**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

**Bài 1: Nêu các đặc điểm của SSID**

* **Độ dài:**
* SSID có thể dài tối đa 32 ký tự.
* Các ký tự có thể bao gồm chữ cái, số, ký tự đặc biệt và khoảng trắng
* **Phân biệt chữ hoa và chữ thường:**
* SSID có thể phân biệt chữ hoa và chữ thường. Ví dụ "HomeWiFi” và "homewifi” sẽ được hệ thống phân biệt là hai SSID khác nhau.
* **Phát sóng:**
* **Broadcast SSID:** SSID được phát công khai, hiển thị trên các thiết bị xung quanh bắt được nó.
* **Hidden SSID:** SSID bị ẩn đi, người dùng cần nhập tên mạng thủ công để có thể tiến hành kết nối.
* **Mức độ bảo mật:**
* SSID không ảnh hưởng trực tiếp đến bảo mật, nhưng việc đặt tên khó đoán có thể tránh được các cuộc tấn công như SSID spoofing hoặc phishing.
* **Cấu hình cho SSID:**
* Một điểm truy cập Wi-Fi (Access Point) có thể phát nhiều SSID. Ví dụ, một router có thể phát hai SSID, một cho guest và một cho local users.
* **SSID mặc định:**
* Khi vừa thiết lập lần đầu, SSID mặc định thường là tên của nhà sản xuất router hoặc thiết bị (ví dụ: "TP-Link 1234", "Netgear56"). Sau đó nên thay đổi SSID mặc định đề tăng cường bảo mật và dễ nhận diện.
* **Phạm vi phủ sóng:**
* SSID thuộc về một mạng không dây cụ thể, chỉ khả dụng trong phạm vì phủ sóng của router hoặc Access Point.
* **Ứng dụng nhiều SSID:**
* Trong môi trường doanh nghiệp, một router hoặc Access Point có thể phát nhiều SSID với các mức bảo mật và quyền truy cập khác nhau

**Bài 2: Tại sao nói WEP là phương thức mã hoá yếu?**

* **Sử dụng khoá mã hoá tĩnh**
* WEP sử dụng một khóa mã hóa tĩnh (cố định) để mã hóa dữ liệu.
* Khóa này không thay đổi trong suốt thời gian kết nối, khiến mạng dễ bị tấn công nếu kẻ xấu thu thập đủ dữ liệu.
* **Độ dài khoá yếu**
* Khóa 64-bit: Chỉ có 40 bit được sử dụng cho mã hóa thực sự (24 bit còn lại là IV - Initialization Vector).
* Khóa 128-bit: Thực tế chỉ có 104 bit cho mã hóa (24 bit là IV).
* **Không đảm bảo tính toàn vẹn thông điệp:**
* CRC-32 không đủ mạnh: WEP sử dụng CRC-32 để kiểm tra lỗi dữ liệu, nhưng không có tính chất mật mã, dẫn đến khả năng giả mạo gói tin mà không bị phát hiện.
* Hacker có thể thay đổi dữ liệu (message tampering) mà không bị phát hiện, làm mất tính toàn vẹn của thông điệp.
* **Không bảo vệ chống lại tấn công Relay**
* WEP không có cơ chế bảo vệ chống lại các cuộc tấn công replay (tái sử dụng gói dữ liệu đã được truyền trước đó).
* **Quản lý khoá kém**
* Do đó không có cơ chế cập nhật khoá. WEP yêu cầu người dùng nhập khóa mã hóa chung (shared key) vào tất cả các thiết bị trong mạng, khóa này không thay đổi trừ khi được người dùng cập nhật thủ công
* Mọi thiết bị sử dụng chung một khóa.
* Khi một thiết bị bị xâm nhập, toàn bộ mạng bị nguy hiểm.
* **Sử dụng RC4 một cách không an toàn**
* RC4 là một thuật toán mạnh, nhưng WEP triển khai sai cách: WEP kết hợp IV và khóa cơ bản (shared key) để tạo ra khóa mã hóa. Tuy nhiên, nếu IV yếu, khóa mã hóa có thể bị đoán hoặc tấn công.

**Bài 3: Lập bảng tổng hợp các chuẩn mã hoá mạng không dây (tên, giải thuật mã hoá, đặc điểm, phương thức hoạt động, độ an toàn,…)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên chuẩn** | **Giải thuật mã hoá** | **Đặc điểm của chuẩn** | **Phương thức hoạt động** | **Độ an toàn** |
| 802.11a | |  | | --- | |  |   WEP, WPA, WPA2 (AES sau này) | - Ra đời năm 1999.  - Hoạt động ở băng tần 5 GHz.  - Tốc độ tối đa 54 Mbps.. | - Sử dụng OFDM để truyền dữ liệu.  - Dùng mã hoá AES | Phụ thuộc vào mã hóa: WEP (thấp), WPA/WPA2 (cao). |
| 802.11b | WEP, WPA, WPA2 | - Ra đời năm 1999.  - Hoạt động ở băng tần 2.4 GHz.  - Tốc độ tối đa 11 Mbps. | - Sử dụng kỹ thuật DSSS (Direct Sequence Spread Spectrum) để truyền dữ liệu. - Sử dụng WEP hoặc WPA để mã hoá | |  | | --- | |  |   Thấp - Trung bình: Băng tần dễ nhiễu, bảo mật phụ thuộc vào giao thức mã hóa. |
| 802.11g | WEP, WPA, WPA2 | - Ra đời năm 2003.  - Hoạt động ở băng tần 2.4 GHz.  - Tốc độ tối đa 54 Mbps. | - Kết hợp OFDM và DSSS.  - Tương thích ngược với chuẩn 802.11b. - Sử dụng AES hoặc TKIP để mã hoá | Trung bình - Cao: Hỗ trợ WPA2 nên an toàn hơn WEP/WPA. |
| 802.11i | WPA2 (AES-CCMP) | - Ra đời năm 2004, tập trung vào bảo mật.  - Yêu cầu sử dụng AES thay thế cho RC4/TKIP. | - Sử dụng giao thức CCMP (Counter Mode Cipher Block Chaining Message Authentication Protocol).  - Dùng AES trong CCMP để bảo mật | Cao: Được xem là chuẩn bảo mật mạnh mẽ. |
| 802.11n | WPA2, WPA3 | - Ra đời năm 2009.  - Hoạt động ở cả băng tần 2.4 GHz và 5 GHz.  - Tốc độ tối đa 600 Mbps. | - Sử dụng MIMO (Multiple Input Multiple Output) để tăng băng thông và giảm nhiễu tín hiệu. - Dùng nhiều kênh (MIMO) và AES để mã hoá | Cao: Hỗ trợ WPA2 và tương thích WPA3. |
| |  | | --- | | 802.16 (WiMAX) |  |  | | --- | |  | | AES-CCM | - Ra đời năm 2001.  - Phát triển để cung cấp truy cập Internet băng rộng không dây tầm xa.  - Tốc độ tối đa 70 Mbps. | - Sử dụng mã hóa AES với giao thức CCM (Counter with CBC-MAC) để bảo mật lưu lượng. - Dùng sóng vô tuyến để kết nối mạng | Cao: Tập trung vào bảo mật AES. |
| Bluetooth (Classic) | SAFER+, E0 | - Ra đời năm 1998.  - Tốc độ thấp (1-3 Mbps).  - Dùng cho kết nối cá nhân (short-range communication). | - Sử dụng mã hóa SAFER+ hoặc E0 để bảo vệ dữ liệu truyền qua giao tiếp không dây. | Thấp - Trung bình: Các phiên bản cũ dễ bị tấn công. |
| Bluetooth  (LE) | AES-CCM | - Ra đời năm 2010 (Bluetooth 4.0).  - Tối ưu cho năng lượng thấp (low-energy) với tốc độ ~1 Mbps. | - Sử dụng mã hóa AES-128 CCM để đảm bảo tính toàn vẹn và bảo mật dữ liệu. | Cao: Tốt hơn Bluetooth Classic nhờ sử dụng AES. |