

# Am\*ng us，但是在工廠： 發掘針對工控領域的中間人 (Man-In-The-Middle)攻擊手法

Linwei Tsao, Threat Researcher, TXOne Networks Inc.  
Canaan Kao, Threat Research Director, TXOne Networks Inc.  
May 14<sup>th</sup>, 2024 @CYBERSEC 2024

# Biography



## **Linwei Tsao TXOne PSIRT and Threat Research at TXOne Networks**

Linwei目前任職於 TXOne Networks 擔任資安威脅研究員，主要任務包含研析 ICS 相關的通訊協定、網路封包、以及開發佈建威脅獵捕系統，以獲得目前最即時的 ICS 攻擊情資。除此之外，亦曾開發多項網路相關的產品，包括數據機韌體，DPI engine/pattern 等。



## **Canaan Kao, TXOne Networks Director**

Canaan 自 2001 年起擔任 DPI/IDS/IPS 工程師。他領導了 MoECC 委託給 NTHU 的 Anti-Botnet 計畫（2009 - 2013）並舉辦了 “Botnet of Taiwan”（BoT）研討會（2009 - 2014）。他在 HitCon2014 CMT、HitCon2015 CMT 和 HitCon 2019 發表過演講。他的主要研究興趣是網路安全、入侵偵測系統、逆向工程、惡意軟體偵測和嵌入式系統。

# Outline

## 01 | 中間人攻擊的定義

中間人攻擊是什麼？

## 02 | 中間人攻擊的目的

講述中間人攻擊如何入侵並破壞您的工廠

## 03 | IT 場域的中間人攻擊概觀

重溫傳統IT場域的中間人攻擊。這些攻擊也是OT中間人攻擊的起手式

## 04 | OT 場域的中間人攻擊

列舉從古老的 Modbus 協議，到幾經翻修的 ODSP，針對協議本身，或是實作缺陷，可以實作的中間人攻擊

## 05 | 中間人攻擊的防禦/緩解

防禦手段/緩解建議



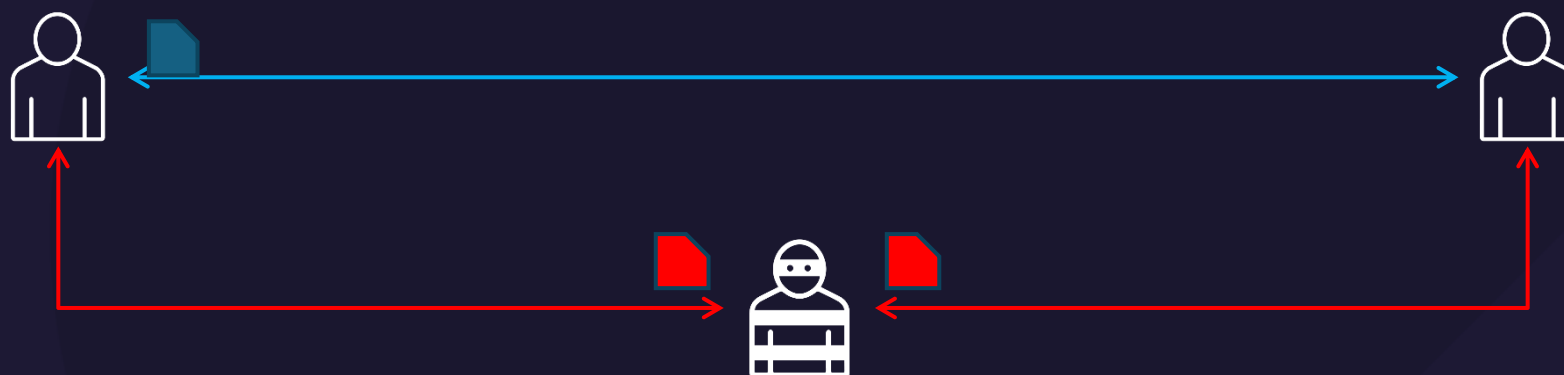


# 中間人攻擊 (Man-In-The-Middle) 的定義



## 中間人攻擊 (Man-In-The-Middle) 的定義

- 攻擊者潛伏在兩個正在溝通的雙方，企圖竊聽，攔截或修改雙方交換的訊息。更有甚者，亦可對其中一方發動攻擊
- 然而，正在溝通的雙方仍以為身處一個正常連線，難以發現已經介入的攻擊者

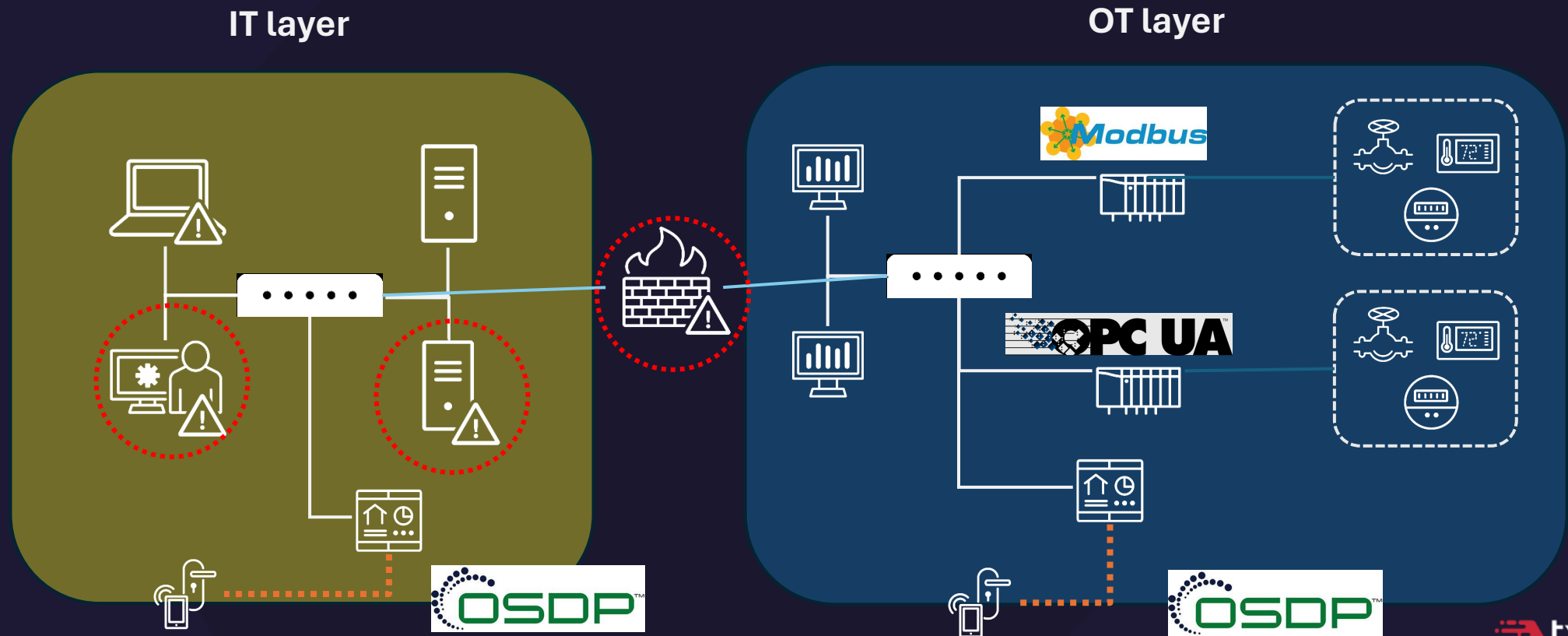




# 中間人攻擊的目的 及對工控場域的影響

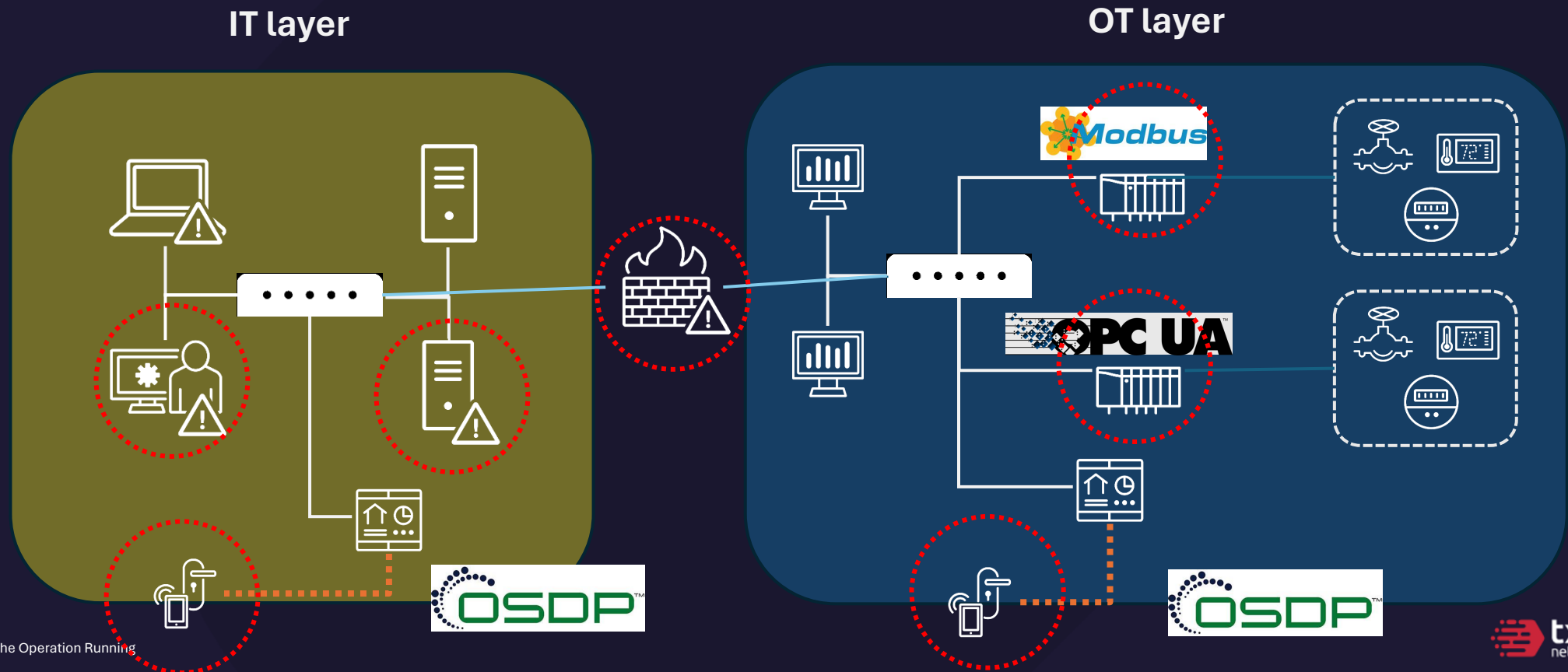
# OT 場域中間人攻擊是怎麼發生的？

- IT 場域防護能力薄弱，或 OT 場域設備直接曝露於外網，導致可疑人員或設備乘隙介入。



# OT 場域中間人攻擊是怎麼發生的？

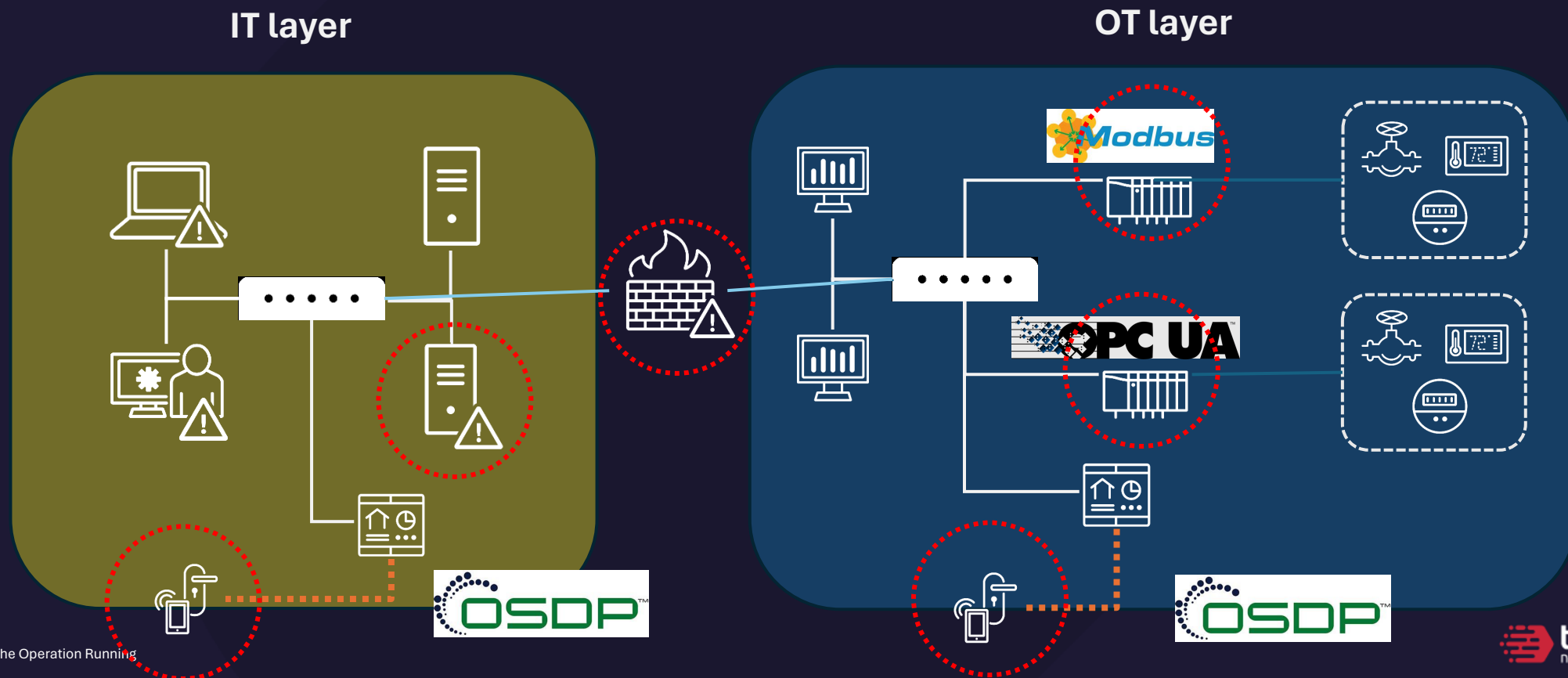
- 相對於 IT 相關協定，老舊或設定不正確的工控設備更容易下手。





# OT 場域中間人攻擊是怎麼發生的？

- 相對於其它攻擊手法，中間人攻擊有更好的隱蔽性。

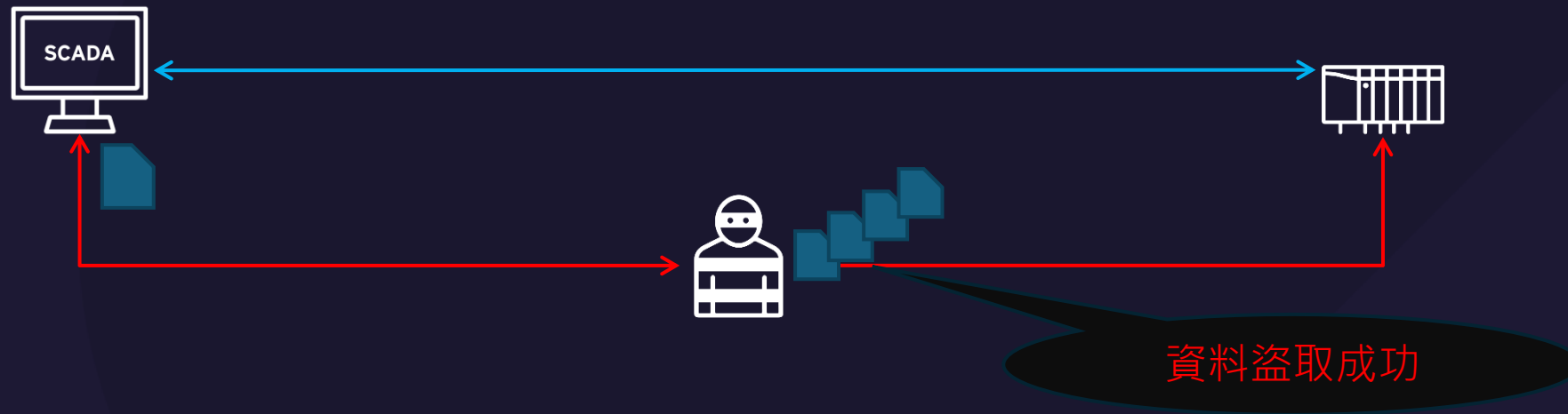


# 中間人攻擊的目的

- 竊聽 (Eavesdropped message)
- 掉包 (Dropped message)
- 延遲傳送 (Delayed message)
- 數據竄改 (Tempered message)

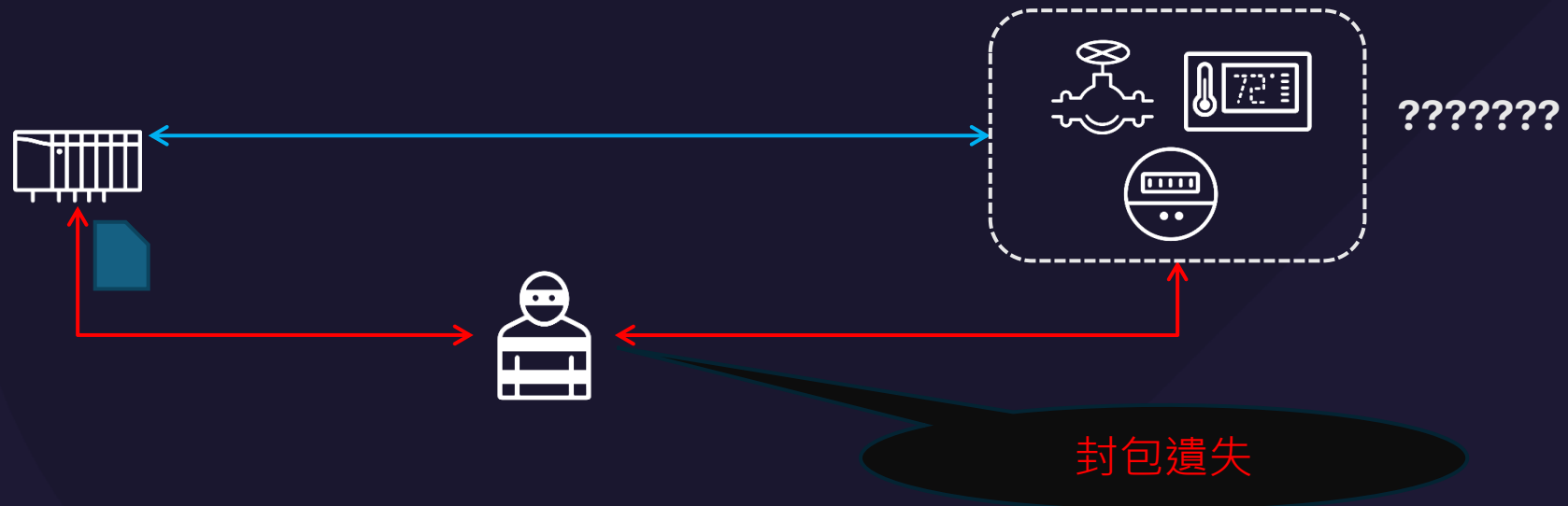
# 中間人攻擊的目的

- 竊聽 (Eavesdropped message)
  - 攻擊者藉由介入雙方的會話 (session) ，並盜取會話之中的內容
  - 負面影響：
    - 造成生產數據、帳號及密碼等機敏資訊外流



## 中間人攻擊的目的

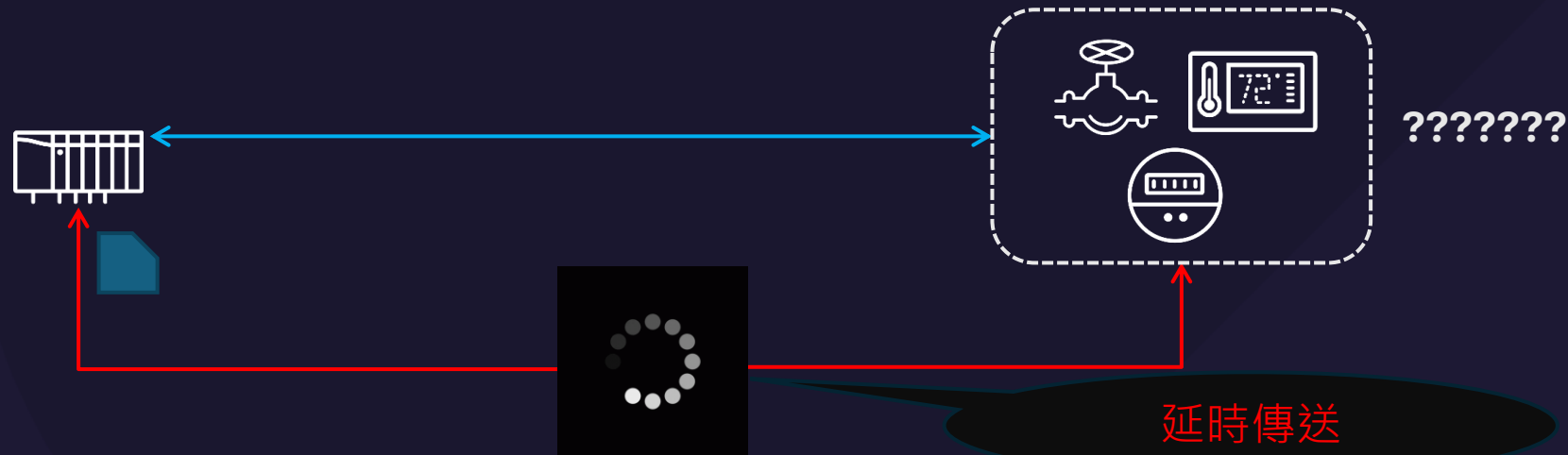
- 掉包 (Dropped message)
  - 攻擊者藉由丟棄雙方會話的內容，讓會話的雙方無法溝通。
  - 負面影響：
    - 無法得知傳感器/作動器的狀態，導致控制器無法正常運作。
    - 控制器無法發送指令至作動器，導致作動器無法正常運作。





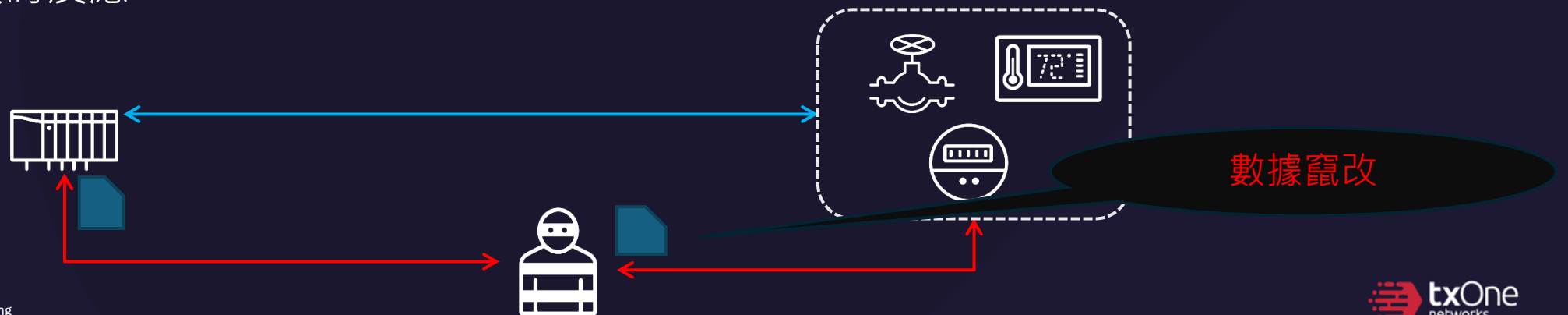
# 中間人攻擊的目的

- 延遲傳送 (Delayed message)
  - 攻擊者藉由延遲雙方會話的內容，讓會話的雙方無法在時限內收到訊息，導致出現無法預期的行為
  - 負面影響：
    - 作動器在錯誤的時間，接收到控制器指令，無法正常運作
    - 控制器在錯誤的時間接收到傳感器/作動器的狀態，無法正常運作



# 中間人攻擊的目的

- 數據竄改 (Tempered message)
  - 攻擊者藉由竄改雙方會話的內容，包括但不限於竄改封包數據 (payload)，發送重覆封包 (如 replay attack)，或是發送格式/資料錯誤的封包，導致會話的雙方出現無法預期的行為。
  - 負面影響：
    - 作動器收到錯誤指令，無法正常運作。
    - 控制器收到偽冒的傳感器/作動器的狀態，無法正常運作，甚至在發生危險時無法及時反應。





# IT 場域的中間人攻擊概觀

# IT場域中間人攻擊

- IP 地址欺騙 (IP spoofing)
  - 修改來源 IP 位置，使流量導向受害者
  - 常用於阻斷式攻擊 (DoS)





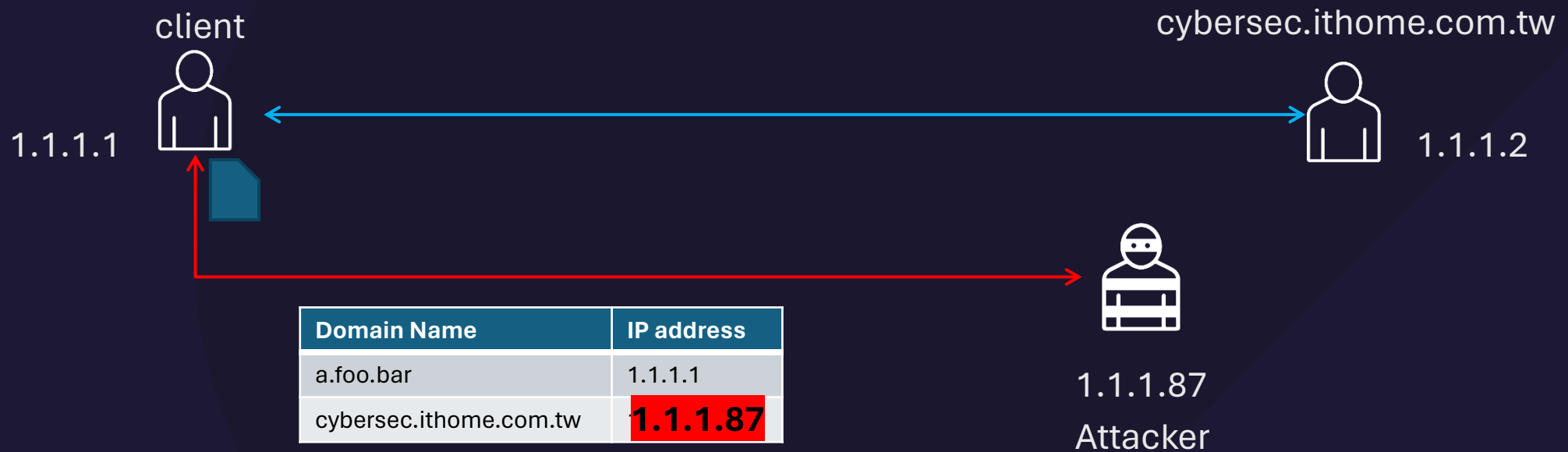
# IT場域中間人攻擊

- 位址解析協議欺騙 (ARP spoofing)
  - ARP 表為硬體位置 (MAC address) 和 IP address 的對映表
  - 攻擊者可藉由污染 ARP 表，誘使受害者與其發起會話，達成劫持的目的



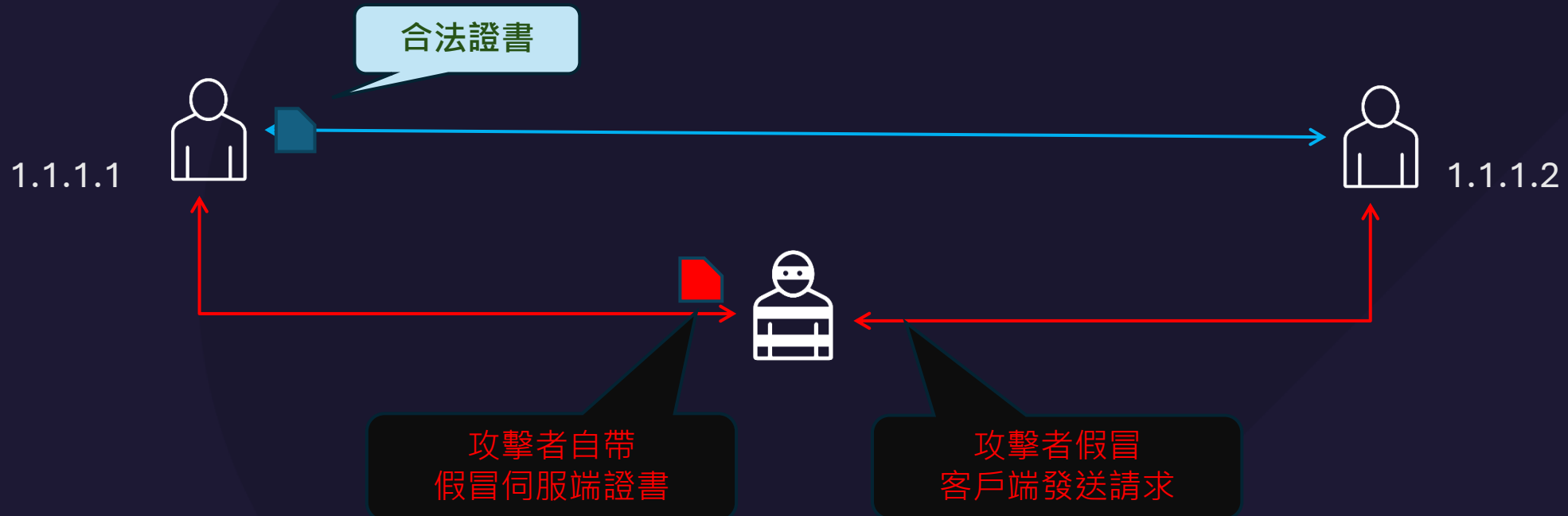
# IT場域中間人攻擊

- 網域解析協議欺騙 (DNS spoofing)
  - DNS Record 為 IP address 和 domain name 的對映表
  - 藉由污染對映表，攻擊者可以欺騙受害者連線，將受害者連結到惡意網站



# IT場域中間人攻擊

- 安全通訊端層劫持 (SSL hijacking)
  - 攻擊者使用偽冒的憑證，從中間串起受害人和伺服器連線。
  - 受害者若未檢查憑證，流量將被攻擊者監聽。

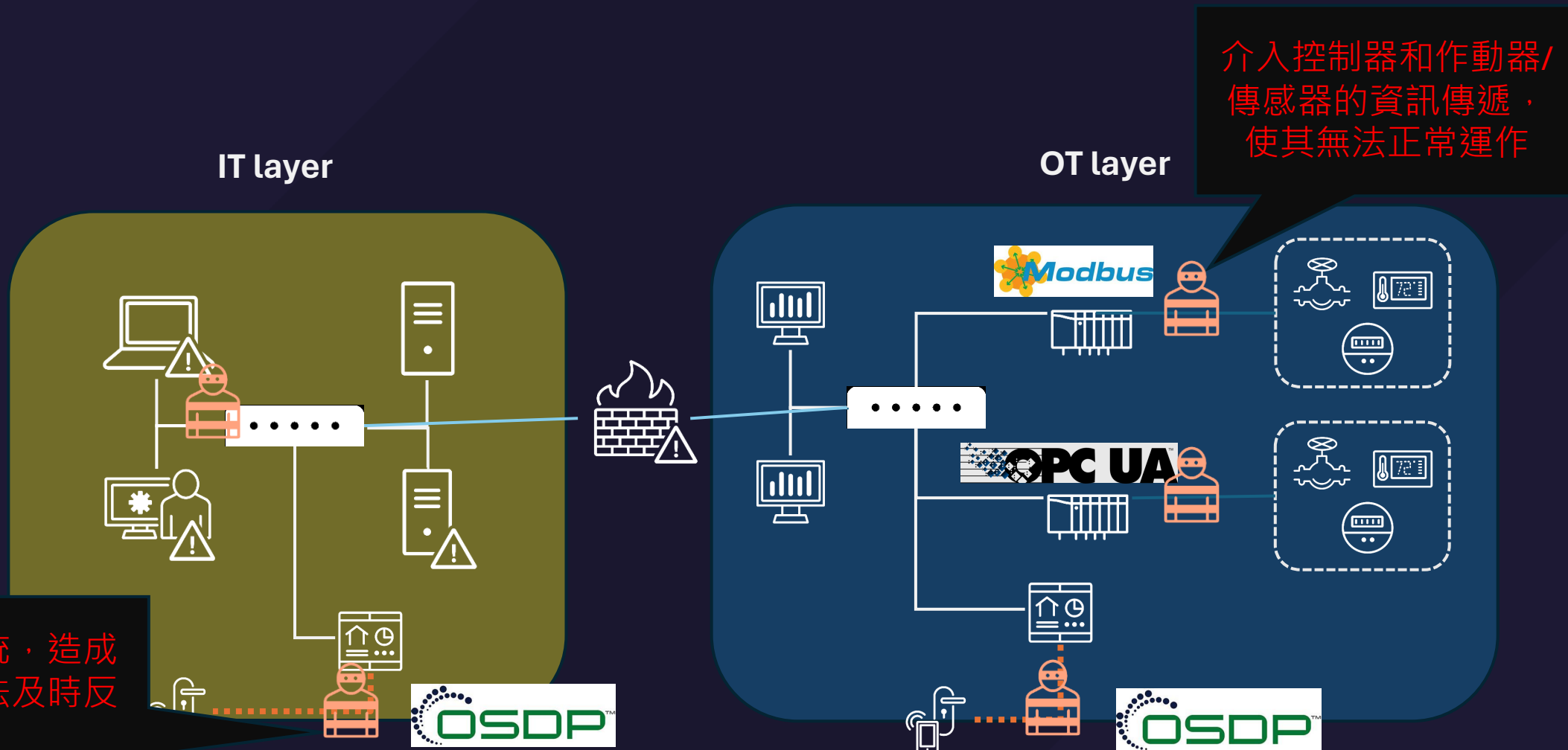




# OT領域中間人攻撃手法



# OT 場域遭受中間人攻擊時，會發生什麼事？



# Modbus



- 自 1979 年開始使用
- 廣泛為各大工控廠商支援
- 無加密
- 無認證

SHODAN Explore Downloads Pricing port:502

TOTAL RESULTS  
498,511

TOP COUNTRIES

Country	Count
United States	403,741
China	31,506
Canada	4,797
Korea, Republic of	4,514
Singapore	3,752

More...

TOP ORGANIZATIONS

Organization	Count
Google LLC	350,100
Fly.io, Inc.	23,163
Aliyun Computing Co., LTD	20,530
Avago Technologies U.S. Inc.	5,160
Fly.io, Inc	4,208

More...

TOP PRODUCTS

Product	Count
OpenSSH	4,558

ps://www.shodan.io/dashboard 2,766

View Report Download Results Historical Trend Browse Images View on Map

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

No data returned

No data returned

Unit ID: 0  
-- Slave ID Data: Illegal Function (Error)

Unit ID: 1  
-- Slave ID Data: Illegal Function (Error)

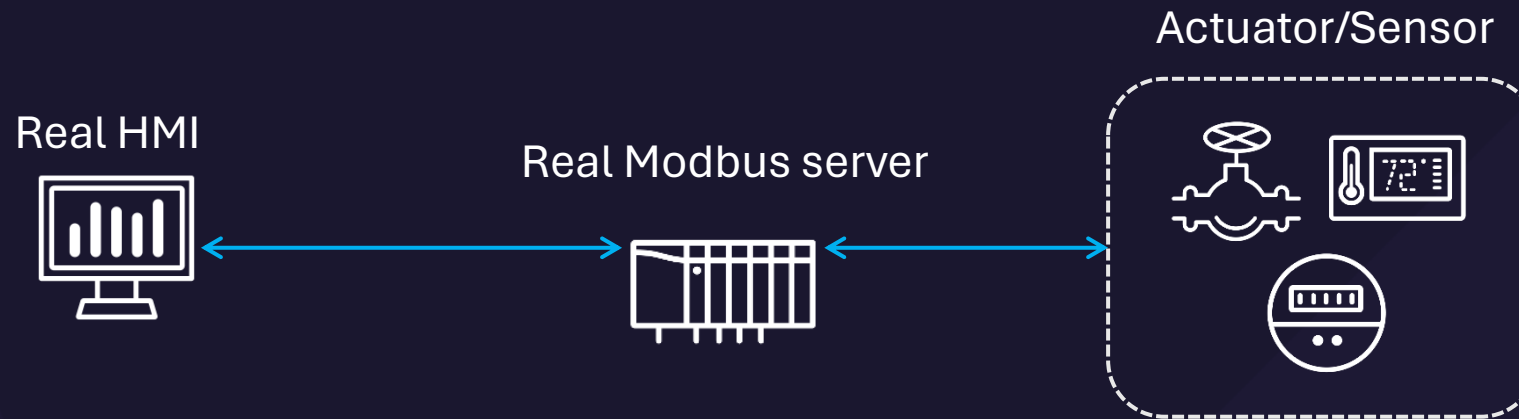
No data returned

HTTP/1.1 200 OK  
CONNECTION: close  
Date: Wed, 17 Apr 2024 15:10:24 GMT

- <https://en.wikipedia.org/wiki/Modbus>
- Shodan.io. <https://www.shodan.io/search?query=port%3A502>

# Modbus

- Demo 情境模擬
  - 一個有安全閥的離心機工作站，正常最高轉速為 7500 RPM，超過自動降頻
  - 目標：破壞離心機，並且在人機界面(HMI)上不會被發現



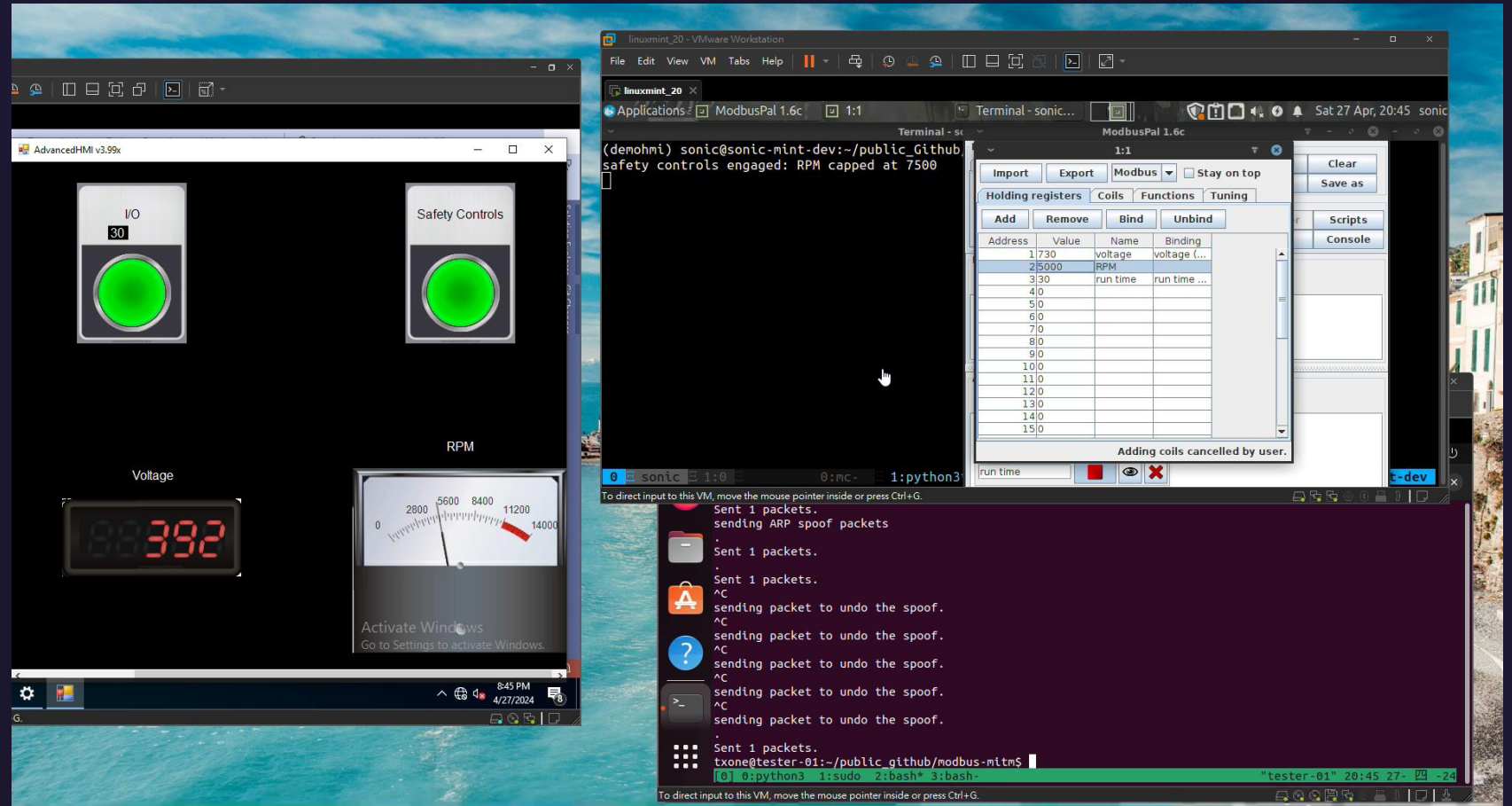
# 正常情况模拟

## Holding Register

Address	Name
1	voltage
2	RPM
3	count

## Coil

Address	Name
1	I/O
2	safety



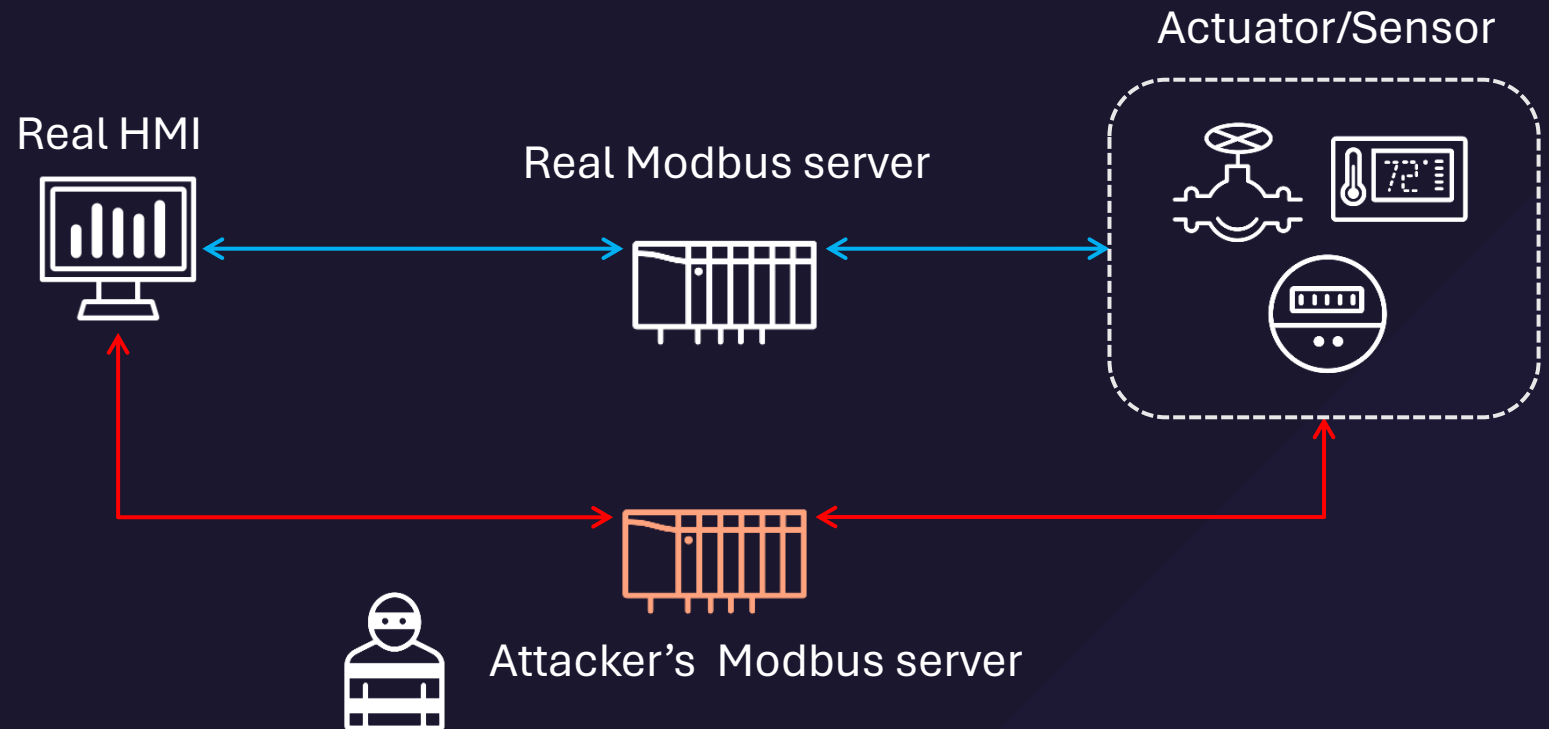


# Modbus

- Demo 情境模擬

建置一個假的  
**Modbus server**

以ARP Spoofing 劫  
持連線，並以虛假  
的 server 雙方溝通



# 建立虛假的 Modbus server

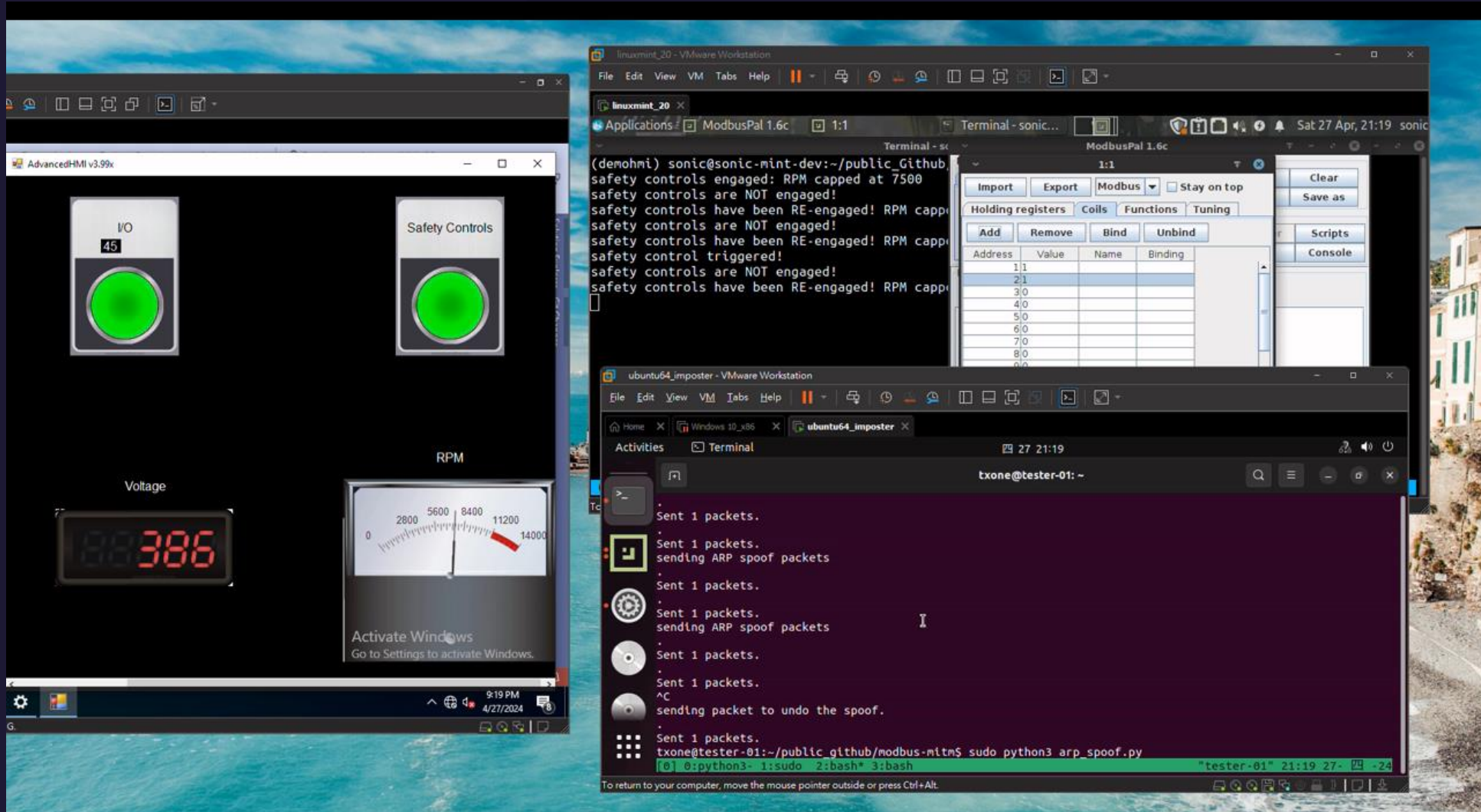
The image displays a virtual machine environment with three main components:

- Linux Mint VM (top left):** Shows a terminal window with a script outputting status messages: `(demohmi) sonic@sonic-mint-dev:~/public_github/`  
`safety controls engaged: RPM capped at 7500`  
`safety controls are NOT engaged!`  
`safety controls have been RE-engaged! RPM capped at 7500`  
`safety controls are NOT engaged!`  
`safety controls have been RE-engaged! RPM capped at 7500`  
`safety control triggered!`  
`safety controls are NOT engaged!`  
`safety controls have been RE-engaged! RPM capped at 7500`
- ModbusPal 1.6c GUI (top right):** A window showing the ModbusPal 1.6c interface. The 'Holding registers' tab is active, displaying a table of registers:
- ModbusPal 1.6c GUI (bottom right):** A window showing the ModbusPal 1.6c interface. The 'Holding registers' tab is active, displaying a table of registers:

Address	Value	Name	Binding
1/0	942	voltage	voltage (...)
2/7500	7500	RPM	RPM
3/942	942	run time	run time ...
4/0	0		
5/0	0		
6/0	0		
7/0	0		
8/0	0		
9/0	0		
10/0	0		

The bottom right window also shows a terminal window with the command `txone@tester-01:~/public_github/modbus-mitm$` and a status bar indicating `Adding coils completed.`

# 以虛假的 Modbus server 劫持連線



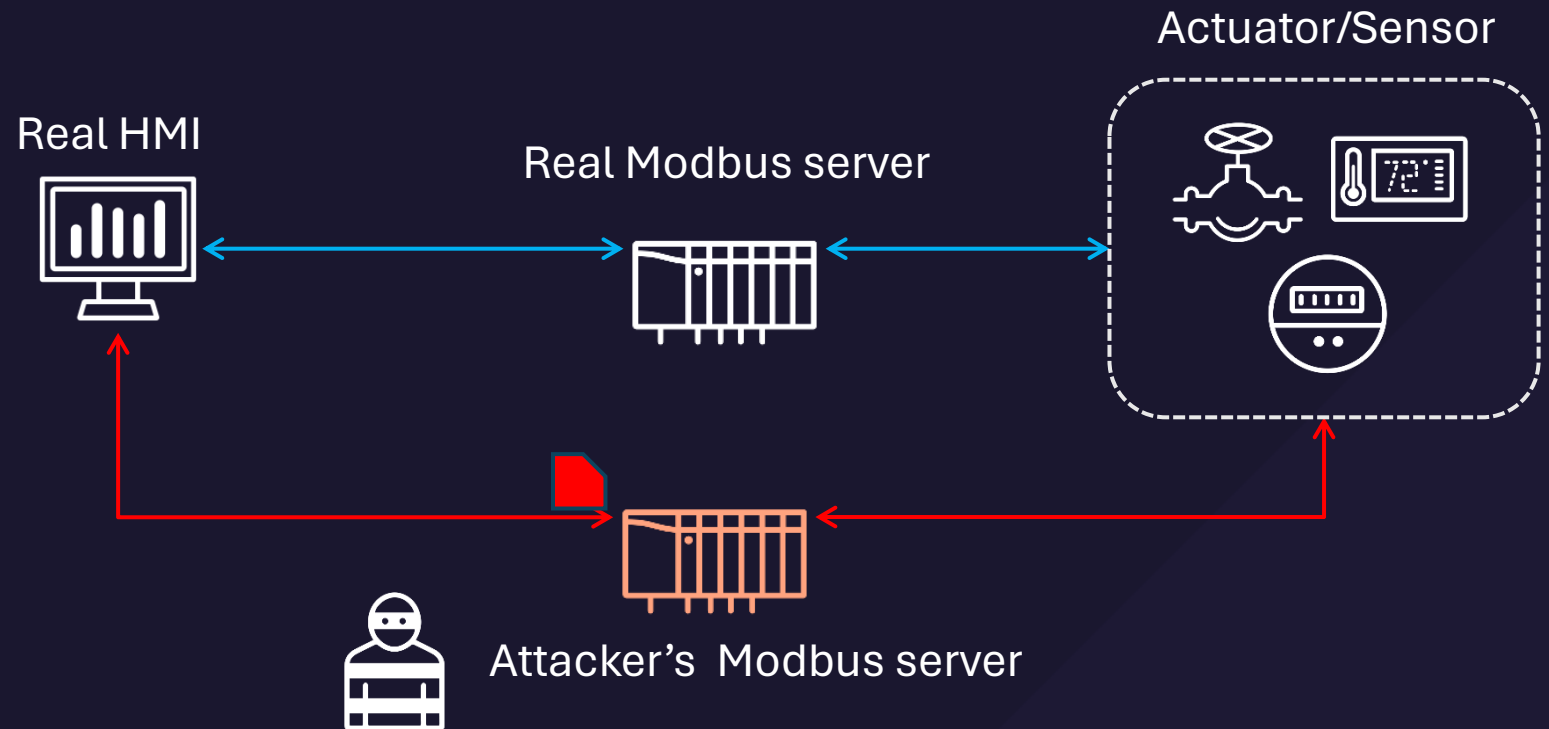
# Modbus

- Demo 情境模擬

建置一個假的  
**Modbus server**

以**ARP Spoofing** 劫持連線，並以虛假的 **server** 雙方溝通

修改數值讓**HMI**無法察覺異常，並修改 **Modbus Slave** 讓渦輪轉速提昇





# 關掉安全閥，並使機器造成損壞

## Holding Register

Address	Name
1	voltage
2	RPM
3	count

## Coil

Address	Name
1	I/O
2	safety

The screenshot displays a ModbusPal 1.6c interface and a terminal window. The ModbusPal interface shows a table of Holding Registers and Coils. The Holding Registers table has columns for Address, Value, Name, and Binding. The Coils table has columns for Address, Value, Name, and Binding. The terminal window shows a script that connects to a client\_real\_server, disables safety controls, and sets RPM to 14000.

ModbusPal 1.6c interface:

Address	Value	Name	Binding
1	820	voltage	
2		RPM	
3		count	

Terminal window (ubuntu64\_imposter):

```
connection = client_real_server.connect()

if connection:
    print('disabling safety controls...')
    client_real_server.write_coils(1, [False], unit=1)
    time.sleep(2)
    print('increasing RPMs to 14000')
    client_real_server.write_registers(1, 14000, unit=1)
    time.sleep(2)
    current_RPM = client_real_server.read_holding_registers(address=0x01, count=1, unit=0x01).registers
    print('centrifuge RPMs are now set to: ' + str(current_RPM[0]))
    client_real_server.close()

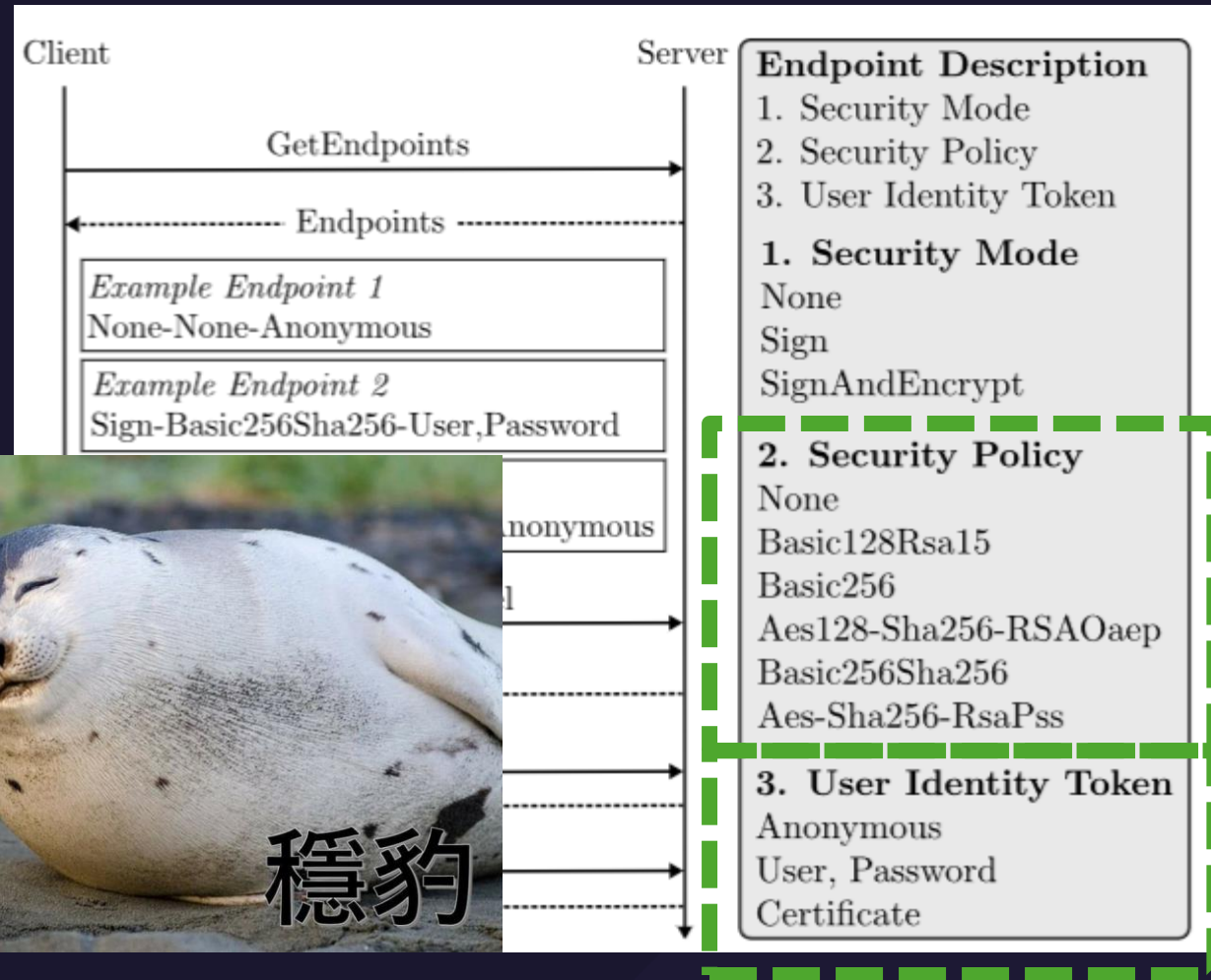
else:
    print('Connection lost, Try again!')
```



# OPC-UA



- 自 2006 年開始使用
- 廣泛為各大工控廠商支援
- 有加密
  - Security Policy
- 有認證
  - Username/password
  - 信任憑證列表



# OPC-UA

- 廣泛為各大工控廠商支援？
  - 根據 2021 年 Alessandro Erba 等人針對各大工控廠商的研究，發現加密跟端點認證實作並未完全
- 有加密？
  - Security Policy 未指定，或指定較弱的加密演算法
- 有認證？
  - 信任憑證列表是否有效？是否正確設定？

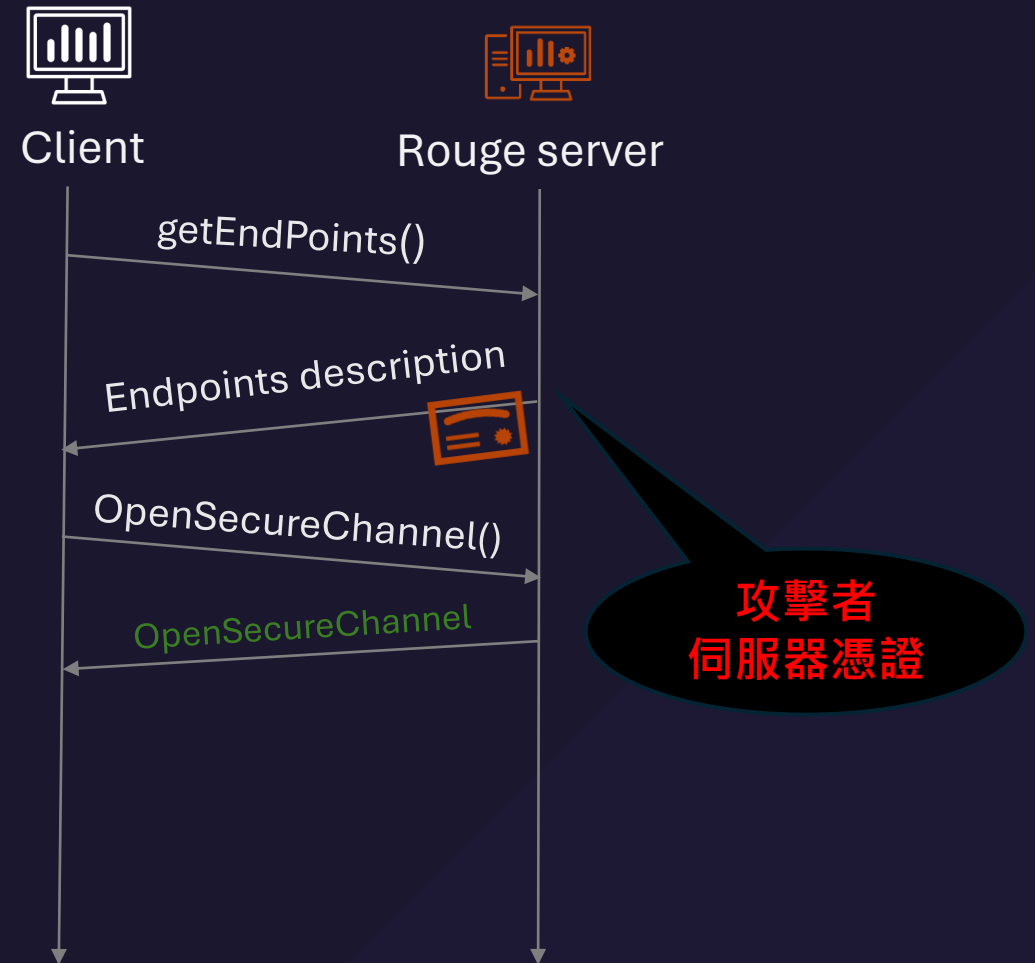
Table 1: OPC UA in proprietary products. ●/○ denotes if the product supports/not supports a feature. ⊙ denotes that there are problems with feature configuration.

Vendor	Platform	OPC Cert.	Pub-Sub	GDS	Security	Trustlist	Recommended Policy
B&R	ADI OPC UA [8]	●	○	○	●	●	Not specified
Bachmann	OPC UA Client/Serv. [4]	○	○	○	⊙	⊙	Not specified
Beckhoff	TC3 OPC UA [5]	○	○	○	⊙	⊙	Deprecated protocols
Beijer	iX Developer [6]	○	○	○	○	○	None
Bosch Rexroth	ctrlX CORE [7]	○	○	○	●	⊙	None not supported
General Electric	iFIX [24]	○	○	●	●	⊙	Basic256Sha256
Honeywell	ControlEdge Builder [28]	○ <sup>+</sup>	○	○	○	○	None
Lenze	Easy Starter [36]	○	○	○	⊙	⊙	Deprecated protocols
Mitsubishi	MX Configurator-R [40]	●	○	○	●	●	None
National Instr.	InsightCM [42]	○	○	○	●	●	None
Omron	SYSMAC-SE2 [45]	●	○	○	●	●	Not specified
Panasonic	HMWIN Studio [54]	○	○	●	●	⊙	Not specified
Rockwell	Factory talk linx [56]	○	○	○	●	●	Not specified
Schneider	Control Expert [18]	●	○	○	●	●	Basic256Sha256
Siemens	STEP 7 [60]	●	○	●	●	⊙	Not specified
Weidmüller	u-create studio [63]	○	○	○	●	●	Basic256Sha256
Yokogawa	SMARTDAC+ [64]	○	○	○	○	○	None
Codesys based platforms							
Codesys	Codesys V3.5 [11]	○	●	○	●	⊙	Not specified
ABB	Automation Builder [1]	○	○	○	●	⊙	Basic256Sha256
Eaton	XSOFT-CODESYS [16]	○	○	○	●	⊙	Not specified
Hitachi	HX Codesys [27]	○	○	○	●	⊙	Not specified
Wago	e!cockpit [62]	●	○	●	●	⊙	Not specified

<sup>+</sup>State of the documentation consulted during the investigation. After a preprint release of this manuscript, the vendor updated the product. Now it supports security and it is certified.

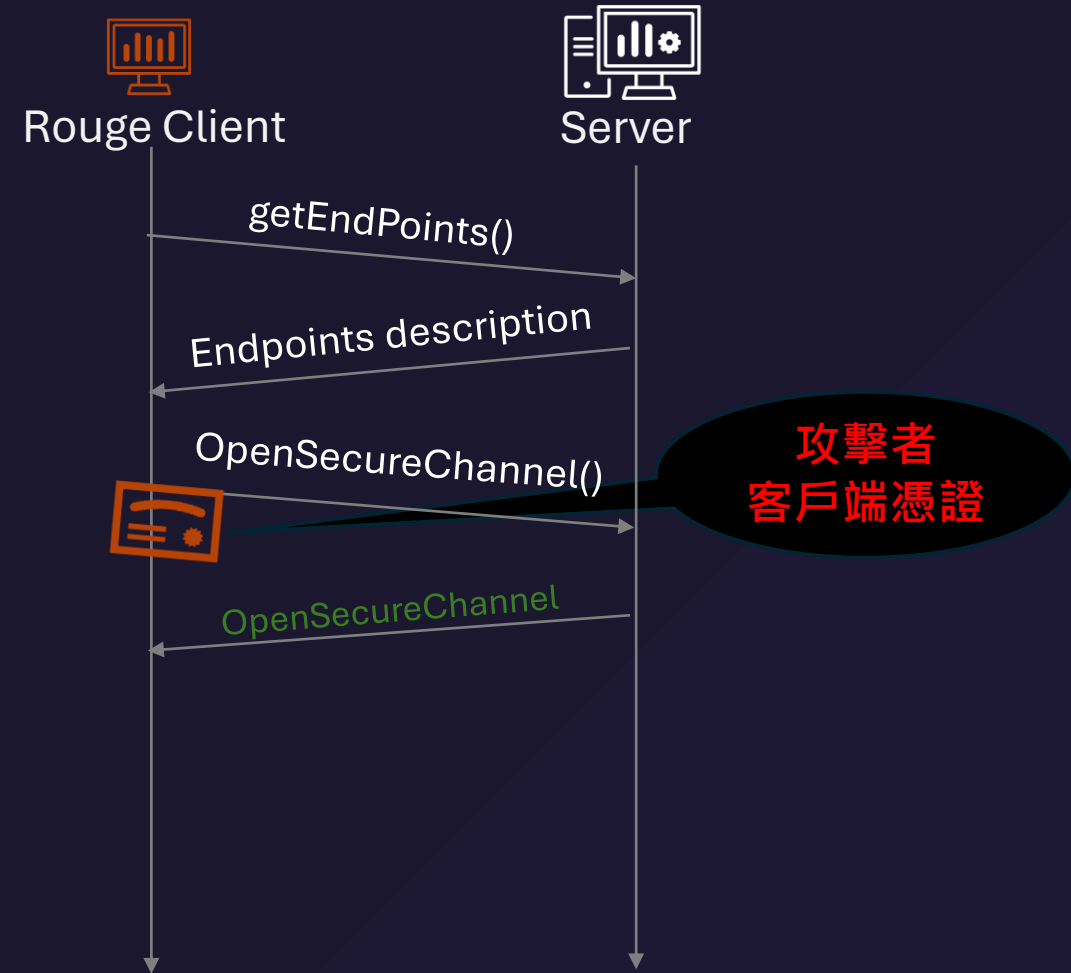
# OPC-UA

- Rouge server 攻擊
  - 若客戶端有正確驗證伺服器端的憑證，則該攻擊無法成立
  - 若客戶端未驗證伺服器端的憑證，攻擊者的伺服器端可使用未受信任的憑證與客戶端連線
- 負面影響：
  - 偷取客戶端的身分資訊



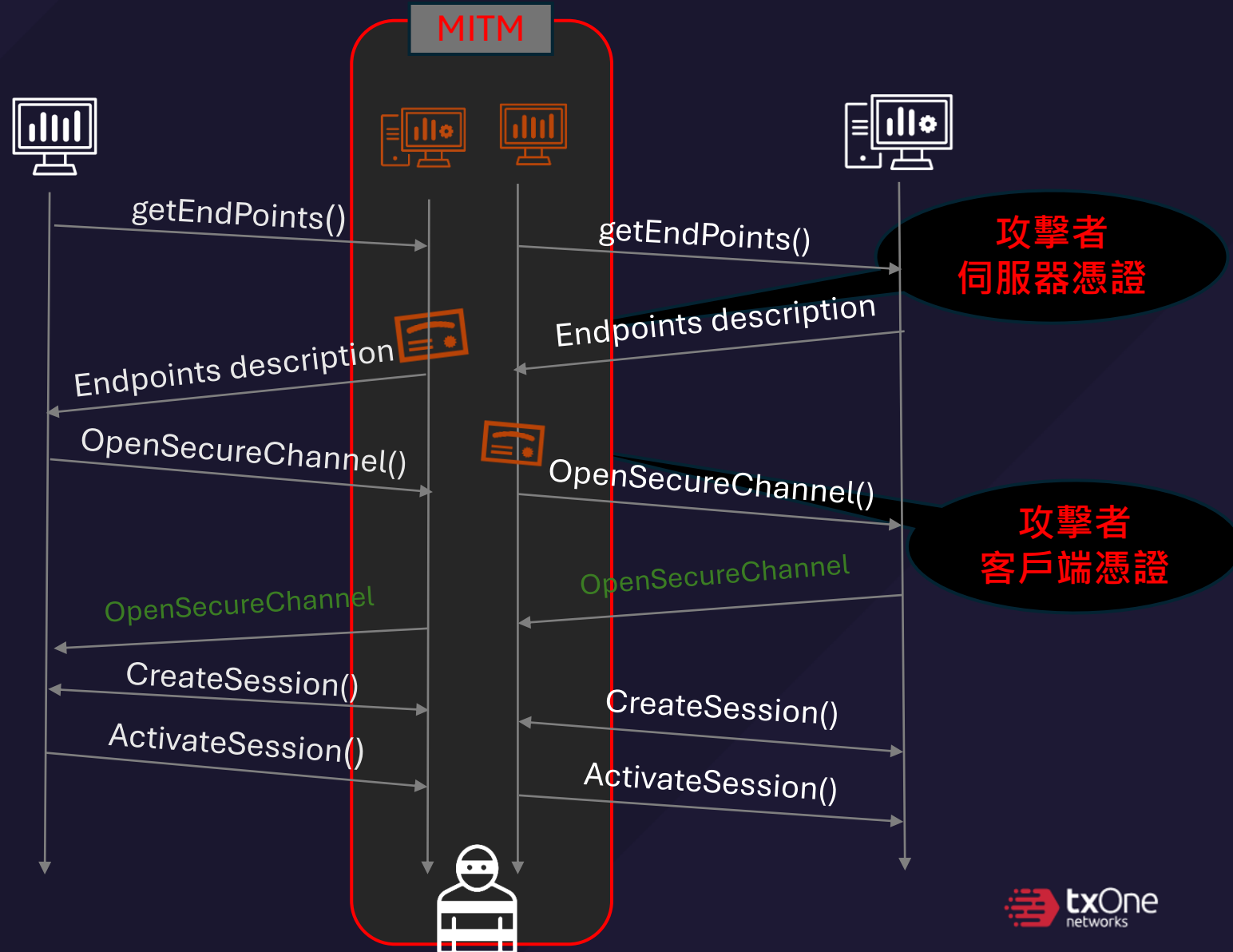
# OPC-UA

- Rouge client 攻擊
  - 若伺服器端有正確驗證伺服器端的憑證，則該攻擊無法成立
  - 若伺服器端未驗證伺服器端的憑證，攻擊者的伺服器端可使用未受信任的憑證與客戶端連線
- 負面影響：
  - 竊聽或篡改伺服器數據或指令



# OPC-UA

- Rouge server 攻擊  
+ Rouge client 攻擊  
= 中間人攻擊成立
- 負面效果：
  - 偷取客戶端的身分資訊
  - 竊聽或篡改伺服器數據或指令





# OSDP



- 普遍用於門禁系統
  - Serial port RS-485
- 取代無任何安全機制的 Wiegand協議
- LibODSP: 開源 OSDP 函式庫，方便實作該協議
  - 支援 C, Python, Rust
- 有加密
  - OSDP secure channel
- 有認證
  - 以MAC 驗證信息防止重播攻擊

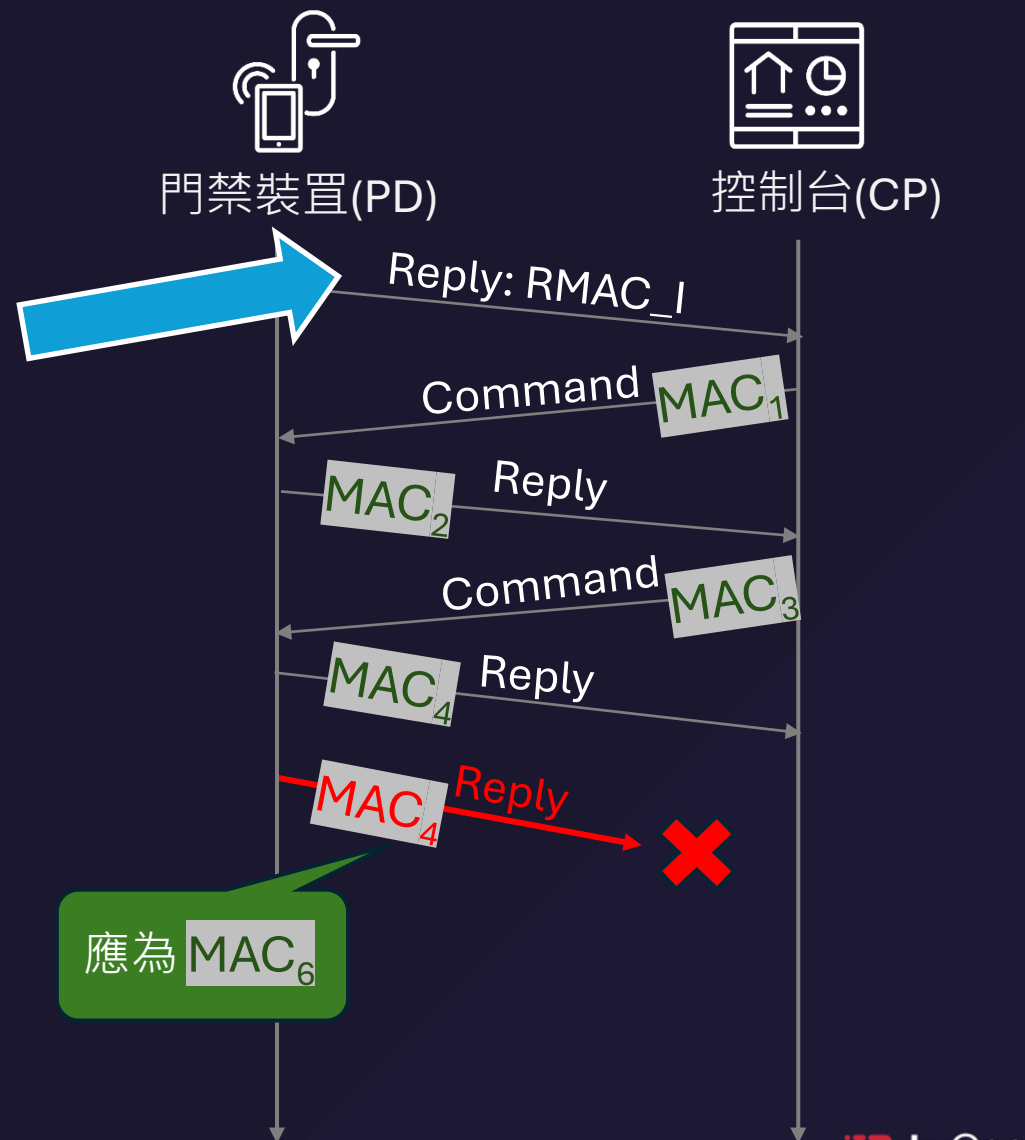
# OSDP

- OSDP Secure Channel
  - 利用 16 bytes MAC 以作為驗證資訊建立信息之後，門禁裝置發送 RMAC\_I 信息至客戶端，之後成為該會話的第一個 MAC。  
**MAC<sub>1</sub>**
  - 客戶端以該 MAC 導出第二個 MAC，並以該 MAC 加密資訊發送至客戶端  
**MAC<sub>2</sub>**








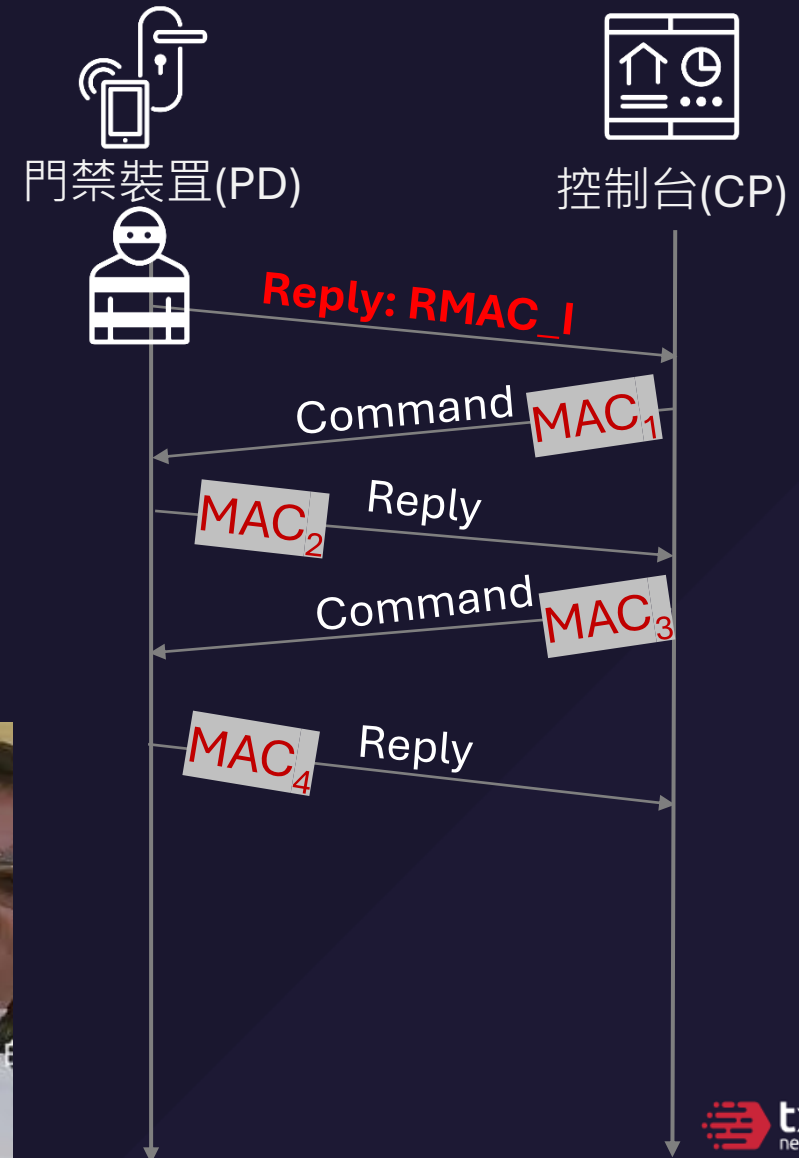
# OSDP

- 攻擊者無法從中發送偽造資訊
  - MAC 驗證不會過
- 如果初始的 MAC 是可以捏造的呢
- LibOSDP 漏洞：藉由捏造 RMAC\_I 以劫持對話。



# OSDP

- 攻擊者可在會話開始時，捏造 RMAC\_I 信息
- 攻擊者可牢牢掌握 
- 進而導出    
- 攻擊者可以送出卡片資訊，且之後的信息都可以被驗證
- 芝麻開門！



# OSDP

- PD Busy Reply 濫用
- 協議等級的漏洞
- 無需驗證或加密
- 可在 security channel 建立後的任何時間發出
- 遭濫用的門禁無法正常運作
  - 門禁系統需重新連線





# OSDP

- PD Busy Reply 濫用
- 協議等級的漏洞
- 無需驗證或加密
- 可在 security channel 建立後的任何時間發出
- 遭濫用的門禁無法正常運作
  - 門禁系統需重新連線
  - 社交攻擊 (?)





# 如何防禦/緩解OT領域中間人攻擊？

## 如何防禦/緩解OT領域中間人攻擊？

- 正確地設置加密及認證方法，以保障會話雙方的安全
  - Modbus-TCP 支援 TLS 加密
  - OPC-UA 開啟信任憑證列表，並且選定強健的加密演算法
- 零信任政策：
  - 嚴格管理存取控制列表，僅給予相關人員最小權限
  - 嚴格驗證並控管進出廠區的設備，避免可疑設備介入關鍵場域操作，造成中間人攻擊的機會
  - 嚴格驗證並控管進出廠區人員，避免可疑人士介入關鍵場域，造成偷竊或破壞





# 結語

## 結語



- 中間人攻擊不僅會發生在 IT 場域，OT 也會發生
- 老舊的工控協議難以抵禦此類攻擊
- 經過幾經翻修，甚至是新版的工控協議，也會因為廠商的實作，或是設定的失誤，讓中間攻擊者有機可乘
- 選擇並設定適當的認證機制，並在之後的會話中加密，有助於減少攻擊發生
- 管控廠中的設備及人員，也可以有效防止攻擊發生



# Q&A

Thank You  
and  
Keep The Operation Running



感謝您參加講座， 掃描QR Code填寫問券即可到Q106攤位上玩遊戲得好禮