An toàn mạng không dây và di động

Bài 2.2 Các tấn công trong mạng không dây

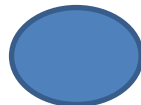
cisco

Nội dung

1. Interception of data
2. Wireless intruders
3. Denial of Service (DoS) Attacks
4. Rogue Aps
5. Một số cấu hình an toàn

Video – WLAN Threats

- This video will cover the following:
- Interception of Data
- Wireless Intruders
- Denial of Service (DoS) Attacks
- Rogue APs



WLAN Threats
Wireless Security Overview

- WLAN là mở cho tất cả những thiết bị trong vùng phủ sóng của một AP và các thông tin đăng nhập thích hợp để liên kết đến nó.
- Các cuộc tấn công có thể được tại ra bởi những người từ bên ngoài, nhân viên bất mãn, hay sự vô ý của nhân viên. Các mạng không dây thường bị đe doạ bởi các nguy cơ sau đây:
  - Chặn bắt dữ liệu
  - Tấn công xâm nhập mạng không dây
  - Tấn công từ chối dịch vụ
  - Giả mạo AP

WLAN Threats
DoS Attacks

- Các cuộc tấn công DoS không dây có thể là kết quả của:
  - Các thiết bị được cấu hình không đúng
  - Kẻ tấn công cố tình can thiệp vào giao tiếp không dây
  - Sự can thiệp tình cờ
- Để giảm thiểu nguy cơ bị tấn công DoS do các thiết bị được cấu hình không đúng và các cuộc tấn công độc hại, hãy làm kiểm soát tất cả các thiết bị, giữ an toàn cho mật khẩu, tạo bản sao lưu và đảm bảo rằng tất cả các thay đổi cấu hình đều được thực hiện trong khung giờ hợp lý.

WLAN Threats
Rogue Access Points

- Giả mạo AP là một AP hoặc bộ định tuyến không giây được được kết nối với mạng công ty mà không có sự cho phép rõ ràng và vi phạm chính sách của công ty
- Sau khi kết nối, kẻ tấn công có thể sử dụng AP giả mạo để chiếm địa chỉ MAC, chặn bắt thông tin, giành quyền truy cập vào tài nguyên mạng hoặc tiến hành một cuộc tấn công trung gian.
- Một điểm phát song mạng cá nhân cũng có thể sử dụng như một AP giả mạo (Ví dụ chức năng phát wifi trên windows)
- Để ngăn chặn việc cài đặt AP giả mạo, các tổ chức phải cấu hình WLC với các chính sách AP giả mạo, sử dụng hệ thống giám sát an ninh mạng.

WLAN Threats
Man-in-the-Middle Attack

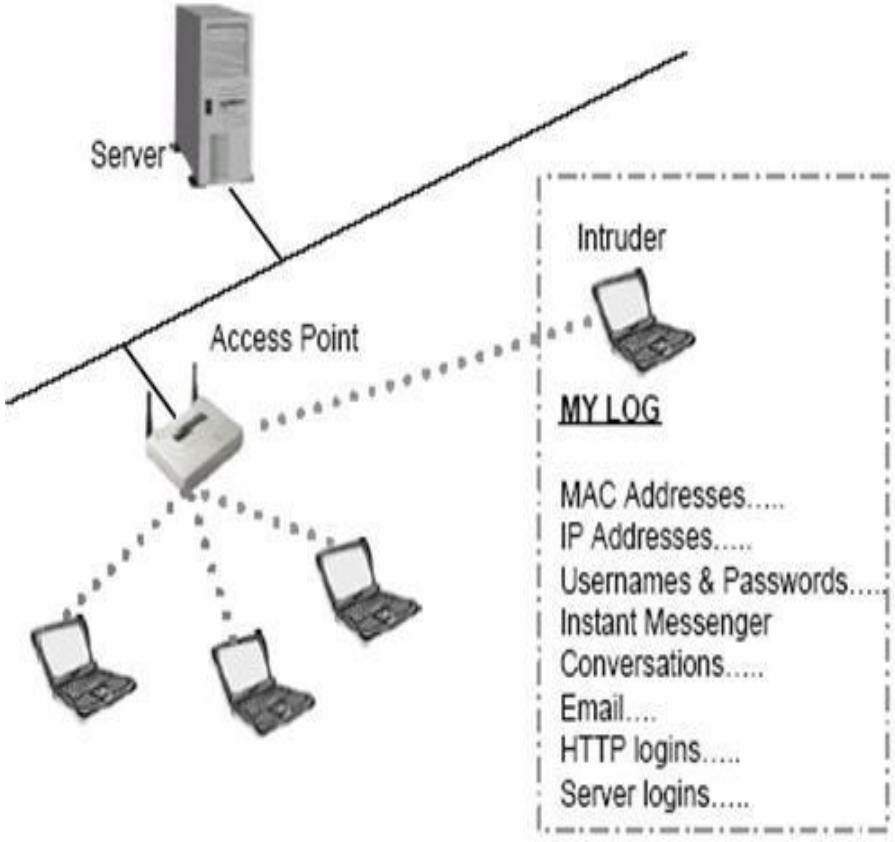
- Tấn công Man in the middle (MITM), tin tặc ở giữa 2 thực thể hợp pháp để đọc hoặc sửa đổi dữ liệu trao đổi giữa 2 bên.
- Một cuộc tấn công MITM không dây phổ biến được gọi là cuộc tấn công "AP đôi xấu xa – evil twin AP", trong đó kẻ tấn công giới thiệu một AP giả mạo và cấu hình nó với cùng SSID như một AP hợp pháp.
- Để chống lại cuộc tấn công MITM thì việc đầu tiên phải xác định các thiết bị hợp pháp trong mạng WLAN. Người dùng phải được xác thực. Sau khi tất cả các thiết bị hợp pháp được biết, mạng có thể được giám sát để tìm các thiết bị hoặc lưu lượng truy cập bất thường

Các kiểu tấn công trên WLAN

- **Một số kiểu tấn công chủ yếu**:
  - Tấn công bị động (nghe trộm – *Passive attacks*).
  - Tấn công chủ động (kết nối, dò và cấu hình mạng -*Active attacks*).
  - Tấn công kiểu chèn ép (*Jamming attacks*).
  - Tấn công theo kiểu thu hút (*Man–in-the-middle attacks*).
  - Tấn công lặp lại (*Replay attacks*).

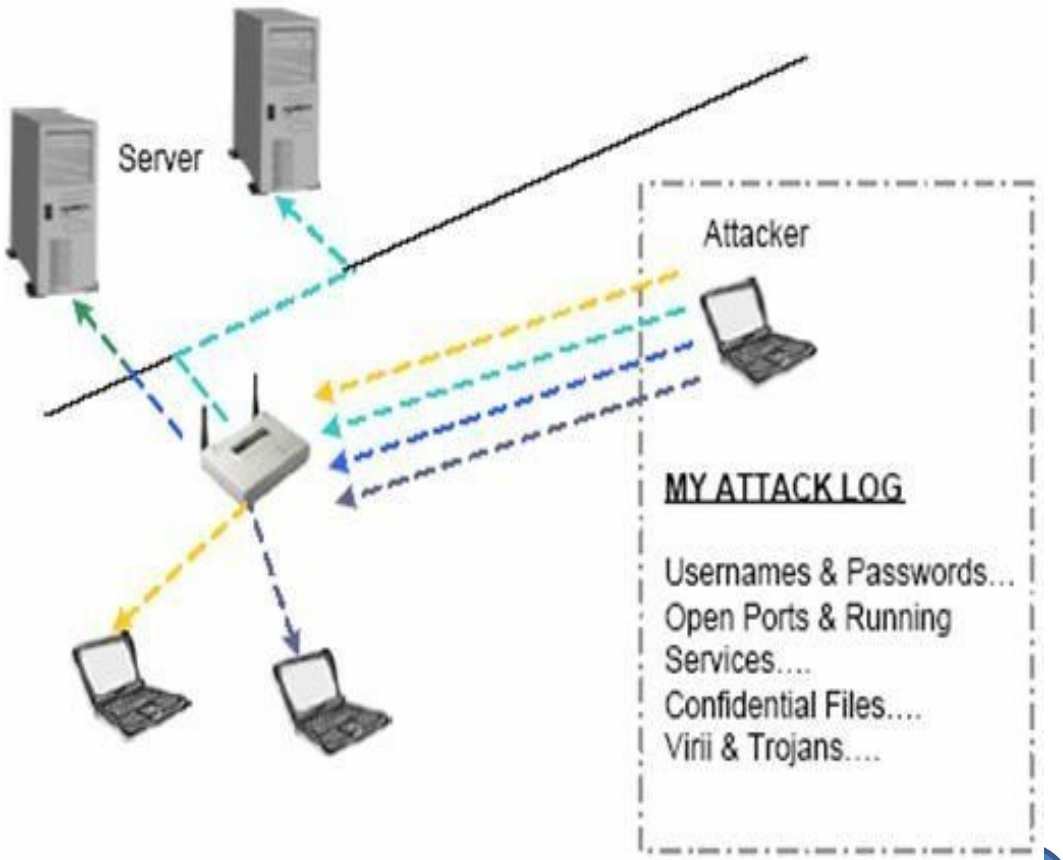
Tấn công bị động

- Tấn công bị động thực hiện như một cuộc nghe trộm.
- Những thiết bị phân tích mạng hoặc những ứng dụng khác được sử dụng để lấy thông tin của WLAN từ một khoảng cách với một anten hướng tính.

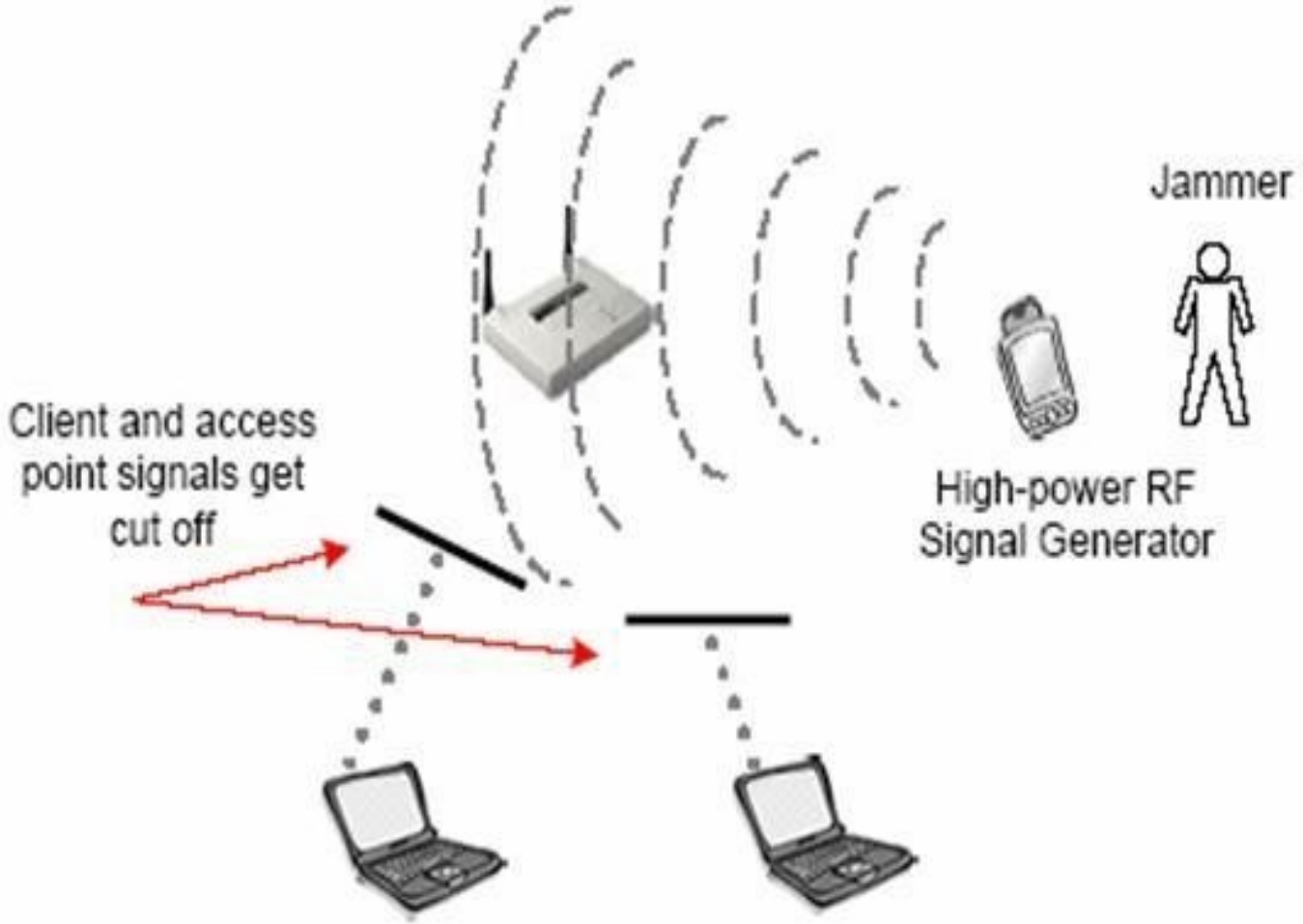


Tấn công chủ động

- Một tấn công chủ động có thể được dùng để tìm cách truy nhập tới một server để lấy những dữ liệu quan trọng, thậm chí thay đổi cấu hình cơ sở hạ tầng mạng.



Tấn công theo kiểu chèn ép



Video – Secure WLANs

- This video will cover the following:
  - SSID Cloaking
  - MAC Address Filtering
  - Authentication and Encryption Systems (Open Authentication and Shared Key Authentication)

Video – Secure WLANs

https://www.youtube.com/watch?v=y0rnmWJKa9A

Secure WLANs
SSID Cloaking and MAC Address Filtering

- Để giải quyết các mối đe doạ, ngăn chặn các tấn công không dây và bảo vệ dữ liệu, hai tính năng bảo mật ban đầu được sử dụng là kỹ thuật che giấu SSID và Lọc MAC

- Kỹ thuật che giấu SSID: Các AP và một số bộ định tuyến không dây cho phép vô hiệu hóa khung báo hiệu SSID. Máy khách không dây phải được cấu hình thủ công với SSID để kết nối với mạng.

- Lọc địa chỉ MAC: Cho phép hoặc từ chối truy cập không dây của máy khách theo cách thủ công dựa trên địa chỉ phần cứng MAC vật lý của họ.

Secure WLANs

802.11 Original Authentication Methods

- Phương pháp hiệu quả nhất để bảo mật mạng không dây là sử dụng hệ thống xác thực và mã hóa. Hai loại xác thực đã được giới thiệu với chuẩn 802.11 ban đầu:

- Mở xác thực hệ thống: Không cần mật khẩu. Thường được sử dụng để cung cấp truy cập Internet miễn phí ở các khu vực công cộng. Máy khách chịu trách nhiệm cung cấp bảo mật như thông qua VPN.

- Xác thực khóa chia sẻ: Cung cấp các cơ chế xác thực và mã hóa dữ liệu giữa máy khách không dây và AP như WEP, WPA, WPA2 và WPA3. Tuy nhiên, mật khẩu phải được chia sẻ trước giữa hai bên để kết nối.

Secure WLANs
Shared Key Authentication Methods

- Hiện nay, có 4 kỹ thuật xác thực khóa chia sẻ khả dụng gồm WEP, WPA, WPA2, WPA3.

	WEP	WPA	WPA2
Cript	RC4	RC4	AES
Key rotation	None	Dynamic session keys	Dynamic session keys
Key distribution	Manual inert over each device	Automatic distribution is possible	Automatic distribution is possible
Authentification	Use WEP key	802.1x & EAP supported	802.1x & EAP supported

Secure WLANs
Shared Key Authentication Methods

Phương pháp xác thực	Mô tả
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF).

Secure WLANs
Authenticating a Home User

- Bộ định tuyến gia đình thường có hai lựa chọn để xác thực: WPA và WPA2, với WPA 2 có hai phương thức xác thực.

- Cá nhân: Dành cho mạng gia đình hoặc mạng văn phòng nhỏ, người dùng xác thực bằng khóa chia sẻ trước (PSK). Máy khách không dây xác thực với bộ định tuyến không dây bằng mật khẩu được chia sẻ trước. Không cần máy chủ xác thực đặc biệt.

- Doanh nghiệp: Dành cho mạng doanh nghiệp. Yêu cầu máy chủ xác thực Dịch vụ người dùng (RADIUS). Thiết bị phải được xác thực bởi máy chủ RADIUS và sau đó người dùng phải xác thực bằng tiêu chuẩn 802.1X, sử dụng giao thức xác thực khả mở rộng (EAP) để xác thực.

Secure WLANs
Encryption Methods

- WPA và WPA2 bao gồm hai giao thức mã hóa:

- Giao thức toàn vẹn khóa tạm thời (TKIP): Được sử dụng bởi WPA và cung cấp hỗ trợ cho thiết bị WLAN cũ. Sử dụng WEP nhưng mã hóa tải trọng Lớp 2 bằng TKIP.

- Tiêu chuẩn mã hóa nâng cao (AES): Được sử dụng bởi WPA2 và sử dụng Chế độ mã hóa bộ đếm với Giao thức mã xác thực thông điệp chuỗi khối (CCMP) cho phép máy chủ đích nhận ra nếu các bit được mã hóa và không mã hóa đã bị thay đổi.

- Lựa chọn chế độ bảo mật doanh nghiệp yêu cầu máy chủ RADIUS Xác thực, Ủy quyền và Kế toán (AAA).
- Có một số thông tin được yêu cầu:
  - Địa chỉ IP máy chủ RADIUS: Địa chỉ IP của máy chủ.
  - Số cổng UDP: CổngUDP 1812 cho Xác thực RADIUS và 1813 cho Kiểm toán RADIUS, nhưng cũng có thể hoạt động bằng các cổng UDP 1645 và 1646.
  - Khóa chia sẻ: Được sử dụng để xác thực AP với máy chủ RADIUS.

Secure WLANs
WPA 3

- Do WPA2 không còn được coi là an toàn, nên WPA3 được khuyến nghị khi khả dụng. WPA3 Bao gồm bốn tính năng:

- WPA3 - Cá nhân: Chống lại các cuộc tấn công bằng cách sử dụng Xác thực đồng thời các công bằng (Simultaneous Authentication of Equals-SAE).
- WPA3 - Enterprise: Sử dụng xác thực 802.1X / EAP. Tuy nhiên, nó yêu cầu sử dụng bộ mật mã 192-bit và loại bỏ sự pha trộn của các giao thức bảo mật cho các chuẩn 802.11 trước đây.
- Mạng mở: Không sử dụng bất kỳ xác thực nào. Tuy nhiên, sử dụng Mã hóa không dây cơ hội (OWE) để mã hóa tất cả lưu lượng truy cập không dây.
- Tích hợp IoT: Sử dụng Giao thức cấp phép thiết bị (DPP) để nhanh chóng tích hợp các thiết bị IoT.

cisco