教育部「5G行動寬頻人才培育跨校教學聯盟計畫」
5G行動網路協定與核網技術聯盟中心

行動邊緣計算
可推廣教材模組

單元-07：邊緣計算之應用與資安議題

授課教師：萬欽德

國立高雄科技大學 電腦與通訊工程系

Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

目標

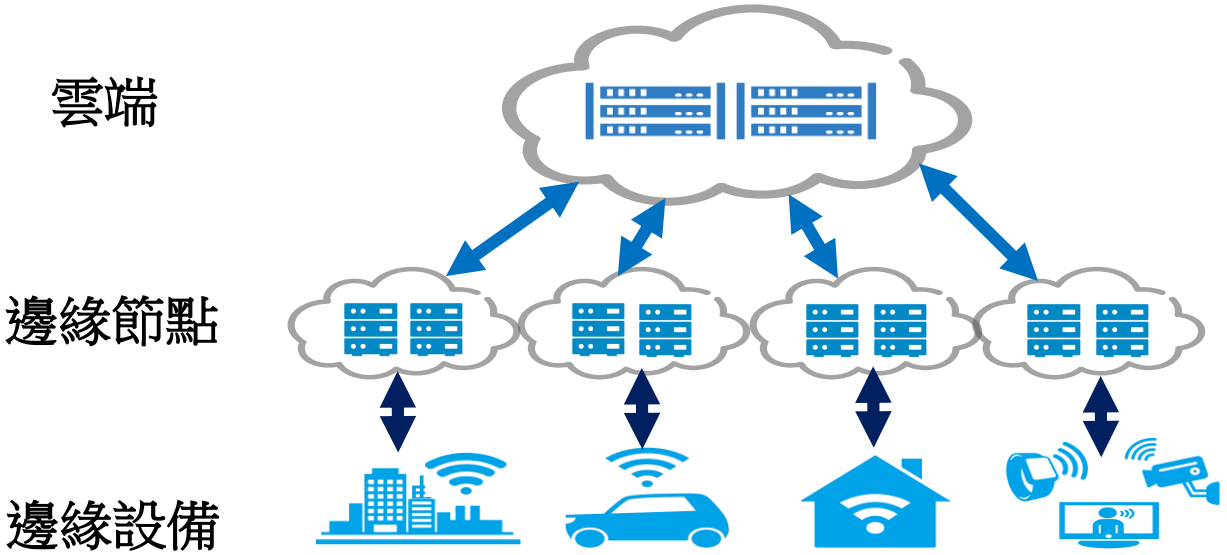
- 由於邊緣運算可滿足5G用戶端網路的高頻寬、低時延及大規模物聯網裝置連接的需求，並提供用戶端設備靈活與快速資料存取服務，因此邊緣運算的資安威脅也將影響用戶端資料存取安全、通訊安全及設備安全等問題
- 藉由研析行動邊緣運算資安威脅，探討用戶端網路資安議題，並透過行動邊緣運算應用資安攻防實作，實證5G用戶端與異質網路等隱私相關之攻擊技術與防護建議，以提升中心5G用戶端網路資安攻防與檢測能量

Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

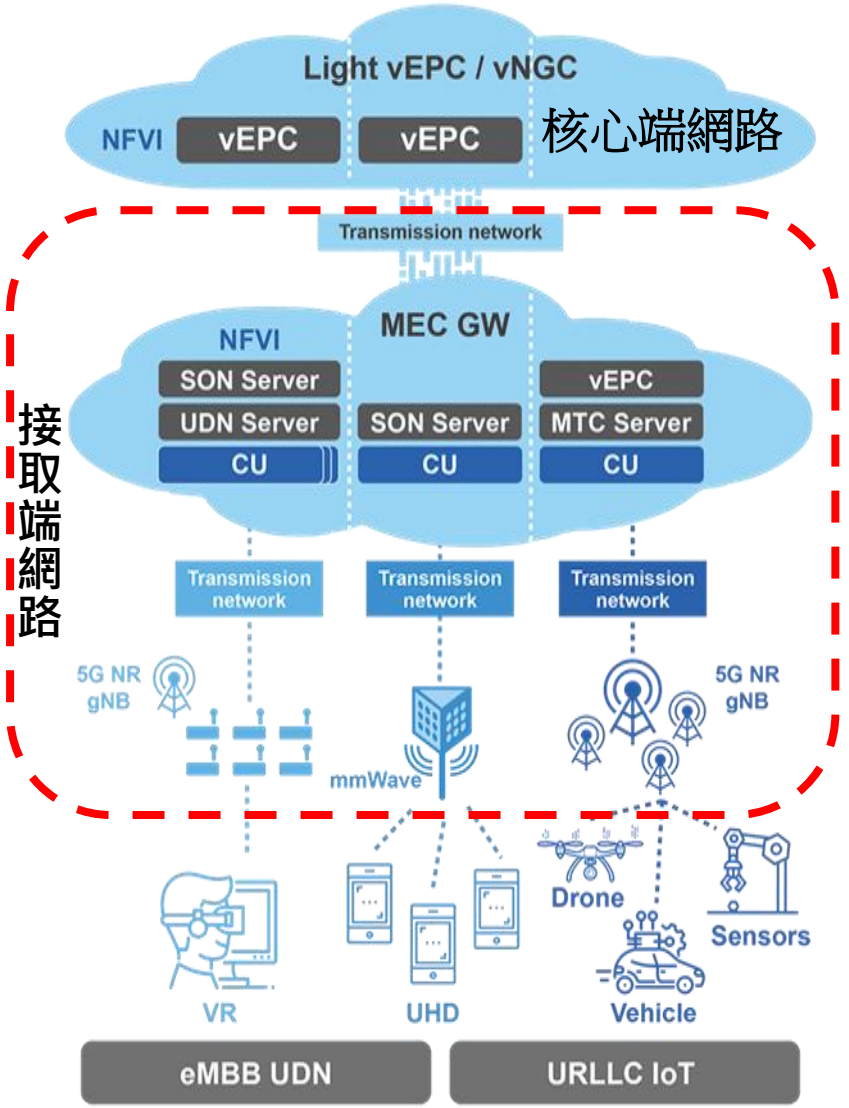
何謂邊緣運算

- **邊緣運算**是一種分布式運算概念，它將智慧邊緣設備透過有線或無線通訊，並允許於邊緣節點進行即時處理和分析資料，在邊緣節點運算中，資料不需要直接上傳到雲端或集中資料處理系統
- 邊緣運算應用於行動通訊的接取端網路，並提供雲端運算能力的網路架構，稱為**行動邊緣運算**



5G行動邊緣運算的重要性

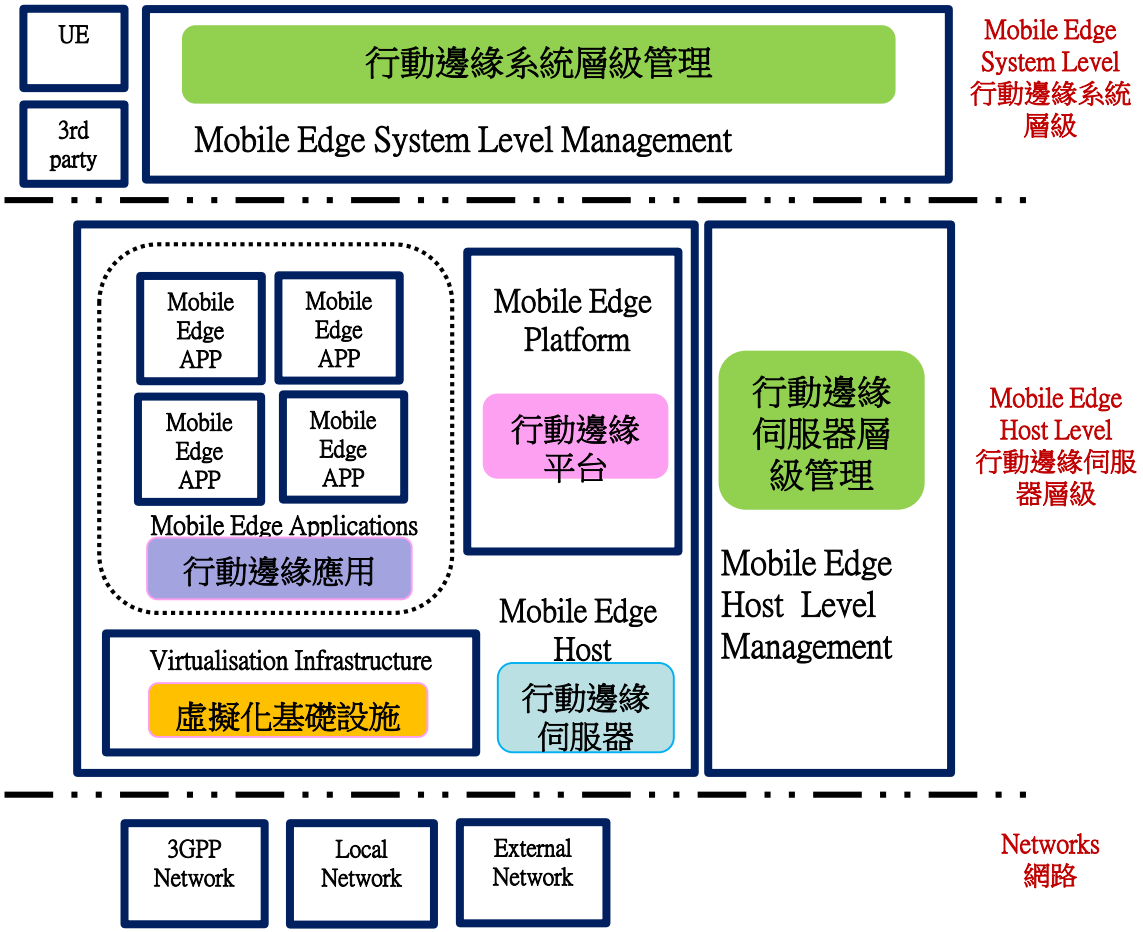
- 行動邊緣運算是由歐洲電信標準化協會(ETSI)提出，主要利用靠近電信網路接取側也就是基地臺端部署通用伺服器，來提供 IT 服務環境以及雲端運算能力
- 行動邊緣運算平台可以支援具有各種垂直服務應用場景，並提供分流核心網路流量，來實現低時延、高流量處理及大量物聯網裝置存取功能
- 由於ETSI主要定義5G行動邊緣運算網路框架，同時行動邊緣運算的通訊協定、身分認證及資料存取管理仍未有一致性規範與要求，因此行動邊緣運算的安全是目前主要挑戰議題



ETSI行動邊緣運算平台框架(1/2)

ETSI行動邊緣運算框架為行動邊緣系統層級、行動邊緣伺服器層級及網路三部分所組成

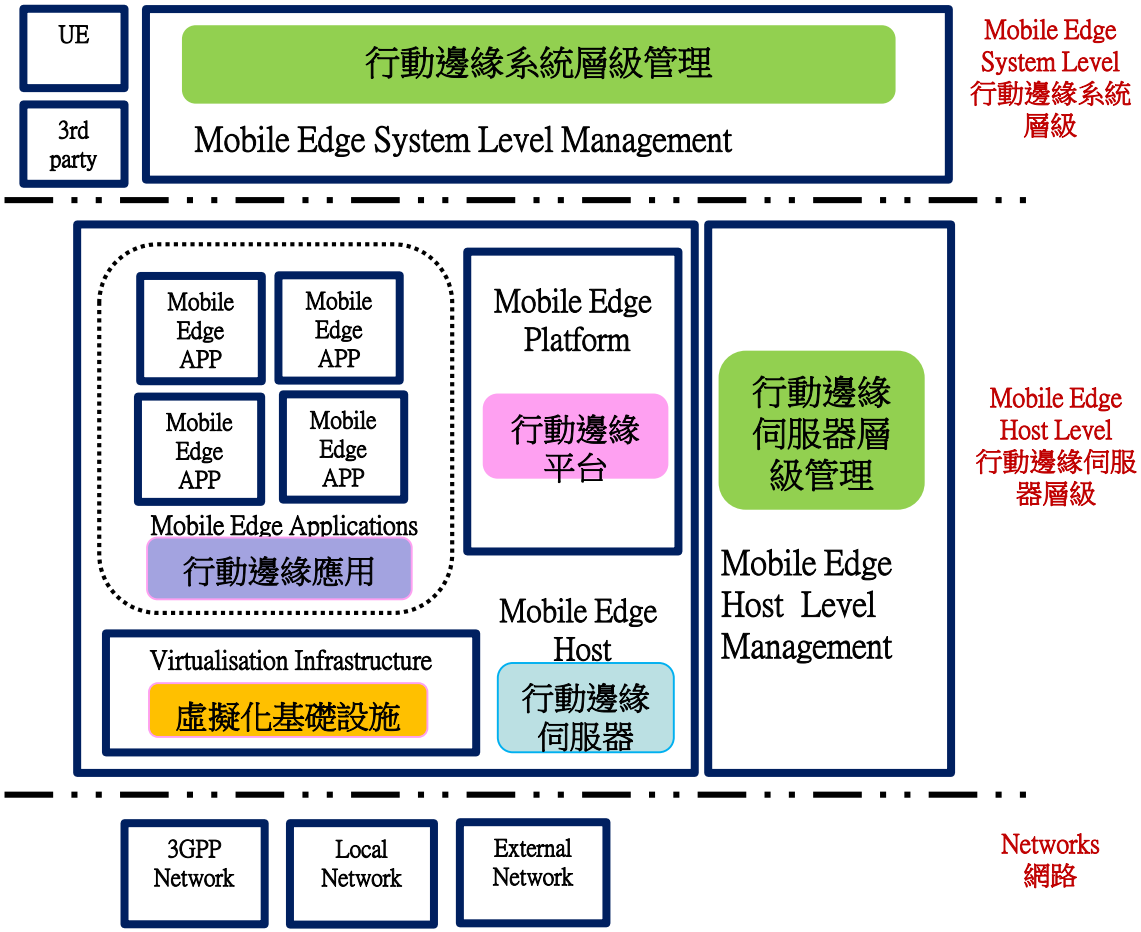
- **行動邊緣伺服器層級(Mobile Edge Host Level)**
  - **行動邊緣伺服器(Mobile Edge Host)**：為一般商用伺服器並於硬體資源上利用虛擬化技術來實現下列各項功能
    - 虛擬化基礎設施(Virtualisation Infrastructure)：為提供平台計算、儲存與網路資源
    - 行動邊緣平台(Mobile Edge Platform)：為用來實現各種應用在特定虛擬化基礎設施上運行，並負責執行資料流量規則與轉發
    - 行動邊緣應用(Mobile Edge Applications))：是運行在行動邊緣平台上的各種應用作業系統與提供應用服務
  - **行動邊緣伺服器層級管理(Mobile Edge Host Level Management)**：提供虛擬化資源管理功能與平台各網路單元管理、 應用規則及需求管理



ETSI MEC標準架構

ETSI行動邊緣運算平台框架(2/2)

- **行動邊緣系統層級(Mobile Edge System Level)**
  - **行動邊緣系統層級管理(Mobile Edge System Level Management)**：為提供用戶端裝置(UE)或第三方(3rd Party)存取服務時，由系統編排管理負責維護行動邊緣系統的整體應用啟動、編排及調度管理
- **網路(Networks)**
  - **3GPP網路(3GPP Network)**：為結合3GPP標準行動通訊網路(4G或5G)的網路架構，進行資料傳輸與分流服務
  - **本地網路(Local Network)**：提供本地端網路資料傳輸服務，資料流量無需經過核心網路
  - **外部網路(External Network)**：提供外部網路資料傳輸服務，資料流量無需經過核心網路，直接與網際網路介接



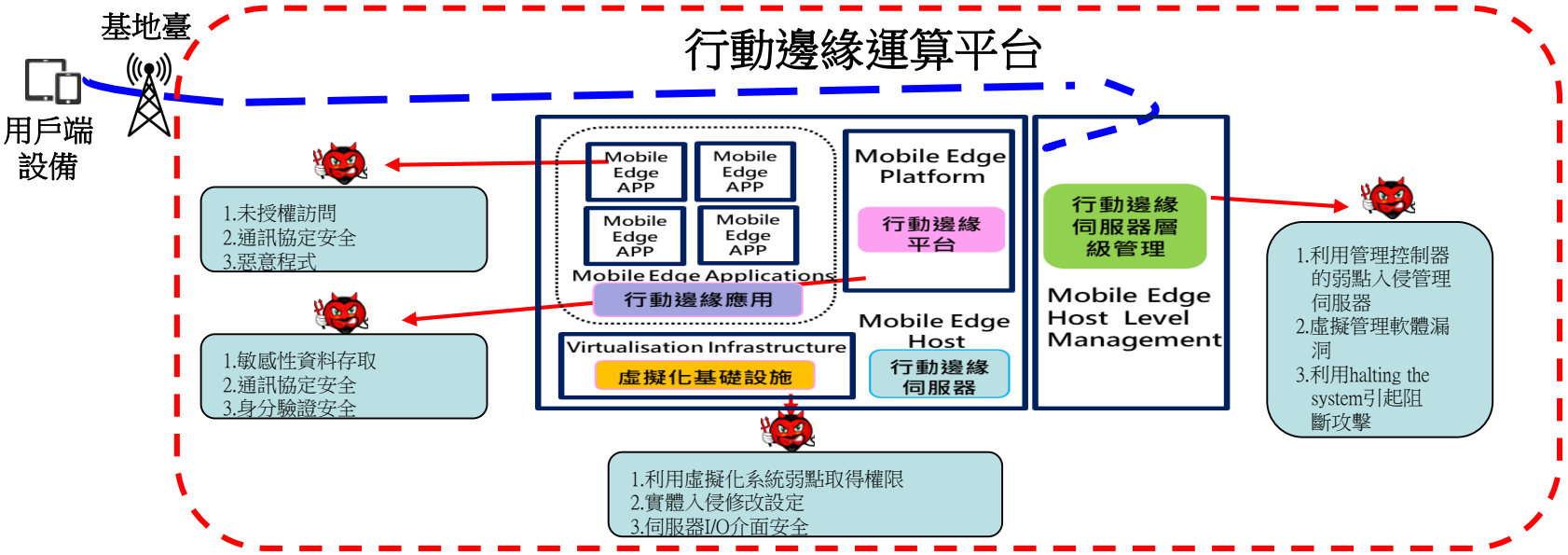
ETSI MEC標準架構

Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

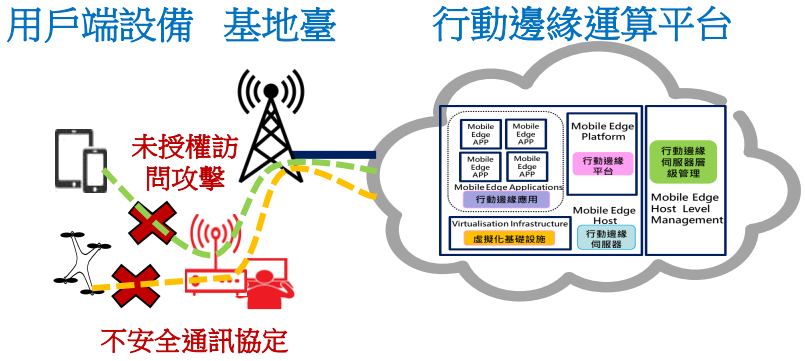
行動邊緣運算平台資安威脅

- 由於行動邊緣運算平台部署在通用伺服器上，且於接取端相對更易被用戶接觸，因此行邊緣運算平台資安威脅已是重點關注議題
  - **行動邊緣應用資安威脅**
    - 用戶端裝置遭惡意程式植入時，可非法訪問 ME APP，導致敏感資料洩漏
  - **行動邊緣平台資安威脅**
    - 攻擊者可透過MEC平台與ME APP通訊協定的漏洞，來攔截資料並進行重送與竄改攻擊
  - **虛擬化基礎設施資安威脅**
    - 攻擊者可利用虛擬化系統與軟體弱點或實體探測伺服器I/O介面，獲得敏感資料並竄改虛擬化系統來影響其他用戶服務
  - **行動邊緣伺服器層級管理資安威脅**
    - 攻擊者可利用管理控制器的弱點，取得平台控制權，並進行資料竊取與影響服務攻擊

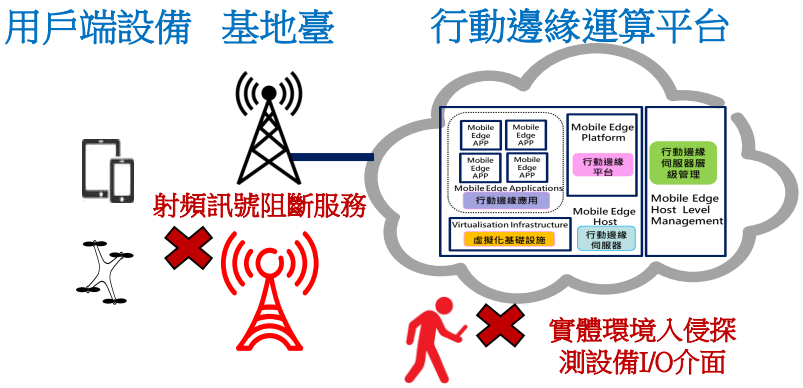


5G行動邊緣運算用戶端資安攻擊議題(1/2)

- 5G邊緣運算提供用戶快速與靈活的應用場景，但邊緣運算平台的資安威脅也關係到用戶端網路資料存取與隱私安全，其中主要來自用戶端的資安攻擊議題如下
  - **身分認證與授權資安議題**
    - 應用服務由第三方提供或異質網路存取，在接取網路的時候，如果沒有與網路之間進行認證與授權如IKEv2通訊漏洞，則面臨惡意偽裝設備接入網路並進行**未授權訪問攻擊**
    - **不安全通訊協定**，由於用戶端裝置與邊緣運算平台通訊協定未考量機密性與完整性設計，則於網路節點間透過嗅探裝置，並攔截用戶敏感性資料的攻擊
  - **網路基礎設施資安議題**
    - 由於行動邊緣運算平台設置於接近用戶端網路且為無人管理環境，攻擊者可藉由**實體環境入侵**並探測設備**實體I/O介面**攻擊，同時也可透過**無線通訊介面射頻訊號干擾**以阻斷用戶端與邊緣運算平台之間的服務



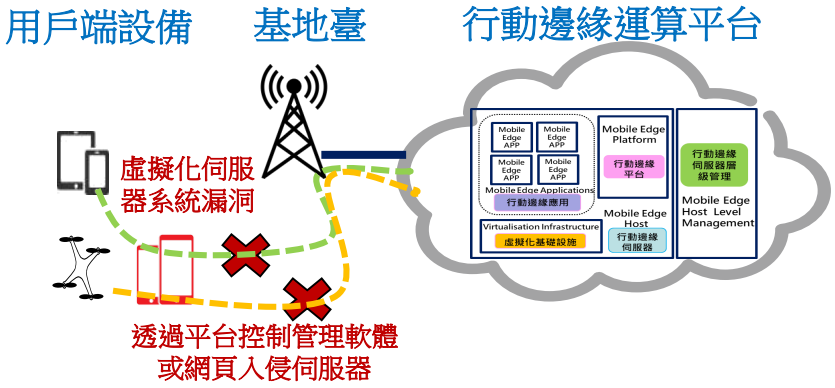
身分認證與授權資安議題



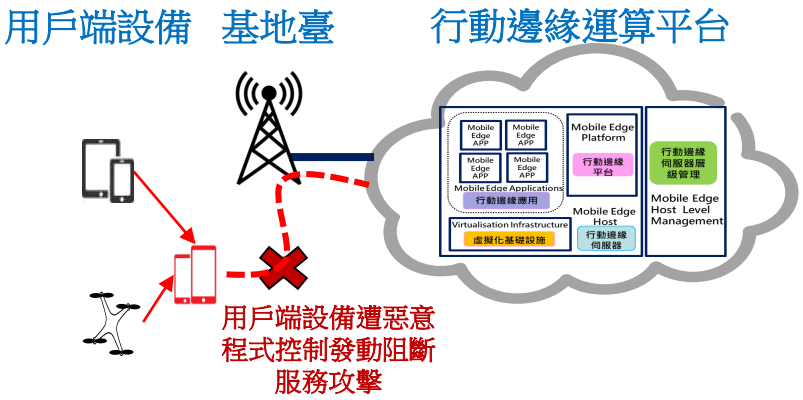
網路基礎設施資安議題

5G行動邊緣運算用戶端資安攻擊議題(2/2)

- **虛擬化資安議題**
  - 攻擊者透過**虛擬化伺服器系統弱點**入侵主機，若虛擬機VM之間的隔離不足，可以竄改其他VM造成服務影響
  - 攻擊者透過用戶端**控制管理軟體**或**網頁應用程式**，入侵管理伺服器並進階攻擊取得更高管理權限，以獲得更多敏感性資訊
- **用戶端設備資安議題**，
  - 大量用戶端設備被**惡意程式**控制後，將造成用戶隱私數據洩漏並向邊緣運算平台發動阻斷服務攻擊



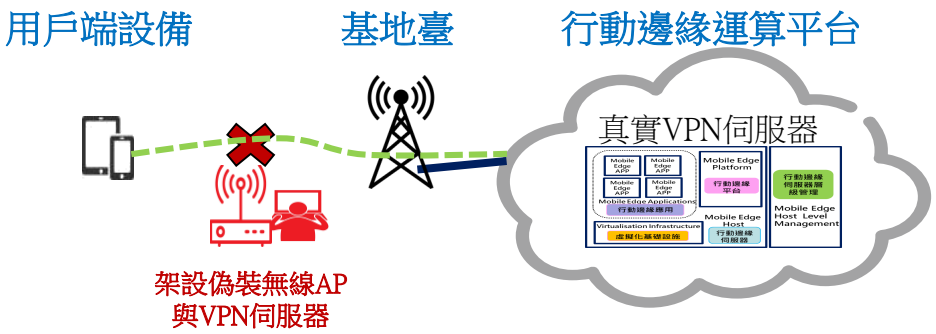
虛擬化資安議題



用戶端設備資安議題

身分認證與授權攻擊

- 利用用戶端設備與行動邊緣平台中的VPN伺服器，執行身分驗證與授權IKEv2協定漏洞攻擊，以竊取用戶敏感資料
  - **攻擊手法**
    - 攻擊者偽造無線熱點(AP)和VPN伺服器，嗅探用戶設備(UE)和真實VPN伺服器之間的資料流量
    - 偽造AP可以攔截並查看用戶端設備認證請求訊息，同時將該認證請求訊息發送到真實VPN伺服器中，當VPN伺服器發送回應訊息，偽造AP攔截該回應訊息給用戶端設備
    - 由於用戶端設備並不知道該回應訊息被偽造，此時用戶是和偽造的VPN伺服器協商出共享金鑰，並藉由金鑰解密出用戶端傳送資料
  - **目的取得用戶認證訊息與敏感資料**
    - 藉由嗅探這些認證訊息，可解密來自用戶端識別資料，以進行資料重送等攻擊

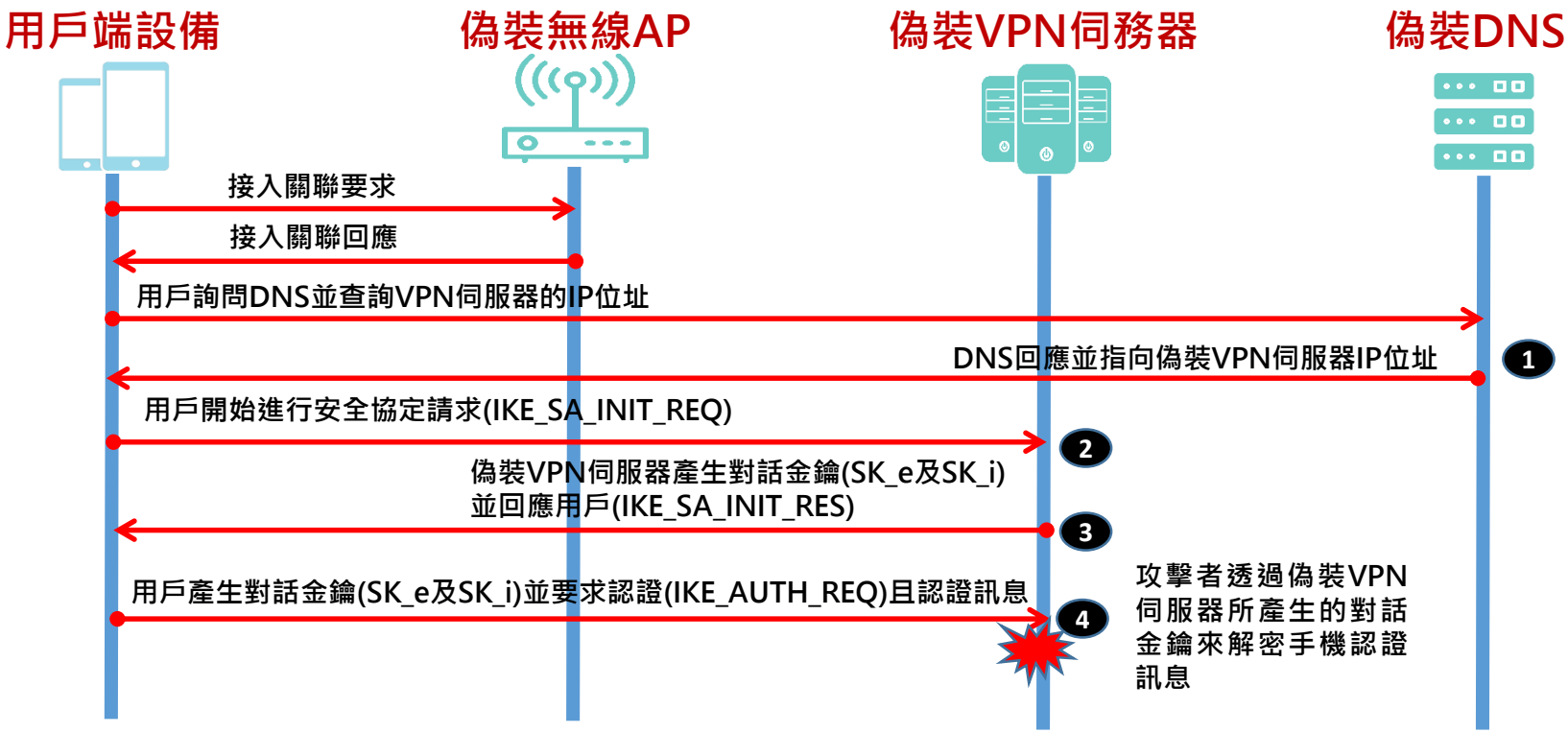


Protocol	Length	Info
ISAKMP	374	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	94	IKE_SA_INIT MID=00 Responder Response
ISAKMP	398	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	330	IKE_SA_INIT MID=00 Responder Response
ISAKMP	442	IKE_AUTH MID=01 Initiator Request
ISAKMP	186	IKE_AUTH MID=01 Responder Response
ISAKMP	186	IKE_AUTH MID=02 Initiator Request
ISAKMP	218	IKE_AUTH MID=02 Responder Response
ISAKMP	154	IKE_AUTH MID=03 Initiator Request
ISAKMP	122	IKE_AUTH MID=03 Responder Response
ISAKMP	138	IKE_AUTH MID=04 Initiator Request
ISAKMP	474	IKE_AUTH MID=04 Responder Response
ESP	174	ESP (SPI=0x1a28cded)
ESP	158	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	1422	ESP (SPI=0x1a28cded)
ESP	494	ESP (SPI=0x1a28cded)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	1006	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	190	ESP (SPI=0x1a28cded)
ESP	174	ESP (SPI=0x784dd6a2)

由Wireshark觀察IKEv2安全協定內容並解譯訊息

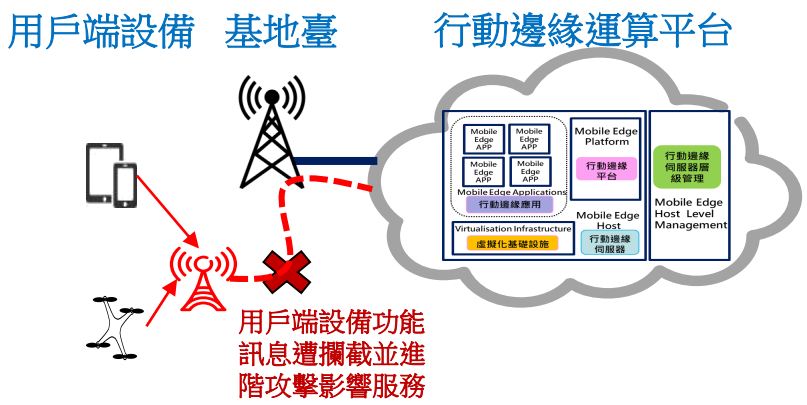
身分認證與授權攻擊流程

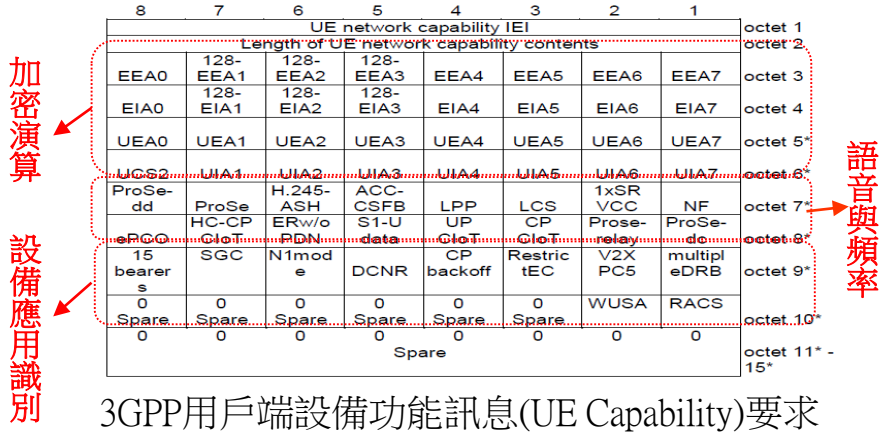
- 前置作業
  - 架設攻擊平台以擷取IKEv2認證協定訊息
    - 硬體：電腦、及WIFI嗅探模組
    - 軟體：SoftAP(模擬無線AP)、Packet Crafter(模擬合法封包工具)及StrongSwan(模擬VPN伺務器)
- 攻擊流程



無線通訊介面攻擊

- 利用用戶端設備在身分認證之前的階段，須與網路端進行交換用戶端設備功能訊息(UE Capability)，同時此訊息並未加密保護，因此架設偽基地臺於用戶端設備與網路端之間，可取得用戶端設備功能訊息以影響用戶服務
  - **攻擊手法**
    - 攻擊者可透過架設偽基地臺方式，以同頻射頻信號，強迫用戶端設備與偽基地臺接取註冊
    - 由於用戶端設備無法識別偽基地臺，將以明文方式(PlainText)發送用戶端設備功能訊息向網路端註冊，攻擊者即可攔截設備功能訊息
    - 攻擊者透過設備功能訊息，可進一步對設備發動重送與阻斷服務攻擊
  - **目的取得用戶端設備功能訊息後，可對特定用戶端設備發動重送攻擊、降階攻擊與聯網裝置功耗功擊，以影響用戶端設備服務**
    - 由於**用戶設備功能訊息含有加密演算內容、頻率訊息、語音訊息及設備識別訊息等**，因此攻擊者可藉由相關設備功能訊息來發動進階攻擊



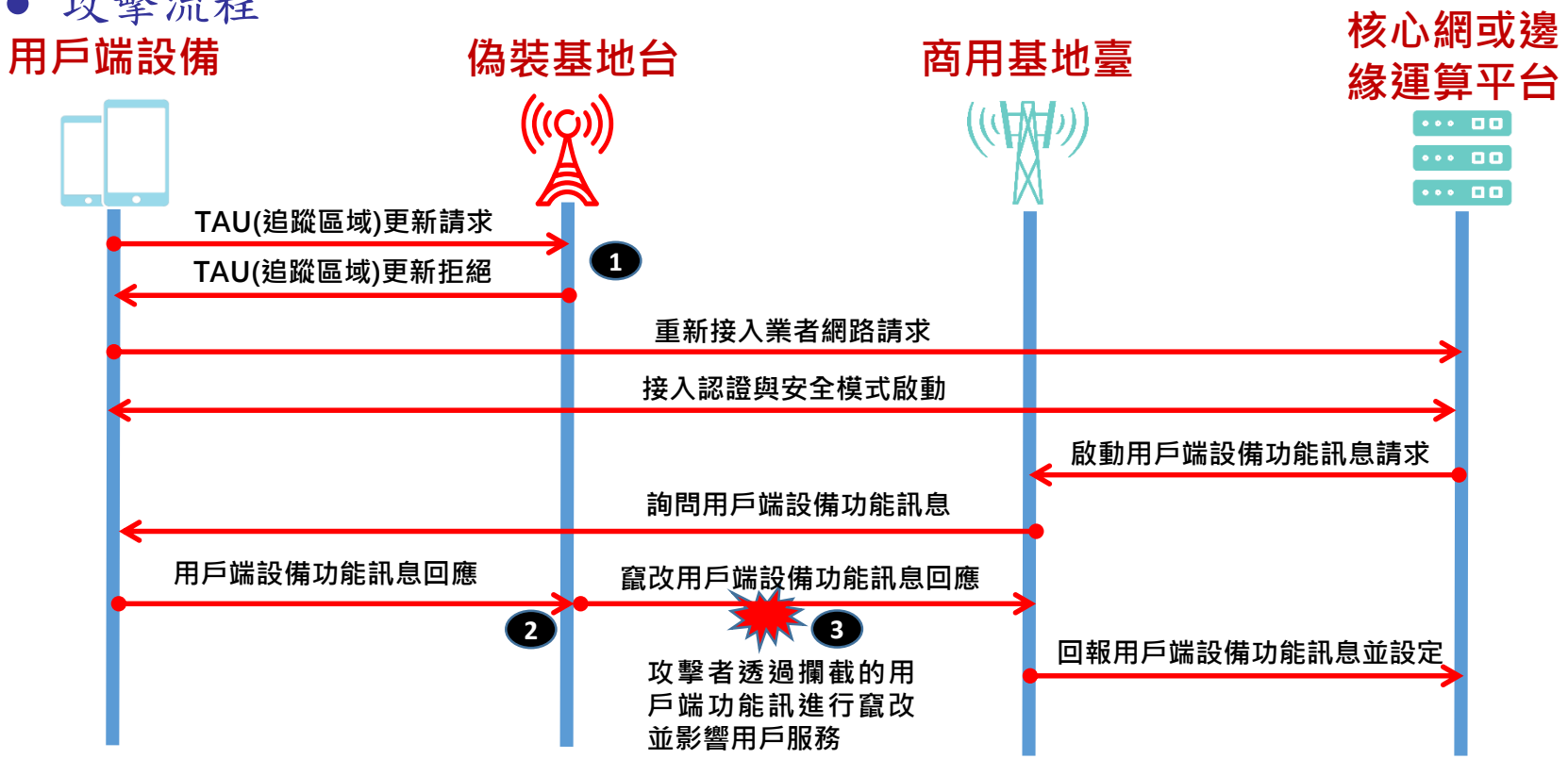


8	7	6	5	4	3	2	1	
UE network capability IEI								octet 1
Length of UE network capability contents								octet 2
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
UCS2	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
ProSe-dd	ProSe	H.245-ASH	ACC-CSFB	LPP	LCS	1xSRVCC	NF	octet 7*
epco	HC-CP CIoT	ERw/o PDN	S1-U data	UP CIoT	CP CIoT	Prose-relay	ProSe-dc	octet 8*
15 bearers	SGC	N1mode	DCNR	CP backoff	Restrict EC	V2X PC5	multipl eDRB	octet 9*
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	WUSA	RACS	octet 10*
0	0	0	0	0	0	0	0	octet 11* - 15*
Spare								

3GPP用戶端設備功能訊息(UE Capability)要求

無線通訊介面攻擊流程

- 前置作業
  - 攻擊者須藉由偽基地臺來擷取用戶端設備功能訊息
    - 硬體：2台USRP B210(無線射頻收發模組)
    - 軟體：srsUE(模擬手機)與srsLTE(無線協定分析)
- 攻擊流程

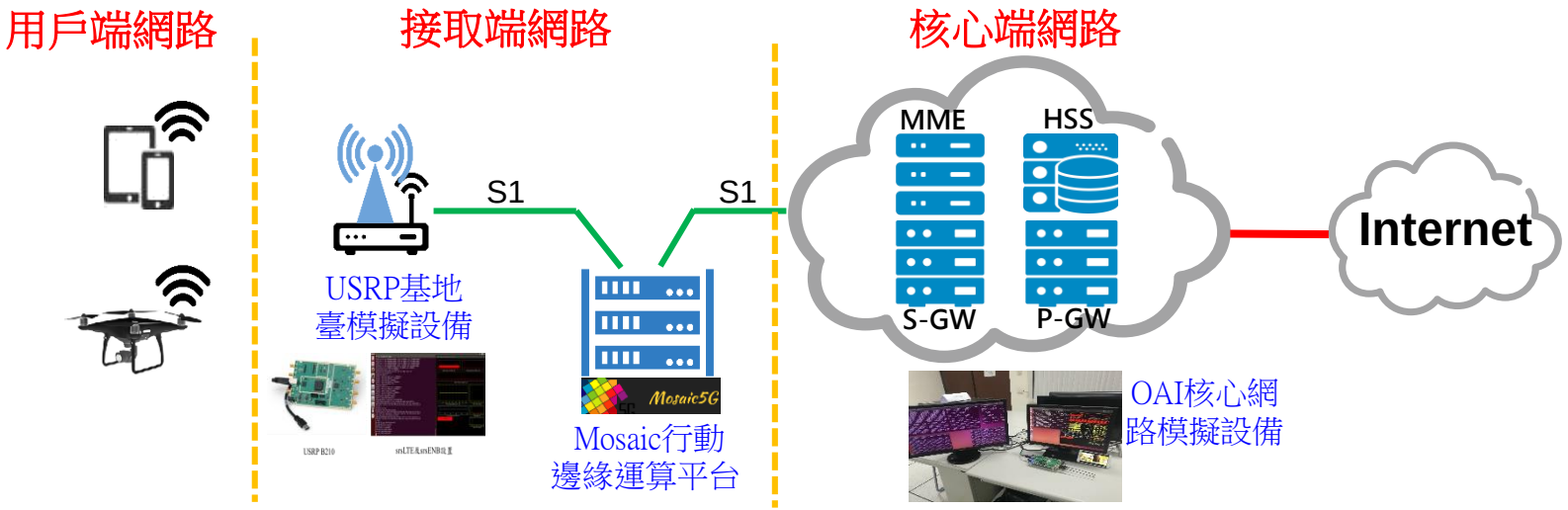


Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

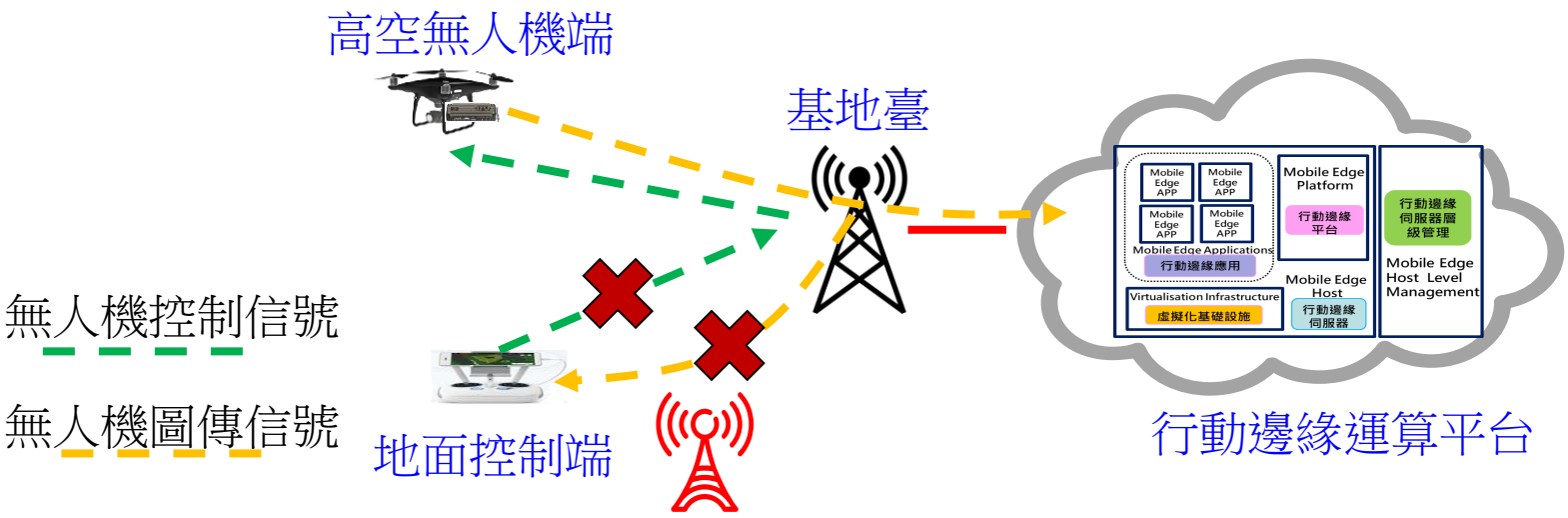
5G邊緣運算攻防平台建置

- 因應5G網路之竊取用戶端隱私資料威脅趨勢，藉由學研合作於中心建置5G邊緣運算通訊模擬平台，通訊模擬平台主要架構
  - 用戶端網路
    - 行動裝置模擬設備(srsUE)與物聯網裝置
  - 接取端網路
    - 基地臺模擬設備(USRP B210)與邊緣運算伺服器(Mosaic開源軟體)
  - 核心端網路
    - 電腦設備(OAI核心網路開源軟體)



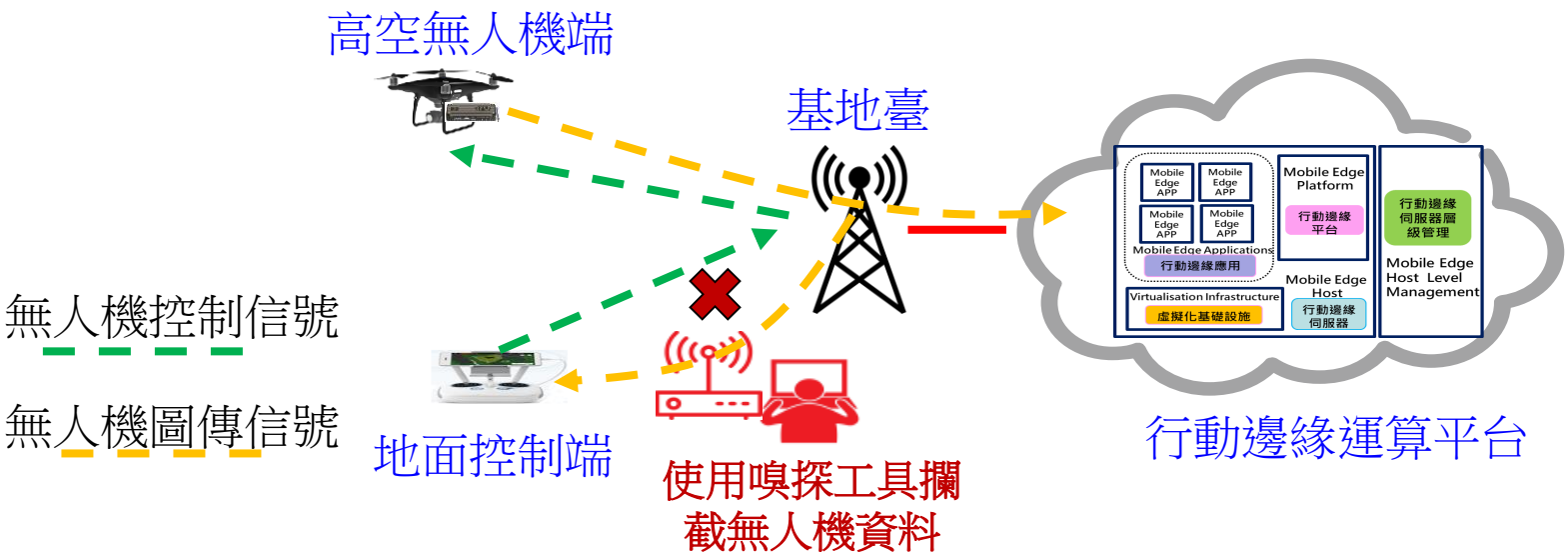
無人機邊緣運算應用資安攻擊實例(1/2)

- 無線通訊射頻信號干擾
  - 利用偽基站射頻信號干擾攻擊，於無人機射頻信號函蓋範圍，發射較強的同頻信號，來阻斷地面控制端信號，造成服務中斷(DoS)



無人機邊緣運算應用資安攻擊實例(2/2)

- 不安全的通訊協定
  - 無人機控制信號協定與圖傳信號協定，未進行完善的加密機制，可透過射頻嗅探工具，於無人機信號函蓋範圍內，嗅探無人機識別資料或圖傳資料內容，造成用戶端資料外洩的疑慮

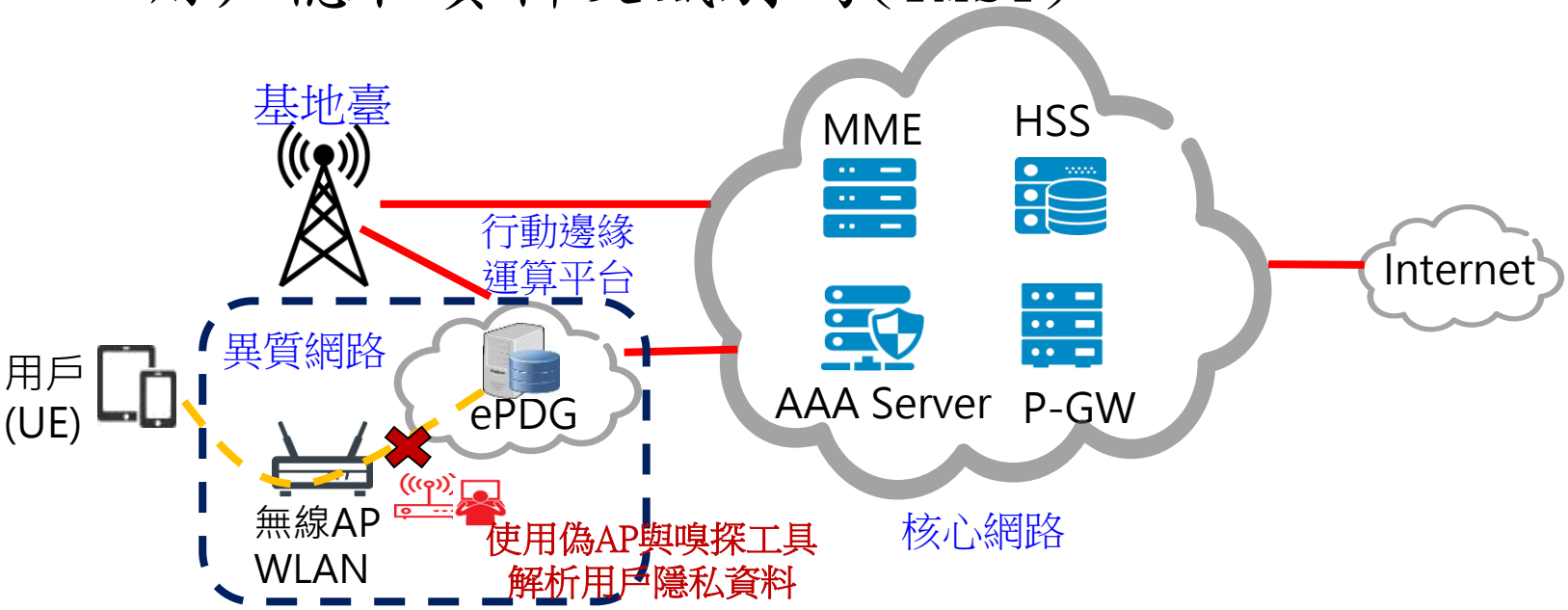


Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

異質網路資安攻擊實例

- 不安全的認證與授權
  - 利用異質網路傳輸通道IKEv2通訊協定的漏洞未進行雙向認證機制，可藉由偽冒WIFI基地台及ePDG閘道，嗅探通道傳送的封包，並解析出用戶隱私資料及識別碼(IMSI)



用戶端網路防護建議(1/2)

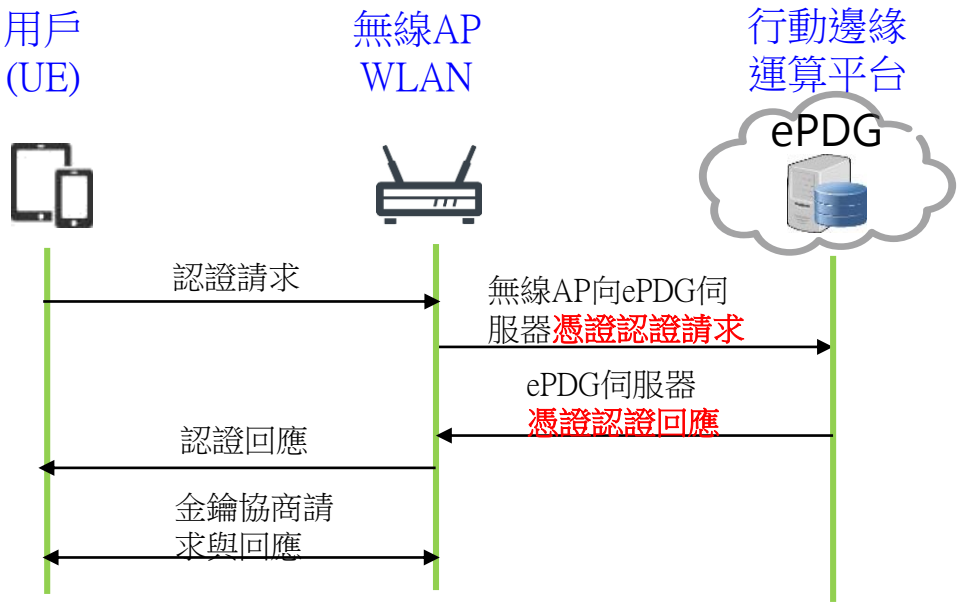
- 偽基地臺防禦方法
  - 可開發偽基地臺偵測APP，藉由比對基地臺資料庫找出異常基地台並發出警告

即時基地臺射頻信號參數　　基地臺資料庫　　偽基地臺偵測告警

- 不安全通訊協定防禦方法
  - 由於通訊協定未考量用戶資料的機密性與完整性，可強化通訊協定的加密要求，以確保用戶資料的安全

用戶端網路防護建議(2/2)

- 不安全的認證與授權
  - 由於用戶端設備與邊緣運節點缺乏完善的認證與授權機制，容易於用戶端網路使用偽冒裝置，竊取用戶隱私資料，建議於用戶端網路裝置啟動憑證雙向確認機制，以防止偽冒裝置運行於網路

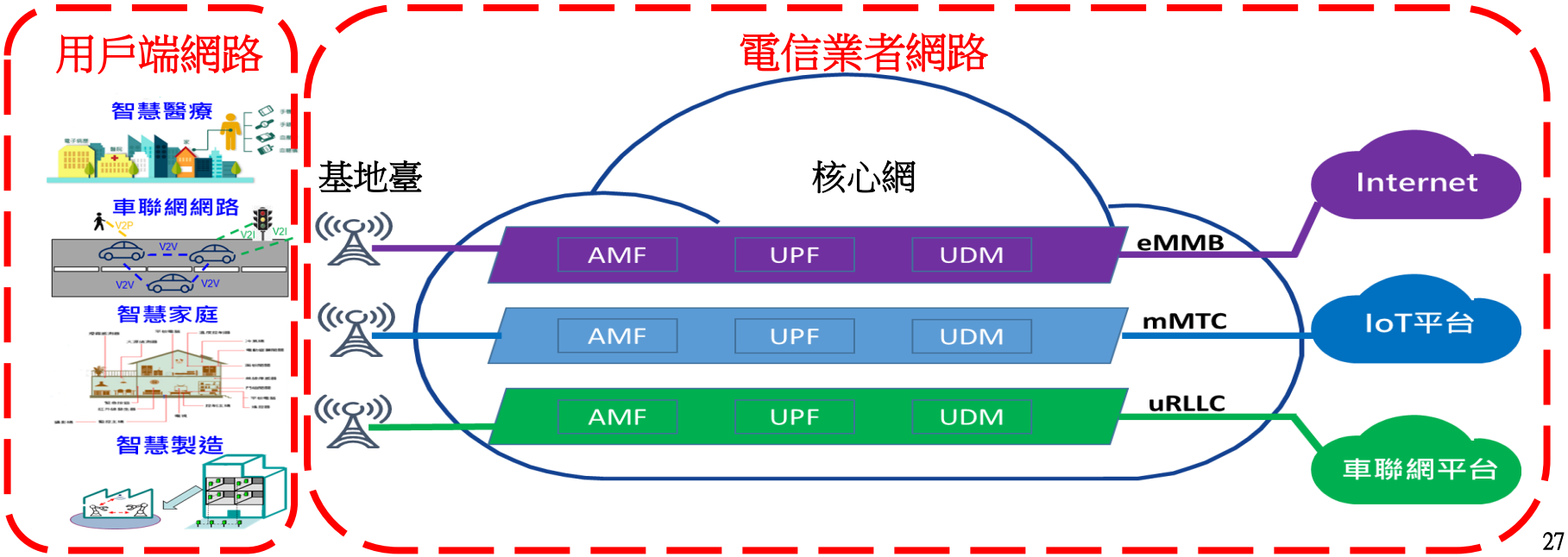


Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

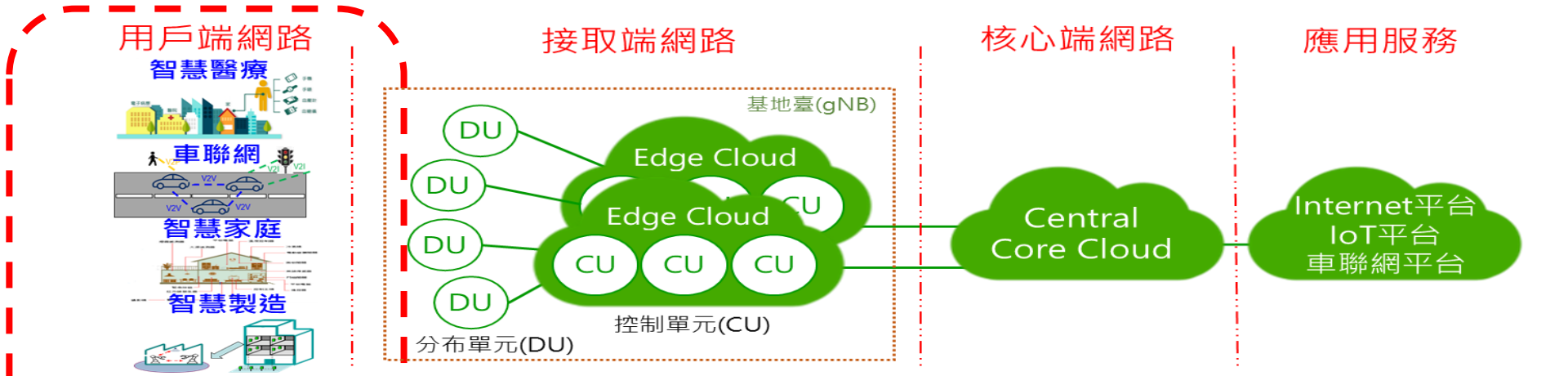
5G應用場景資安風險

- 5G網路為因應高頻寬流量、低時延及大量物聯網裝置應用需求，其網路架構中的接取端網路、核心端網路及應用平台由電信業者來布建管理，而用戶端網路則由用戶依應用服務來布建管理，以實現5G網路的垂直應用服務
- 而電信業者建置之網路資安要求是由權責機關國家通訊傳播委員會(NCC)負責規管，而用戶端網路應用之資安要求則由用戶自行規劃管理，因此容易成為網路主要資安風險



5G應用場景主要資安威脅

- 由5G網路應用系統，可了解用戶端網路應用是透過無線傳輸通道與網路端進行身分認證、資料存取及應用服務，是5G網路的第一道關口，也是主要資安威脅來源
- 因此5G用戶端網路服務的差異化與不同等級終端裝置，容易成為攻擊目標，同時也衍生出用戶端物聯網裝置安全性不足、影響裝置可用性及隱私資料洩漏等資安威脅



用戶端網路資安威脅

- 物聯網裝置安全性不足
- 竊取用戶隱私資料
- 影響用戶裝置可用性

接取端網路資安威脅

- 行動邊緣計算平台威脅
- 異質網路連接缺乏完善之身分認證機制
- 實體環境入侵威脅

核心端網路資安威脅

- SDN/NFV資安威脅

應用服務資安威脅

- 因應即時回應、大規模物聯網裝置及高頻寬應用服務之資安威脅

5G應用場景攻防規劃分析

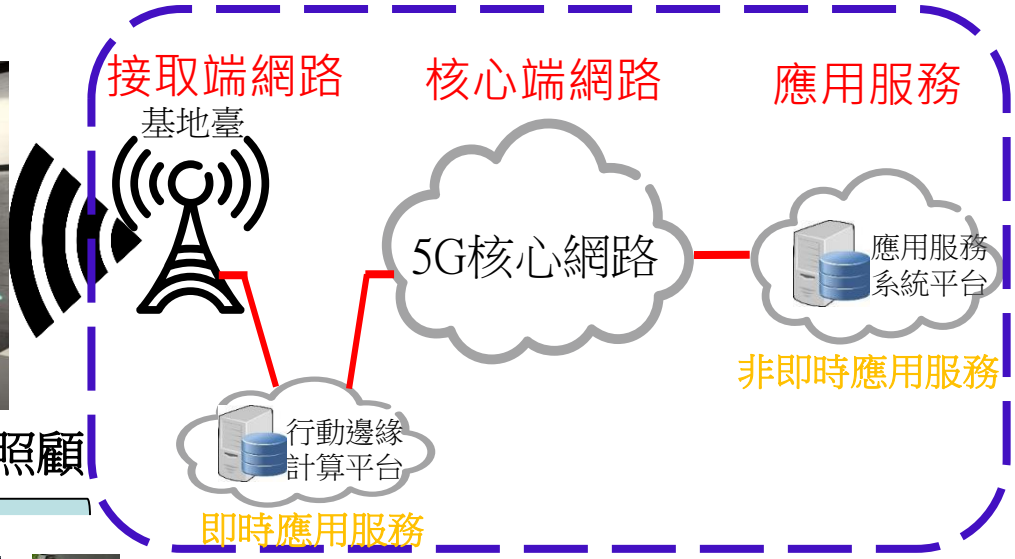
- 由5G應用之車聯網、智慧醫療、智慧製造及智慧家庭網路架構分析，其應用場景皆可互聯於建置的5G網路通訊模擬平台
- 但由於各應用場域與設備取得不易，或相關應用標準仍制定中，因此將選擇較為成熟的智慧家庭應用場景進行攻防技術研究

5G應用場景	應用場景建置分析
車聯網	車聯網通訊標準仍訂定中、場域及設備取得不易(V2I閘道器)
智慧醫療	場域或醫療設備取得不易
智慧製造	場域或智慧製造設備取得不易
智慧家庭	可透過無線AP設備或用戶端裝置模擬攻防技術研究

5G智慧家庭應用場景

- 智慧家庭
  - 智慧家庭結合網際網路、自動控制、感測器等技術，整合家中的各種裝置與中央管理系統，形成人性化的智慧居住空間
- 5G智慧家庭應用特點
  - 為滿足使用者對高畫質影音娛樂需求，利用5G增強型行動寬頻(eMBB)的高傳輸頻寬特性，以實現高畫質(8K)居家娛樂應用場景

5G智慧家庭應用場景(用戶端網路)

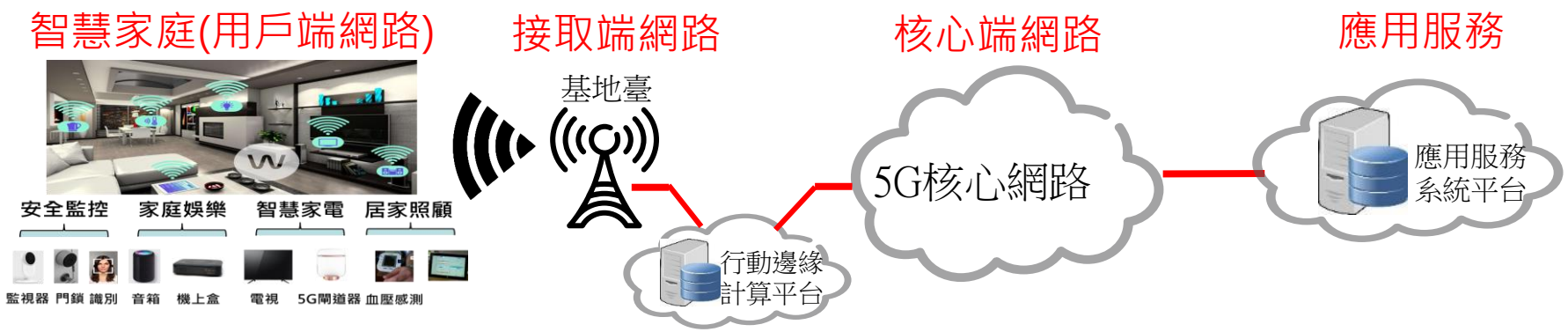


安全監控 家庭娛樂 智慧家電 居家照顧

監視器 門鎖 識別 音箱 機上盒 電視 5G閘道器 血壓感測 照護平台

5G智慧家庭應用資安威脅

- 5G智慧家庭主要因應各種家用情景，因此終端裝置種類眾多，裝置通訊協定及介面規格不一，且無強制裝置資安檢測要求，容易成為駭客攻擊目標，也是主要的資安威脅



用戶端網路資安威脅

- 智慧家庭裝置安全性不足
- 竊取用戶隱私資料
- 影響智慧家庭裝置可用性

接取端網路資安威脅

- 異質網路連接缺乏完善之身分認證機制
- 行動邊緣計算平台威脅

核心端網路資安威脅

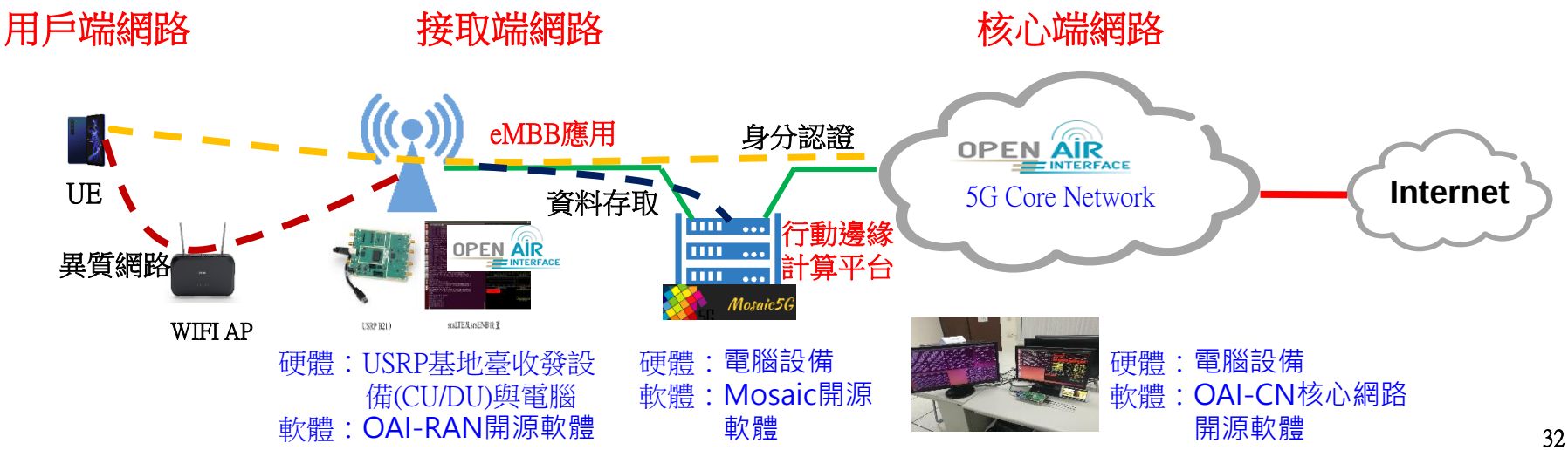
- SDN/NFV資安威脅
  (透過網路切片功能進行非法訪問)

應用服務資安威脅

- 因應eMBB的高頻寬應用服務之資安威脅
  (入侵影音伺服器並影響服務)

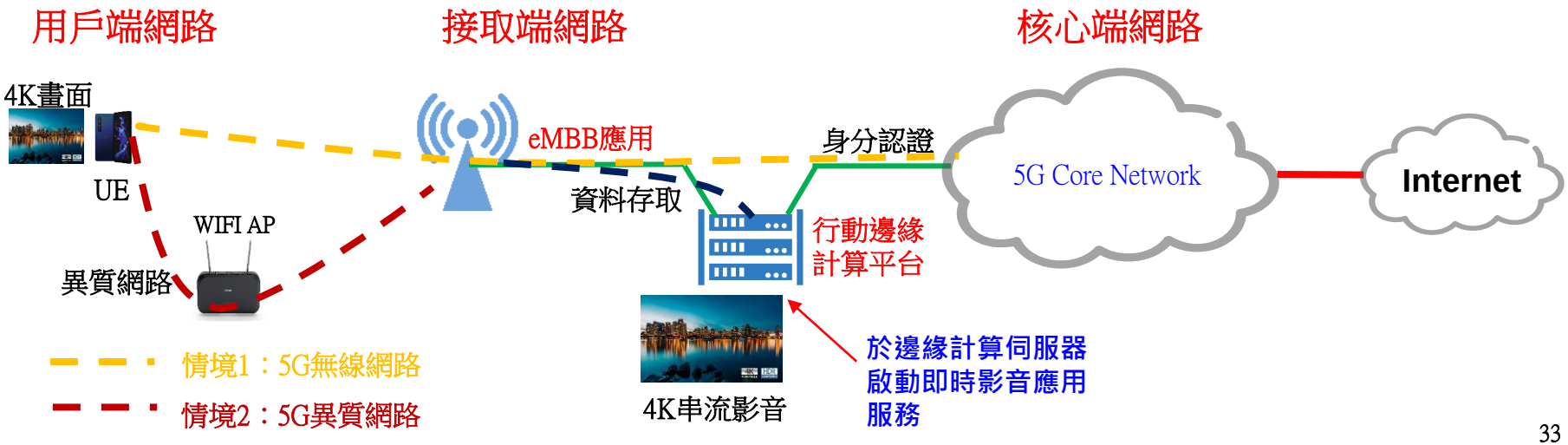
5G網路通訊模擬平台建置

- 為驗證5G智慧家庭應用資安威脅，建置以5G邊緣計算架構的通訊模擬平台，進行5G增強型行動寬頻(eMBB)應用場景資安攻防實證技術研究，其平台架構如下
  - 用戶端網路
    - 行動裝置模擬設備(srsUE)或5G用戶端裝置
  - 接取端網路
    - 基地臺射頻收發模擬設備(USRP B210)、基地台控制電腦(OAI-RAN接取開源軟體)及邊緣計算伺服器(Mosaic開源軟體)
  - 核心端網路
    - 電腦設備(OAI核心網路開源軟體)



5G智慧家庭應用情境

- 藉由建置5G網路通訊模擬平台，應用eMBB網路特性與行動邊緣計算平台，用戶可透過終端裝置順暢觀看4K影音服務
  - 情境1：5G無線網路
    - 用戶手機直接與5G基地臺通訊，存取行動邊緣計算平台4K影音應用服務
  - 情境2：5G異質網路
    - 用戶手機透過異質網路(如WIFI)，存取行動邊緣計算平台4K影音應用服務



5G智慧家庭應用攻擊情境

- 攻擊者可利用5G無線射頻通訊信令、協議及應用服務等漏洞，並透過簡易射頻嗅探工具執行資安攻擊

5G智慧家庭應用資安攻擊(1/3)

- 由前述5G智慧家庭資安威脅分析，以智慧家庭用戶端增強型行動寬頻(eMBB)應用場景，攻擊者只要於無線網路涵蓋範圍內，透過射頻嗅探工具，即可擷取用戶端隱私等資料、影響應用服務及入侵裝置等資安攻擊

智慧家庭用戶端資安威脅	攻擊情境	資安漏洞種類	攻擊手法	攻擊結果
影響用戶裝置可用性	模擬5G增強型行動寬頻(eMBB)應用場景，當智慧裝置與邊緣計算網路影音平台連線進行高畫質影音服務時，攻擊者透過無線射頻信號干擾，造成智慧裝置服務中斷	4G與5G網路用戶端裝置信號強度判別漏洞	偽基地臺攻擊手法[2] [1]	阻斷智慧家庭端網路服務
竊取用戶隱私資料	模擬5G增強型行動寬頻(eMBB)應用場景，當智慧行動裝置與5G網路端連線時，攻擊者透過監聽與嗅探工具取得裝置識別碼，並發送惡意簡訊，誘騙用戶點選以植入惡意程式	4G網路用戶身分識別資料以明文傳輸漏洞	傳呼通道攻擊手法[3] [1] 降階網路攻擊手法[1] [4]	擷取用戶唯一識別碼(IMSI)或臨時識別碼(TMSI)並發送惡意簡訊誘騙用戶點選以控制用戶裝置
智慧家庭裝置安全性不足	模擬5G增強型行動寬頻(eMBB)應用場景，當內建SIM卡的智慧裝置與5G網路射頻信號雙向協議時，攻擊者可嗅探並取得智慧裝置識別訊息，加以竄改訊息重送，來影響智慧裝置聯網效能	5G網路射頻信號(RRC)以明文傳輸識別訊息漏洞	無線射頻信號攻擊手法[4] [1] 中間人攻擊手法[1]	取得智慧家庭裝置識別訊息並進階重送攻擊或降低裝置服務效能

5G智慧家庭應用資安攻擊(2/3)

- 智慧家庭應用為有效利用傳輸頻寬，因此於接取端整合無線異質網路(如WIFI)，但由於異質網路接入5G接取端網路時，也融合多種認證協議，攻擊者可透過異質網路接入認證協議漏洞，並透過射頻嗅探工具或偽裝設備來取用戶端認證訊息等隱私資料

智慧家庭接取端資安威脅	攻擊情境	資安漏洞種類	攻擊手法	攻擊結果
異質網路連接缺乏完善之身分認證機制	模擬智慧家庭異質網路接入，當5G無線路由器與接取端行動邊緣計算平台認證伺服器進行身分認證協議時，攻擊者於無線網路中加入偽裝AP與偽裝認證伺服器，執行重送攻擊方式，來嗅探智慧裝置認證訊息	4G與5G異質網路接入認證協議漏洞	無線接入認證協議攻擊手法[5]	智慧家庭裝置或異質網路身分認證協議漏洞取得用戶身分識別資料或金鑰
行動邊緣計算平台威脅	模擬智慧家庭裝置接入接取端行動邊緣計算平台，由於智慧裝置帳號設定安全性不足，攻擊者取得用戶裝置帳號，入侵邊緣計算特定應用平台來影響用戶裝置服務	5G行動邊緣計算存取控制漏洞	中間人攻擊手法[6]	智慧家庭裝置的帳號設定安全行不足，入侵邊緣計算平台，來影響用戶裝置服務

5G智慧家庭應用資安攻擊(3/3)

- 基於虛擬化技術的網路切片(Network Slicing)功能已為5G核心網路關鍵技術，以提供應用服務的效能品質(QoS)穩定服務，但也由於切片網路資源劃分策略複雜與接入信令多樣化而面臨資安威脅

智慧家庭核心端資安威脅	攻擊情境	資安漏洞種類	攻擊手法	攻擊結果
網路切片功能資安威脅	模擬智慧家庭網路切片應用功能，由於業者切片隔離功能安全性不足，攻擊者可偽裝合法用戶，非法訪問或注入流量攻擊，來影響其他切片服務	5G網路切片隔離功能漏洞	切片流量注入攻擊手法[7]	智慧家庭裝置網路切片功能應用，由於業者切片功能隔離安全性不足，使用流量攻擊並影響其他切片用戶服務

- 5G智慧家庭主要利用增強型行動寬頻(eMBB)特性，因此用戶端裝置將透過業者局端應用伺服器進行資料存取等服務，但由於應用伺服器的通訊協議或軟硬體安全性不足而造成智慧家庭應用資安威脅

智慧家庭應用服務資安威脅	攻擊情境	資安漏洞種類	攻擊手法	攻擊結果
應用服務平台安全性不足	模擬5G增強型行動寬頻(eMBB)應用場景，由於局端應用伺服器安全性不足，攻擊者可透過通訊協議漏洞，入侵應用伺服器，來影響用戶裝置服務	4G與5G網路應用伺服器安全性不足漏洞	通訊協議攻擊手法[8]	由於局端應用伺服器安全性不足，入侵應用伺服器，影響用戶裝置服務

5G智慧家庭應用攻防技術實作規劃(1/2)

- 綜整5G網路資安威脅與資安要求，並以5G智慧家庭應用來規劃用戶端、接取端、核心端及應用服務攻防技術概

5G用戶端資安威脅	用戶端資安要求	智慧家庭用戶端資安威脅	攻擊驗證	防護驗證
用戶端隱私識別資料攔截威脅	用戶隱私識別碼保護(R1)	竊取用戶隱私資料	傳呼通道攻擊手法	傳呼通道攻擊防護
			降階網路攻擊手法	
用戶終端裝置軟體及硬體資安威脅	用戶端裝置軟體及硬體可信環境要求(R2)	影響用戶裝置可用性	偽基地臺攻擊手法	偽基地臺攻擊防護
		智慧家庭裝置安全性不足	無線射頻信號攻擊手法	無線射頻信號攻擊防護
			中間人攻擊手法	

5G接取端資安威脅	接取端資安要求	智慧家庭接取端資安威脅	攻擊驗證	防護驗證
異質網路接入資安威脅	接取端(異質)網路接入存取協議要求(R11)	異質網路連接缺乏完善之身分認證機制	無線接入認證協議攻擊手法	無線接入認證協議攻擊防護
行動邊緣計算平台威脅	MEC平台通訊協議要求(R10)	行動邊緣計算平台威脅	中間人攻擊手法	MEC通訊協議攻擊防護

5G核心端資安威脅	核心端資安要求	智慧家庭核心端資安威脅	攻擊驗證	防護驗證
SDN/NFV資安威脅	網路切片安全隔離要求(R13)	網路切片功能資安威脅	切片流量注入攻擊手法	網路切片隔離技術防護

5G應用服務安威脅	應用服務資安要求	智慧家庭應用服務資安威脅	攻擊驗證	防護驗證
應用服務資安威脅	應用服務系統平台資安管理要求(R23)	應用服務平台安全性不足	通訊協議攻擊手法	通訊協議攻擊防護

5G智慧家庭應用攻防技術實作規劃(2/2)

- 由於建置5G網路通訊模擬平台為基本仿真架構，且核心網路模擬器的網路切片技術與應用服務平台功能尚未完備，因此將規劃主軸為用戶端與接取端的資安威脅，待模擬平台功能完備之後，將深入探討核心端與應用服務資安攻防技術
- 同時由國際5G資安攻擊趨勢文獻，可了解5G主要攻擊趨勢為利用用戶端與接取端的無線射頻信號資安漏洞，攻擊者藉由簡易無線嗅探工具與開源軟體，即可竊取用戶隱私或影響服務，因此將先規劃用戶端與接取端的5G智慧家庭資安攻擊技術項目為主

智慧家庭用戶端增強型應用情境攻擊規劃	偽基地臺攻擊	傳呼通道與無線射頻訊號攻擊	降階與中間人攻擊
	1.受害者使用手機或電視機等裝置觀看4K節目，利用偽基地臺信號干擾，造成用戶無法收看並嘗試開關裝置，重新對網路端認證接入	2.利用無線嗅探工具，於受害者重新接入網路時，嗅探傳呼通道或射頻訊信令，統計並確認用戶識別碼或擷取裝置訊息識別	3.確認受害者識別碼，即可透過降階攻擊發送惡意簡訊誘騙受害者點選並取得控制權，或藉由修改裝置訊息，利用重送攻擊影響裝置運作

智慧家庭接取端增強型應用情境攻擊規劃	無線接入認證協議攻擊	中間人攻擊
	1.受害者使用手機透過異質網路(WIFI)接入電業信網路或行動邊緣計算平台觀看影音節目時，於網路加入偽無線AP與VPN伺服器，誘騙受害者接入偽無線AP及VPN伺服器，並取得受害者金鑰或認證訊息	2.取得受害者認證訊息後，可嘗試登入邊緣計平台，入侵平台非法存取資料，或影響平台服務

參考資料

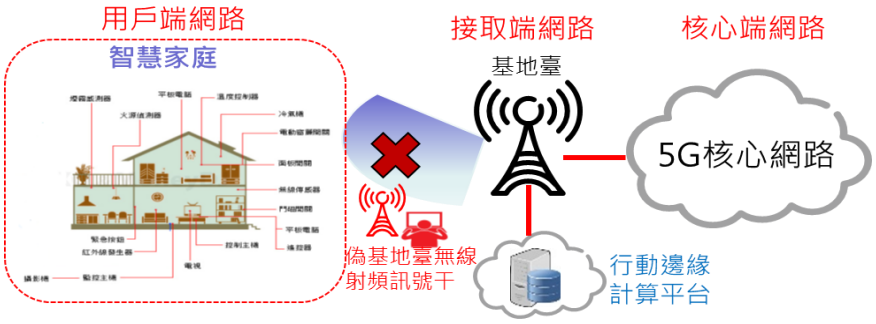
1. Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In 25th Annual Network and Distributed System Security Symposium, NDSS, San Diego, CA, USA, February 18-21.
2. D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G mobile wireless networks,” IEEE Access, vol. 6, pp. 4850–4874, 2018.
3. Syed Rafiul Hussain, Mitziu Echeverriay, Omar Chowdhuryy, Ninghui Li and Elisa Bertino, “ Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information”in 26th Annual Network and Distributed System Security Symposium NDSS, San Diego, CA,USA,24-27 February 2019
4. Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019.New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’19). ACM, New York, NY, USA, 221–231. https://doi.org/10.1145/3317549.3319728
5. Jie Huang, Nataniel Borges, Sven Bugiel, Michael Backes. Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling”. In ACSAC ’18, December 3–7, 2018, San Juan, PR, USA https://dl.acm.org/citation.cfm?id=3274753
6. Roman, R., Javier, L. and Masahiro, M. (2016) Mobile Edge Computing, Fog – A Survey and Analysis of Security Threats and Challenges. Future Generation Computer Systems.
7. V. A. Cunha, E. d. Silva, M. B. d. Carvalho, D. Corujo, J. P. Barraca, D. Gomes, et al., "Network slicing security: Challenges and directions", Internet Technology Letters, vol. 2, no. 5, 2019.
8. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and Beyond. IEEE Commun. Surv. Tutor. 2019

Outline

- 目標
- 邊緣運算介紹
- 5G行動邊緣運算資安議題
- 5G邊緣運算攻防平台建置
- 5G用戶端網路攻擊技術規劃
- 5G應用之資安威脅與風險
- 5G應用場景攻防技術與平台規劃

偽基地臺攻擊方法

- 利用偽基地臺射頻信號干擾攻擊，於物聯網裝置無線射頻信號函蓋範圍，發射較強的同頻信號，來阻斷控制端信號，造成服務中斷(DoS)
  - **偽基地臺攻擊手法**
    - 攻擊者利用射頻嗅探工具掃描鄰近商用基地臺參數，並紀錄商用基地臺頻率、訊號強度及Cell_ID等參數
    - 將商用基地臺頻率、訊號強度及Cell_ID等參數設置於偽基地臺並增加發射功率
    - 由於用戶端裝置基於無線射頻信號強度選擇設置，將會選擇射頻信號強度較強的偽基地臺請求接入存取，偽基地臺將接入裝置視為非法裝置並阻斷請求造成用戶端裝置服務中斷
  - **目的使用戶裝置中斷服務**
    - 藉由用戶端裝置無線射頻性號強度變化選擇，只要透過簡易偽基地臺設置，即可造成用戶端裝置服務中斷

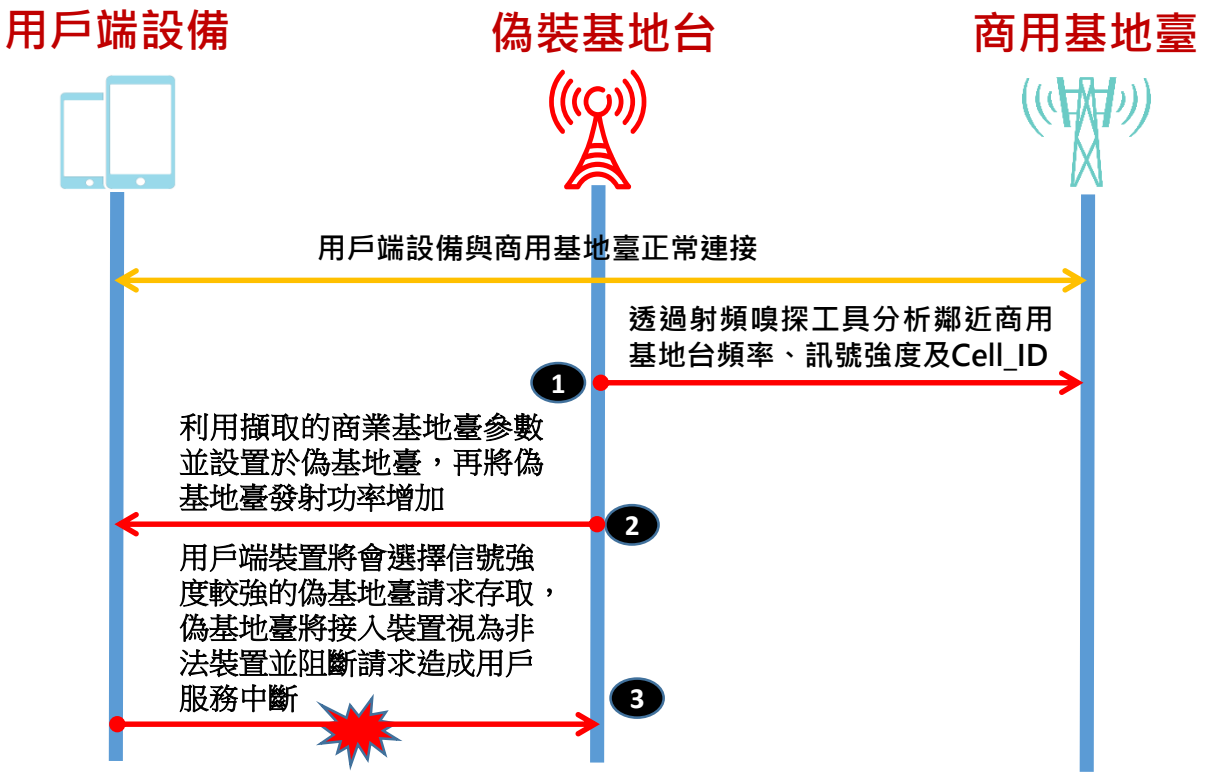



```
eNBs =
(
  ////////// Identification parameters:
  eNB_ID    =  0xf406;
  cell_type =  "CELL_MACRO_ENB";
  eNB_name  =  "eNB_Eurecom_LTEBox";
  tracking_area_code  =  "4401";
  mobile_country_code =  "466";
  mobile_network_code =  "92";
  ////////// Physical parameters:
  component_carriers = (
    {
      node_function                 = "eNodeB_3GPP";
      node_timing                   = "synch_to_ext_device";
      node_synch_ref                = 0;
      frame_type                    = "FDD";
      tdd_config                    = 3;
      tdd_config_s                  = 0;
      prefix_type                   = "NORMAL";
      eutra_band                    = 8;
      downlink_frequency            = 945000000L;
      uplink_frequency_offset       = -45000000;
      Nid_cell                      = 0;
      N_RB_DL                       = 25;
      Nid_cell_mbsfn                = 0;
```

偽基地臺頻率、訊號強度及Cell_ID設定

偽基地臺攻擊流程

- 前置作業
  - 攻擊者須藉由偽基地臺來阻斷用戶端裝置服務
    - 硬體：2台USRP B210(無線射頻收發模組)、控制電腦
    - 軟體：srsUE(模擬手機)與srsLTE(無線協定分析)
- 攻擊流程



偽基地臺攻擊防護建議

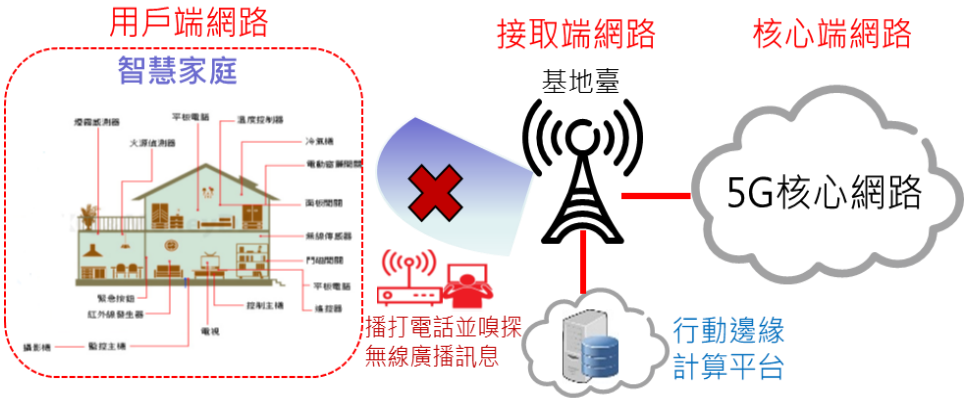
- 影響用戶裝置可用性資安威脅主要以偽基地臺方式攻擊用戶端裝置並影響網路服務
- 因此可透過偽基地臺偵測方法，以防禦用戶端裝置遭阻斷服務或不安全通訊攻擊
  - 可開發偽基地臺偵測APP，藉由比對基地臺資料庫找出異常基地台並發出警告

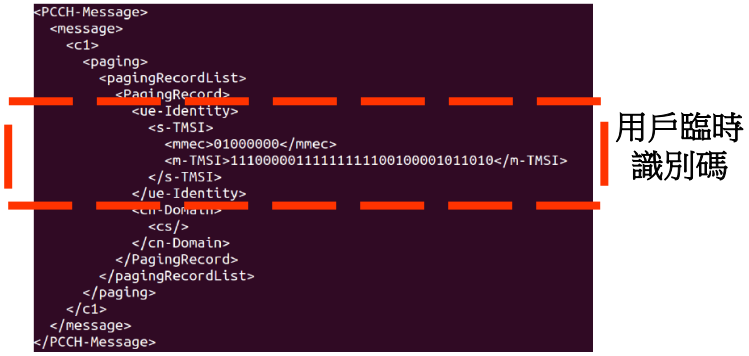
即時基地臺射頻信號參數　基地臺資料庫　偽基地臺偵測告警

偽基地臺偵測APP

傳呼通道攻擊方法

- 利用5G傳呼通道資安漏洞，可藉由射頻嗅探工具，嗅探廣播訊息資料並進一步取得用戶端裝置臨時識別碼(TMSI)等隱私資料
  - **傳呼通道攻擊手法**
    - 利用當有電話或訊息傳到閒置的手機前，核心網路端會透過當地基地台，廣播發出內含TMSI的傳呼(Paging)訊息
    - 攻擊者只要鎖定受害者的電話號碼，並在短期間內接連撥打多次電話給受害者又迅速掛掉，來啟動傳呼訊息，UE也不會收到來電提醒
  - **目的取得臨時用戶識別碼(TMSI)**
    - 藉由嗅探這些傳呼訊息，只要10通電話以下就能確認用戶TMSI識別碼

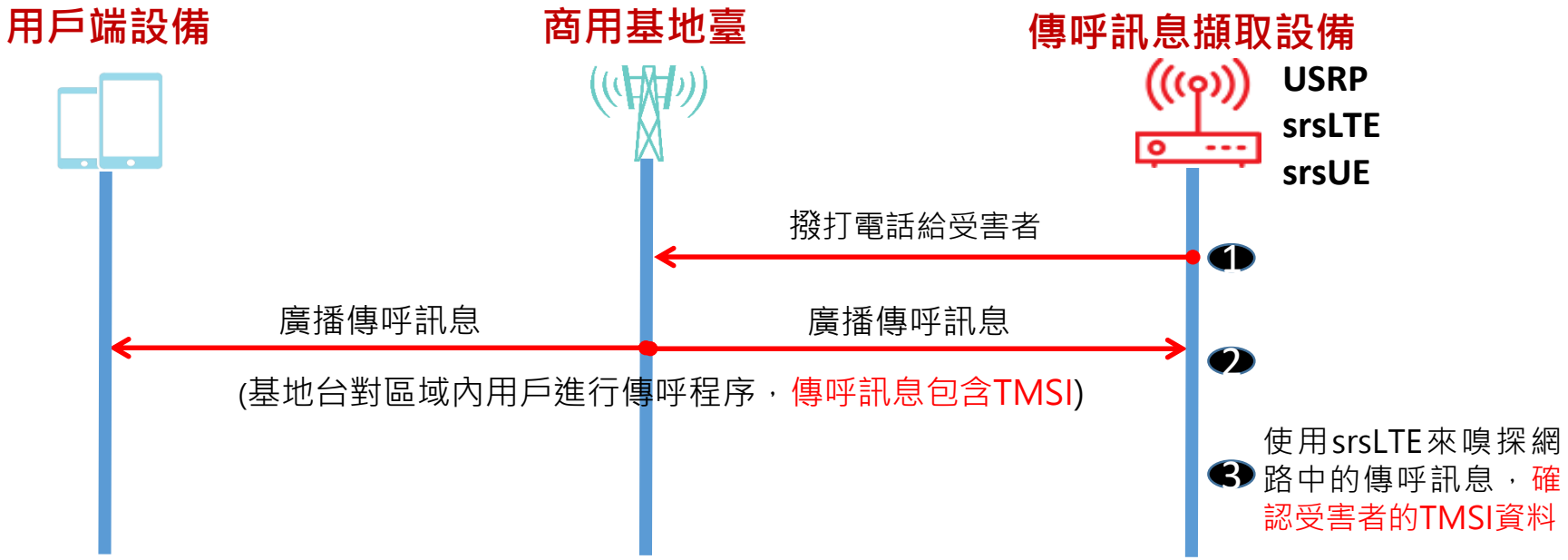




嗅探到的廣播訊息並解譯出用戶隱私資料

傳呼通道攻擊流程

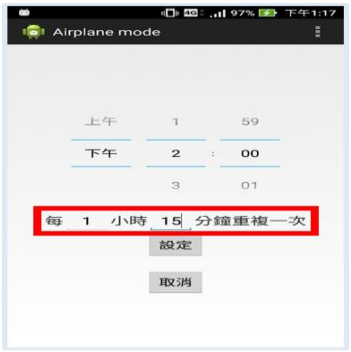
- 前置作業
  - 攻擊者事先得知目標用戶的電話號碼
  - 架設攻擊平台以擷取訊息
    - 硬體：USRP B210(無線射頻收發模組)、控制電腦
    - 軟體：srsUE(模擬手機)與srsLTE(無線協議分析)
- 攻擊流程



傳呼通道攻擊防護建議

- 由於3GPP對用戶端裝置識別資料更新時間並未規範，而造成用戶隱私洩漏疑慮
- 因此可藉由監測用戶臨時識別碼駐留時間並定期更新，以防止識別碼被鎖定攻擊
  - 藉由開發的監測APP，監控用戶端裝置臨時用戶識別碼(TMSI)的駐留時間，並由APP啟動重新設置用戶端裝置接入網路功能，將可更新臨時用戶識別碼(TMSI)，以防止該識別碼被鎖定攻擊

設定開啟飛航模式時間



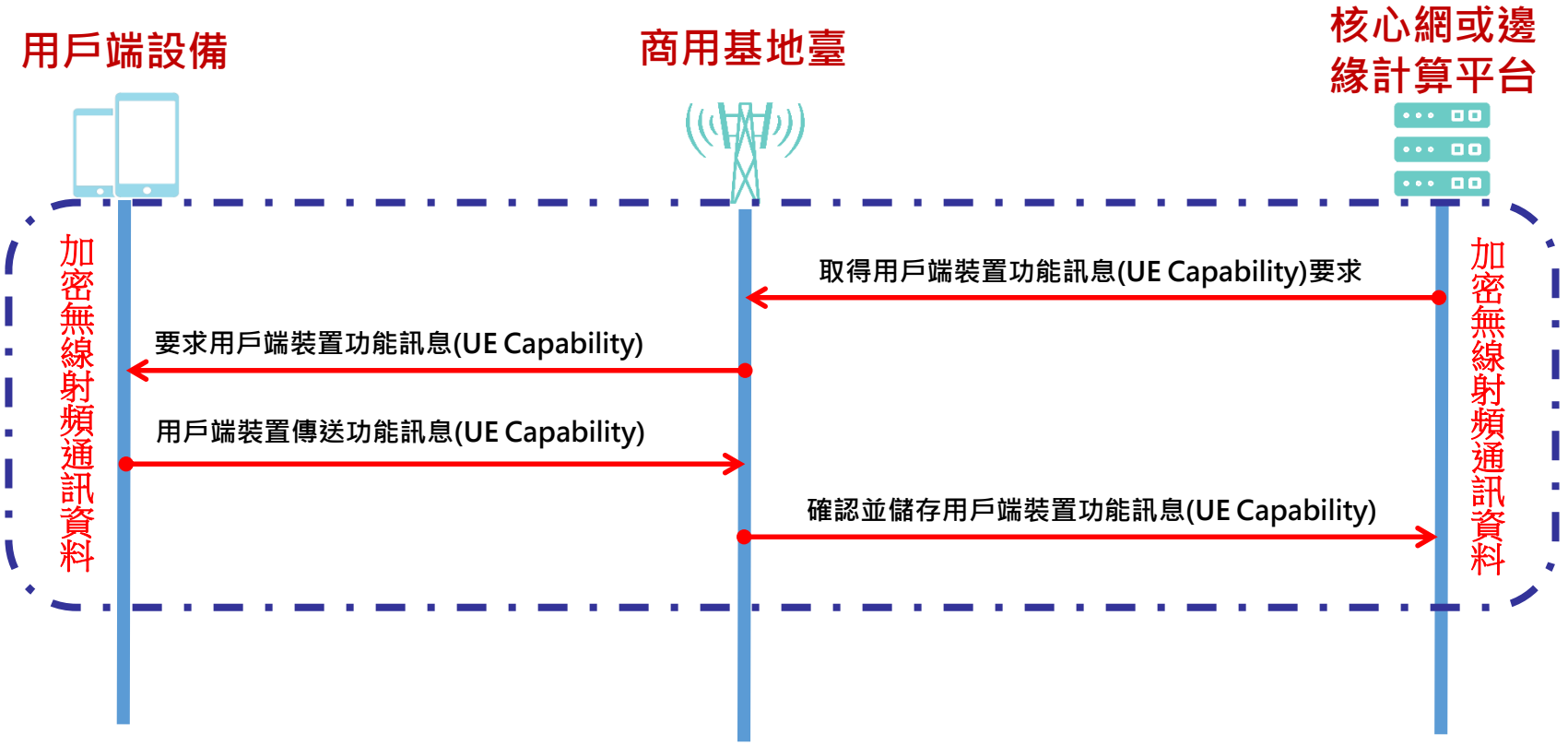
設定每隔多久重複執行一次程式，未設定只會執行一次

按下設定會顯示設置成功，並讓程式在背景執行

用戶隱私資料更新APP

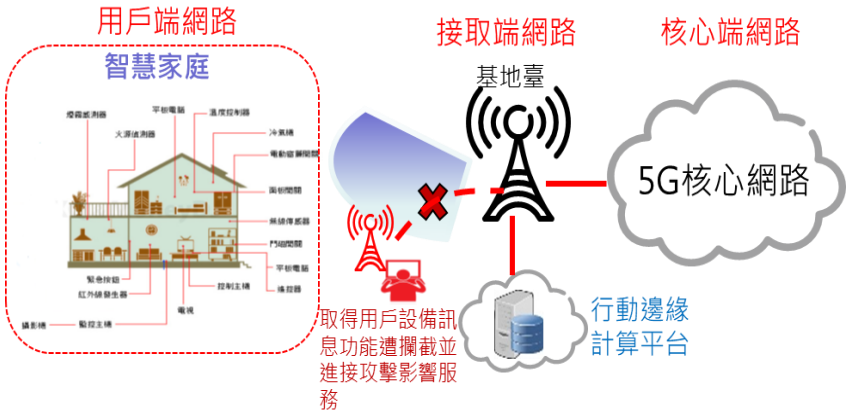
無線射頻信號攻擊防護建議

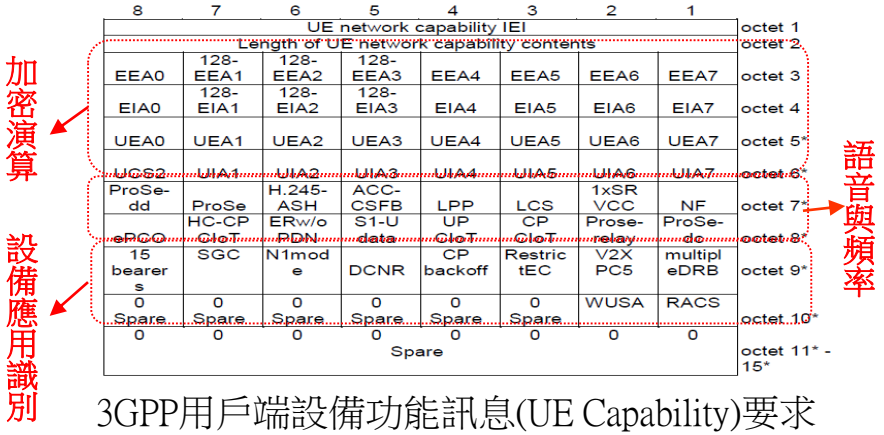
- 由於物聯網裝置與網路端缺乏完善的無線通訊加密要求，因此攻擊者可嗅探無線射頻信號，取得物聯網裝置功能訊息並進階影響用戶服務
- 因此可透過強化物聯網裝置與網路端的無線射頻通訊加密要求，使攻擊者無法解譯無線射頻信號內容的物聯網裝置功能訊息



無線射頻信號攻擊方法

- 利用5G無線射頻通訊協定(RRC)漏洞，未與物聯網裝置進行完善的加密機制，可透過射頻嗅探工具，嗅探物聯網裝置功能訊息(UE Capability)，造成用戶端裝置資料外洩的疑慮
  - **無線射頻信號攻擊手法**
    - 攻擊者可透過架設偽基地臺方式，以同頻射頻信號，強迫物聯網裝置與偽基地臺接取註冊
    - 由於物聯網裝置無法識別偽基地臺，將以明文方式(PlainText)發送用戶端設備功能訊息向網路端註冊，攻擊者即可攔截設備功能訊息
    - 攻擊者透過設備功能訊息，可進一步對設備發動重送與阻斷服務攻擊
  - **目的取得用戶端設備功能訊息後，可對特定用戶端設備發動重送攻擊、降階攻擊與聯網裝置功耗功擊，以影響用戶端設備服務**
    - 由於**用戶設備功能訊息含有加密演算內容、頻率訊息、語音訊息及設備識別訊息等**，因此攻擊者可藉由相關設備功能訊息來發動進階攻擊



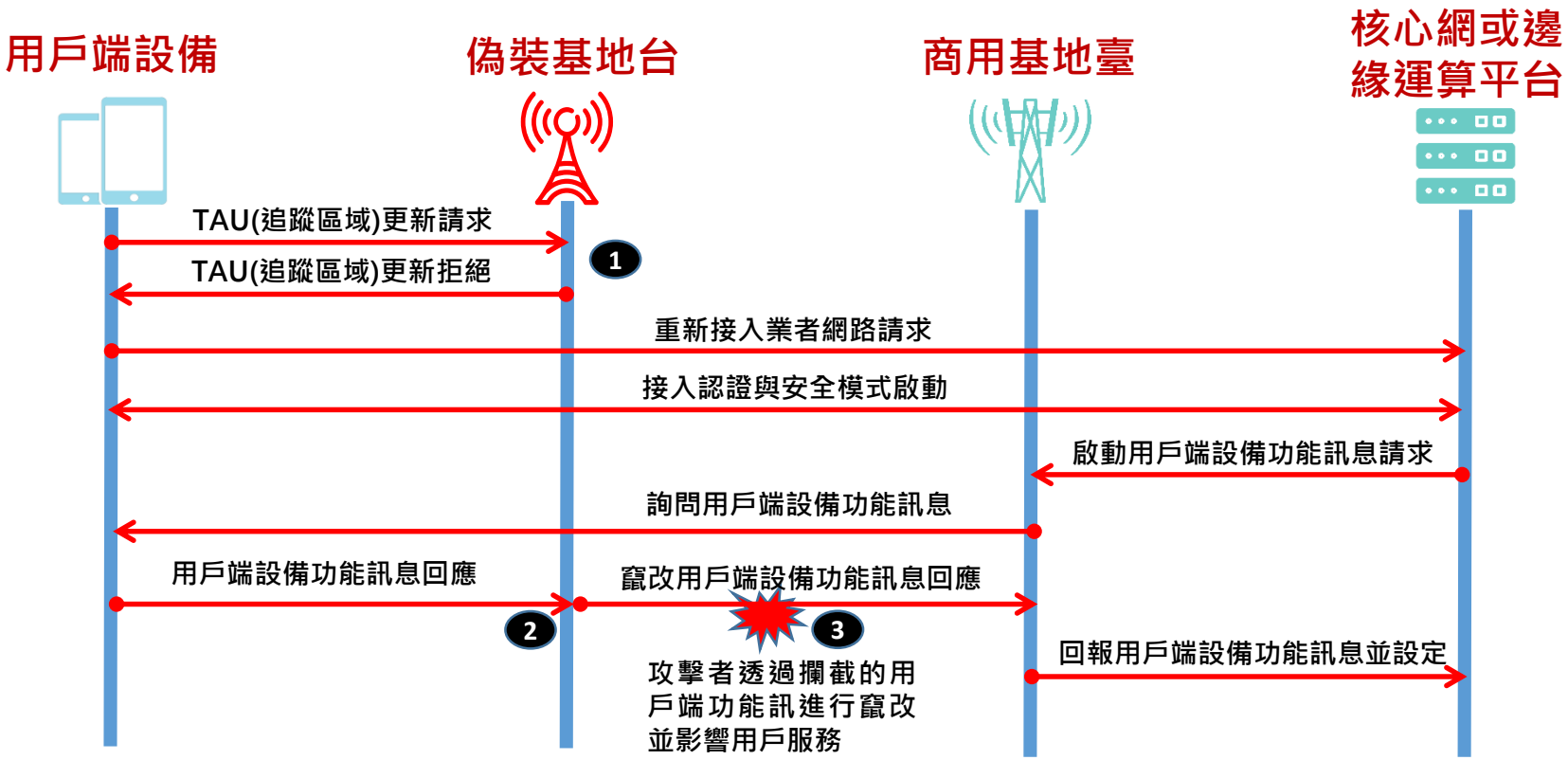


8	7	6	5	4	3	2	1	
UE network capability IEI								octet 1
Length of UE network capability contents								octet 2
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
UCS2	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
ProSe-dd	ProSe	H.245-ASH	ACC-CSFB	LPP	LCS	1xSRVCC	NF	octet 7*
ePCO	HC-CP CIoT	ERw/o PDN	S1-U data	UP CIoT	CP CIoT	Prose-relay	ProSe-dc	octet 8*
15 bearers	SGC	N1mode	DCNR	CP backoff	Restrict EC	V2X PC5	multipl eDRB	octet 9*
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	WUSA	RACS	octet 10*
0	0	0	0	0	0	0	0	
Spare								octet 11* - 15*

3GPP用戶端設備功能訊息(UE Capability)要求

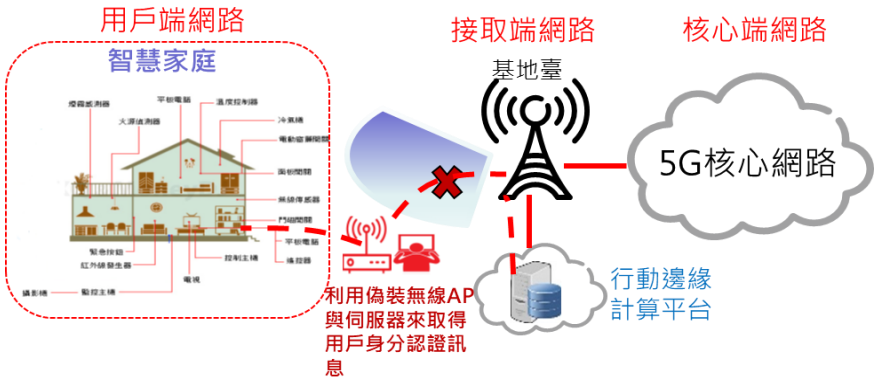
無線射頻信號攻擊流程

- 前置作業
  - 攻擊者須藉由偽基地臺來擷取用戶端設備功能訊息
    - 硬體：2台USRP B210(無線射頻收發模組)、控制電腦
    - 軟體：srsUE(模擬手機)、srsLTE(無線協定分析)、OAI(核心網)
- 攻擊流程



無線接入認證協議攻擊方法

- 利用用戶端設備與異質網路中的無線AP與VPN伺服器，執行身分驗證與授權IKEv2協議漏洞攻擊，以竊取用戶敏感資料
  - **無線接入認證協議攻擊手法**
    - 攻擊者偽造無線熱點(AP)和VPN伺服器，嗅探用戶設備(UE)和真實VPN伺服器之間的資料流量
    - 偽造AP可以攔截並查看用戶端設備認證請求訊息，同時將該認證請求訊息發送到真實VPN伺服器中，當VPN伺服器發送回應訊息，偽造AP攔截該回應訊息給用戶端設備
    - 由於用戶端設備並不知道該回應訊息被偽造，此時用戶是和偽造的VPN伺服器協商出共享金鑰，並藉由金鑰解密出用戶端傳送資料
  - **目的取得用戶認證訊息與敏感資料**
    - 藉由嗅探這些認證訊息，可解密來自用戶端識別資料，以進行資料重送等攻擊

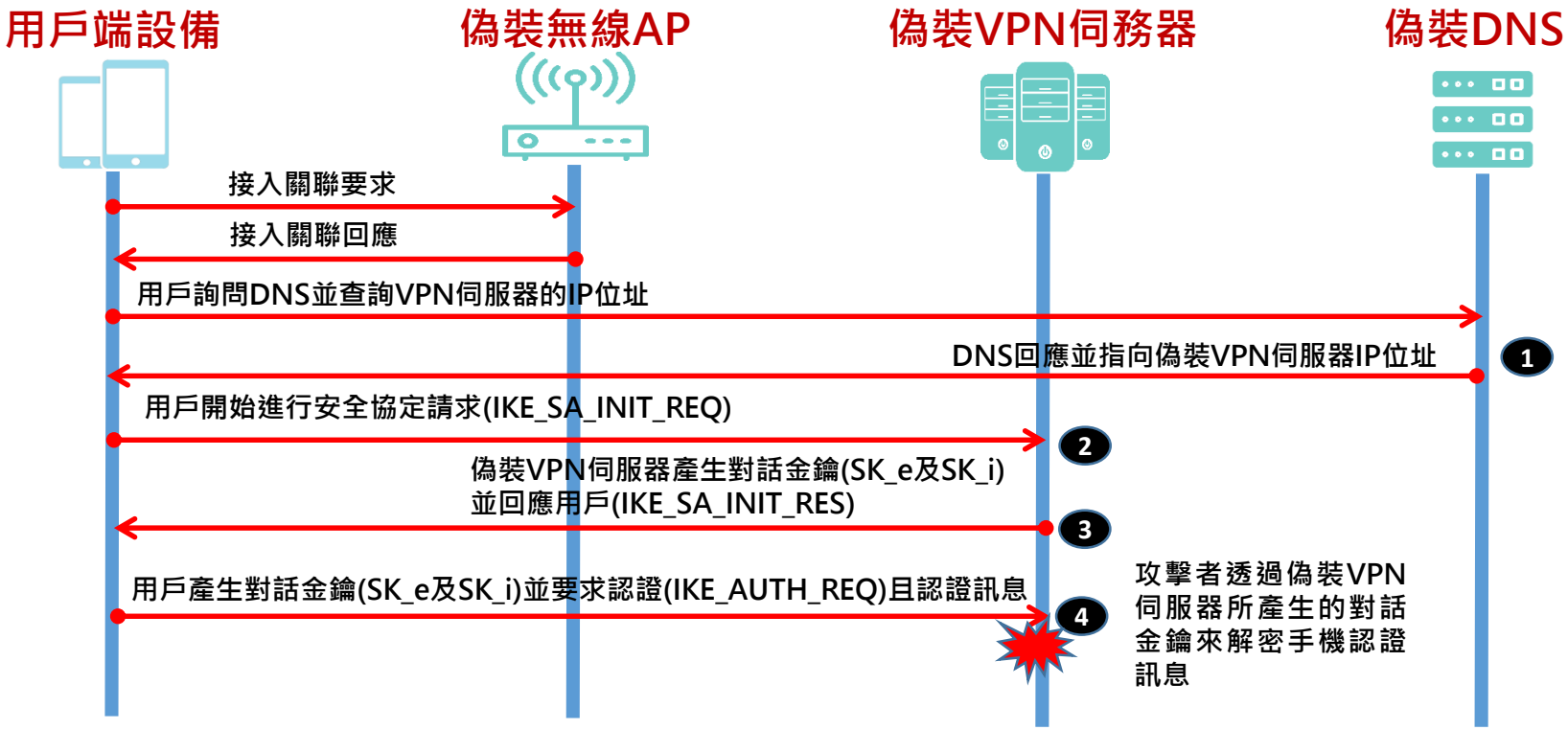


Protocol	Length	Info
ISAKMP	374	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	94	IKE_SA_INIT MID=00 Responder Response
ISAKMP	398	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	330	IKE_SA_INIT MID=00 Responder Response
ISAKMP	442	IKE_AUTH MID=01 Initiator Request
ISAKMP	186	IKE_AUTH MID=01 Responder Response
ISAKMP	186	IKE_AUTH MID=02 Initiator Request
ISAKMP	218	IKE_AUTH MID=02 Responder Response
ISAKMP	154	IKE_AUTH MID=03 Initiator Request
ISAKMP	122	IKE_AUTH MID=03 Responder Response
ISAKMP	138	IKE_AUTH MID=04 Initiator Request
ISAKMP	474	IKE_AUTH MID=04 Responder Response
ESP	174	ESP (SPI=0x1a28cded)
ESP	158	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	1422	ESP (SPI=0x1a28cded)
ESP	494	ESP (SPI=0x1a28cded)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	1006	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	190	ESP (SPI=0x1a28cded)
ESP	174	ESP (SPI=0x784dd6a2)

由Wireshark觀察IKEv2安全協定內容並解譯訊息

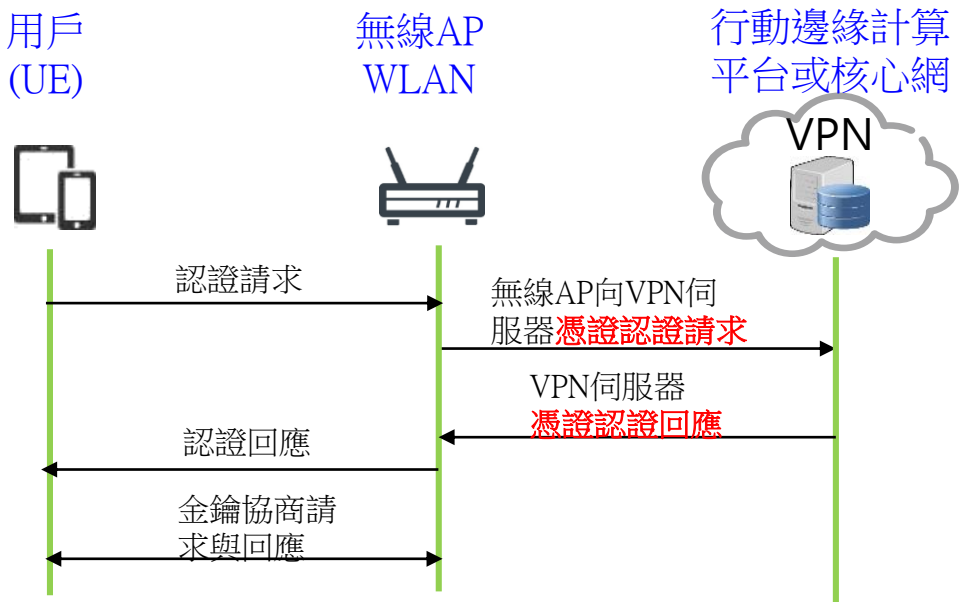
無線接入認證協議攻擊流程

- 前置作業
  - 架設攻擊平台以擷取IKEv2認證協定訊息
    - 硬體：控制電腦、及WIFI嗅探模組
    - 軟體：SoftAP(模擬無線AP)、Packet Crafter(模擬合法封包工具)及StrongSwan(模擬VPN伺務器)
- 攻擊流程



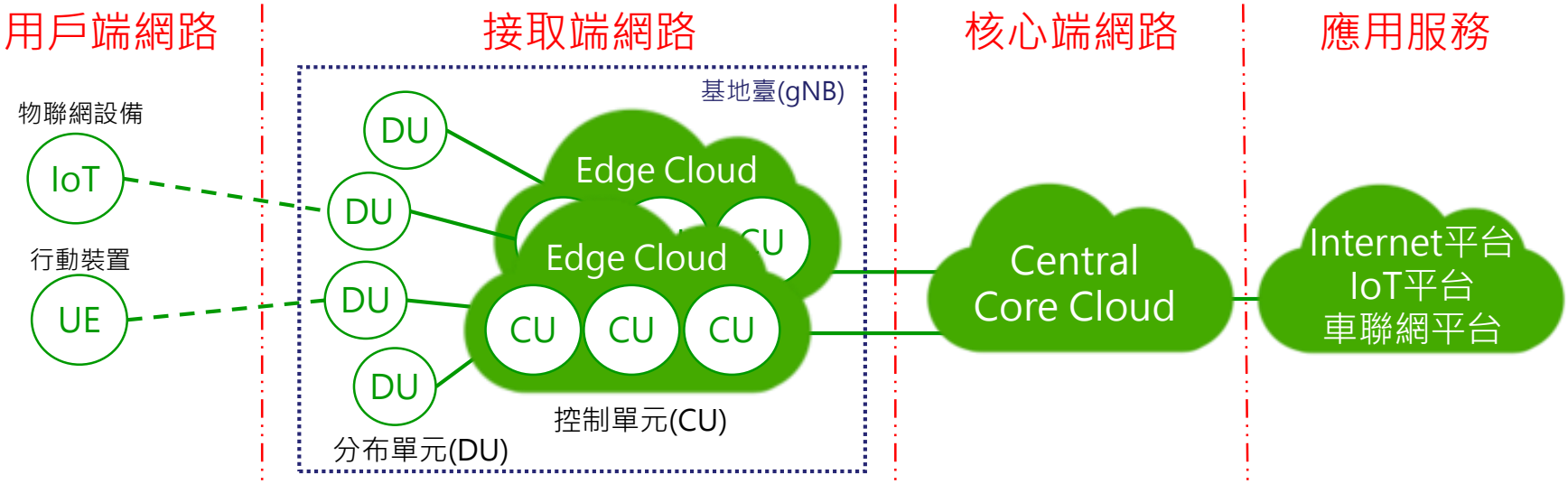
無線接入認證協議攻擊防護建議

- 由於用戶端裝置與異質網路端協議缺乏雙向認證，使攻擊者能藉由此漏洞來竊取用戶認證資料
- 因此可透過強化協議憑證的雙向確認機制，防禦用戶端裝置不安全的認證與授權
  - 由於用戶端設備與邊緣運節點缺乏完善的認證與授權機制，容易於用戶端網路使用偽冒裝置，竊取用戶隱私資料，建議於用戶端網路裝置啟動憑證雙向確認機制，以防止偽冒裝置運行於網路



5G網路之資安威脅

- 由於5G網路之重要變革在基地臺與核心網路，並提供多元之應用場景，因此5G網路之資安威脅主要來自於「接取端網路」、「核心端網路」及「應用服務」等面向



用戶端網路資安威脅

- 物聯網裝置安全性不足
  (如通訊缺乏加解密機制、軟/韌體資安漏洞等)

接取端網路資安威脅

- 行動邊緣計算平台威脅
  (如存取控制不足、軟體資安漏洞等)
- 異質網路連接缺乏完善之身分認證機制

核心端網路資安威脅

- SDN/NFV資安威脅
  (如網路切片越權存取、跨網路切片之DoS攻擊、虛擬機器共用實體資通基礎設施導致資料外洩等)

應用服務資安威脅

- 因應即時回應、大規模物聯網裝置及高頻寬應用服務之資安威脅
  (如通訊過程缺乏完整加密機制、認證請求超過應用服務處理能力導致服務癱瘓等)

5G資安要求

5G資安要求	
■ R1：用戶隱私識別碼保護	■ R13：網路切片安全隔離要求
■ R2：用戶端裝置軟體及硬體可信環境要求	■ R14：網路切片維運管理要求
■ R3：用戶端身分認證方式要求	■ R15：VNF之間認證與通訊要求
■ R4：用戶端身分識別管理要求	■ R16：NFV管理與流程編排要求
■ R5：無線接取網路通訊協議要求	■ R17：核心網內部網元通訊要求
■ R6：無線接取網路設備通訊介面保護	■ R18：SDN存取控制要求
■ R7：MEC數據存取要求	■ R19：漫遊網路資料保護
■ R8：MEC隱私保護	■ R20：支援不同類型應用接入認證與一致開放之認證要求
■ R9：MEC維運管理要求	■ R21：群組認證與身分管理要求
■ R10：MEC平台通訊協議要求	■ R22：低時延認證與網路節點加密要求
■ R11：接取端(異質)網路接入協議要求	■ R23：應用服務系統平台資安管理要求
■ R12：接取端實體環境設施保護	■ R24：端對端裝置通訊資料保護

5G資安威脅與防護建議(1/5)

用戶端網路

資安威脅	資安要求	防護建議
用戶端隱私識別資料攔截威脅	■ R1：用戶隱私識別碼保護	4G網路用戶IMSI是以明文方式傳送，造成用戶隱私洩漏問題，5G網路已要求用戶IMSI機密性，並以公私鑰加密方式，將用戶IMSI加密，以防範用戶接入認證時，IMSI被揭露之資安問題
		用戶TMSI除可使用加密方式來保護，另外可由用戶端裝置加入控制APP並將臨時識別碼定時更新或電信服務商由網路系統進行經常性更改臨時識別碼，以防止被鎖定及追蹤
用戶終端裝置軟體及硬體資安威脅	■ R2：用戶端裝置軟體及硬體可信環境要求	5G用戶端裝置應先經由軟體及硬體資安測試要求，以確保用戶端裝置能安全接入5G網路，或用戶端裝置可安裝防禦型APP進行數據加密，來防止裝置被入侵或遭破解等資安問題
用戶端身分認證資安威脅	■ R3：用戶端身分認證方式要求	可以使用閘道器或以一個群組為單位代表各個裝置執行身分驗證方法，透過閘道器與分組認證方式，可避免所有裝置直接接入網路端之架構，並減輕網路端認證信令流量處理
	■ R4：用戶端身分識別管理要求	5G網路可採用不同用戶端裝置或不同應用服務之認證、授權及存取管理方式來進行流量管理與監控，另外也可將流量監控管理機制內建於基地台來識別用戶端裝置流量，來防範用戶端流量攻擊

5G資安威脅與防護建議(2/5)

接取端網路

資安威脅	資安要求	防護建議
無線接取端網路(RAN)通訊介面資安威脅	■ R5：無線接取網路通訊協議要求	5G無線接取網路通訊協議雖採用雙向認證，但在無線廣播鍊路層(RRC)仍採用單向接收機制，因此可利用非對稱加密的機制，來對廣播訊息加密，以防止惡意偽造的虛假告警訊息
	■ R6：無線接取網路設備通訊介面保護	5G接取網路應確保無線傳輸資料的機密性與完整性要求，特別是接取端控制單元(CU)與分布式(DU)單元的介面及X2介面是否採用IPsec協議機制來確保傳輸資料的機密性與完整性
行動邊緣計算平台資安威脅	■ R7：MEC數據存取要求	MEC平台隱私及數據保護策略，應規定能够使用之通訊協議、介面、位置及流量並可參考下列要求: 介面使用限制：限定應用能够使用的介面與服務 數據讀取限制：指定應用能够讀取的用戶數據 虛擬鏡像限制：禁止應用使用非法的虛擬鏡像
	■ R8：MEC隱私保護	MEC平台為為雲端化架構，用戶的敏感性資料將儲存於MEC平台，因此應特別需要考量用戶敏感性資料保護，可透過加密機制保護資料或使用去識別化機制來過濾保護，防止隱私資料被竊取問題
	■ R9：MEC維運管理要求	MEC的維運管理須強化MEC控制器的設定要求，並進行統一協調與監管理，MEC控制器是代理服務提供方或連接應用的請求，使服務提供方無法直接連至運行於平台內部邊緣節點上來防止越權訪問，同時，MEC控制器負責監管應用發往外界的全部通信，應過濾所有數據流訊息，並阻止其流向非法第三方
	■ R10：MEC平台通訊協議要求	行動邊緣計算平台通訊協議為開放式協議，應強化行動邊緣計算平台間通訊協議的機密性與完整性保護，來確保通訊數據的安全

5G資安威脅與防護建議(3/5)

接取端網路

資安威脅	資安要求	防護建議
異質網路接入資安威脅	■ R11：接取端(異質)網路接入協議要求	5G接取網路應同時考量3GPP與非3GPP網路接入安全信令協議控制，特別是異質網路接入要求，應具體考量協議安全機制包括雙向接入認證，傳輸信令協議加密與完整性保護
接取端實體環境入侵威脅	■ R12：接取端實體環境設施保護	由於接取機房為無人機房,容易遭實體入侵來操控接取設備而影響5G網路安全，因此應強化5G接取機房環境監控，接取設備告警及日誌管理以防範實體入侵資安問題

核心端網路

資安威脅	資安要求	防護建議
網路切片資安威脅	■ R13：網路切片安全隔離要求	由於網路切片是共享相同的核心網基礎設施，爲了確保一個切片的異常不會影響到其他切片，一方面，核心網可以採用實體隔離的方案，爲安全性要求較高的切片分配相對獨立的實體資源，另一方面，還可以採用邏輯隔離方案，藉助成熟的虛擬化技術，在網路層通過劃分VLAN/VXLAN 子網進行隔離，在管理層通過分權分域實現切片管理與編排的隔離
	■ R14：網路切片維運管理要求	5G網路切片管理應採用切片ID識別授權與認證作法，來確保不同切片間的服務與QoS之外，同時透過切片流量監控與動態配置能力，可防範流量攻擊或越權訪問

5G資安威脅與防護建議(4/5)

核心端網路

資安威脅	資安要求	防護建議
核心網路功能虛擬化(NFV)資安威脅	■ R15：VNF之間認證與通訊要求	應強化核心網路VNF 網元間的通訊安全要求，網元間 的通訊啟動雙方相互認證功能，並且通訊內容需受到機密性、完整性的保護，另外並針對VNF內部安全隔離及安全區域進行劃分以提升攻擊難度
	■ R16：NFV管理與流程編排要求	NFVO為5G網路管理模組，同時負責協調網路服務、組成網路服務的VNF及承接各VNF的虛擬資源的控制與管理，因此可透過此模組來模擬防火牆，入侵偵測及流量偵測功能，來建立核心網路的資安防護能力
核心網內部通訊協議資安威	■ R17：核心網內部網元通訊要求	5G核心網路使用服務基礎架構(SBA)，因此需要相對應資安機制，針對核心網路網元間註冊，認證及控制也就是啟動核心網路網元間通訊協議，如HTTPS、QUIC及TLS資安協議，以確保網元間通訊安全
軟體定義網路(SDN)資安威脅	■ R18：SDN存取控制要求	SDN防護策略主要分成Statistical(統計)與Policy(白名單規則)方式，進行資安強化。Statistical類型主要針對網路流量之行為與屬性進行塑模，若新進流量未符合該模型，即為異常。Policy類型主要為白名單規則，僅符合規則的流量可以通過，常見於防火牆功能
漫遊網路資料攔截資安威脅	■ R19：漫遊網路資料保護	5G網路漫遊安全問題，應強化5G網路傳輸層與應用層間的信令協議安全，並進行端到端安全保護，因此啟動IPsec協議，可使得電信業者間的轉接設備無法解析到核心網路之間的敏感訊息如密鑰，用戶身分及短訊等，以確保完整與機密性保護

5G資安威脅與防護建議(5/5)

應用服務

資安威脅	資安要求	防護建議
增強移動寬頻、大規模物聯網及低時延高可靠度應用應用接入資安威脅	■ R20：支援不同類型應用接入認證與一致開放之認證要求	為支援多種接入技術與認證協定的框架進行統一的認證與安全管理，目前國際標準建議5G 增強移動寬頻(eMBB)認證框架應基於EAP可擴展認證設定，來因應5G 增強移動寬頻(eMBB)高流量應用服務，並防範認證協議資安漏洞問題
	■ R21：群組認證與身分管理要求	為針對大量物聯網接入的資安要求，5G網路可於行動邊緣平台上布建分布式認證伺服器，來進行群組認證與身分識別，以防範流量攻擊或越權訪問
	■ R22：低時延認證與網路節點加密要求	5G低時延高可靠度連接(uRLLC)為降低時延認證與加密要求了，為使本地加解密更快速，可採取的防護措施包含:使用更有效率的加密演算法、利用虛擬化網路或雲端網路中的計算資源、實施硬體加速以及採用可進行平行運算的加解密演算法，以有效防範隱私洩漏資安問題
應用服務系統平台資安威脅	■ R23：應用服務系統平台資安管理要求	5G網路應用服務平台除透過5G網路系統監控與管理方式幫助檢測違規情況，另外仍需建立不同營運商之間的網路稽核合作機制，對各自網路布建設備或系統平台定期進行資安查核與檢測工作
端對端之通訊資安威脅	■ R24：端對端裝置通訊資料保護	由於5G網路端對端的通訊認證將繞過核心網路，因此將藉重接取端的分布式認證架構並採用公鑰基礎上 進行屬性加密，來實現端對端的通訊加密並確保通訊數據的機密性與完整性

教材資料：感謝國家資通安全會報技術服務中心
蔡志明研究員協助編撰