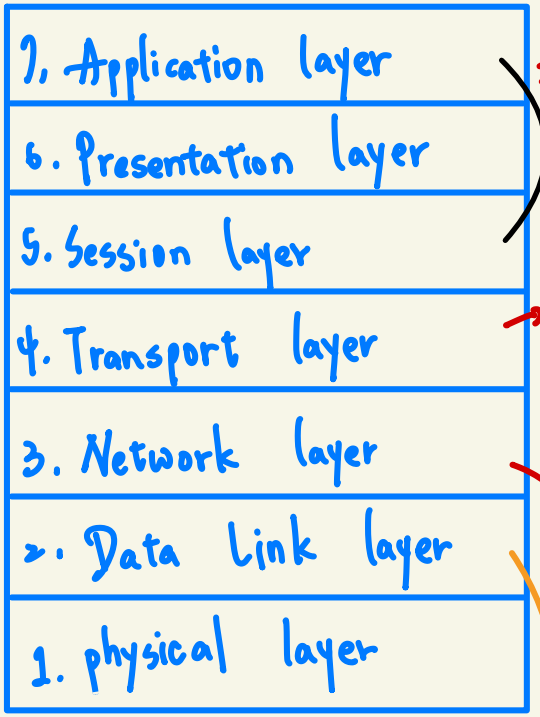
Computer Security Capstone

Project 1:
TLS Connection Hijacking

Chi-Yu Li (2025 Spring)
Computer Science Department
National Yang Ming Chiao Tung University



ssh ...

提供為應用軟体而設計的介面，ex http . https

可能統稱為 5.(應用層)

把傳輸表頭(TH)加至資料以形成封包。表頭包含傳輸協定，ex：TCP (会檢查資料是否完整)

決定路徑的選擇 & 轉寄，將網路表頭(NH)加至封包。NH 包含了網路資料 ex：IP、路由器 等

ex: IP header

負網路尋址，錯誤偵測 & 改錯

OSI 架構，

還有一種 IPS 架構。

Goal

- Understand how to hijack a TLS connection
- You will learn about
  - Establish TLS connections with customized certificates
  - Handle multiple network connections
  - Importance of certificates and identity verification

ARP (Address Resolution Protocol): 位址解析協定，通過網路位址找尋 MAC 位址。ex: 用 IP address 找 MAC address.

arp -a: 若沒有寫特定的 IP address, 則會查詢在該網域底下所有連線裝置的 IP & MAC address.

DNS: 網域名稱系統，將 human-readable 的網域 (ex: amazon.com) 轉為 IP address

What is HTTPS?

- Nowadays, HTTPS (HyperText Transfer Protocol Secure) is commonly used to secure HTTP connections between end devices and web servers

- In HTTPS, the communication is encrypted using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) convention

What is TLS?

是安全協議，加密傳輸層(transport layer)到應用層(Application layer)之間的通信.

- TLS is the successor to SSL
  - It is a security protocol that provides privacy and data integrity for Internet communications

- Key Features
  - Encryption: Protects data transmitted over the network from eavesdropping.
  - Authentication: Uses digital certificates to verify the identity of parties.
  - Data Integrity: Ensures that data has not been altered during transmission

TLS Primer: Certificate and CA

- TLS certificates are crucial for establishing secure connections
  - Containing public keys, identity information, and digital signature
  - Facilitating encryption, authentication, and data integrity

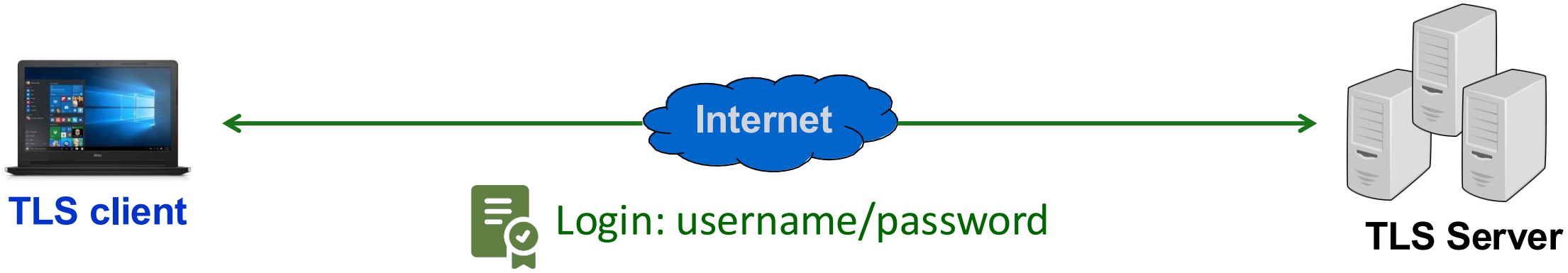
- A certificate authority (CA) is a trusted entity that issues certificates
  - Ensuring the authenticity of websites, domains and organizations
  - Help users verify they are connected to an official website, preventing fake or spoofed sites created by attackers

TLS Primer: Cipher Suite

- Cipher Suites are predefined sets of algorithms that dictate how TLS protects data
- Components of a Cipher Suite
  - (1) Key Exchange Algorithm
    - Securely exchanging cryptographic keys between a client and a server
  - (2) Encryption Algorithm
    - Encrypting the data being transmitted
  - (3) Hashing Algorithm
    - Ensuring the integrity and authenticity of the message
  - E.g. TLS_RSA_WITH_AES_128_GCM_SHA256
    (1) (2) (3)

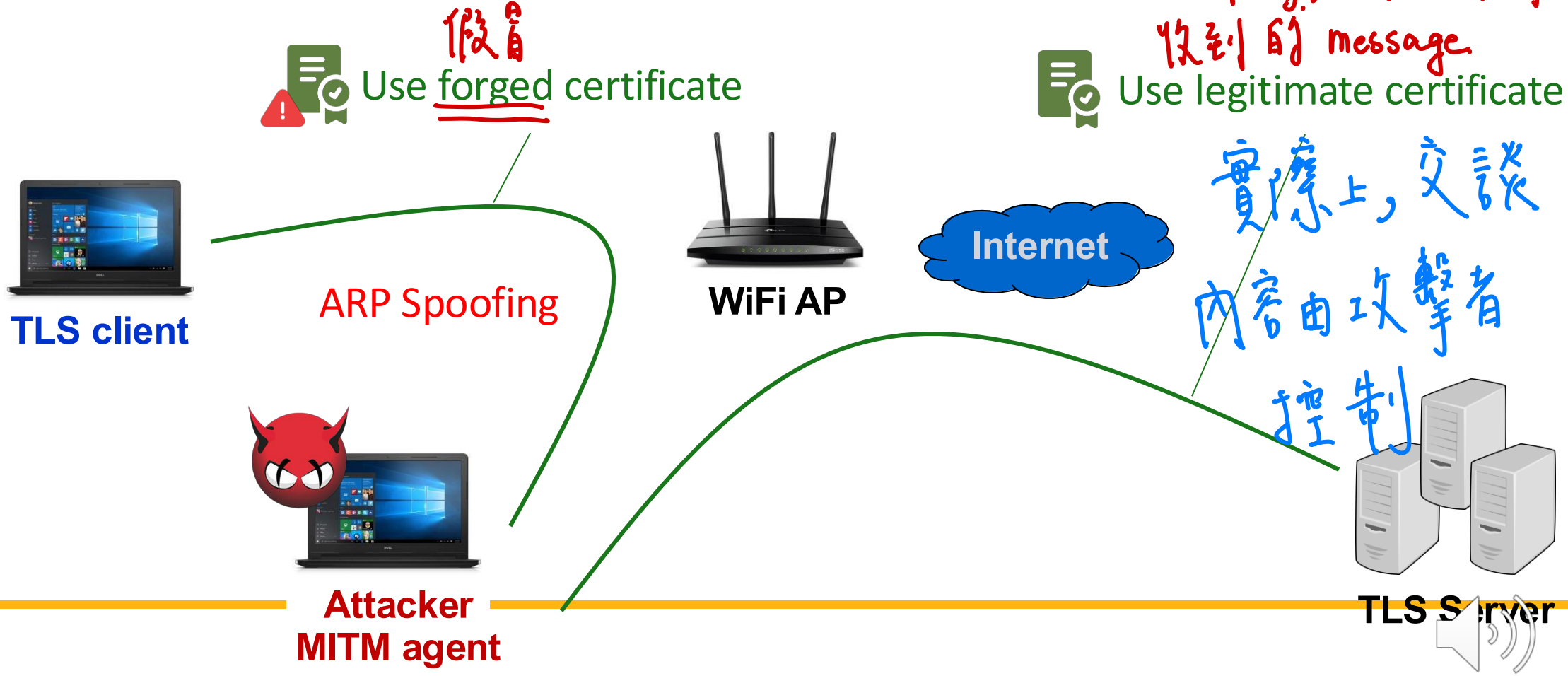
Normal TLS connection

- Establish a secure connection with a legitimate certificate



Attack Scenario : MITM attack!! attacker 和通訊的二端分別建立獨立的聯絡，並交換其所收到的 message

- How can Attacker steal Victim's user credential?



MITM：通常發生在未加密的 Wi-Fi 存取點的接收範圍
(public wifi)

Wi-Fi 存取點：是電腦網路中連接無線網路至有線網路（乙太網）的裝置，aka 無線基地台
(Wireless Access Point；WAP)
可以是單獨裝置，也可以與路由器（router）整合

和熱點（hotspot）不同，hotspot 是連接無線區域網的物理地點（ex：手机分享）

路由器：將運算裝置（ex：電腦）聯接至其它的聯網裝置，三個主要功能：

① 確定路徑：決定來源到目的所採用的路徑。

② 資料轉傳：將資料傳送至所選擇路徑的下一個裝置。

③ 負載平衡：router 有時会用多個路徑，傳送相同封包副本，減少資料遺失。

HTTP 預設 port：80　　HTTPS 預設 port：443。

DNS：Domain Name System：將「域名（Domain），aka「網址」，轉換成 IP address.

網路上由詳細步驟將網址轉成 IP address.

HTTP 通訊協定中的內容 Request & Response 有標準化格式，包含 header & body（零件的內容，可為無內容）

4個主要內容

1. 標準化內容格式
2. 分為 header、body
3. http status code
4. http request method.

1. IP address
2. http request method
3. http status code. 常見的 200、404 ...
4. ⋮

網路卡：aka 網路介面控制器（network interface controller，nic），是一塊被設計用來允許電腦在電腦網路上進行通訊的硬件。擁有一組獨一無二的 Mac address，寫於卡片上的一塊 ROM 中。屬於 OSI 的第2層（Data Link Layer）。沒有2個的網卡有相同的 Mac address

Media Access Control

IP addresses & MAC addresses are two distinct types of addresses used in computer networking.

- IP address are assigned to devices on a network to identify and communicate with them over the Internet or local network. They are assigned to devices by a Dynamic Host Configuration Protocol (DHCP) server or by manual configuration. IP addresses can be either dynamic or static, and they can change over time.

- MAC addresses are unique identifiers assigned to network interfaces of devices by their manufacturers. They are used to identify devices within a local network, such as a LAN (Local Area Network). MAC addresses are usually fixed and CAN NOT be changed unless the device's network interface is replaced.

MAC Address	IP Address
A device's mac address can retreive by ARP protocal	A device attached with IP can retrieve by RARP protocal
NIC's Card's Manufacturer provides MAC	Internet Service Protocol (ISP) provides IP
operates in data link layer	operates in network layer
identifying the device	identifying the connection of the device on the network.
MAC address won't change	IP modifies with time & environment
MAC sharing isn't allowed	multiple devices can share the same IP

接下來要討論有關幾個 IP 常見的問題

- DHCP: is responsible for automatically assigning private IP address to devices

這是一個如何將 IP address 指派給 devices 的協議。跟據 devices 使用時間，地點位置，動態的指派一組可用 IP 給一個 device.（這個協議重點在於指派可用 ip 給 devices）

How it works: A DHCP server dynamically assigns IP addresses to devices for a limited lease time. When the lease expires, the same IP will be reassigned to another device.

- NAT: (Network Address Translation) - Multiple Devices sharing a public IP.

（這個方法是將一個 public IP match 到一組 private IP）

How it works: A router assigns private IP address to devices on a local network. When these devices access the internet, the router translates all their requests into a single public IP address.

重點

- NAT 與 DHCP 常一起使用，先透過 NAT 產出一組 private IP 後，再由 DHCP 將其 assign 給許多 devices.

★ Takeaway

DHCP assigns private IPs to devices in a local network

NAT translate those private IPs to a single public IP for internet access.

DHCP works inside the network, NAT works at the network boundary (routers).

ARP spoofing：利用自己的 MAC address，使受害主机的 ARP cache 中毒.

		Address Used.
Layer 3	Network Layer	IP address ⇒ tell us where the packet should go globally
Layer 2	Data Link Layer	MAC address ⇒ tell us which router/AP should go next.

Hence, IP address in Network Layer won't change.

MAC address in Data Link Layer will change every time (rewritten in each loop)

Packet : [Ethernet Header | IP Header | TCP/UDP header | Payload]

Ethernet Header — Data Link Layer header (if using Ethernet as the Data Link protocol)

- Source MAC
- Dest MAC
- Ether Type (0x0800 for IPv4)

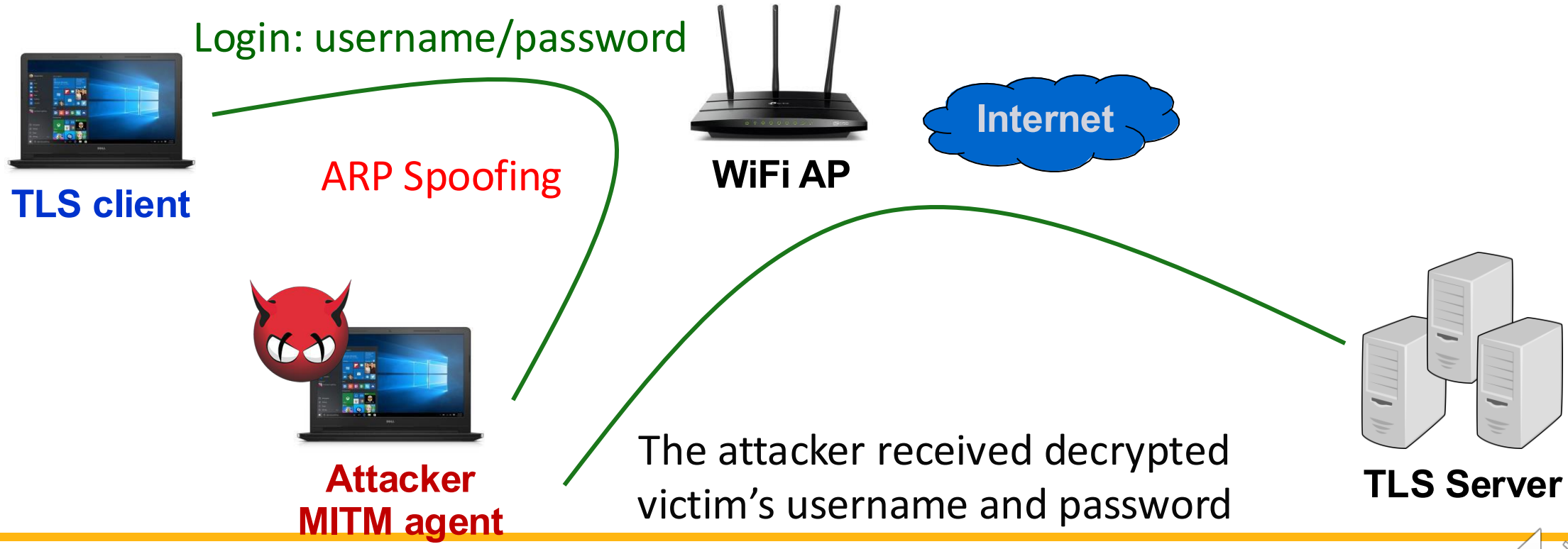
IP Header — Network Layer header (if using IP as the Network Layer protocol)

- source IP
- Dest IP
- TTL, protocol..

TCP/UDP header — Transport Layer

Attack Scenario

- How can Attacker steal Victim's user credential?



Major Ideas

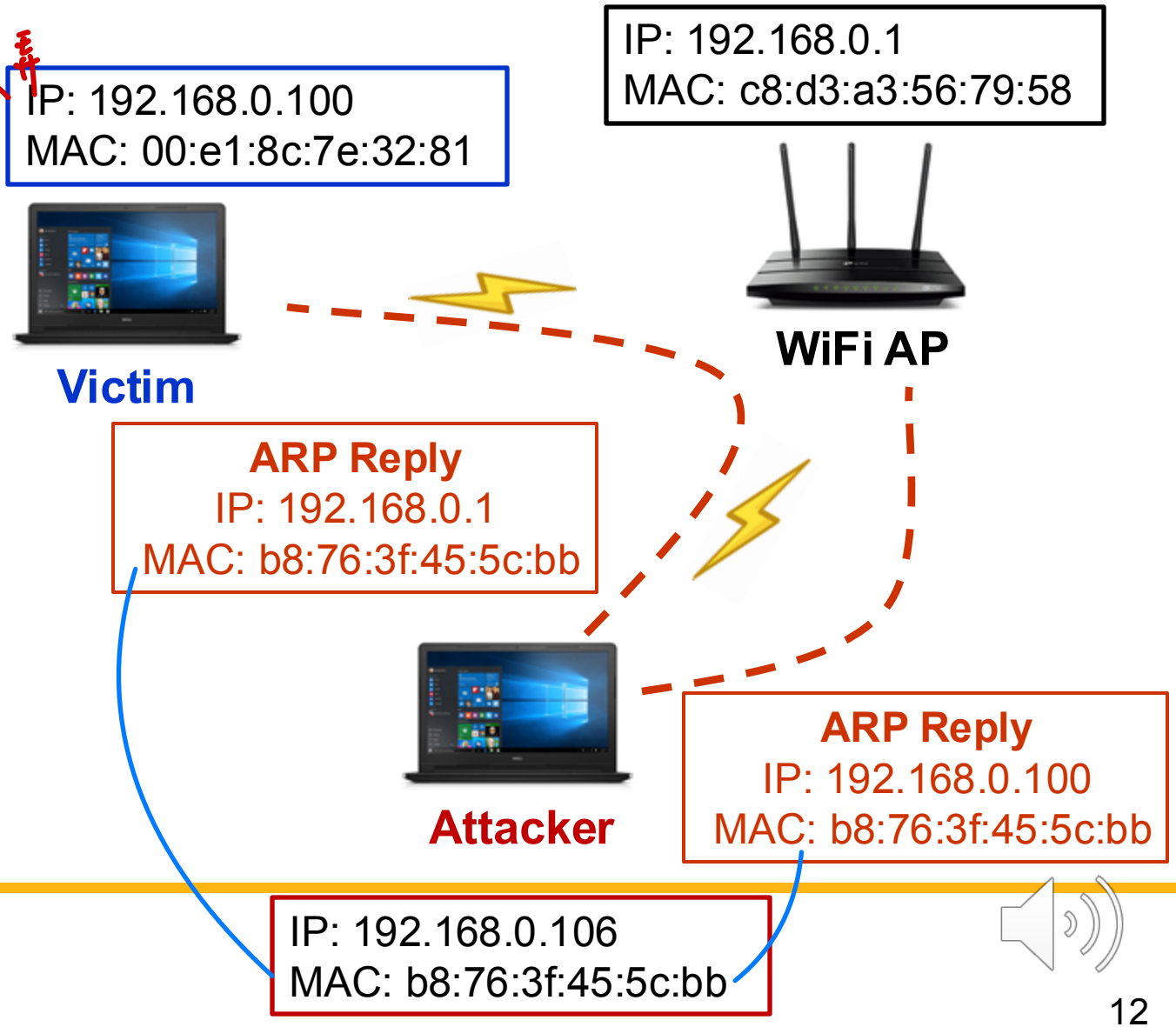
- Redirect Victim's traffic to Attacker
  - Man-in-the-middle based on ARP spoofing
- Dual Connection Establishment
  - What you need to implement in this project

What is ARP (Address Resolution Protocol)?

- A communication protocol: discovering the link layer (or MAC) address associated with a given IP
- A request-response protocol: messages are encapsulated by a link-layer protocol
  - ARP request: broadcast
  - ARP response: unicast
- Never routed across internetworking nodes

What is ARP Spoofing?

- Generate spoofed ARP replies for all other client devices
  - Hint: ARP format and thread
- Both uplink and downlink should be considered
  - Other client devices' network services can work normally



Experimental Setting

MITM：中間人攻擊：Man in the middle attack.

- The attacker VM executes the command below to redirect specific TLS packets to the MITM agent:
  - `sudo ./setup.sh`

This command is to ignore the certificate erron. so the browser won't block.

- The victim VM should start the browser using the following command to establish a TLS connection with a forged certificate:
  - `google-chrome --ignore-certificate-errors --user-data-dir=/tmp/chrome_dev`
    - In real-life situations, such as IoT environments, where certificates are often not verified or when a certificate is injected into the browser, this type of attack can be launched
  - Recommend to open the browser in Incognito mode.

Experimental Setting: ARP Spoofing

Gateway 10.0.2.1

Victim 10.1.2.5

- Attacker VM executes the command below in the MITM agent
  - `sudo arpspoof -i INTERFACE -t GATEWAY_IP CLIENT_IP`
  - `sudo arpspoof -i INTERFACE -t CLIENT_IP GATEWAY_IP`

your MAC address

→ 你等於把在 victim 的 arp table 中的 IP 對應到的 mac address 改成你的網卡 address

```
csc2025@csc2025-vbox:~$ sudo arpspoof -i enp0s3 -t 10.0.2.6 10.0.2.1
[sudo] password for csc2025:
8:0:27:b5:13:37 8:0:27:26:3a:90 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 8:0:27:26:3a:90 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 8:0:27:26:3a:90 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 8:0:27:26:3a:90 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b5:13:37
```

```
csc2025@csc2025-vbox:~$ sudo arpspoof -i enp0s3 -t 10.0.2.1 10.0.2.6
[sudo] password for csc2025:
8:0:27:b5:13:37 52:54:0:12:35:0 0806 42: arp reply 10.0.2.6 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 52:54:0:12:35:0 0806 42: arp reply 10.0.2.6 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 52:54:0:12:35:0 0806 42: arp reply 10.0.2.6 is-at 8:0:27:b5:13:37
8:0:27:b5:13:37 52:54:0:12:35:0 0806 42: arp reply 10.0.2.6 is-at 8:0:27:b5:13:37
```

- Victim VM executes `arp -a` to check ARP table
  - If the gateway's mac address is the same with that of the attacker, ARP spoofing is successful

```
csc2025@csc2025-vbox:~/Project1$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5c6:c4ed:b631:71f9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b5:13:37  txqueuelen 1000  (Ethernet)
        RX packets 140  bytes 47456 (47.4 KB)
```

```
csc2025@csc2025-vbox:~$ arp -a
? (10.0.2.15) at 08:00:27:b5:13:37 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:58:a7:12 [ether] on enp0s3
_gateway (10.0.2.1) at 08:00:27:b5:13:37 [ether] on enp0s3
```

MITM Agent

TLS Client

Task I: Hijacking a TLS Connection

- TLS Client to MITM Agent:
  - The MITM agent can use a forged certificate to establish a TLS connection.
    - Configure the server settings (TLS version, check mode, etc.) so that the victim accepts the TLS connection.

- MITM Agent to TLS server:
  - The MITM agent can retrieve the destination address from the victim's packet
  - The MITM agent uses this address to connect to the TLS server.
    - A fixed address for the TLS server connection is not allowed.
      - Should be able to connect to different websites.

Because modern websites don't have fixed IP address. DNS service IP address may change.

Task II: Hijacking multiple TLS conn. concurrently

- The program should still work normally when connecting to another website
  - Handling concurrency
    - Ensure the program can manage multiple TLS connections concurrently
    - Consider using threading, fork(), or asynchronous I/O (select(), epoll()) to avoid blocking connections
  - Session management
    - Each connection should maintain its own independent TLS session context
    - Avoid session interference between multiple websites being accessed simultaneously

Verification Steps

- 1. MITM agent can correctly hijack a TLS connection (60%)
  - A sub-connection between TLS client and MITM agent
  - A sub-connection between MITM agent and TLS server
- 2. Fetch the username/password and show on the terminal (20%)
  - MITM agent prints out the username/password inputted to nycu portal
- 3. MITM agent can concurrently hijack multiple TLS connections (20%)

Verification Steps

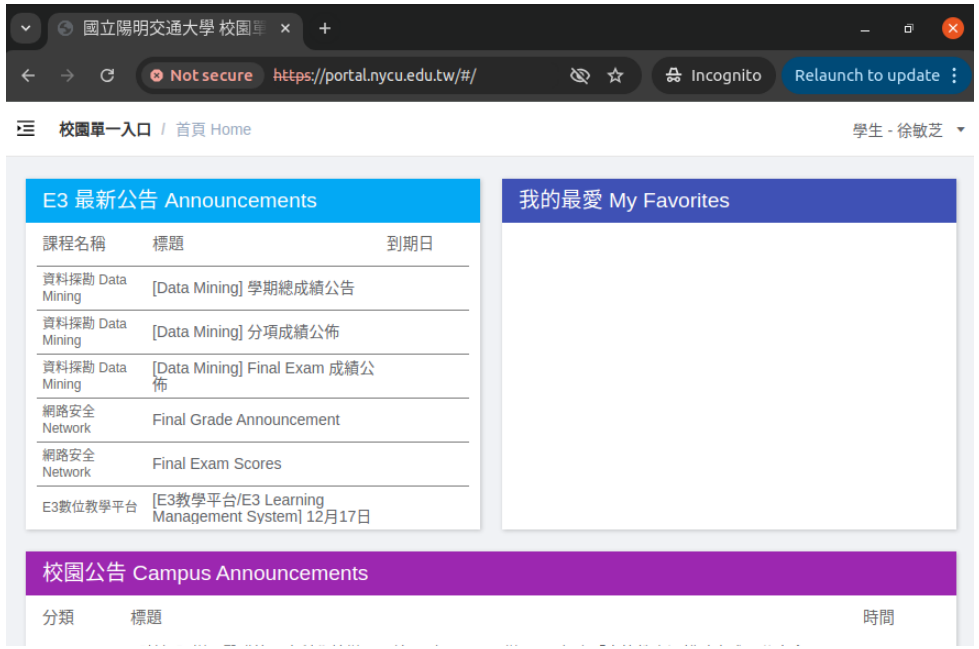
- 1. MITM agent can correctly hijack a TLS connection (60%)
  - When executing the attack program, the client can successfully connect to the school's portal webpage.
  - The program should also print out the destination IP and port.

```
csc2025@csc2025-vbox:~/Project1/student_id$ sudo ./attack.py 10.0.2.6 enp0s3
TLS Connection Established : [140.113.41.157:443]
```

Verification Steps

- 2. Fetch the username/password and show on the terminal (20%)
  - MITM agent prints out the username/password inputted to nycu portal

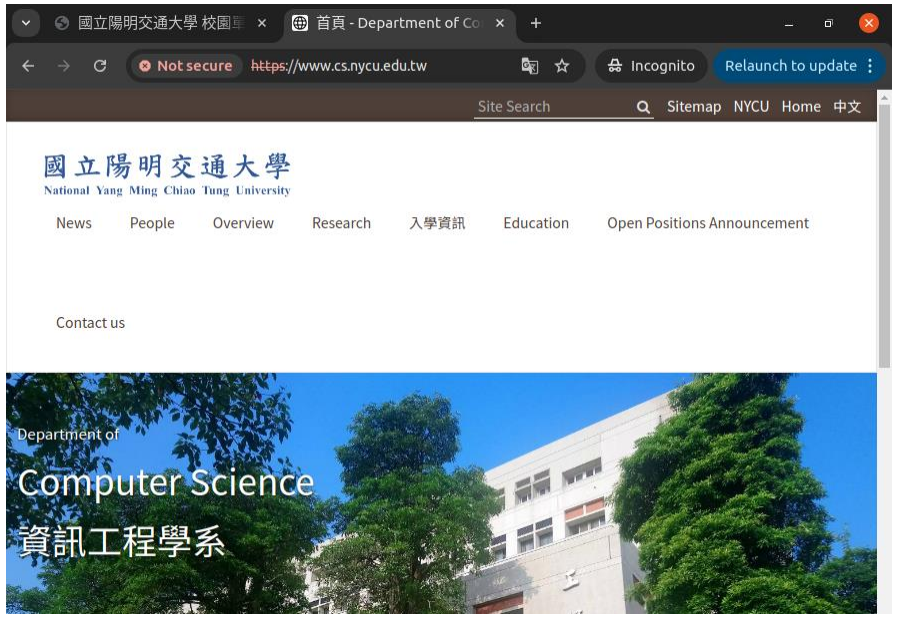
```
csc2025@csc2025-vbox:~/Project1/student_id$ sudo ./attack.py 10.0.2.6 enp0s3
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
id: 313[redacted], password: [redacted]
```



Verification Steps

- 3. MITM agent can concurrently hijack multiple TLS connections (20%)
  - The program still works normally when connecting to other HTTPS websites

```
csc2025@csc2025-vbox:~/Project1/student_id$ sudo ./attack.py 10.0.2.6 enp0s3
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
id: 313[redacted], password: [redacted]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.41.157:443]
TLS Connection Established : [140.113.96.55:443]
TLS Connection Established : [140.113.96.55:443]
TLS Connection Established : [140.113.96.55:443]
TLS Connection Established : [140.113.96.55:443]
```



Important: How to Prepare Your Attack Programs?

- You need to develop and run your program in the provided VM
  - **VM Image**: Please download it from the provided link
    - Username/password: csc2025/csc2025
  - Network setting: **NAT Network**
- Do not hardcode the network interface. You are allowed to assign it during execution.
  - During the demo, the program may be run on either VMware or VirtualBox, so ensure that no fixed values are used.
- Only Python is allowed for the development.

Important: How to Prepare Your Attack Programs?

- Must provide an attack program named **attack.py** (Missing: -20%)
- Test requirements for the program
  - Due to the environment settings, this project focuses on hijacking websites within the school's IP domain (140.113.*.*)
    - You can use the nslookup command to verify if a specific host is within the school IP domain
  - During the demo, all certificates will be provided by the TA and will be located in the ../certificates/directory
- The program must work with the following test commands:
  - `sudo ./attack.py <victim ip>` or `sudo ./attack.py <victim ip> <interface>`
- You are allowed to team up. Each team has at most 2 students.
  - Teams: discussions are allowed, but no collaboration

Project Submission

- Due date: 3/19
- Makeup submission (75 points at most): TBA (After the final)
- Submission rules
  - Put your source code files into a directory and name it using your student ID(s)
    - If your team has two members, please concatenate your IDs separated by "-"
  - Zip the directory and upload the zip file to E3 (only upload python files)
  - A sample of the zip file: 01212112-02121221.zip

```
01212112-02121221.zip
└── 01212112-02121221(dir)
    ├── attack.py
    └── bbb.py
```

- If files are not in a directory after unzip, 10 points will be deducted.

Online Project Demo

- Demo date: 3/21
- TA will prepare your zip file and run your programs for the demo on behalf of you
  - TA will run your program in the same given virtual environment
- You will
  - be asked to launch a TLS hijacking attack
  - be not allowed to modify your codes or scripts in the demo
  - be asked some questions
  - be responsible to show and explain the outcome to TA

Questions?