從 Hacker視角看智慧家庭資訊安全防護

Information Security of Smart Home from Hacker Perspective

精品科技資安顧問 陳伯榆

智慧家庭帶來許多便利，也帶來了資安隱私問題

FineArt

智能燈光控制

亮度、情境顏色調整與定時照明。

遠端嗅探與控制

影音控制

定時、多情境、集中與控制。

遠端控制與智慧電視入侵...

智慧門鎖與車庫

視訊對講、門禁，遠端開鎖。

遠端控制、行為窺視

智能警衛

社區安全、留言、包裹通知

遠端控制、窺視、門禁失效

智慧插座與家電

智能家電空調溫濕控制與通知

遠端嗅探與控制

窗簾門窗控制

採光狀態通知與啟動

遠端嗅探控制與窺視

智慧安全監視

小孩寵物監視、居家安全

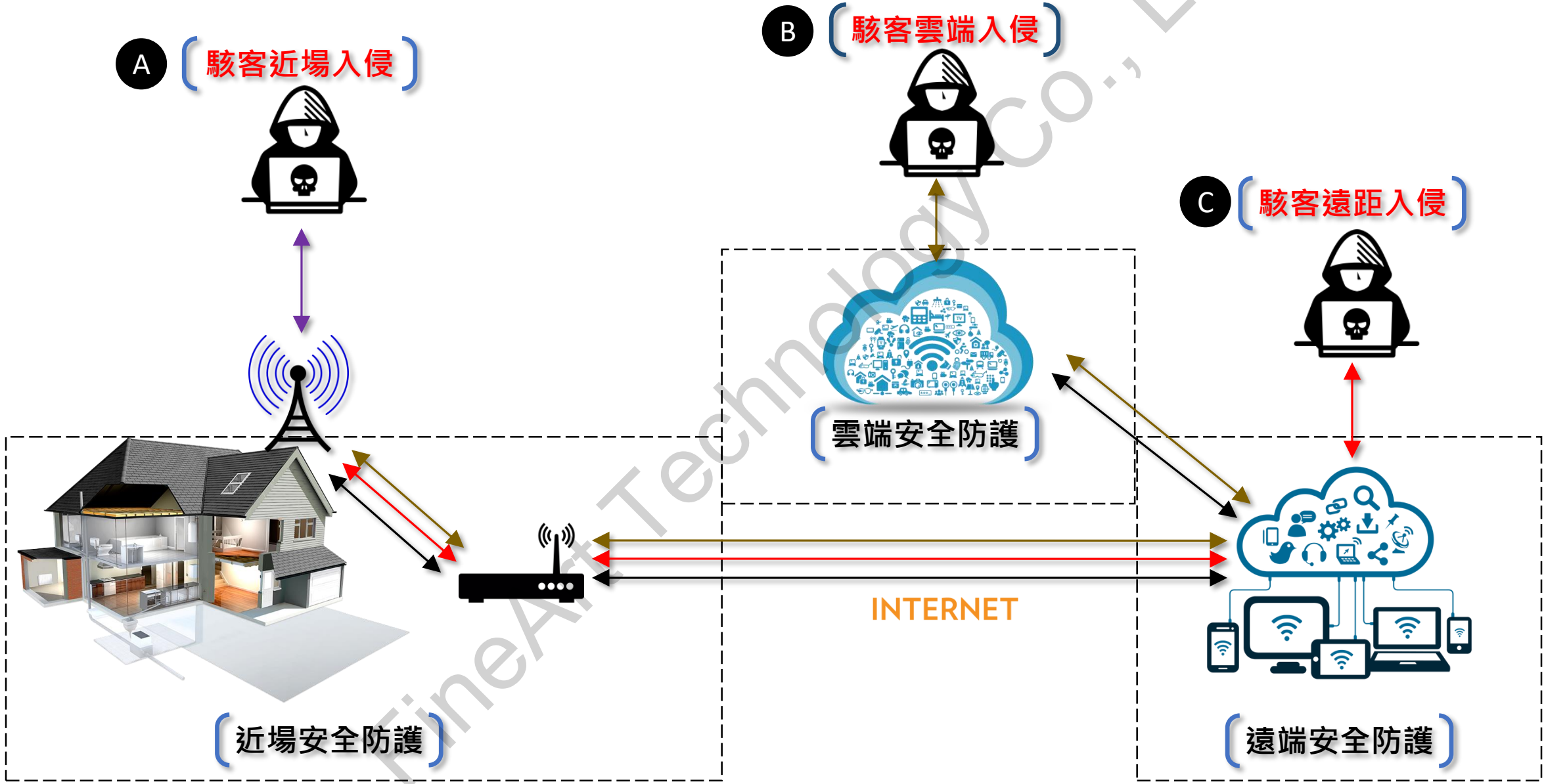
遠端控制、窺視

園林灌溉系統

時間與水量控制

遠端嗅探控制

從駭客入侵視角看智慧家庭在資訊安全的風險



駭客視角在「近場」入侵、嗅探與捕捉手法

駭客近場入侵

http://ubertooth.sourceforge.net/hardware/one/

使用Ubertooth One 進行嗅探

Wi-Fi AP 入侵手法多樣，除常見密碼強度與預設未變更外，還有自身韌體漏洞以及管理系統安全強度不足...等內外問題合成。

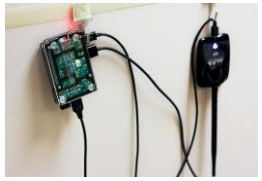
駭客還可利用WiFi Pineapple，進行MITM入侵擷取。

有許多專門Wi-Fi Hacking tools 與裝置整合應用，來入侵、嗅探、MITM...無線網路通訊。甚至透過無線印表機為中介入侵。

2 入侵Bluetooth

1 入侵Wi-Fi AP

中華電信，北中南區VDSL 都有一組預設的帳號密碼，直接使用VDSL隨附Wi-Fi，可以進行相關環境變更與修改。



Wi-Fi Hacking tools 3

6 入侵VDSL

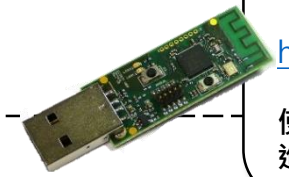
Decoding LoRa 4

5 Hacking Zigbee

https://www.tiny-dev.com/decoding-lora-with-hackrf-gnuradio/

使用SDR 進行側錄解譯再重放

近場安全防護

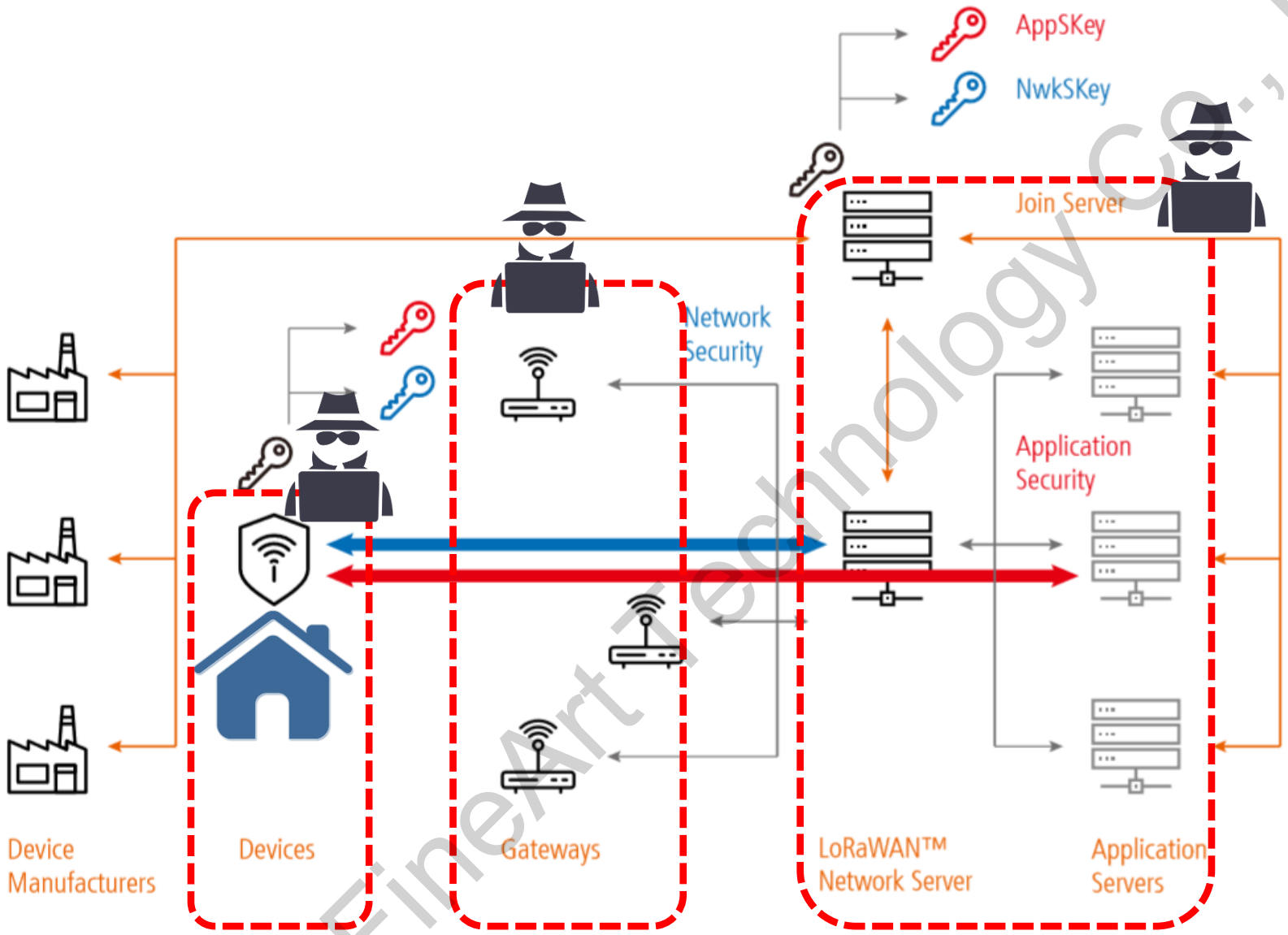


http://blog.attify.com/2017/04/24/hack-iot-devices-zigbee-sniffing-exploitation/

https://github.com/riverloopsec/killerbee

使用Attify Zigbee Framework 或是killerbee 進行入侵

在「LoRa」與「LoRaWan」的嗅探與捕捉



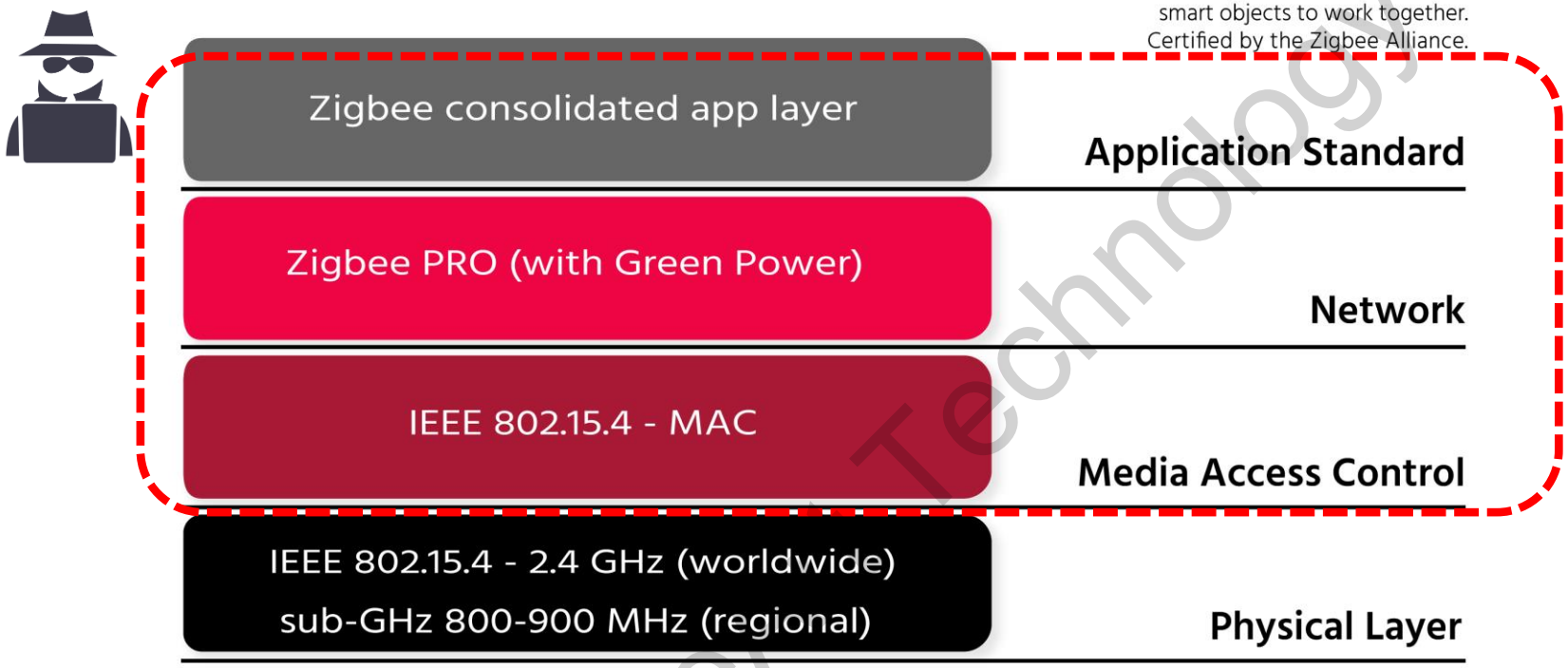
https://www.lora-alliance.org/lorawan-white-papers

DEF CON - Matt Knight - Reversting LoRa Deconstructing a Next Gen Proprietary LP

https://github.com/rpp0/gr-lora

GNU Radio blocks for receiving LoRa modulated radio messages using SDR

在「 Zigbee 」的嗅探與捕捉



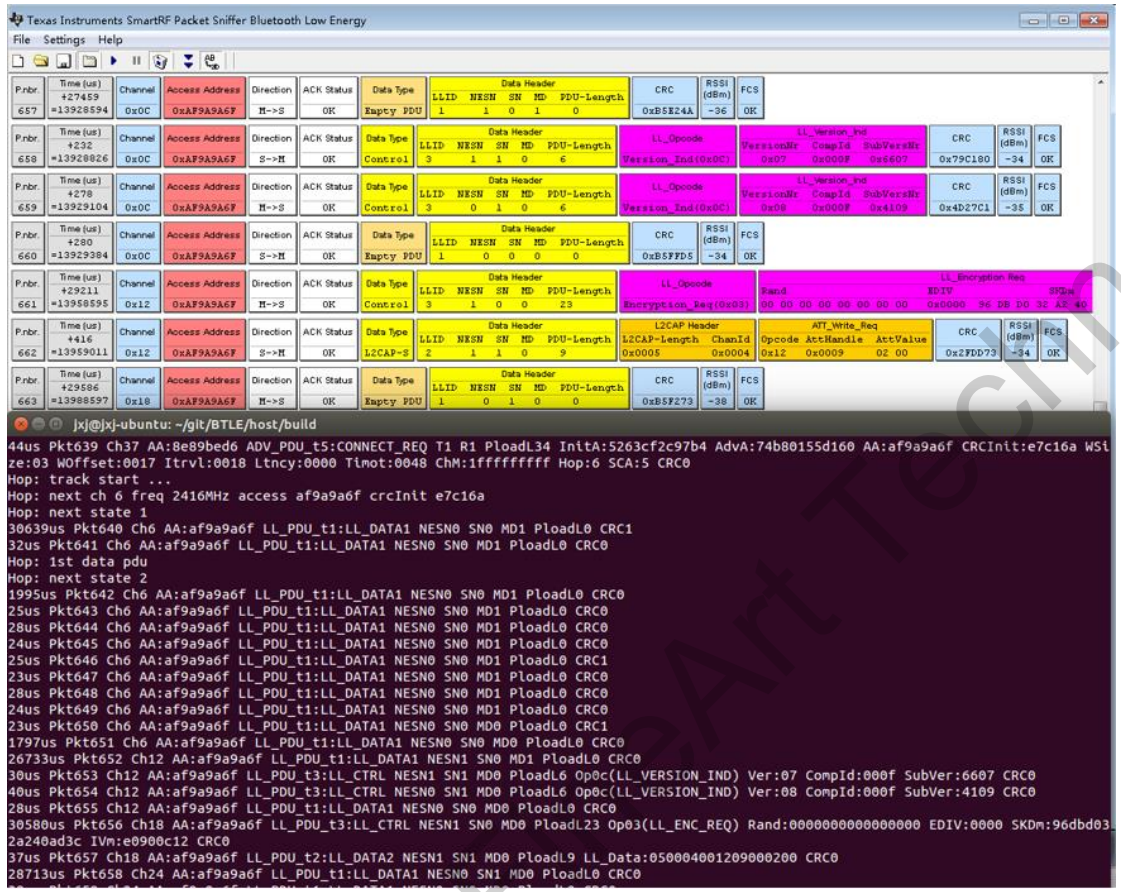
http://www.zigbee.org/

ZigBee Exploited The Good, The Bad, And The Ugly

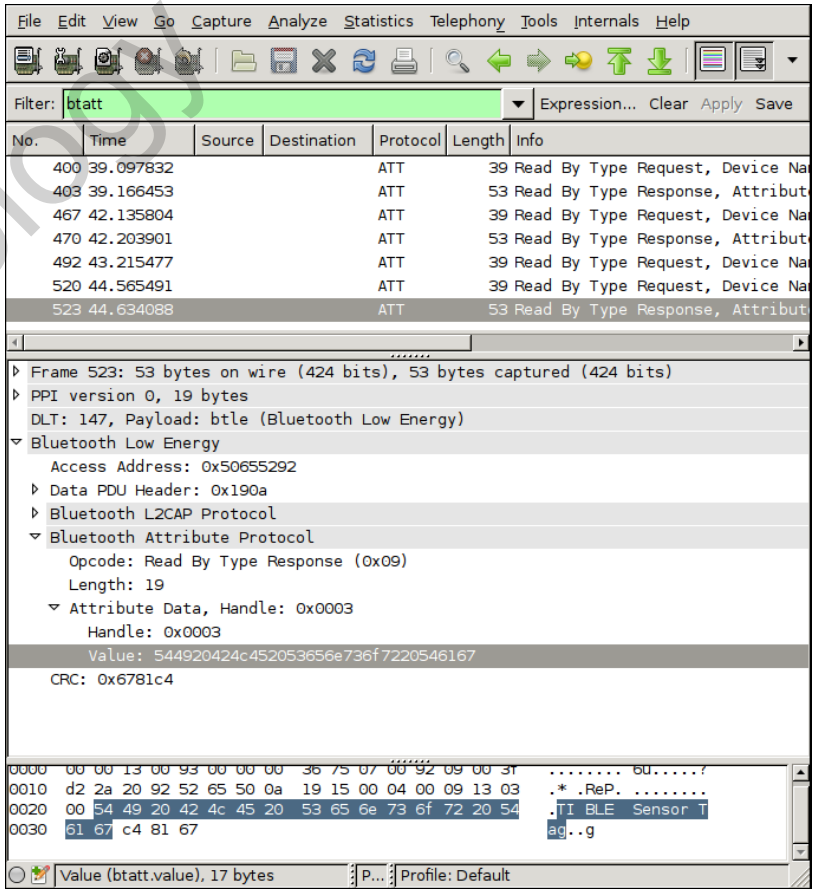
Hacking ZigBee Light

在「 BLE 」「 BL」的嗅探與捕捉

- 使用TI-CC2540藍牙低功耗模組，搭配SmartRF PACKET-SNIFFER監聽器軟體，對三種藍牙廣播通道嗅探。(40個頻道中：37、38、39為廣播用，其他37個頻道用在資料傳輸)。也可以HackRF BTLE作為替代使用。以下是對比圖。



要捕獲通信中的藍芽封包，必須使用Ubertooth One來處理，也必須搭建環境：安裝Python & libn1-dev, libusb...、libbtbb、ubertooth、wireshark、kismet、BLE解密工具crackle (https://github.com/mikeryan/crackle)



駭客視角在「遠距雲端」入侵的手法

FineArt

1 遠距入侵

Wi-Fi AP 入侵手法多樣，除常見密碼強度與預設未變更外，還有自身韌體漏洞以及管理系統安全強度不足...等內外問題合成。

駭客還可利用WiFi Pineapple，進行MITM入侵擷取。

駭客遠距入侵

駭客雲端入侵

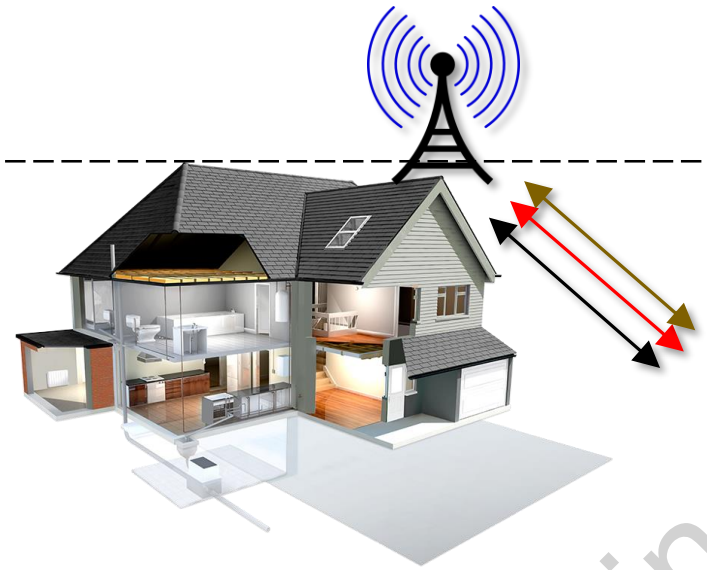
2 裝置商雲端入侵

廠商所提供智能家庭的雲端服務，Web 程式與資料庫強度不足。駭客設法繞過防守侵入backend端竊取資料或是遠端入侵

雲端安全防護

3 遠距IoT入侵

- 缺乏整合的資安評估與架構規劃
- Web Console 程序強度不足
- Logon Password 預設，無變更
- 暴露在外，無法防禦暴力破解
- Debug 通訊埠易於嗅探與暴力破解
- 採用低安全協定HTTP, Telnet
- 嵌入式OS，安全強度不足
- 除錯用與隱藏的帳密外流或隱匿通道



INTERNET

近場安全防護

遠端安全防護

駭客工具軟體，讓智慧家庭安全被試煉

FineArt

嗅探/入侵/DDoS/滲透...軟體工具篇

1. Airbase-ng
2. Aircrack-ng
3. Airdecap-ng
4. Airdecloak-ng
5. Aireplay-ng
6. Airmon-ng
7. Airodump-ng
8. airodump-ng
9. Airolib-ng
10. Airserv-ng
11. Airtun-ng
12. Asleap
13. Besside-ng
14. Bluelog
15. BlueMaho
16. Bluepot
17. BlueRanger
18. Bluesnarfer
19. Bully
20. coWPAtty
21. crackle
22. eapmd5pass
23. Easside-ng
24. Fern Wifi Cracker
25. FreeRADIUS-WPE
26. Ghost Phisher
27. GISKismet
28. Gqrx
29. gr-scan
30. hostapd-wpe
31. ivstools
32. kalibrate-rtl
33. KillerBee
34. Kismet
35. makeivs-ng
36. mdk3
37. mfcuk
38. mfoc
39. mfterm
40. Multimon-NG
41. Packetforge-ng
42. PixieWPS
43. Pyrit
44. Reaver
45. redfang
46. RTLSDR Scanner
47. Spooftooph
48. Tkiptun-ng
49. Wesside-ng
50. Wifi Honey
51. wifiphisher
52. Wifitap
53. Wifite
54. Wpaclean
55. Radiotap
56. Scapy
57. LANs.py
58. LAZY script
59. PineAP
60. BoopSuite
61. WiFi-Pumpkin
62. Charon
63. WiFi-Pumpkin
64. FruityWifi
65. nfernal-Twin
66. CommView
67. PwnSTAR
68. WiFiSlax
69. AirSnort
70. CoWPAtty
71. Airjack
72. WepAttack
73. inSSIDer
74. WepDecrypt
75. OmniPeek
76. CloudCracker
77. Pyrit
78. EasyCreds

硬體篇

1. Hak5 Pineapple
2. HackRF
3. SDR 裝置
4. SySS Radio Hack Box
5. Raspberry
6. iU880B LoRaWAN
7. WiMonitor
8. 3g/4g 網卡
9. A Universal RFID Key

技術篇

1. Python
2. Web hacking
3. Linux 指令
4. Kali Linux
5. 封包分析
6. 網路架構
7. 網路服務滲透
8. 裝置協定與入侵程式

特殊篇

1. Mousejack（無線滑鼠）
2. Hijacker（Android）
3. SDR+inspectrum（無線訊號）
4. Xiaopan（Wi-Fi 專用OS）
5. WAIDPS（無綫防護偵測）
6. kisMAC（Mac用）
7. Cain & Able（破密）

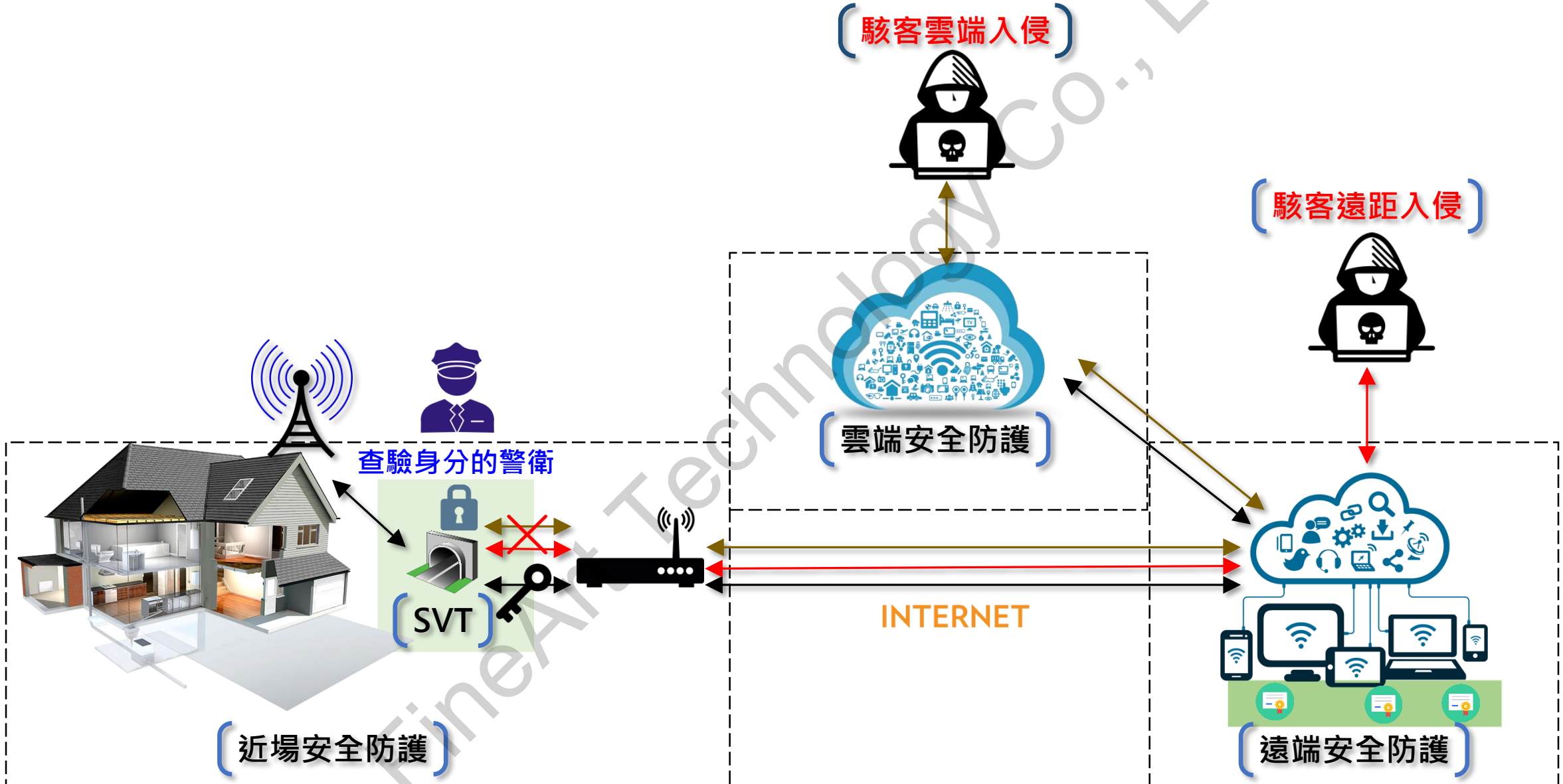
各協定下滲透、嗅探、捕捉與重放裝置

Decoding the LoRa IoT Protocol with an RTL-SDR	Zigbee, BLE Sniffer USB dongle (TI) CC240	SDR with HackRF (GSG)	Ubertooth One for BLE (GSG)
			
WIFI PINEAPPLE nano (HAK5)	**Radio Dongle USB (GSG)**	**WiMonitor Wi-Fi (HACKER ARSENAL)**	**Proxmark 3 RFID & NFC**
			

回到近場智慧裝置安全設計與建議

	端點裝置端	中介端	Wi-Fi AP	SVT	VDSL	Cloud Backend	使用者控制端
裝置特徵協定	Asus IoT Device (Lighting、Home Robots、…多類裝置) Lan、Wi-Fi、LoRa、藍芽、ZigBee、… 	例如： Asus IoT Gateway LoRa Gateway ZigBee Gateway 	市面各類功能不一的Wi-Fi Router 802.11xx 		VDSL Cable Modem 	Backend Cloud Service 	Smartphone App Laptop App & Remote Pad App 
安全設計	• 使用Radius 認證機制，取代傳統WPA/WPA2 加密金鑰機制。依賴 Wi-Fi AP 是否具備而定。 • 使用Mac ACL 這是最低限度，以白名單方式防守。缺點是Mac 偽造，以及只認證未加密。 • 繼續使用WPA2，必須要建立起防堵WPA2 四方交握漏洞的防禦模式 • 或是採用LoRa, ZigBee智慧裝置，但其中介管理裝置可能也會回到Wi-Fi 接取。 • 裝置不要直接對外放行。	• 同左建議事項，因為中介管理裝置可能也會回到Wi-Fi 接取。 • 裝置不要直接對外放行。	• 選擇較高階商用機種，具VPN或是 Radius 功能是最合適的模式。 • 登入帳號密碼，要定期期更換。 • 關閉Web遠端登入隱藏SSID。 • 定期更新韌體與監看管理者登入記錄 • 防火牆建議啟動，來解決廠商預設除錯用服務協定。		• VDSL 更換密碼，採強固行密碼。 • 關閉VDSL 無線網路服務功能，改由Wi-Fi AP來運作。 • 將 VDSL 管理功能中，安全設定提高 • Disable 非必要服務與協定。	• 只能信賴智慧家庭裝置廠商的安全機制。 • 關閉非必要雲端管控端點裝置的功能。	• Client端的智慧手機、平板、以及電腦，都必須要有安全防護機制。 • 有效識別非友善來源的存取與程序安裝。

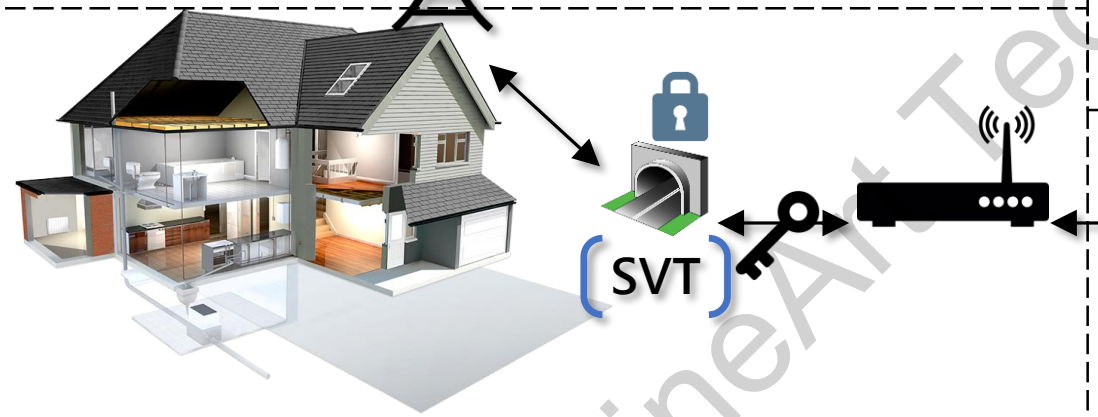
實驗場域：SVT遠端安全設計，攔阻遠距入侵



實驗場域：SVT運作原理與程序(敵我識別)

未來進階整合設計
- 搭載Radius 機制，讓智慧裝置都透過安全註冊方式，放行對外連線，大幅降低「近場」入侵植入的問題。
- 擁有自身防火牆機制以及防駭安全區設計...等自體防禦
- 版本更新由雲端派送更新，派送時將與Client裝置私鑰驗證後進行。(解決駭客繞行偽造問題)

- 安全session key 防護
- 驗證通過後，才放行連線作業



SVT

近場安全防護

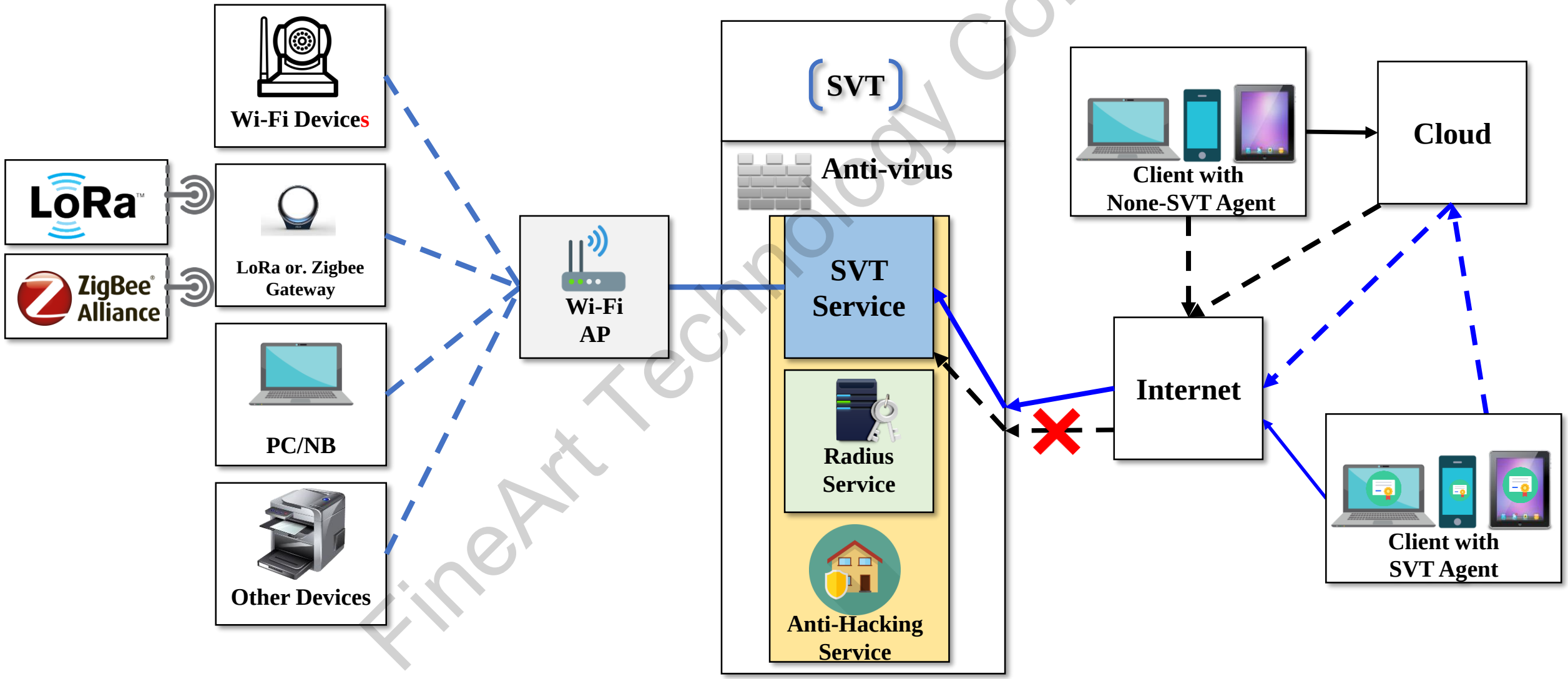
雲端安全防護

- 端點裝置，會置入一個Agent
- Agent 具有相關加密防護機制
- 連接智慧家聽網絡時，會建立一個安全加密通道
- 並確認驗證據其合法身分才能存取，相關裝置資訊。

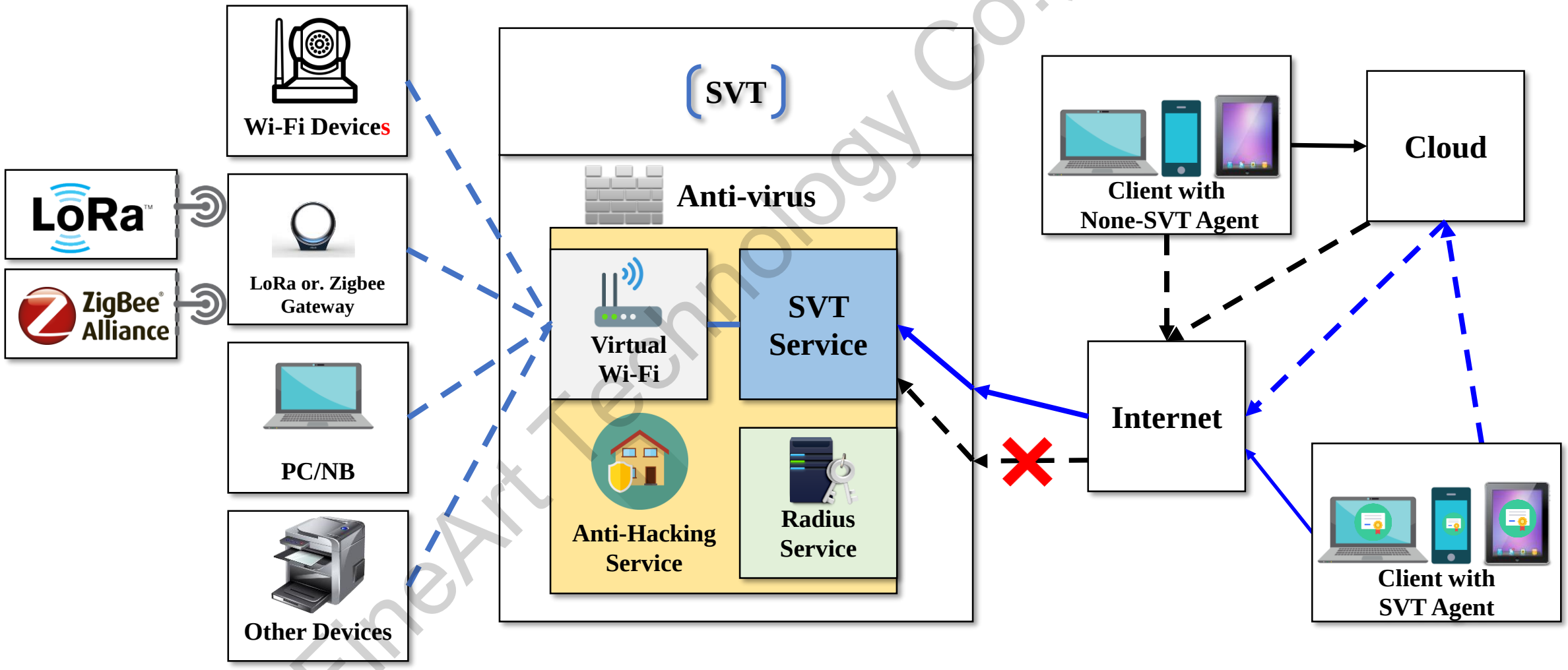
INTERNET

遠端安全防護

實驗場域：SVT防護示意圖-I(敵我識別)



實驗場域：SVT進階防護示意圖-II(敵我識別)



徹底的預防是一種幻想。我們仍需要為美好安全的智能生活繼續努力。