

Network Security

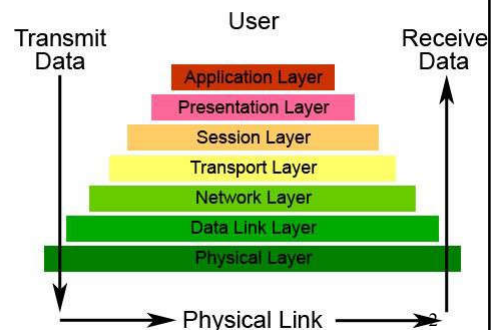
Security in Physical Layer

1

Fundamentals of physical layer security

- Many people who study networking get the impression that the physical layer is only about actual network hardware.
- PHY contains
 - Definition of Hardware Specifications
 - Encoding and Signaling
 - Data Transmission and Reception
 - Topology and Physical Network Design

The Seven Layers of OSI



2

Fundamentals of physical layer security

- In all communication systems, the issues of authentication, confidentiality, and privacy are handled in the **upper** layers of the protocol stack using variations of private-key and public-key cryptosystems.
- Nowadays, many results from information theory, signal processing, and cryptography suggest that there is much security to be gained by accounting for the imperfections of the **physical layer** when designing secure systems.



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

3

3

Fundamentals of physical layer security

- For example, while noise and fading are usually treated as impairments in wireless communications, information-theoretic results show that they can be harnessed to “**hide**” messages from a potential eavesdropper or authenticate devices, without requiring a additional secret key.
- Such results, if they can be implemented in a cost-efficient way without sacrificing much data rate, call for the design of security solutions at the physical layer to complement communications security mechanisms.

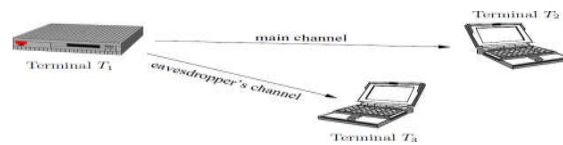


VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

4

4

Fundamentals of physical layer security



The communication between terminals T1 and T2 is being eavesdropped by an unauthorized terminal T3.

When terminals T2 and T3 are not collocated, radiofrequency signals observed at the outputs of the main channel and eavesdropper's channel are usually different.

Natural discrepancies are caused by physical phenomena, and for wireless communications, the most notable effects are fading and path-loss.

For instance, if T1 broadcasts a video stream, the signal obtained by T3 may be significantly degraded compared to the one received by T2; this degradation can even prevent T3 from understanding the content of the video stream.



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

5

5

Physical Layer threats

- Networks are made up of devices and communication links
- Devices and links can be physically threatened
- Vandalism, lightning, fire, excessive pull force, corrosion, wildlife, wear-down, wiretapping, crosstalk, jamming
- We need to make networks mechanically resilient and trustworthy



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

6

How can two computers communicate?



- Encode information into physical “signals”
- Transmit those signals over a transmission medium



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

7

Types of Media

- Metal (e.g., copper): wired
- EM/RF (e.g., IEEE 802.11): wireless
- Light (e.g., optical fiber)

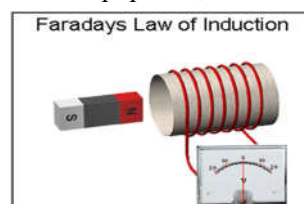
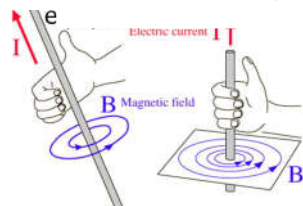


VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

8

Noise, Jamming, and Information Leakage

- When you move a conductor through a magnetic field, electric current is induced (*electromagnetic induction*)
 - EMI is produced from other wires, devices
 - Induces current fluctuations in conductor
 - Problem: *crosstalk*, conducting noise to equipment, etc

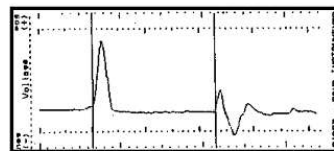


9

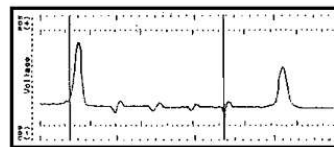
Eavesdropping on copper cables



Faulty Amplifier



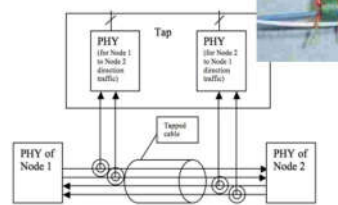
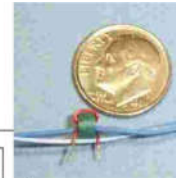
Wire Tap



10

Physical Tapping

- Conductive Taps
 - Form conductive connection with cable
- Inductive Taps
 - Passively read signal from EM induction
 - No need for any direct physical connection
 - Harder to detect
 - Harder to do with non-electric conductors (e.g., fiber optics)



11

Fundamentals of physical layer security

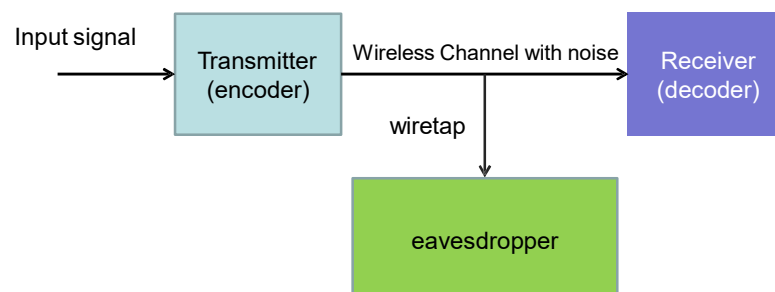


Fig. 1 Wiretap channel model



12

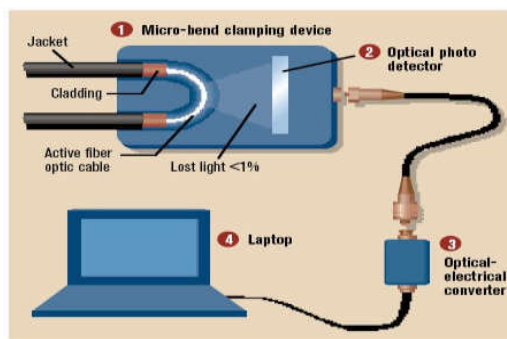
12

Fundamentals of physical layer security

- The common secure communication framework does not account for the physical reality of communication channels.
- Especially, it does not consider the degradation of signals because of noise or fading.
- This observation naturally leads to the introduction of a more realistic communication model, now known as the wiretap channel, where noise in the main channel and eavesdropper's channel is explicitly introduced.

13

Eavesdropping on optical cables



14

Case Study: Submarine Cable

- 1970: U.S. learned of **USSR** undersea cable
 - Connected Soviet naval base to fleet headquarters
- Joint US Navy, NSA, CIA operation to tap cable in 1971
- Saturation divers installed a 3-ft long tapping device
 - Coil-based design, wrapped around cable to register signals by induction
 - Signals recorded on tapes that were collected at regular intervals
 - Communication on cable was unencrypted
 - Recording tapes collected by divers monthly



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

15

Case Study: Submarine Cable

- 1972: Bell Labs develops next-gen tapping device
 - 20 feet long, 6 tons, nuclear power source
- No detection for over a **decade**
 - Compromise to Soviets by Robert Pelton, former employee of NSA
- Cable-tapping operations continue
 - Tapping expanded into Pacific ocean (1980) and Mediterranean (1985)
 - USS Parche refitted to accommodate tapping equipment, presidential commendations every year from 1994-97
 - Continues in operation to today, but targets since 1990 remain classified

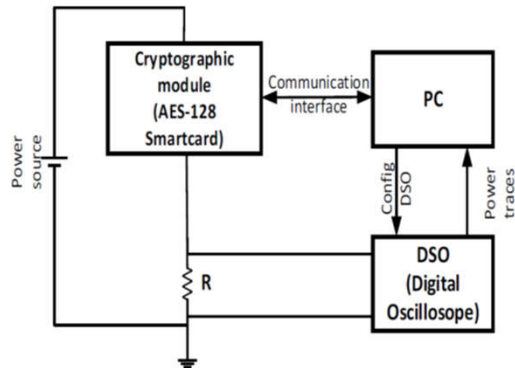


VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

16

Power analysis attacks

- Power consumption traces are recorded during the execution of the cryptosystem using a high-speed oscilloscope
 - SPA
 - CPA
 - DPA
 - SCA



17

SPA - Simple Power Analysis

if $b = 0$ then $r = \text{op1}(x)$ else $r = \text{op2}(x)$

- If the power consumptions for operations op1 and op2 are different (amplitude/duration), the recorded power traces show differences for $b = 0$ and $b = 1$. If b is a **secret key bit**, the power trace directly “shows” the value of b on the oscilloscope

18

Protection method - countermeasures

- Hiding is to make the power consumption independent of the intermediate values manipulated and intermediate operations performed in the device.
 - This can be done using a device and/or algorithms with a random power consumption (e.g. random dummy operations, random shuffling of operations).
 - This can also be done using a device, algorithms and data representations where the power consumption is always the same for all operations and for all manipulated values.

DPA - Differential Power Analysis

- When differences are too small (weak signal and/or noisy environment), simple power analysis does not work anymore. Then, statistical methods have to be used to extract secret information using a large amount of power traces
- The set of power traces is analyzed and compared to a theoretical power model of the cryptosystem

Preventing DPA

- Reduce signal sizes
 - cannot reduce the signal size to zero
- Introduce noise into power consumption measurements
- Nonlinear key update procedures can be employed to ensure that power traces cannot be correlated between transactions
 - Hash a 160-bit key with SHA should destroy partial information an attacker might have gathered about the key



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

21

CPA - Correlation Power Analysis

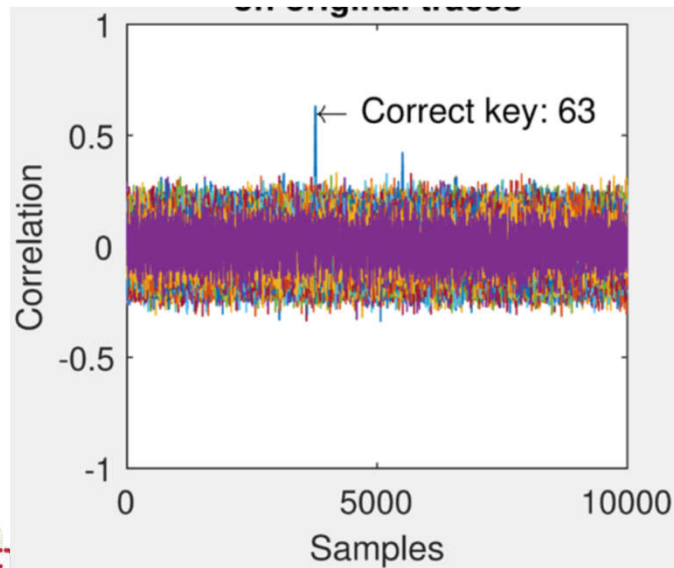
- Step 1: Choose a model for the target's power consumption.
- Step 2. Get some different plaintexts of the target. (Record every power trace of the target's power consumption)
- Step 3. For all possible options for the key, use the plaintexts of step 2 and the key to calculate the intermediate value of target and then the power consumption according to the model.
- Step 4. Calculate the Pearson correlation coefficient between the modeled power consumption of step 3 and the real power consumption of step 2.

$$r_{i,j} = \frac{\sum_{d=1}^D [(h_{d,i} - \bar{h}_i)(t_{d,j} - \bar{t}_j)]}{\sqrt{\sum_{d=1}^D (h_{d,i} - \bar{h}_i)^2 \sum_{d=1}^D (t_{d,j} - \bar{t}_j)^2}}$$



22

CPA attack on original traces



23

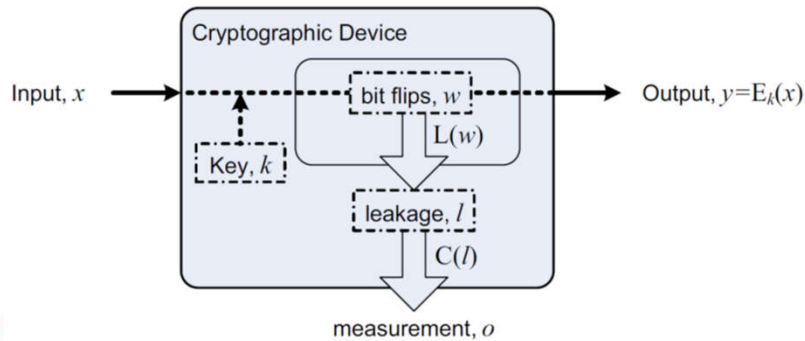
Preventing CPA

- Masking: make random the intermediate values processed by the cryptosystem
 - Intermediate values are combined with a random mask which changes from execution to execution
 - The cryptosystem has to be modified to integrate masking and unmasking operations

24

SCA - Side Channel Attacks

- During the computation of the device, intermediate values depending on the input x and unknown key k are changed and lead to some bit flips modeled by w
- Changing the internal states of the target device leaks through a side-channel leakage function $L(w) = I$



25

TDR - Time Domain Reflectometry

- The instrument measures the time between emission and reception which is proportional to the distance
 - Pulses of low power microwaves are sent along the conductors - rods or cables
 - At the point where the waves meet the product surface, the waves are reflected by the product
 - The intensity of the reflection depends on the dielectric constant of the product



26

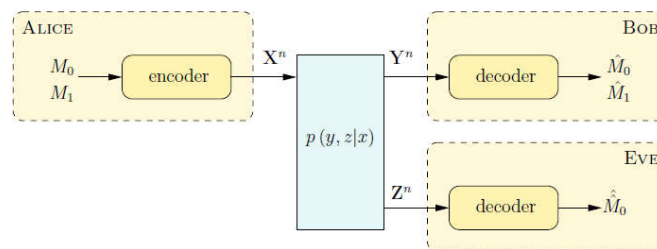
Tapping Cable: Countermeasures

- Physical inspection
- Physical protection
 - E.g., encase cable in pressurized gas
- Use faster bitrate
- Monitor electrical properties of cable
 - TDR: sort of like a hard-wired radar
 - Power monitoring, spectrum analysis

25

27

Fundamentals of physical layer security

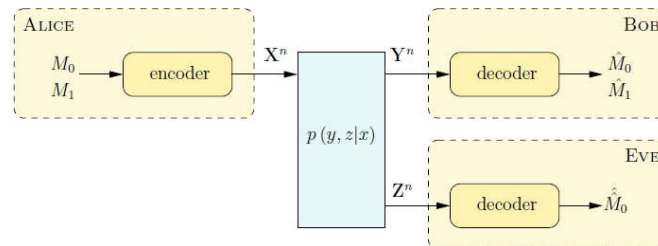


It is also assumed that Alice wishes to send a common message M_0 to both Bob and Eve and a private message M_1 to Bob only. In the PLS, the common objective is to maximize the the secrecy capacity, which is usually defined as the data rate of confidential messages.

28

28

Fundamentals of physical layer security

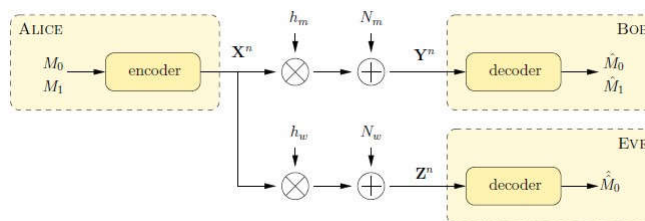


Essentially,

1. Z should provide no information about M1
2. Y can be decoded into M with negligibly small probability of error

29

Fundamentals of physical layer security



Secrecy Capacity of Gaussian Wiretap Channel

$$C_s = \begin{cases} \frac{1}{2} \log_2 \left(1 + \frac{h_m^2 P}{\sigma_m^2} \right) - \frac{1}{2} \log_2 \left(1 + \frac{h_w^2 P}{\sigma_w^2} \right) & \text{if } \frac{h_m^2 P}{\sigma_m^2} > \frac{h_w^2 P}{\sigma_w^2}, \\ 0 & \text{otherwise.} \end{cases}$$

30

Fundamentals of physical layer security

- To achieve security in PHY, there are multiple approaches,
 - Preprocessing Scheme
 - Coding
 - Key generation
 - Artificial Noise Scheme
 - Game Theortic Scheme
 - Signal Processing
 - Cooperation Communications
 - Many others



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

31

31



SOICT

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Security in WLAN

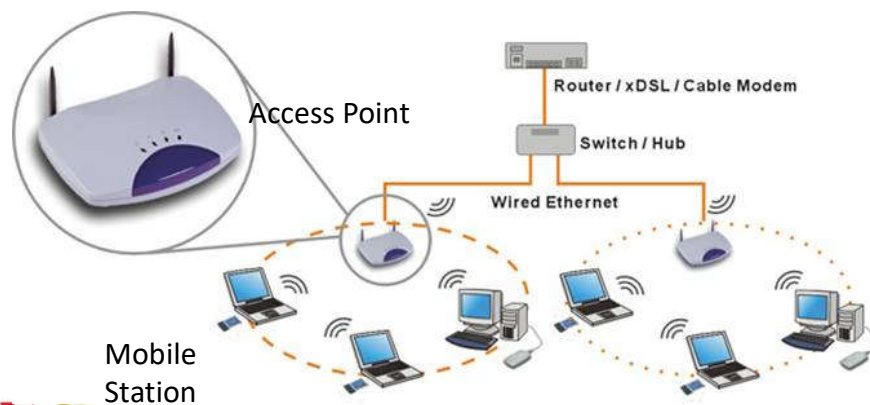
32

Overview

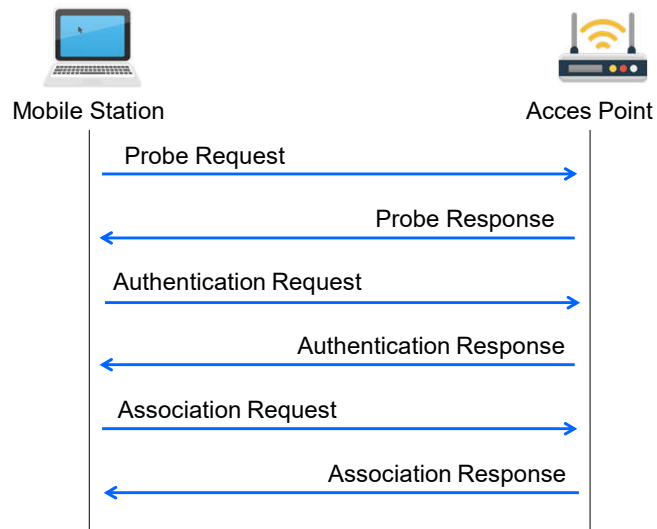
- WLAN (Wireless Local Area Network) is a computer network that links 2 or more devices using a wireless transmission medium.
- The original IEEE 802.11 standard was officially released in 1997
- IEEE 802.11x (WiFi standard) denotes a set of WLAN standards developed by the IEEE LAN/MAN standardization committee (IEEE 802.11).
- IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n standards specifying infrastructure and transmission technology
- IEEE802.11i: standard specification of security protocols in WLAN
- ...
- IEEE802.1X: access control for WLAN

WLAN components

- A typical WLAN consists of two parts: wireless access devices (Mobile Station-MS), Access Points (Access Points - AP).

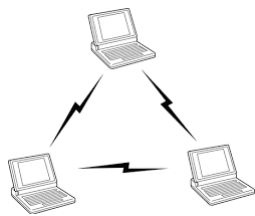


How to connect to a WLAN



35

WLAN deployment



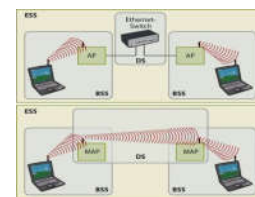
Ad-hoc

- No AP
- Peer – peer



BSS

- Centralized connection



ESS

- Centralized connection
- Extend by connect BSSs

36

Coffee Shop

1. WiFi connect

Connection setup

SOICT VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

37

37

Coffee Shop

WEP Open:
No authentication, no encryption

Easy to be eavesdropped

Eve

SOICT VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

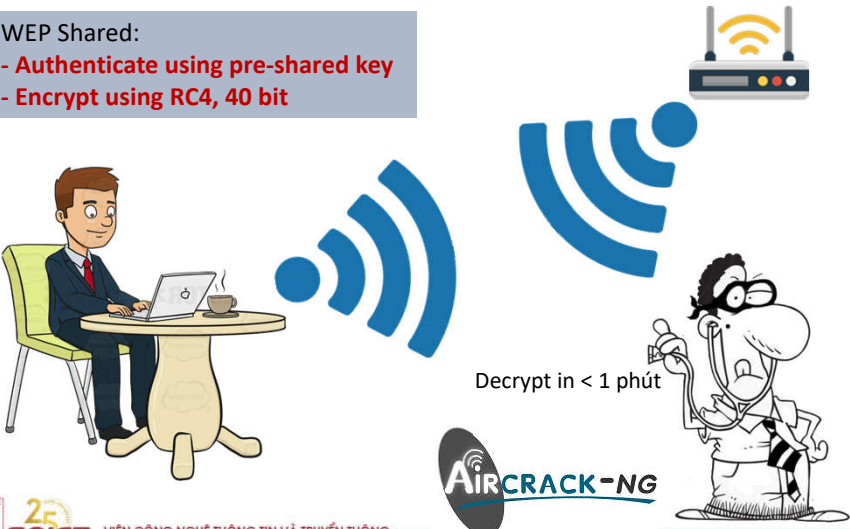
38

38

Coffee Shop

WEP Shared:


- Authenticate using pre-shared key
- Encrypt using RC4, 40 bit



Decrypt in < 1 phút

AIRCRAK-NG

Eve 39


 VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

39


Coffee Shop

WPA/WPA2:

- WPA: Encrypt using RC4, 128 bit
- WPA2: Encrypt using AES-128



SSID: WifiStation
password: guessme!



 VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

40

40

Coffee Shop

WPA2 Personal

SSID: WifiStation
password: guessme!

Kích thước khóa
Số vòng lặp

Laptop and AP calculation:

$$K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$$

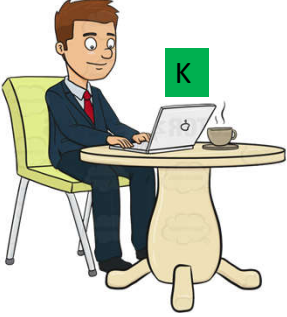

SOICT VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

41

41

Coffee Shop

WPA2 Personal

K

SSID: WifiStation
password: guessme!

Laptop and AP share the same private key K. The key is used for encryption and key exchange processes

SOICT VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

42

42

Coffee Shop

WPA2 Personal

Passive eavesdrop

If the key is kept securely, Eve must use brute force attack or dictionary attack

Attack speed is low as PBKDF2 uses loop-calculation.

Laptop and AP calculation :
 $K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$

SSID: WifiStation
password: guessme!

Eve 43

43

Coffee Shop

WPA2 Personal

Passive eavesdrop

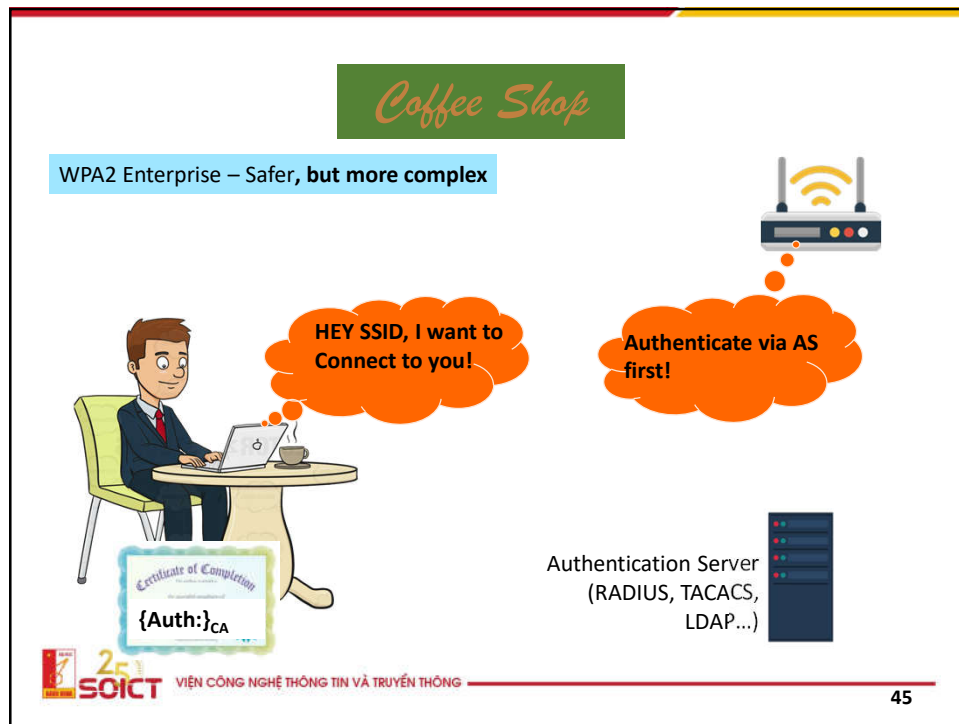
Obviously, Eve can buy a coffee and get the password to access WiFi network → calculate the key K and decrypt captured packets

Laptop and AP calculation :
 $K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$

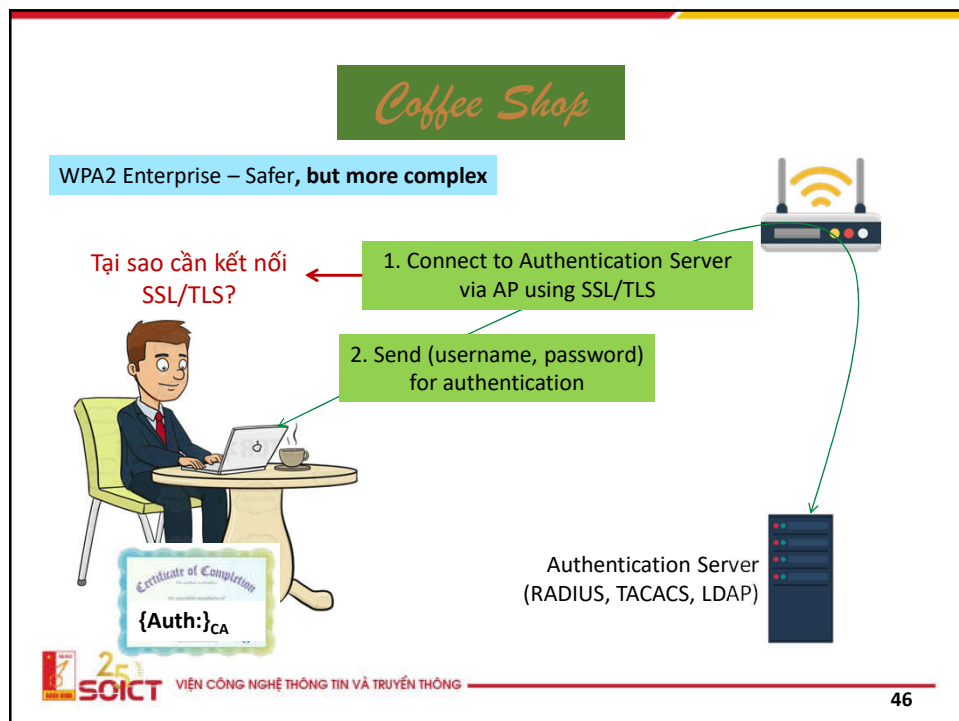
SSID: WifiStation
password: guessme!

Eve 44

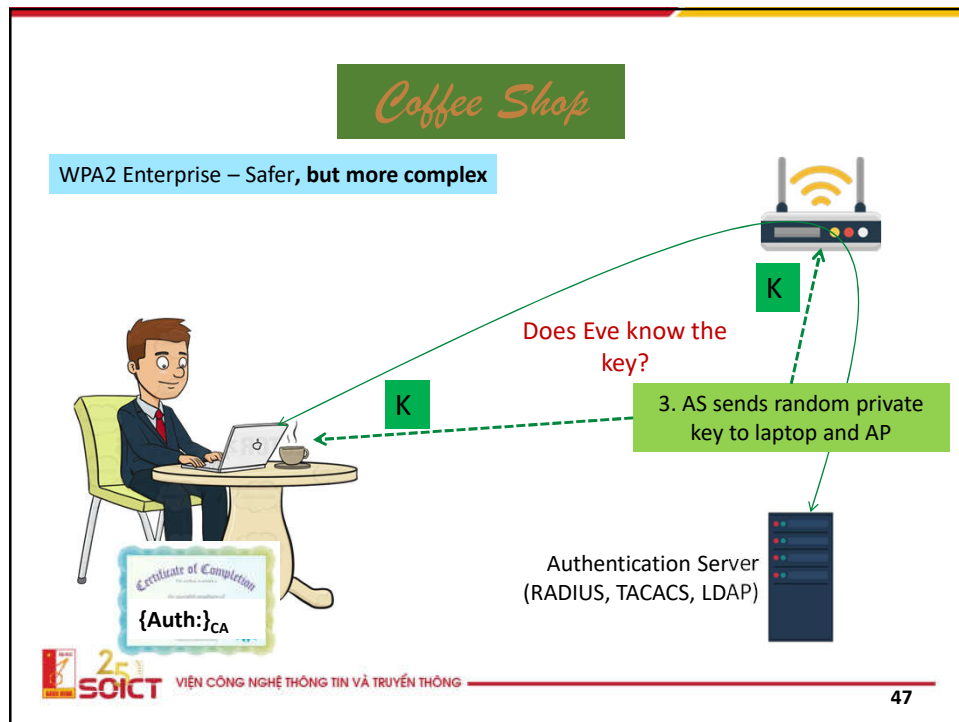
44



45



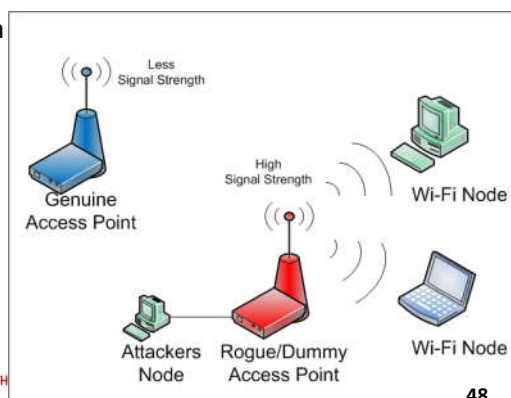
46



47

Threats in WLAN

- Jamming: create noise by sending stronger signals with the same frequency
- Purpose:
 - Fake computer
 - Rogue AP
 - DoS: destroy connection between host and AP



48

Other threats in WLAN

- Disassociation: send disassociation frame to host or AP to disrupt the current connection
- Deauthentication attack: send deauthentication frame to host to require re-authentication
- Purpose:
 - Capture WiFi password
 - Let the host to connect to Rogue AP
- Rogue AP
 - Collect authentication information between AP and host
 - Active eavesdrop
 - Attack man-in-the-middle
 - Defence: use network management tool to find the connected strange device



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

49

49



ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Security in LAN

50

Attack Switch

- MAC flooding: send packets with fake MAC address → MAC table is overloaded → The normal packets are forwarded by broadcasting:
 - Broadcasting storm → consume bandwidth and resource of other nodes
 - Eavesdropping attack
- Fake MAC address
- Defence: Port Security

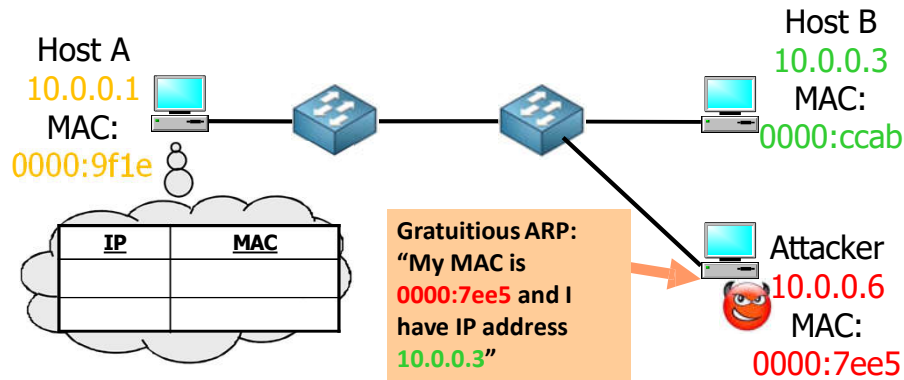
51

Attack ARP protocol

- Address Resolution Protocol: find MAC of an IP
 - Broadcast ARP Request is connectionless
 - No authentication in ARP Response
- Attack:
 - ARP Spoofing
 - DoS
- Defence: Dynamic ARP Inspection

52

ARP Spoofing



- More dangerous if the MAC address of gateway router, Local DNS Server are fake :
 - Eavesdropping
 - Man-in-the-middle



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

53

53

Attack DHCP protocol

- Dynamic Host Configuration Protocol
- Provide IP address automatically for newcoming hosts:
 - IP
 - Gateway router
 - DNS server
- Use UDP, port 67(server) and 68(client)

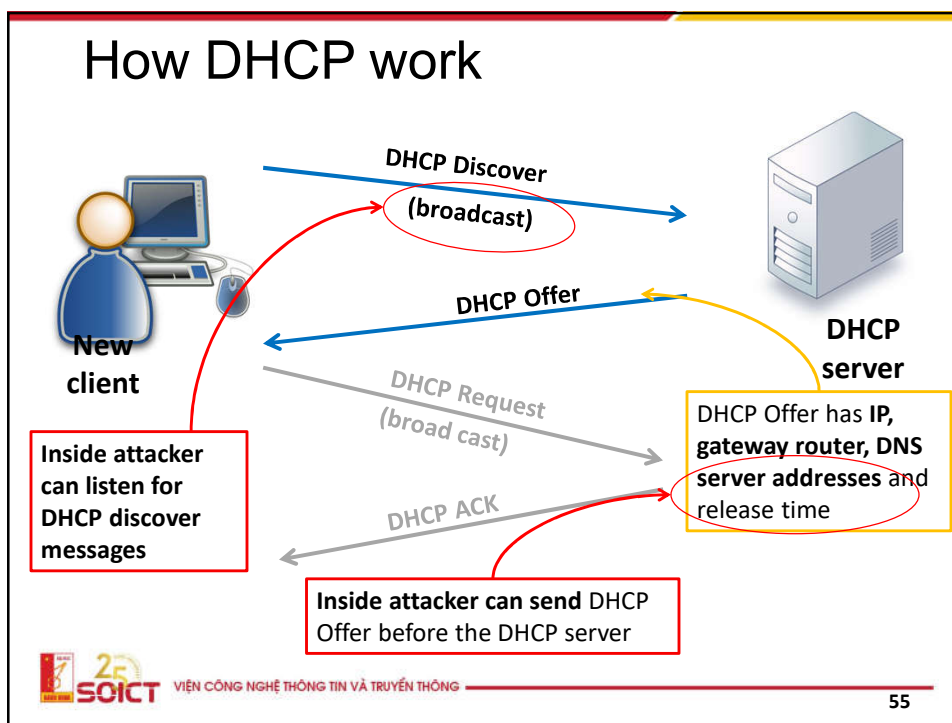


VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

54

54

How DHCP work



55

Attack DHCP

- Lỗi hỏng: Bất kỳ máy trạm nào yêu cầu cũng được cấp phát địa chỉ IP
 - Nguy cơ: Tấn công DoS làm cạn kho địa chỉ(DHCP Starvation)
- Lỗi hỏng: Không xác thực cho các thông tin cấp phát từ DHCP server → DHCP Spoofing
 - Nguy cơ: Thay địa chỉ DNS server tin cậy bằng địa chỉ DNS của kẻ tấn công.
 - Nguy cơ: Thay địa chỉ default router, cho phép kẻ tấn công:
 - Chặn bắt, do thám thông tin
 - Tấn công phát lại
 - Tấn công man-in-the-middle
 - Phòng chống: DHCP Snooping

56

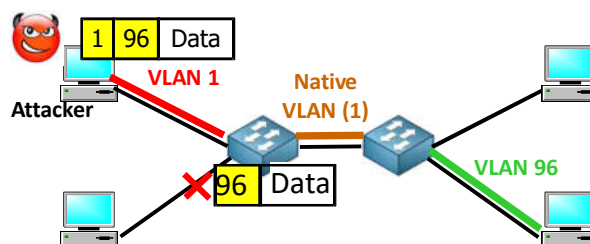
Attack VLAN

- VLAN: logic broadcast domain on switch → split traffic in layer 2
 - Access control
 - Resources separation
- Each VLAN has a different IP range
- Ethernet frame added VLAN tag (802.1Q hoặc ISL)
- Frame swttich within the same VLAN

57

VLAN hopping

- Purpose: access different VLANs from Native VLAN
- Vulnerability: frames transfered in Native VLAN do not need VLAN tag
- Fool the switch to switch frames into target VLAN
- Double-tag attack on IEEE 802.1Q



- **How to defend?**

58

Attack VLAN: DTP and VTP

- Dynamic Trunking Protocol: automatically configure trunking mode for switch port
 - Attack by sending DTP packet to fool the switch to connect to VLAN of attacker
 - Defence: turn off dynamic mode, assign access mode for all switch ports
- VLAN Trunking Protocol: automatically forward VLAN configuration information from VTP server to VTP client
 - Attack by send fake frame to delete 1 VLAN (DoS) or add a new VLAN for all switches (broadcast storm)
 - Defence : allow VTP on trusted port, authenticate when using VTP



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

59

59



60