國立陽明交通大學資通安全教學與研究中心

The Center for Education and Research in Cybersecurity

臺灣資安科技研究中心

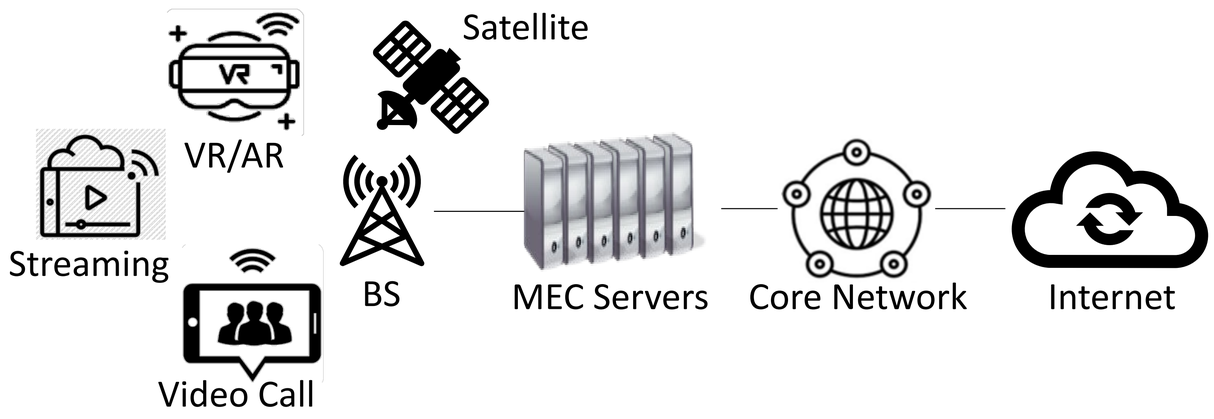
Taiwan Academic Cybersecurity Center

次世代行動網路安全技術與基礎研究

計畫目標與關鍵技術

整體目標：

- ☑提升下世代**通訊網路安全**
- ☑確保網路的可靠性和效率
- ☑保護網路免受**網路安全威脅**
- ☑**技術發展**與**理論研究**併重



主題一：通訊網路之**旁路攻擊**弱點

加密通話封包判斷．狀態推斷攻擊．用戶ID推斷攻擊

主持人：李奇育、謝秉均

主題二：網路威脅情資自動探勘

網路威脅攻擊途徑擷取．多資料來源自動擷取威脅情資

主持人：林盈達、黃仁竑、林柏青

主題三：**人工智慧**標準化情境運用

通訊架構資安檢測．生成式人工智慧隱私保護．可信度檢測

主持人：曾煜棋、李大嵩、劉恩成

主題四：**軟硬體強固**技術

程式分析與執行防護．資料流追蹤．模糊測試．軟硬體協同設計

主持人：黃俊穎、吳育松、黃世昆、葉宗泰

主題五：高效率與可靠**計算**

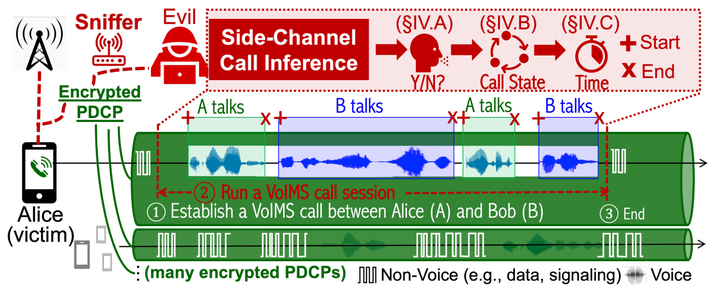
具適應性的韌性函數．量子密碼最小困難性假設

主持人：蔡錫鈞、高孟駿

通訊網路之旁路攻擊弱點

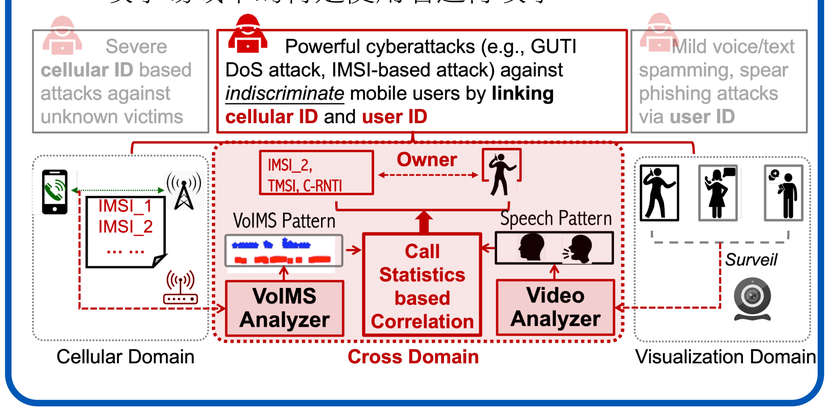
❑關鍵技術一：旁路加密5G通話封包判斷和狀態推斷攻擊

- 攻擊者Evil 竊聽使用者Alice的傳輸加密封包
- 可成功判斷使用者之通話狀態和通話時間
- 已使用五支手機和三個電信商完成驗證



❑關鍵技術二：搭配旁路加密通話封包進行用戶ID推斷攻擊

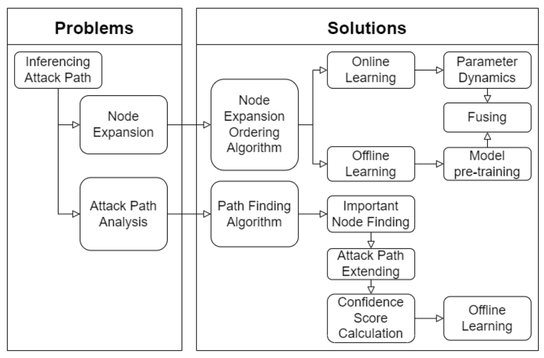
- 搭配網路攝影機，基於用戶通話的狀態，連結連結電信ID和用戶ID (例如IMSI和RNTI)，進而針對攻擊場域中的特定使用者進行攻擊



網路威脅情資自動探勘

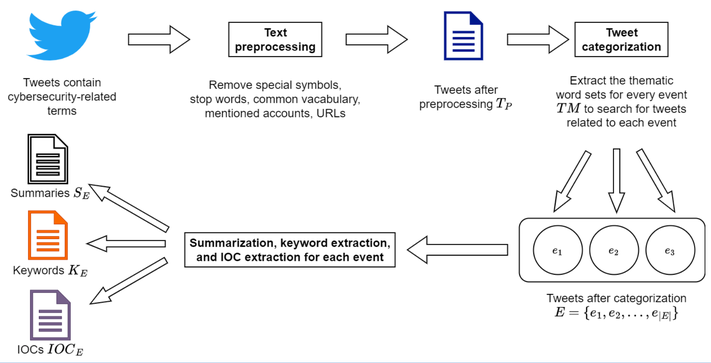
❑關鍵技術一：自動從威脅情資資料中推論出攻擊路徑

- 路徑找尋演算法：降低76.0%的搜尋成本
- 節點擴展演算法：降低25.6%的擴展次數



❑關鍵技術二：從多資料來源的發文中擷取網路威脅情資

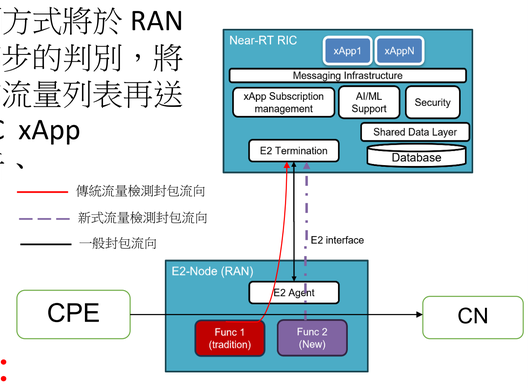
- 即時性：從Twitter的情資中，前10%的領先事件相較既有情資平台領先至少4天
- 熱門度：超過95%的擷取情資有被公開情資提及



人工智慧標準化情境運用

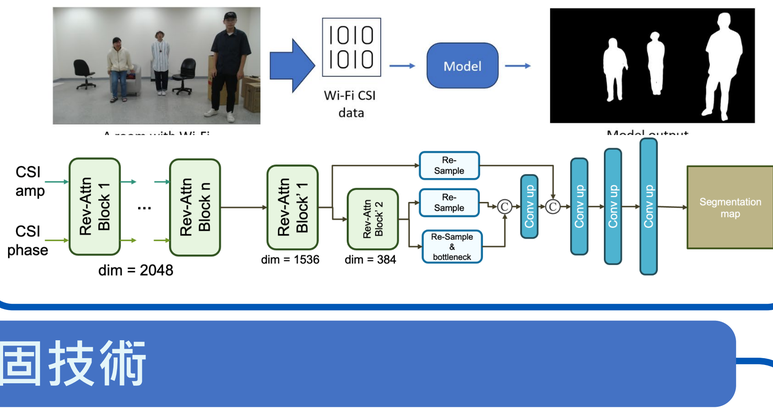
❑關鍵技術一：6G開放系統架構之AI資安檢測技術

- 新式流量檢測方式將於 RAN 端環境中做初步的判別，將判定為異常的流量列表再送往 Near-RT RIC xApp 進行後續分析、處理和決策



❑關鍵技術二：具備隱私保護的生成式AI關鍵技術

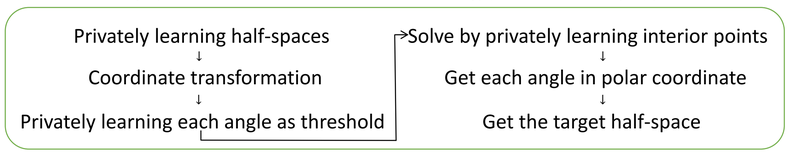
- Wi-Fi CSI：使用 CSI 訊號，設計一個能適應不同環境的AI模型，取得環境中人體分割圖
- 電腦視覺：使用非RGB的資料來進行具備隱私保護的監控，如分割圖和骨架。提出 MP-PolarMask方法用於更快更準確的分割，成果已被接受於 CVPRW 2024
- 電腦視覺 + 陀螺儀：除了從骨架進行動作辨識，可結合陀螺儀的輔助，增強動作辨識的準確度



高效率與可靠計算

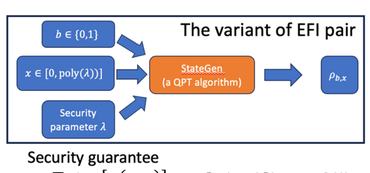
❑關鍵技術一：有效地建構韌性函數

- 設計一個新演算法，有效改善 privately learning halfspaces 的sample complexity為 $\tilde{O}\,(d \log^*|\mathcal{X}|)$
- 已掌握 resilient function 的建構方法以及其性質



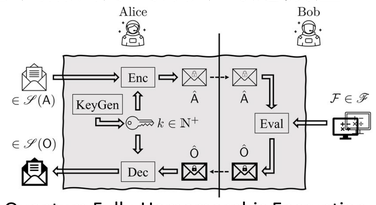
❑關鍵技術二：多項式級別之 EFI Pairs 可提供之隨機性

- 探討 polynomially many EFI pairs 的隨機性與可分辨性
- 透過 EFI pairs 的 partial trace，以及其為 polynomial size 的性質，證明此情況下無法得到額外的隨機性



Security guarantee

1. $\sum_x |\Pr[A(\rho_{0,x})] - \Pr[A(\rho_{1,x})]| \le \text{negl}(\lambda)$
2. $\sum_x \frac{1}{2}\|\rho_{0,x} - \rho_{1,x}\| \ge \frac{1}{\text{poly}(\lambda)}$



Quantum Fully-Homomorphic Encryption (QFHE)

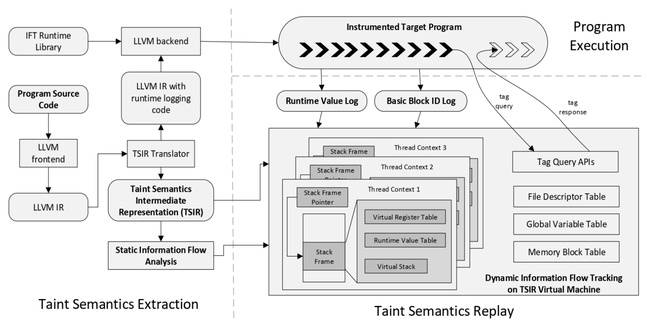
❑關鍵技術三：量子電路同態加密與驗證技術

- 探討現有之 Trapdoor permutation 與 Trapdoor claw-free function 以外，可用於驗証量子能力之困難函式
- 與量子驗證 (proof of Quantumness) 與量子計算驗證 (verifiable Quantum computation) 有密切相關

軟硬體強固技術

❑關鍵技術一：動態資訊流追蹤

- 完成控制流監控程式碼插樁機制和基本區塊資料流語意模型設計與萃取機制實作
- 實現對於測試程式的資料流追蹤，並且使用真實程式(如nginx)進行資料流追蹤實驗，驗證系統設計
- 完成TSIR Replay VM功能實作，結合邊緣運算AI技術來改善source與sink變數的識別準確度與效率

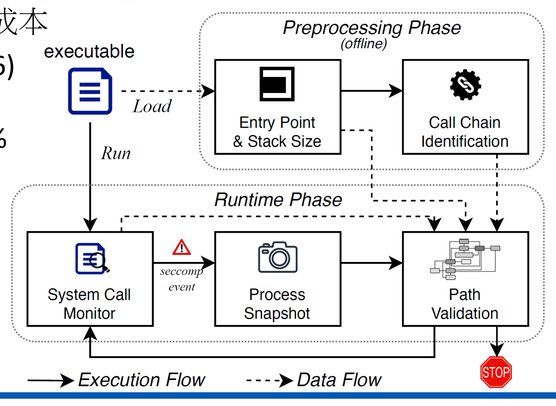


❑關鍵技術二：系統呼叫防護機制

- 建構軟體式程式系統呼叫防禦機制，提供基於程式執行脈絡的系統呼叫控制
- 執行效能成本

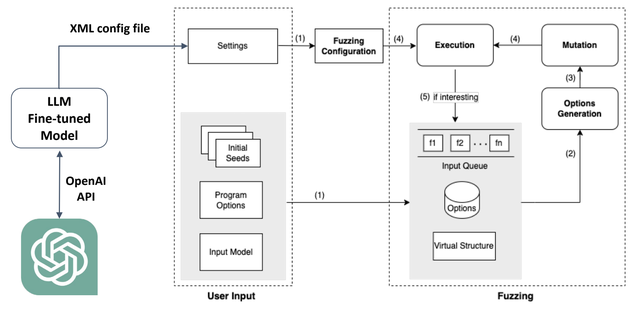
(SPEC CPU 2006)

- Max ~2%
- Average ~1%



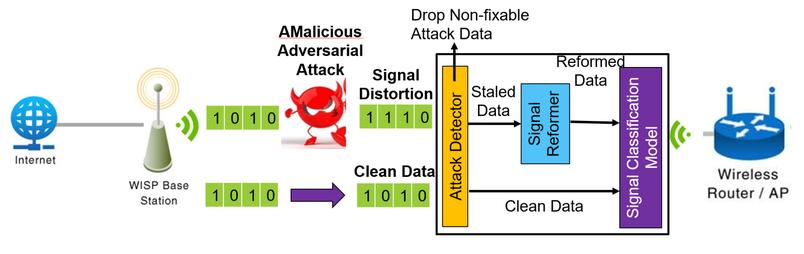
❑關鍵技術三：模糊與組合測試技術

- 多參數模糊測試技術：漏洞通報並被分配 42個 CVE
- 模糊組合測試
  1. 設計 API-based LLM 微調模型，自動生成影音處理程式之多參數組態選項
  2. 識別具安全性威脅之「500 錯誤」回應
- Structured Fuzzing：改善基於Preach Fuzzer Pit 描述方式之模糊測試方法



❑關鍵技術四：AI對抗式攻擊防禦技術

- 結合隨機傅立葉轉換以及輕量化的auto-encoder模型，對於惡意攻擊訊號進行修復以及偵測，並且對於不同的無線訊號的Adversarial Attack方法和類型進行探討
- 已可有效抵擋16種不同的無線訊號惡意攻擊



NSTC

NYCU 國立陽明交通大學