Contents

[1. Tổng quan 1](#_Toc155369512)

[2. Phân loại 2](#_Toc155369513)

[3. Các kiểu chứng thực 3](#_Toc155369514)

[4. WEP, WPA và WPA2 4](#_Toc155369515)

[ WEP 4](#_Toc155369516)

[ WAP 5](#_Toc155369517)

[ WPA2 7](#_Toc155369518)

[ Phân biệt WEP, WPA và WPA2: 9](#_Toc155369519)

[ Các vấn đề của WEP 9](#_Toc155369520)

[ IV(initialization vector-Vector khởi tạo) yếu 10](#_Toc155369521)

[5. Các mối đe doạ 10](#_Toc155369522)

[6. Phương pháp tấn công 10](#_Toc155369523)

[7. Công cụ tấn công 10](#_Toc155369524)

[8. Tấn công mạng Bluetooth 10](#_Toc155369525)

[9. Biện pháp phòng chống 10](#_Toc155369526)

[10. Công cụ bảo mật Wi-fi 10](#_Toc155369527)

[11. Kiểm thử hệ thống 10](#_Toc155369528)

# 1. Tổng quan

* Wi-Fi is developed on IEEE 802.11 standards, and it is widely used in wireless communication. It provides wireless access to applications and data across a radio network.
* Wi-Fi sets up numerous ways to build up a connection between the transmitter and the receiver such as DSSS, FHSS, Infrared (IR) and OFDM.
* Advantages
* Installation is fast and easy and eliminates wiring through walls and ceilings.
* It is easier to provide connectivity in areas where it is difficult to lay cable.
* Access to the network can be from anywhere within range of an access point.
* Public places like airports, libraries, schools or even coffee shops offer you constant Internet connection using Wireless LAN
* Disadvantages:
* Security is a big issue and may not meet expectations.
* As the number of computers on the network increases, the bandwidth suffers.
* Wi-Fi standards changed which results in replacing wireless cards and/or access points.
* Some electronic equipment can interfere with the Wi-Fi networks.

# 2. Phân loại

Các loại mạng không dây:

* Extension to a Wired Netword
* Multiple Access Points
* LAN-to-LAN Wireless Network
* 3G Hotspot

Chuẩn mạng không dây:

* 802.11a: Bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz
* 802.11b: Bandwidth up to 11 Mbps, and uses the unregulated radio signaling frequency (2.4 GHz)
* 802.11g: Bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range
* 802.11i: A standard for Wireless Local Area Networks (WLANs) that provides Improved encryption for networks that use 802.11a, 802.11b and 802.11g standards
* 802.11n: Uses multiple input, multiple output (MIMO) technology to give Wi-Fi more speed (over 100Mbps) and range
* 802.16: A group of broadband wireless communications standards for Metropolitan Area Networks (MANs)
* Bluetooth: Supports a very short range (~10 meters) and relatively low bandwidth (1-3 Mbps) designed for low-power network devices like handhelds

Service Set Identifier (SSID):

* SSID is a token to identify a 802.11 (Wi-Fi) network: by default it is the part of the packet header sent over a wireless local area network (WLAN).
* The SSID remains secret only on the closed networks with no activity, that is inconvenient to the legitimate users.
* It acts as a single shared identifier between the access points and clients
* SSID access points broadcasts the radio signals continuously received by the client machines if enabled
* Security concerns arise when the default values are not changed, as these units can be compromised
* A key management problem is created for the network administrator, as SSID is a secret key instead of a public key
* A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any"
* If the SSID of the network is changed, reconfiguration of the SSID on every network is required, as every user of the network configures the SSID into their system

# 3. Các kiểu chứng thực

Chế độ xác thực Wi-Fi:

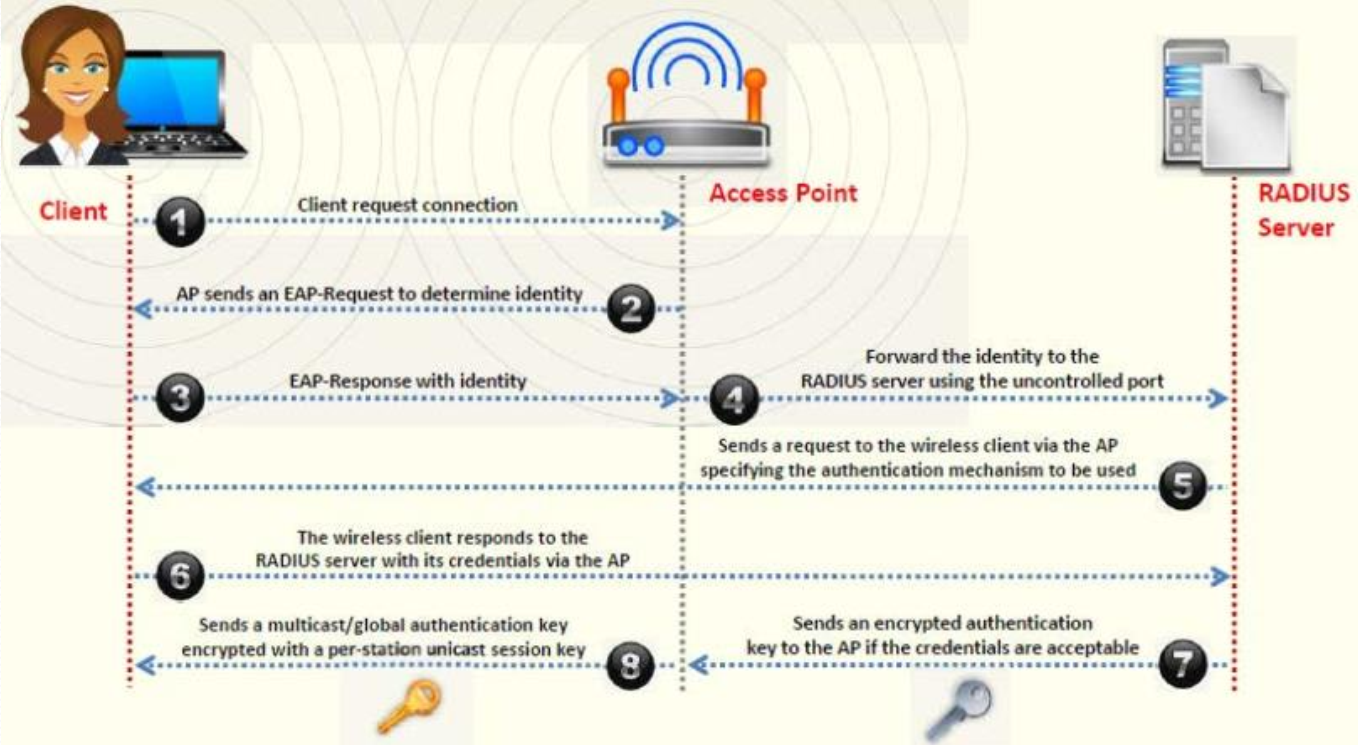
* Open System Authentication Process

1. Client sends an 802.11 authentication management frame that contains its SSID
2. AP checks the client’s SSID and sends back an authentication verification frame
3. Client connects to network

* Shared Key Authentication Process

1. Authentication request sent to AP
2. AP sends challenge text
3. Client encrypts challenge text and sends it back to AP
4. AP decrypts, and if correct, authenticates client
5. Client connects to network

Quy trình xác thực Wi-Fi bằng máy chủ xác thực tập trung



Các loại kết nối không dây:

* WEP: It is an old and original wireless security standard which can be cracked easily
* TKIP: A security protocol used in WPA as a for replacement WEP
* LEAP: It is a proprietary WLAN authentication protocol developed by Cisco
* RADIUS: It is a centralized authentication and authorization management system
* 802.11i: It is an IEEE standard that specifies security mechanisms for 802.11 wireless networks
* WPA: Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security
* WPA2: WPA2 uses AES (128 bit) and CCMP for wireless data encryption
* WPA2 Enterprise: It integrates EAP standards with WPA encryption
* AES: It is a symmetric-key encryption, used in WPAZ as a replacement of TRIP
* EAP: Uses multiple authentication methods such as token cards, Kerberos, certificates etc
* CCMP: CCMP utilizes 128-bit keys, with a 48-bit Initialization vector (TV) for replay detection

# 4. WEP, WPA và WPA2

## WEP

* Wired Equivalent Privacy (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions.
* WEP uses 24-bit Initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission.
* 64-bit WEP uses a 40-bit key
* 128-bit WEP uses a 104-bit key size
* 256-bit WEP uses 232-bit key size
* It was developed without:
* Academic or public review
* Review from cryptologists
* WEP Flaws: It has significant vulnerabilities and design flaws

Cách WEP hoạt động:

A diagram of a computer

Description automatically generated

1. A 32-bit Integrity Check Value (ICV) is calculated for the frame data

2. The ICV is appended to the end of the frame data

3. A 24-bit Initialization Vector (IV) is generated and appended to the WEP encryption key

4. The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream

5. The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data

6. The IV is added to the encrypted data and ICV to generate a MAC frame

## WAP

Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards

It improves on the authentication and encryption features of WEP (Wired Equivalent Privacy)

TKIP (Temporal Key Integrity Protocol):

* TKIP utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication
* TKIP mitigates the WEP key derivation vulnerability by not reusing the same Initialization Vector

128-bit Temporal Key

* Under TKIP, the client starts with a 128-bit “temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a key that is used to encrypt data via the RC4
* It implements a sequence counter to protect against replay attacks

WPA Enhances WEP

* TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys
* Temporal keys are changed for every 10,000 packets. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

Cách hoạt động của WPA:

A computer screen shot of a diagram

Description automatically generated

1. Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to RC4 algorithm to generate a Keystream
2. MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using Michael algorithm
3. The combination of MSDU and MIC is fragmented to generate frame MAC Protocol Data Unit (MPDU) WFP
4. A 32-bit Integrity Check Value (ICV) is calculated for the MPDU
5. The combination of MPDU and ICV is bitwise XORed with Keystream to produce the encrypted data
6. The IV is added to the encrypted data to generate MAC

Temporal Keys:

* In WPA and WPA2, the encryption keys (temporal keys) are derived during the four-way handshake
* Encryption keys are derived from the PMK that is derived during the EAP authentication session
* In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK PTK

A diagram of a network

Description automatically generated

1. AP sends an ANonce to client which uses it to construct the Pairwise Transient Key (PTK)
2. Client respond with its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC)
3. AP sends the GTK and a sequence number together with another MIC which is used in the next broadcast frames
4. Client confirm that the temporal keys are installed

## WPA2

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control

Provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm

WPA2-Personal:

* WPA2-Personal uses a set-up password (Pre-shared Key, PSK) to protect unauthorized network access
* In PSK mode each wireless network device encrypts the network traffic using a 256 bit key which can be entered as a passphrase of 8 to 63 ASCII characters

WPA2-Enterprise

* It includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc.
* Users are assigned login credentials by a centralized server which they must present when connecting to the network

Cách WPA2 hoạt động:

* In the CCMP procedure, additional authentication data (AAD) is taken from the MAC header and included in the CCM encryption process. This protects the frame against alteration of the non- encrypted portions of the frame
* A sequenced packet number (PN) is included in the CCMP header to protect against replay attacks. The PN and portions of the MAC header are used to generate a nonce that in turn is used by the CCM encryption process

A diagram of a computer program

Description automatically generated

## Phân biệt WEP, WPA và WPA2:

A screen shot of a computer program

Description automatically generated

(Encryption Algorithm: thuật toán mã hóa

Integrity Check Mechanism: Cơ chế kiểm tra tính toàn vẹn)

## Các vấn đề của WEP

* The IV is a 24-bit field Is too small and is sent in the cleartext portion of a message
* Identical key streams are produced with the reuse of the same IP for data protection, as the IV is short key streams are repeated within short time
* Lack of centralized key management makes it difficult to change the WEP keys with any regularity
* When there is IV Collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet
* IV is a part of the RC4 encryption key, leads to a analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic
* Use of RC4 was designed to be a one-time cipher and not intended for multiple message use
* No defined method for encryption key distribution
* Wireless adapters from the same vendor may all generate the same [V sequence. This enables attackers to determine the key stream and decrypt the ciphertext
* Associate and disassociate messages are not authenticated
* WEP does not provide cryptographic integrity protection. By capturing two packets an attacker can flip a bit in the encrypted stream and modify the checksum so that the packet is accepted
* WEP is based on a password, prone to password cracking attacks
* An attacker can construct a decryption table of the reconstructed key stream and can use it to decrypt the WEP Packets in real-time

## IV(initialization vector-Vector khởi tạo) yếu

* In the RC4 algorithm, the Key Scheduling Algorithm (KSA) creates an IV based on the base key => The IV value is too short and not protected from reuse and no protection again message replay
* A flaw in the WEP implementation of RC4 allows “weak” IVs to be generated => The way keys are constructed from the IV makes it susceptible to weak key attacks (9FMS attack)
* Those weak IVs reveal information about the key bytes they were derived from => No effective detection of message tampering (message integrity)
* An attacker will collect enough weak IVs to reveal bytes of the base key=> It directly uses the master key and has no built-in provision to update the keys

# 5. Các mối đe doạ

# 6. Phương pháp tấn công

# 7. Công cụ tấn công

# 8. Tấn công mạng Bluetooth

# 9. Biện pháp phòng chống

# 10. Công cụ bảo mật Wi-fi

# 11. Kiểm thử hệ thống