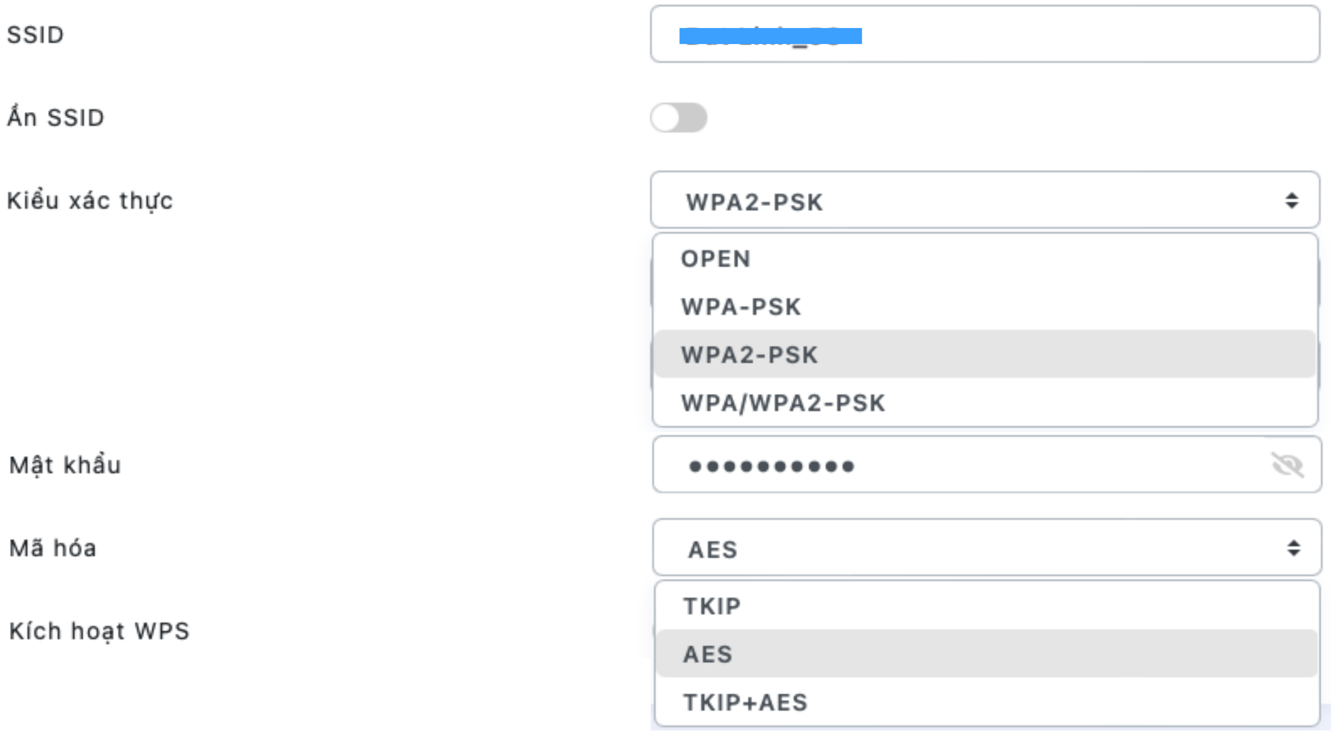
CRYPTOGRAPHY & APPLICATION

Wireless Security

Group 2 - 19MMT



SSID [redacted]

Ẩn SSID

Kiểu xác thực WPA2-PSK

Mật khẩu ●●●●●●●●●●●

Mã hóa AES

Kích hoạt WPS

OUR TEAM

Tran Thien Phuc

19127245

Tran Anh Quan

19127251

Trieu Nguyen Minh Huy

19127424

Tang Thanh Quang

19127531

TABLE OF CONTENTS

01

WEP

One of the first security protocols for Wi-Fi

02

WPA

A temporary solution to overcome the vulnerabilities of 802.11 in 2003

03

WPA2

Security update of WPA

04

RSN

Robust Security Network

01

WEP

One of the first security protocols for Wi-Fi

HISTORY OF WEP

- Introduced in 1977
- The first attempt at wireless protection
- Add security to wireless networks by encrypting data

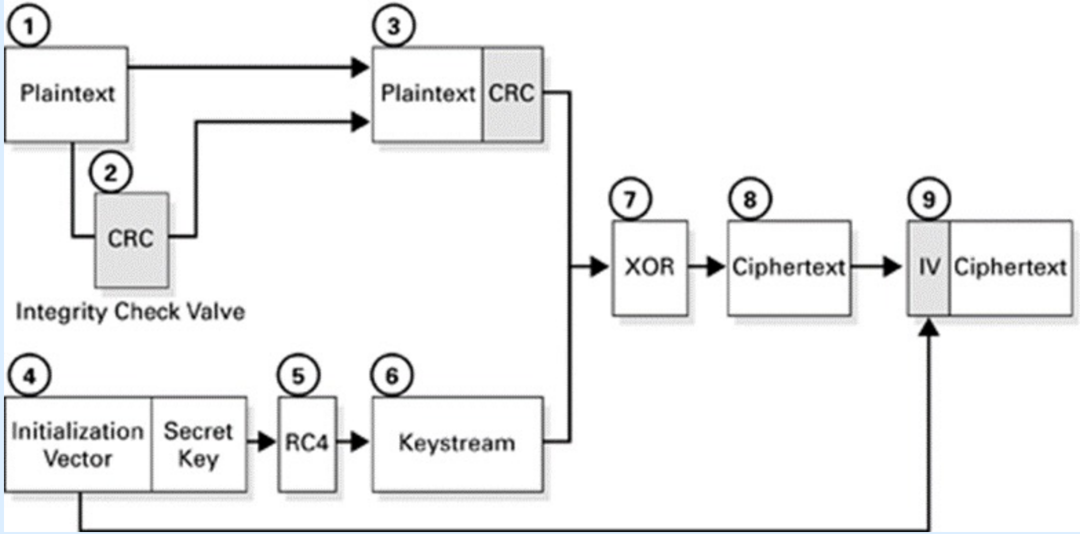
HOW IT WORKS?

1. Generate Initialization Vector

- Ensure that the value used as a seed for the RC4 PRNG is always different
- There is no guidance on how to implement IVs
- Forced to repeat IVs, and violate RC4’s cardinal rule of never repeating keys

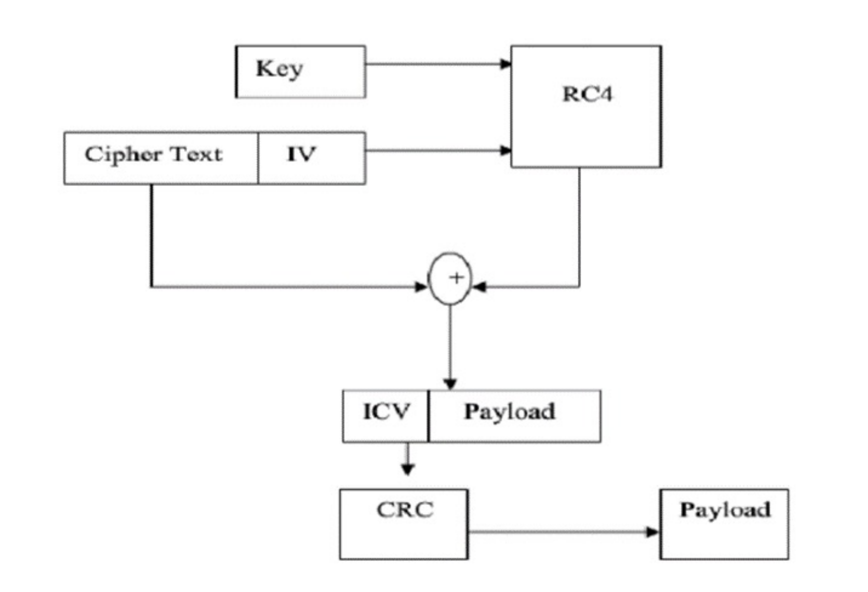
HOW IT WORKS?

2. Encryption



HOW IT WORKS?

3. Decryption

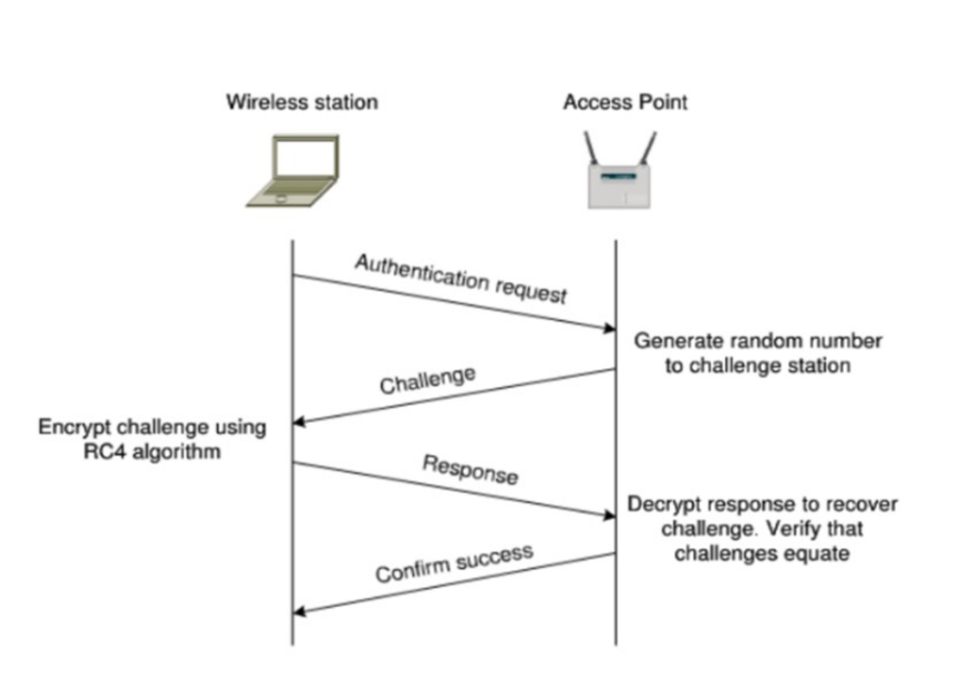


HOW IT WORKS?

4. Authentication

In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake:

- The client sends an authentication request to the Access Point.
- The Access Point replies with a clear-text challenge.
- The client encrypts the challenge-text using the configured WEP key and sends it back in another authentication request.
- The Access Point decrypts the response. If this matches the challenge text, the Access Point sends back a positive reply.


Wireless station
Access Point
Authentication request
Generate random number to challenge station
Challenge
Encrypt challenge using RC4 algorithm
Response
Decrypt response to recover challenge. Verify that challenges equate
Confirm success

ADVANTAGE AND DISADVANTAGE

Advantage

1. All wireless devices support basic WEP encryption
2. Self-synchronization
3. Computational and resource optimization

Disadvantage

1. Reused IV
2. Weak keys are susceptible to attack
3. Message integrity checking is ineffective

02

WPA

A temporary solution to overcome the vulnerabilities of 802.11 by the end of 2003

WPA TO THE RESCUE!

TKIP (Temporal Key Integrity Protocol)

addresses these weaknesses:

Replay attacks

IVs can be used out of order

Forgery attacks

ICV using 32-bit CRC is linear and can be manipulated

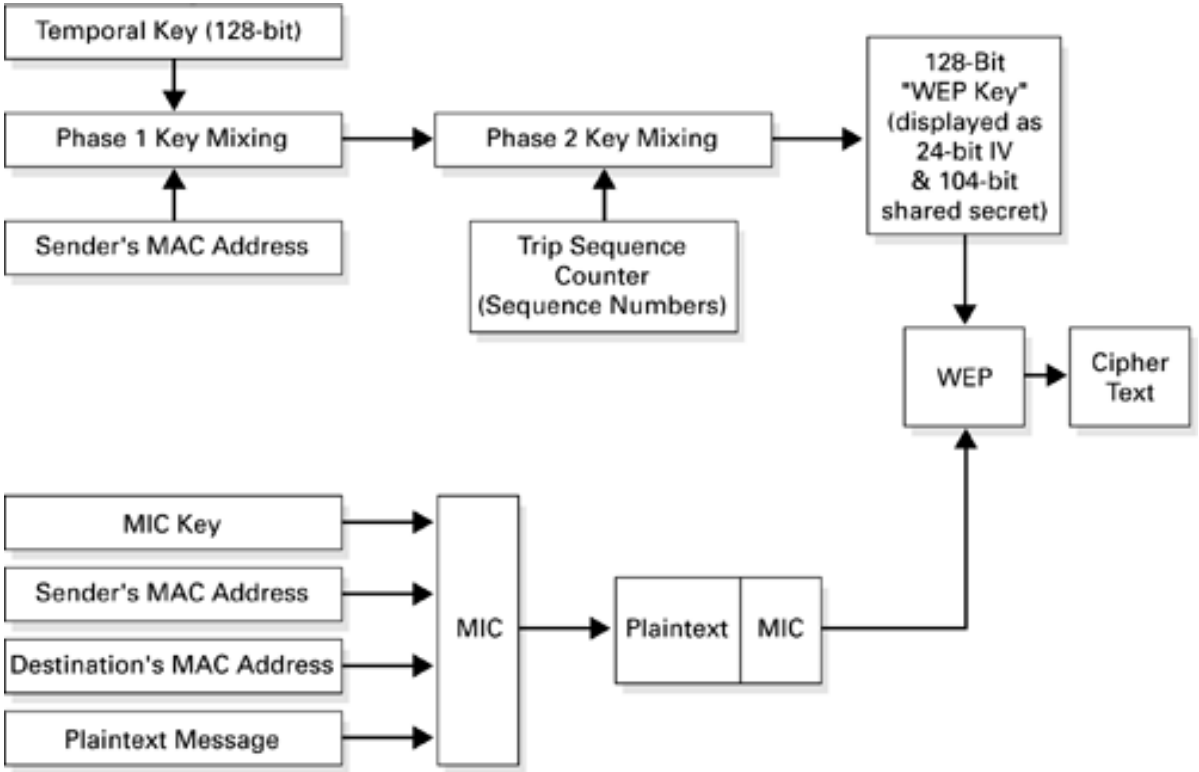
Key collision attacks

IV collisions

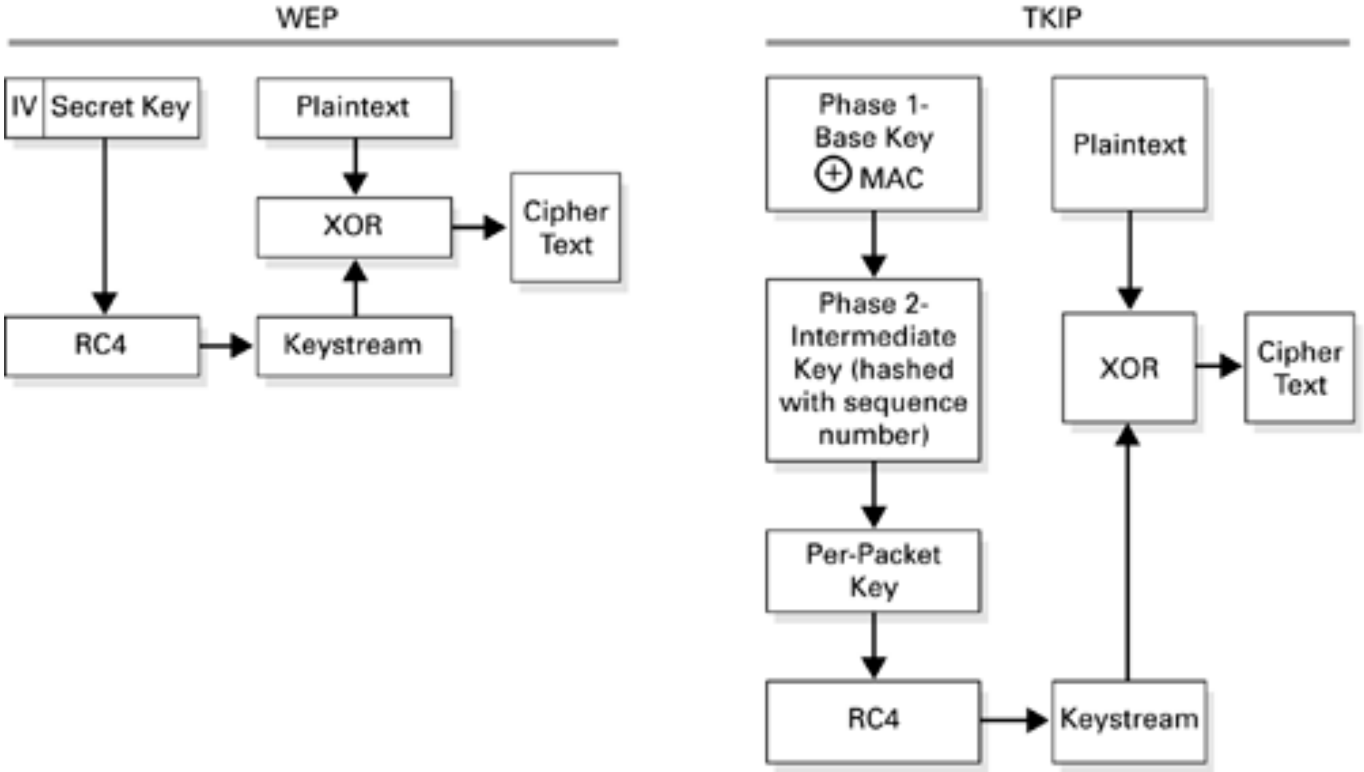
Weak key attacks

RC4 stream cipher is vulnerable to FMS attacks

TKIP IN DETAIL

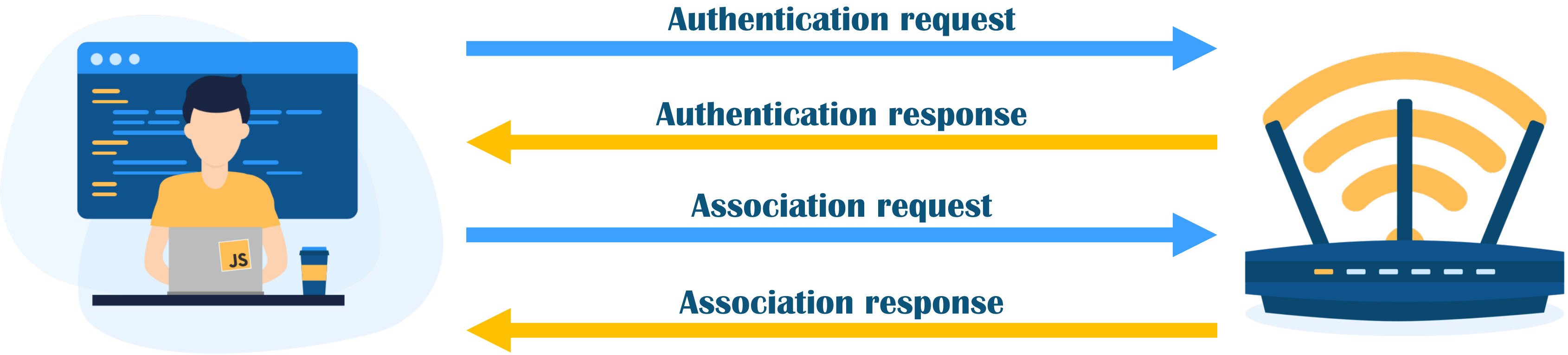


PER-PACKET KEY MIXING



KEY MANAGEMENT IN WPA

4-way handshake



Authentication request

Authentication response

Association request

Association response

ATTACK STEPS

Step 1

Enable observation mode

Step 2

Find the network and the clients connected to it

Step 3

Perform a dictionary attack

03

WPA2

Security update of WPA

INTRODUCTION

To overcome limitations of **WPA**, a long-term solution is to quickly develop a better security standard, more closely following the IEEE 802.11i standard, which is the **WPA2** (Wi-Fi Protected Access 2) standard, which is supported by Wi-Fi. -Fi Alliance officially replaced WPA in 2006.

HOW IT WORKS?

Like WPA, WPA2 is designed for security on all 802.11b, 802.11a, 802.11g and 802.11n versions supporting multi-channel, multi-mode and allowing implementation over IEEE 802.11X/EAP or PSK.

It increases data security, controls network access, and overcomes all the weaknesses of WEP and WPA.

COMPARISON WITH WPA

WPA

Uses **TKIP** (Temporal Key Integrity Protocol) for encryption and **Michael's algorithm** for ensuring the integrity of each data packet

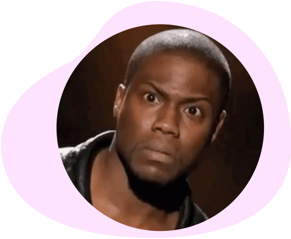
WPA2

Uses **AES** to ensure confidentiality, data integrity and uses **CCMP** for data encryption and packet integrity checking

DISADVANTAGES OF WPA2

WPA2 requires hackers to have access to a Wi-Fi network first before they can hack into other clients on the same network.

Hackers only need to be within range of the device to be able to use the Key Reinstallation Attack (KRACK) method to penetrate the connection between the device and the hotspot.



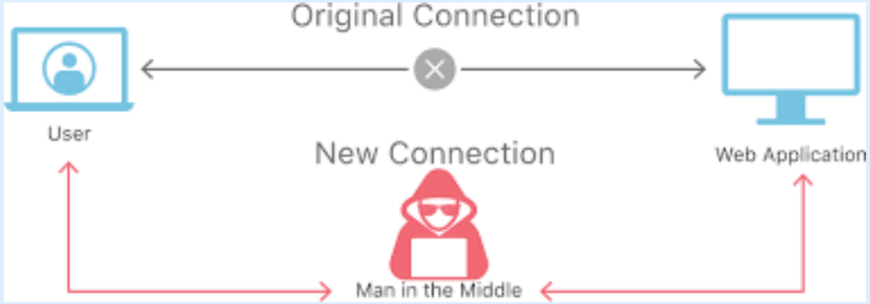
Hackerman

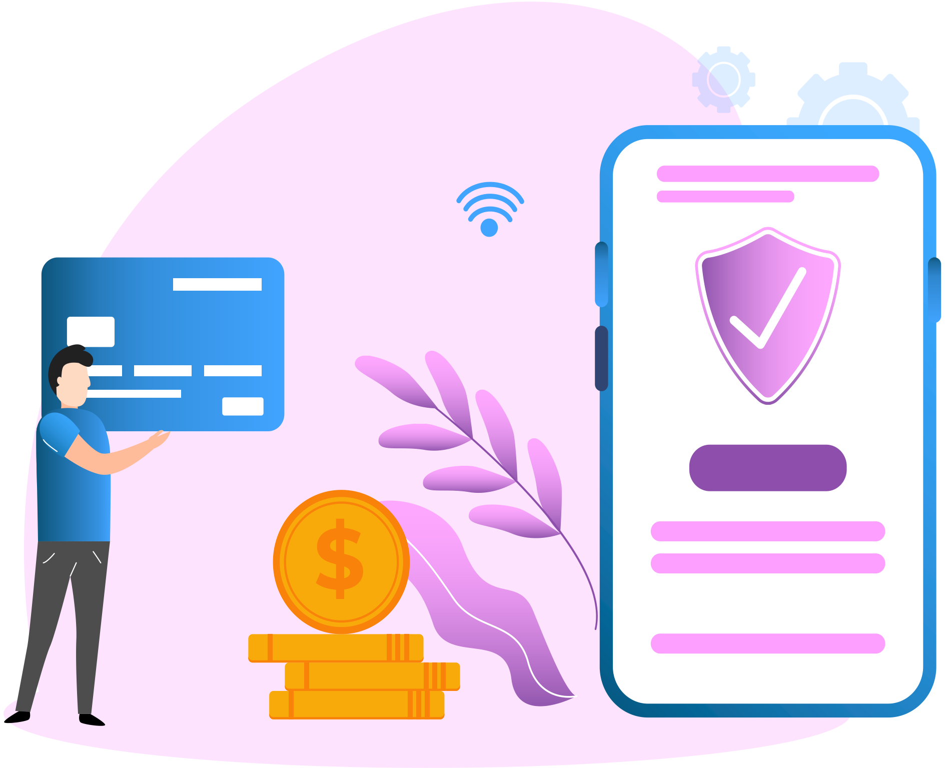
Why your Internet so slow?

Key Reinstallation Attack

KRACK undermines an important aspect of WPA2's **4-way handshake**, allowing hackers to intercept and manipulate the generation of new encryption keys during a secure connection.

This approach allows an attacker to read any information that is supposedly encrypted.





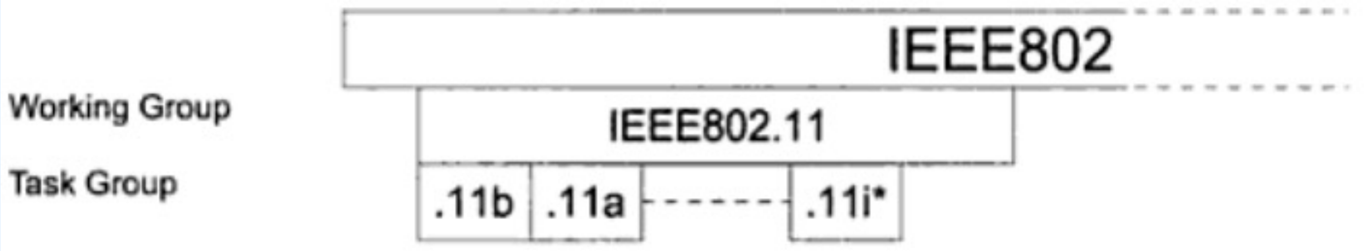
04

RSN

Robust Security Network

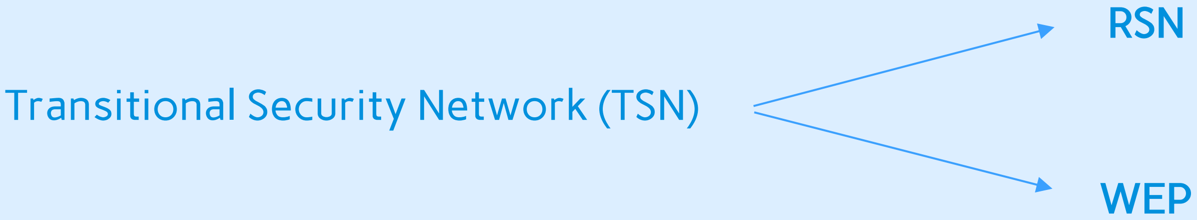
802.11 foundation

IEEE (Institute of Electrical and Electronics Engineers) created a group called SA (Standards Association) . IEEE-SA have responsible for creating 802 standards .



802.11 foundation

IEEE 802.11i define new wireless network called Robust Security Network. **RSN** is the same as **WEP**.



Transitional Security Network (TSN)

RSN

WEP

Definition

The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as **WPA2**, also called **RSN** (Robust Security Network)

Those keys will be created after authentication process so they called **temporal keys** and **session key** . Besides, they constantly update by the time and will be deleted when the "*safe situation"* closed .

Unlike **WEP**, **RSN** have many keys inside key architecture and most of them will not be known until the authentication process ends .

COMPARISON WITH WPA

Share architecture

WPA

Focus on TKIP

Specifically on one way to implement a network

More

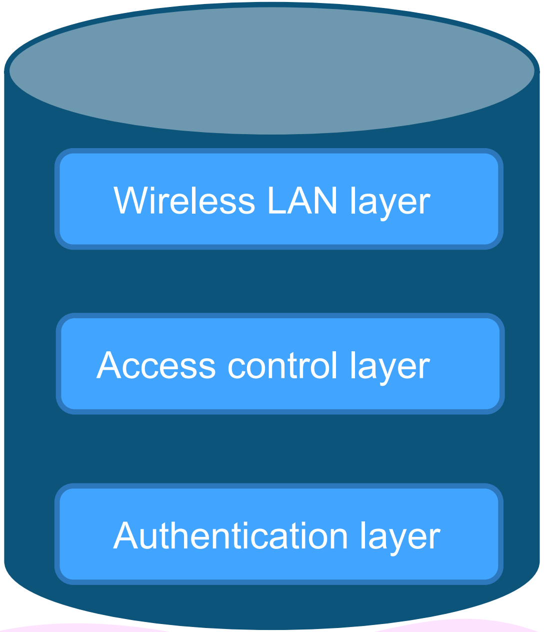
Flexibility

RSN

Supports AES and TKIP encryption algorithms

Available ad-hoc mode

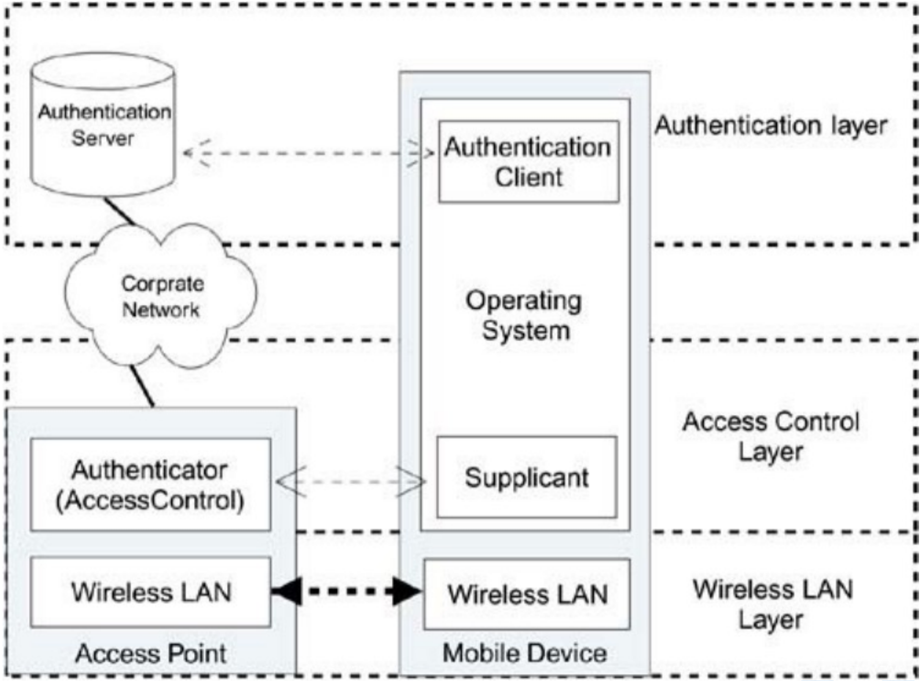
Security Layer



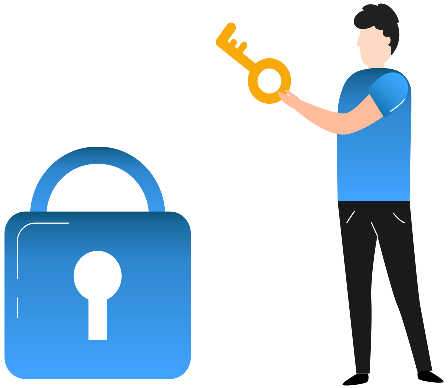
Wireless LAN layer

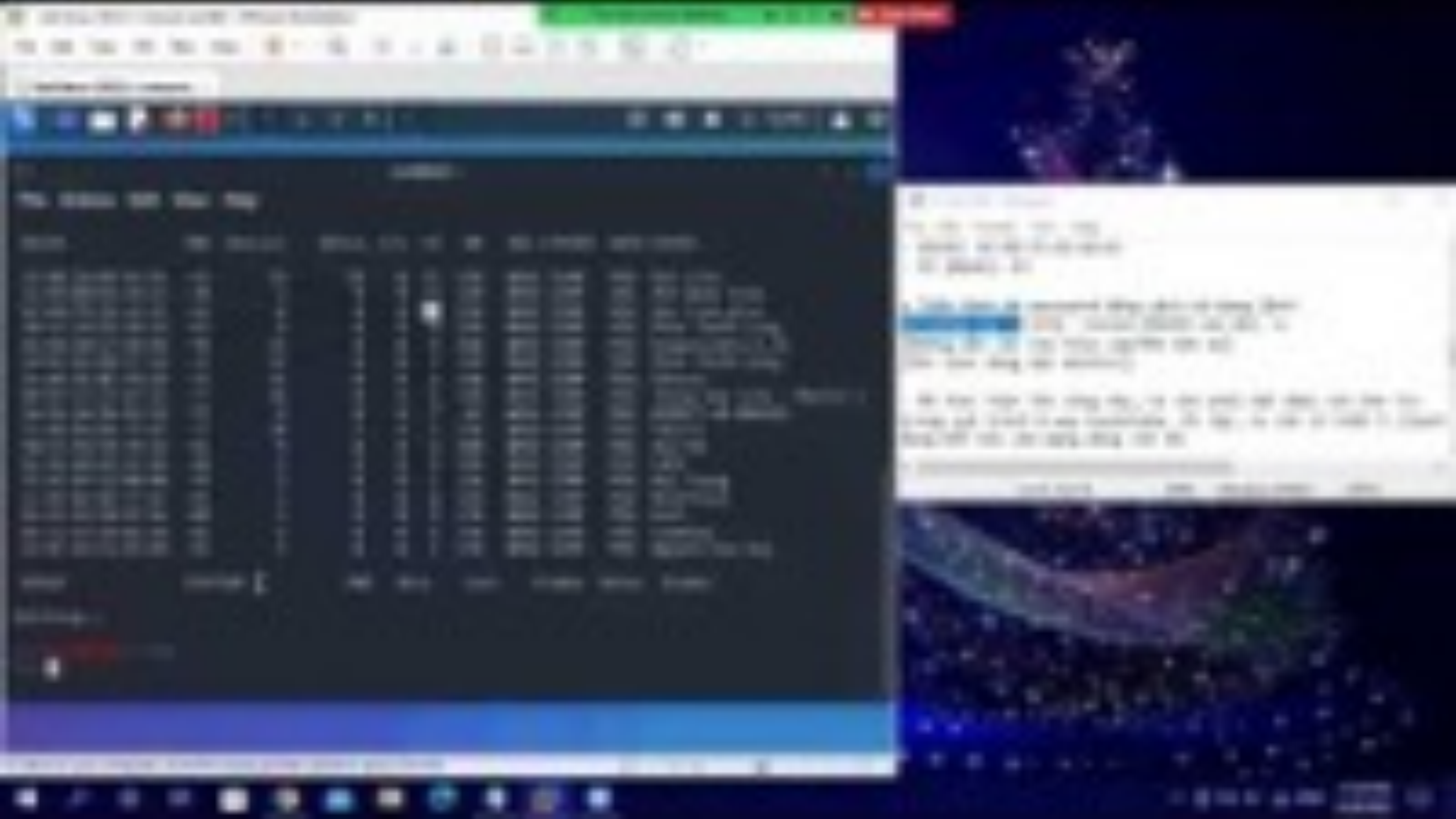
Access control layer

Authentication layer



DEMO
ATTACK WPA/WPA2





RESOURCES

REFERENCES

1. Barken, L. (2004). How secure is your wireless network?: Safeguarding your wi-fi-lan. Prentice Hall PTR.
2. Nguyễn Hiếu Minh (FIT - MTA). Slide: An ninh mạng không dây (IEEE 802.11).
3. Nguyễn Hoàng Việt. (6.2015). Giải pháp đảm bảo an toàn mạng không dây theo chuẩn 802.11I
4. Wiki IEEE 802.11i-2004.
5. An Nhiên. (10.2017). WPA2 là gì? WPA2 đã bị hack như thế nào?
6. Wired Equivalent Privacy – Wikipedia.
7. Advantages and Disadvantages of WEP WPA Network Security - Bright Hub.
8. Ad-hoc network Wiki.

PHOTOS

Barken, L. (2004). How secure is your wireless network?: Safeguarding your wi-fi-lan. Prentice Hall PTR.

VECTORS

- Slidesgo.com
- Delesign.com

THANKS!

Do you have any questions?

See our report at: https://hackmd.io/@mhud/mmt_group2

Our demo video: https://youtu.be/BKpCf0WzZcg