

經濟部 111 年度
5G 資安防護系統開發計畫
合作研究計畫

《5G 資安自動化檢測技術》
建議書徵求文件

財團法人資訊工業策進會

中華民國 111 年 4 月

111年度合作研究計畫建議書徵求文件

一、簡介

近年來資訊安全事件頻傳，個人、企業和政府都因為各式不同的資訊安全事件而造成財務和名譽上的損失。資訊安全的重要性日益提升，除了個人和企業資安意識的提升之外，政府亦拋出「資安即國安」的施政方向，以提升並保障國內各級資訊系統的安全為目標。軟體和系統安全是保障資訊安全最根本的基礎。當軟體和系統實作出現缺陷時，這些缺陷和弱點就可能被有心人士用以發動資訊安全攻擊。然而，現有的軟體和系統數量龐大且複雜，如何有效率地針對現有的軟體和系統進行系統性系統化地安全測試，以識別潛在的缺陷和風險，便成為一個重要的議題。

為了維持新興網路如5G和物聯網環境下的可靠性，確保使用者和裝置上網的隱私和安全，O-RAN軟體聯盟(O-RAN Alliance)定義了開放網路元件之間的資安規範。本合作計畫(以下簡稱本計畫)將嘗試針對O-RAN軟體聯盟所定義的端對端測試安全規範，針對S-Plane PTP DoS Attack (Network layer)與C-Plane eCPRI DoS Attack (Network layer)等兩個測項進行研究，預計開發相關測試工具，藉以檢測O-DU實作的潛藏問題。

二、計畫目標

本計畫預計研究O-RAN軟體聯盟的S-Plane PTP與C-Plane eCPRI通訊協定，並開發相關安全測試工具。本計畫主要針對O-RAN軟體聯盟測試規範O-RAN.TIFG.E2E-Test.0-v02.00第七章所定義的7.2.1 S-Plane PTP DoS Attack (Network layer)與7.2.2 C-Plane eCPRI DoS Attack (Network layer)兩個測項進行研究，並開發相關測試工具。此工具必須能產生10Mbps, 100 Mbps, 1Gbps等不同速率，並能設定不同的MAC位址，以及產生S-Plane PTP與C-Plane eCPRI等不同的封包，以提供O-DU安全檢測，找出相關軟體可能的系統弱點和風險。本計畫預期研發的技術將可以產生攻擊O-DU的S-Plane PTP與C-Plane eCPRI協定等DoS封包，針對O-DU軟體進行分析並產生測試資料，以期分析出潛藏的協定設計或實作缺陷或弱點，提升整體系統的安全。

三、計畫範圍

本計畫應針對S-Plane PTP與C-Plane eCPRI通訊協定建構一通訊軟體安全檢測工具，以測試O-DU對於DoS攻擊的防護能力，並提供主計畫系統進行整合與呈現。

四、預期成果

本計畫研發之模組，應可針對 S-Plane PTP 與 C-Plane eCPRI 通訊協定產生 DoS 攻擊資料，以供研發人員或測試人員了解 O-DU 通訊協定實作的可能缺陷。本計畫預計產出中期末報告各一份（含教育訓練）。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、執行方式

本計畫預計將結合本會在資安測試軟體開發的基礎，以及學界在 O-RAN 測試平台建置的實務經驗及，透過雙方相互合作討論的方式來進行，本計畫亦需提供教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 完成相關文獻蒐集等先前技術整理
2. 完成 S-Plane PTP 與 C-Plane eCPRI 通訊協定安全檢測工具

六、計畫期程及預估計畫總經費

計畫執行區間：111年04月01日至111年12月15日

總經費：80萬元

七、驗收標準(含教育訓練)

1. 期中、期末報告：分別預計於 111 年 8 月 30 日與 111 年 11 月 30 日完成期中與期末報告：
 - 期中報告的內容包含：系統架構的規劃方式及先前技術整理說明
 - 期末報告的內容包含：S-Plane PTP 與 C-Plane eCPRI 通訊協定 DoS 攻擊工具使用說明及功能展示。
2. 雛形系統：期末完成 S-Plane PTP 與 C-Plane eCPRI 通訊協定 DoS 攻擊工具執行檔及功能驗證。
3. 提供教育訓練：針對計畫成果移交、系統運作機制及操作說明等提供教育訓練。
4. 進度討論會議：每月召開一次進度研討會議。

八、技術能力需求

本計畫執行人員須具備 O-RAN 領域相關基礎知識背景與基站開發實務經驗。

1. O-RAN 相關背景：須瞭解 5G 基站等各項協定技術，並熟悉 5G 基站前傳

介面(Fronthaul Interface)，能掌控本計畫研發所需核心技術。

2. 相關計畫參與經驗：熟悉 5G 基站運作原理，並具相關系統開發及計畫執行參與經驗。