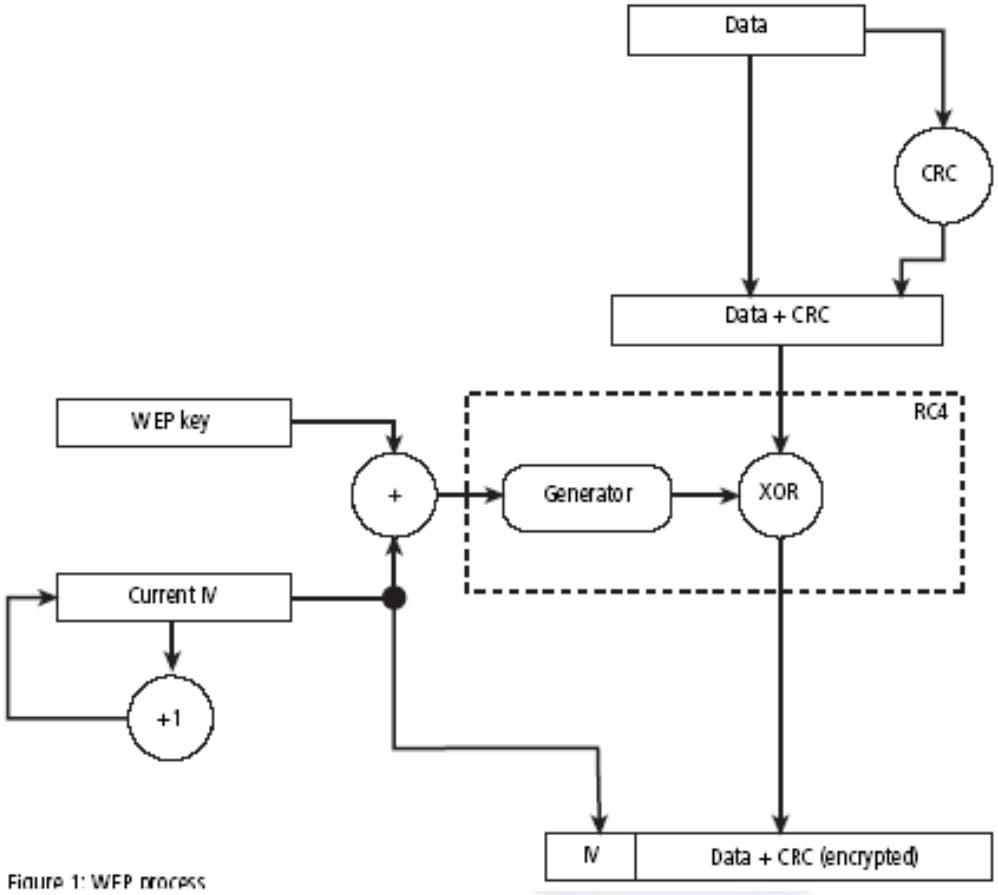


Figure 1: WEP process

- Khóa bí mật k là WEP key
- Tính toán CRC32
- CRC+data
- Chọn IV ngẫu nhiên, nối với khóa k: (k+IV)
- Tạo khóa giả ngẫu nhiên
- Gửi IV đến bên nhận bằng cách đặt nó phía trước bản mã C:

C=(data+CRC) xor RC4(k+IV))

WEP

- **RC4 trong WEP**
  - Mã hóa dòng dùng khóa đối xứng
  - Mã hóa và giải mã nhanh(10 lần nhanh hơn so với DES)
  - **Khóa bí mật k**
    - Gõ bằng tay
    - 40bits/128bits
  - **Vector khởi tạo IV**
    - Dùng PRG để tạo ra số ngẫu nhiên kích thước 24bits
    - Gửi trong phần rõ trước bản mã: (IV+C)
  - Khóa mã hóa RC4 độc lập với bản rõ

WEP

- **Dịch vụ bí mật**
  - Vector khởi tạo(IV) được gởi trong phần rõ của gói tin
  - Vì vậy khi nắm bắt được vector khởi tạo và một số lượng gói tin, kẻ tấn công có thể xác định được khóa mã hóa
  - http://sourceforge.net/projects/wepcrack/
  - Tóm lại RC4 không phải là thuật toán yếu nhưng việc hiện thực RC4 trong WEP là thiếu sót và mở dẫn đến bị thỏa hiệp.

WEP

- **Dịch vụ toàn vẹn**
  - Kiểm tra tính toàn vẹn trên mỗi gói tin. checksum
  - Dùng CRC(cyclic redundancy check) của 32 bits.
  - CRC được tính toán trên mỗi gói tin trước khi gói tin được mã hóa.
  - Dữ liệu và CRC được mã hóa và gởi đến đích.
  - CRC không phải mật mã an toàn tuy nhiên nó được bảo vệ bằng mã hóa.
  - Do khi hiện thực mã hóa, WEP có một số thiếu sót dẫn đến sự toàn vẹn của các gói tin cũng dễ bị thỏa hiệp.

WEP

- **Chi tiết các điểm yếu**
  - 10/2000: Jesse Walker của Intel đã công bố ”Unsafe at any keysize; An analysis of the WEP encapsulation”
  - 03/2001: Scott Fluhrer, Itsik Mantin, Adi Shamir công bố "Attacks on RC4 and WEP“, “Weaknesses in the Key Scheduling Algorithm of RC4“.

Các tính năng an ninh cải tiến

- **Wi-Fi Protected Access (WPA)**
  - Giải quyết hầu hết các điểm yếu của WEP
  - Là một tập con của 802.11i, tương thích 802.11i
  - Mục tiêu là cải thiện vấn đề mã hóa và xác thực người dùng
  - Gồm 2 chế độ hoạt động
    - WPA doanh nghiệp: TKIP/MIC ; 802.1X/EAP
    - WPA cá nhân: TKIP/MIC; PSK

Các chế độ hoạt động WPA

- **Doanh nghiệp**
  - Dùng 802.1x/EAP cho xác thực.

username
password

- **Nhà hay văn phòng nhỏ**
  - Dùng chế độ "Pre-Shared Keys (PSK)".
  - Người dùng cung cấp khóa chủ trên mỗi máy tính.
  - Khóa chủ kích hoạt TKIP và việc quay vòng khóa.
- **Chế độ hỗn hợp**
  - Hoạt động với WEP nếu máy trạm nào không hỗ trợ WPA.

Chế độ WPA doanh nghiệp

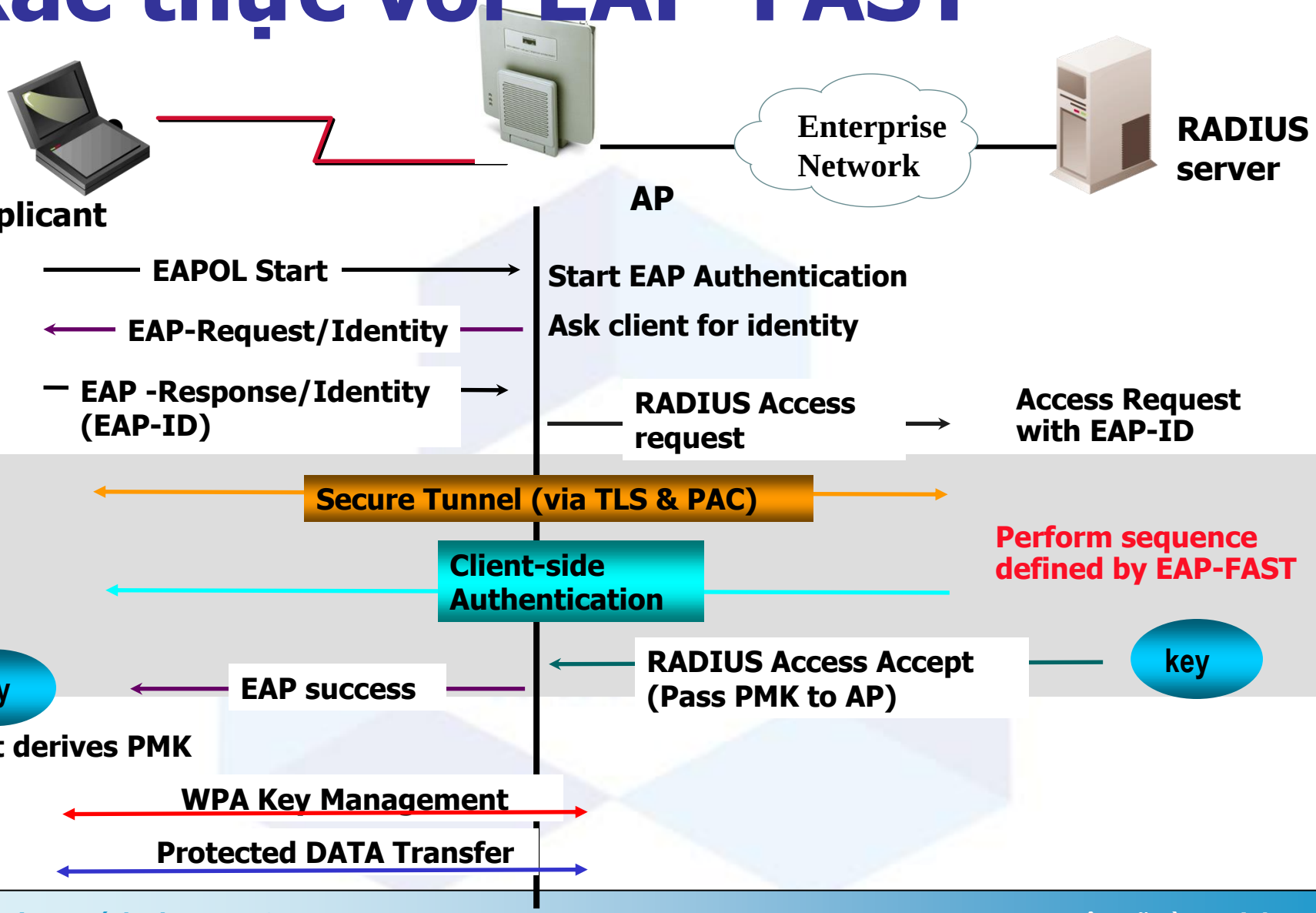
- **Xác thực(IEEE 802.1X/EAP)**
  - Xác thực lẫn nhau. Vì vậy bạn không bị tham gia các mạng giả mạo và cung cấp các thông tin bí mật của bạn.
  - Hỗ trợ nhiều phương thức xác thực như dựa trên mật khẩu, chứng chỉ số.
  - Quản lý thông tin người dùng tập trung.
  - Một AAA server là cần thiết.
  - Dùng giao thức RADIUS cho AAA và phân phối khóa.

authentication
author
audit

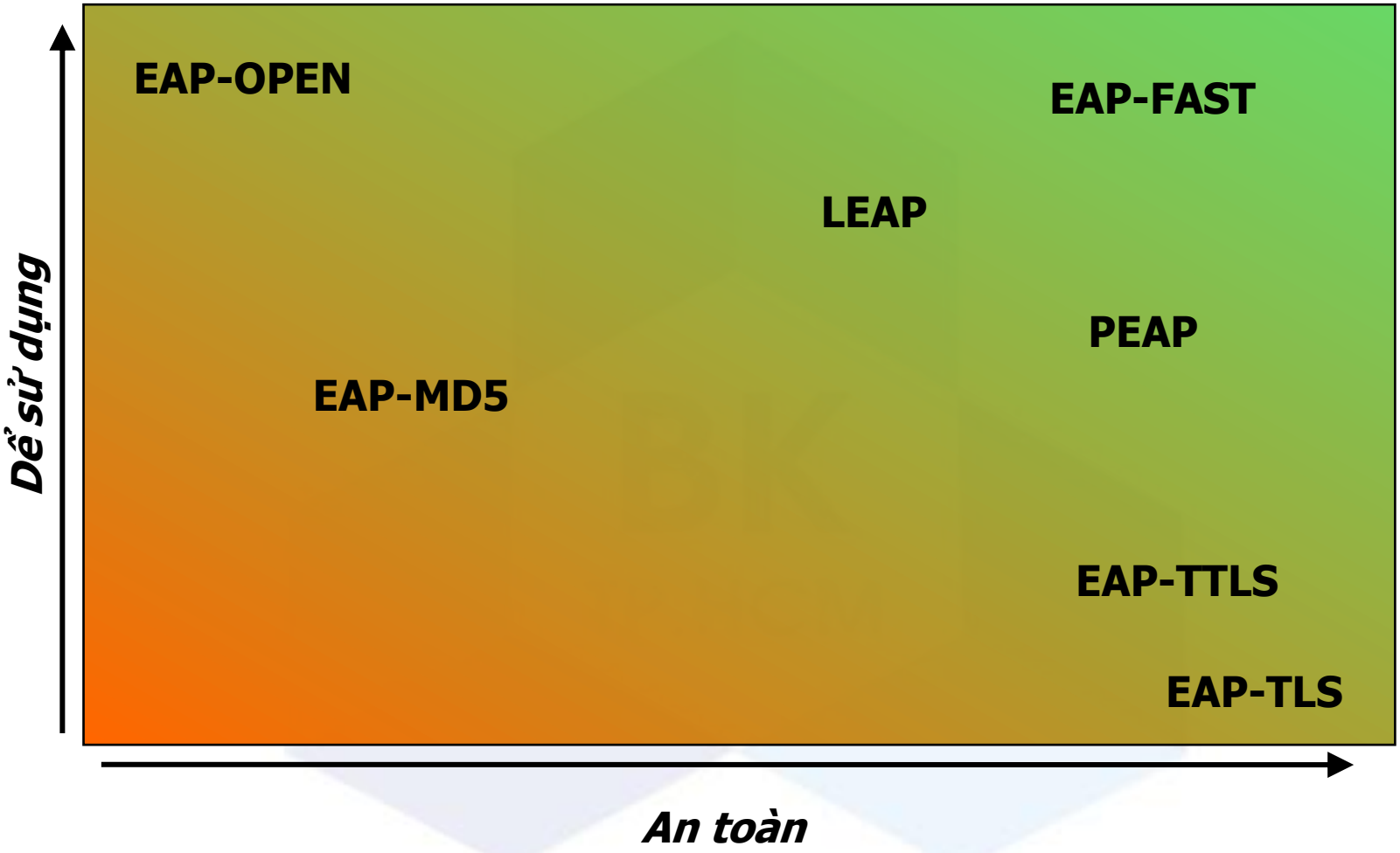
EAP(Extensible Authentication Protocol)

- **Cisco LEAP**
  - Dùng Username/password
  - Dễ bị tổn thương bởi tấn công mật khẩu/ dựa trên băm.
- **EAP-TLS**
  - Xác thực lẫn nhau dùng chứng chỉ X.509
  - Mặc định của 802.11i
- **EAP-TTLS/PEAP**
  - TLS qua đường hầm
  - Không yêu cầu chứng chỉ của client.
- **EAP-GTC**
  - Xác thực dùng mật khẩu một lần
- **EAP-FAST**
  - Client & server có cùng khóa, thiết lập đường hầm an toàn
  - Xác thực xảy ra trên đường hầm an toàn
  - Giống như xác thực VPN

Xác thực với EAP-FAST



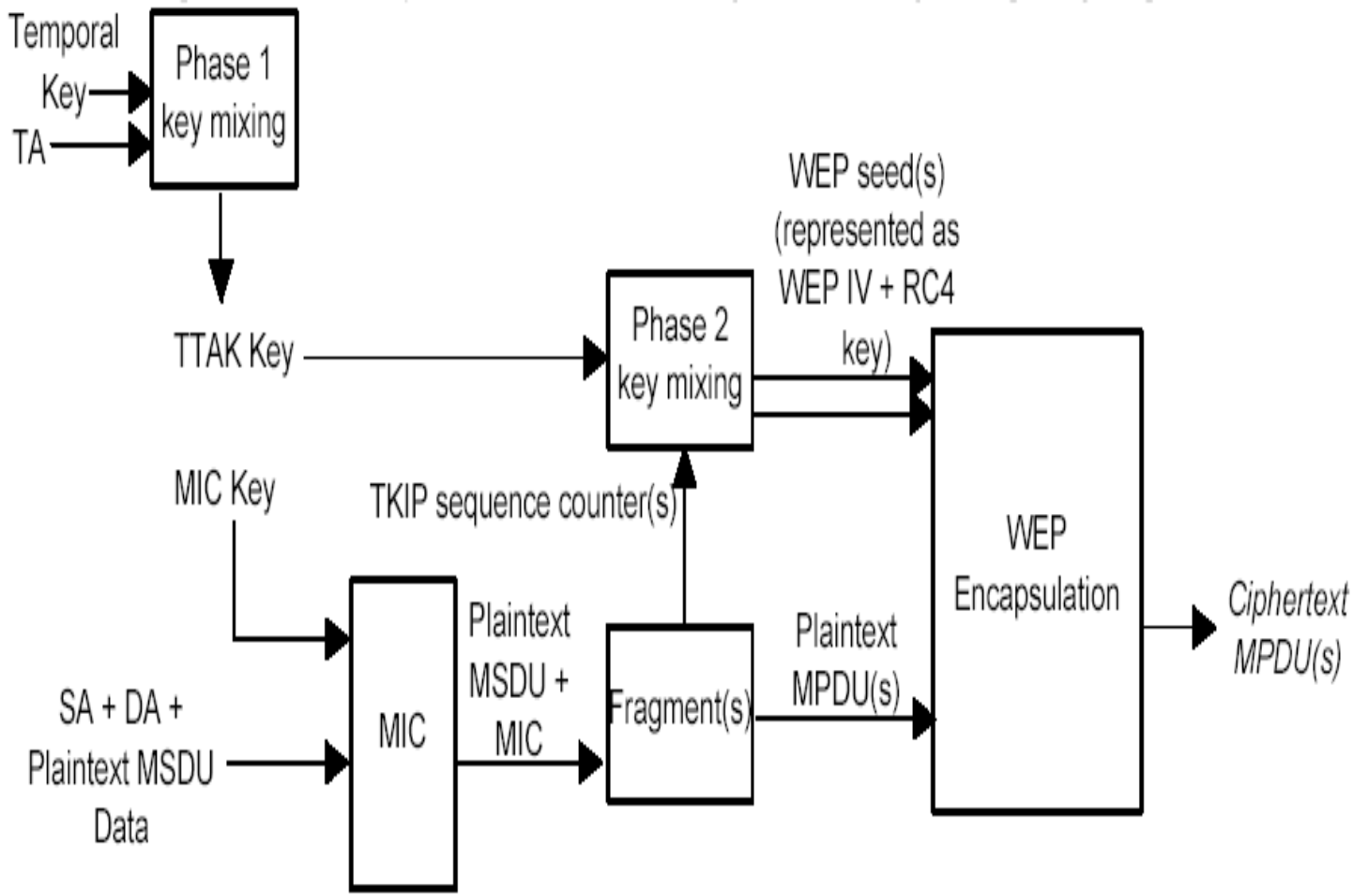
Đánh giá các loại EAP



Chế độ WPA doanh nghiệp

- **Mã hóa(TKIP/MIC)**
  - **TKIP**
    - Temporal Key Integrity Protocol.
    - Sửa lỗi phục hồi khóa trong WEP. Bảo vệ IV bằng cách loại bỏ khả năng dự đoán.
    - Sử dụng thuật toán mã hóa RC4 như WEP.
    - Thêm MIC ở cuối của mỗi thông điệp bản rõ nhằm đảm bảo thông điệp đó không bị giả mạo.
  - **MIC**
    - Message Integrity Code.
    - Chống lại tấn công bit-flip.
    - Phải được hiện thực trên client & AP.

Chế độ WPA doanh nghiệp



Chế độ WPA doanh nghiệp

- **Mã hóa (TKIP/MIC)**
  - Dùng khóa 64 bits
  - Chia gói tin thành các khối 32 bits
  - Dùng shifts, XORs, + đến mỗi khối 32 bits để lấy ra thẻ xác thực 64 bits
  - Khóa MIC được tính toán trên dữ liệu địa chỉ nguồn và địa chỉ đích
    - MIC = MIC_key(SA, DA, PlainMSDU)
    - Tránh bắt gói, thay đổi và gởi lại các gói tin

Chế độ WPA doanh nghiệp

- **Mã hóa (TKIP/MIC)**
  - Mỗi khóa mã hóa trên mỗi gói.
  - IV có chiều dài 48bits dẫn đến giảm việc tái sử dụng IV.
  - IV mã hóa trước khi gởi.
  - MIC thay thế CRC.
  - Có thể nâng cấp dể dàng cho phần cứng hỗ trợ WEP.

Chế độ WPA cá nhân

- **Mã hóa (TKIP)**
- **Authentication (PSK - Pre-shared key)**
  - Chế độ đặc biệt (không có hạ tầng 802.1x)
  - Passphrase được cung cấp trên tất cả máy trạm và các Access Point
  - Dựa trên bắt tay khóa bốn lần
    - Hai lần đầu: máy trạm và access point trao đổi các giá trị ngẫu nhiên để xác thực lẫn nhau.
    - Hai lân kế tiếp : access point hướng dẫn máy trạm để cài đặt khóa được tính toán trước. Máy trạm xác nhận.

Các tính năng an ninh cải tiến

- **WPA2/802.11i**
  - WPA là một giải pháp tình thế
  - WPA2 là chuẩn IEEE 802.11i
  - 802.11i dùng khái niệm an ninh mạng mạnh mẽ(RSN -Robust Security Network)
  - Khác biệt lớn nhất: AES được dùng cho mã hóa
  - Mã hóa AES được thực hiện trong phần cứng
  - Đòi hỏi bộ xử lý mạnh hơn

Các chế độ hoạt động WPA2

- **Doanh nghiệp**
  - Xác thực dùng 802.1X/EAP
  - Mã hóa dùng AES-CCMP
- **Nhà hay văn phòng nhỏ**
  - Xác thực dùng PSK
  - Mã hóa dùng AES-CCMP
- **AES-CCMP**
  - AES là mã hóa khóa đối xứng
  - Chiều dài khối và khóa là 128 bits
  - CCMP: Counter-Mode/CBC-Mac Protocol
  - Mã hóa dùng chế độ Counter
  - Toàn vẹn dữ liệu dùng CBC-MAC

So sánh các chuẩn an ninh WLAN

	WEP	WPA	WPA2
Mã hóa	RC4	RC4 với TKIP/MIC	AES
Quay vòng khóa	Không	Các khóa phiên động	Các khóa phiên động
Phân phối khóa	Gõ bằng tay vào mỗi thiết bị	Phân phối tự động	Phân phối tự động
Xác thực	Dùng khóa WEP	Có thể dùng 802.1x & EAP	Có thể dùng 802.1x & EAP

Kết luận và các khuyến cáo

- An ninh mạng nói chung không phải là một trạng thái mà là một tiến trình.
- Các khuyến cáo cho an ninh WLAN
  - Dùng thiết bị tương thích và có chứng nhận Wi-Fi
  - Thay đổi SSID và không quảng bá SSID
  - Cấu hình lọc địa chỉ MAC nếu bạn quản lý được người dùng và các Access Point
  - Cấu hình WEP với khóa có chiều 128 bits và thay đổi khóa WEP thường xuyên nếu không thể nâng cấp firmware hỗ trợ WPA/WPA2
  - Nâng cấp firmware để cấu hình WPA/WPA2 và dùng 802.1x/EAP để xác thực người dùng