經濟部 109 年度

《5G+系統暨應用淬鍊計畫》

合作研究計畫

惡意加密流量分類系統

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年 07 月 08

109年度合作研究計畫建議書徵求文件

一、 簡介

5G技術將帶來便利性及多元創新應用服務，但也伴隨而來網路資安威脅、商業模式轉換等新興挑戰。現行資安產品多以資安檢測手法與針對固定設備之異常行為監控為解決方安架構，借由終端防護、閘道管理、資安監控 維運中心及代理國外資安產品等方式進行系統整合，難以滿足5G網路功能 虛擬化系統動態服務部署,以及服務串接之應用服務環境之動態防護需求,更欠缺一致、自動化調適管理之能力。

電信網路由2G發展到5G，於2.5G GPRS 加入封包交換機制，開始實現數據傳輸的功能。在3G時代，將控制面（control plane）與用戶面（user plane）分離，分別負責控制與承載的功能。4G LTE網路進而分別以MME取代 SGSN 與 SGW/PGW 取代 GGSN 。5G開始朝向虛擬化架構。不論如何電信網路的演化，其中在數據傳輸皆是以 GTP（GPRS Tunnelling Protocol）的通信協定進行資料的交換。GTP 為基於IP的通訊協定，用於在 GSM、UMTS、LTE 網路中承載 GPRS進行資料傳輸。

二、 計畫目標

本研究案將建構可用於Pre-5G/5G平台的加密惡意流量偵測機制，UE的資料傳輸無論是往MEC或是進入網際網路，皆由GTP所承載。過往加密惡意流量的研究，著重在一般網際網路流量的惡意加密流量分析。本研究欲對由GTP所傳輸的所加密的TCP/IP流量以不解密的方式進行惡意行為檢測，對於惡意軟體所發出的流量進行分析，達到在資料流於加密狀態仍可進行安全性的檢測。

三、 計畫範圍

本計劃範圍為研究5G場域於TCP/IP通道的惡意程式加密流量可識化技術，需於實際場域蒐集多種惡意程式所對外溝通流量，並且在不進行解密的狀態之下，針對流量進行特徵萃取，以達到惡意程式流量可識化的結果，加強核網通訊以及多接取邊緣運算的安全性。

四、 預期成果

本計畫將於pre-5G前哨環境之下，自行產生對外惡意程式數據流量，並在不解密的狀態下進行可識化分析。

- 錄製由TCP/IP環境下的惡意程式加密流量，至少10種不同種類勒索軟體，每種惡意程式需要錄製500個以上的flow。
- 可識化惡意程式偵測系統，可自動化由網路流量進行偵測，並提供系統報告書。需以深度學習中CNN模型(Mobilenet V2，輕巧快速又不失準確率)、RNN 模型(LSTM)和機器學習中LightGBM和Catboost演算法進行訓練，並比較4種演算法的優劣結果，預期偵測率達95%以上。
- 系統需針對主機上的應用程式進行流量切割，分流出各應用程式的流量。
- 提供模型偏移以及重新訓練的衡量機制
- 需佈署於資安所所提供的實際場域並與SecBuzzer ESM介接測試，本開發系統將處理從醫院mirror的流量，提供測試報告。
- 期中研究報告一份
- 期末研究報告一份
- 研究內容需投稿國外期刊或研討會論文一篇

※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

- 合作計畫執行單位應配合本會計畫監控機制。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，雙週本單位進行研究心得報告與研討，報告內容以計畫範圍相關之技術主題為主。
- 交付說明

項次	交付項目	交付內容	數量	交付型態	交付期限
1	惡意程式加密流量錄製	• TCP/IP環境下的惡意程式加密流量 • 10種不同種類勒索軟體 • 每種惡意程式需要錄製500個以上的flow	1 式	電子檔	109 年 8 月 15 日
2	期中研究報告一份	• 惡意流量錄製場域與方式說明 • 惡意流量特性分析	1 份	紙本及電子檔	109 年 9 月 15 日
3	可識化惡意程式偵測系統一式	• 原始程式碼含使用說明 • 可識化惡意程式偵測演算法偵測率需達 95%	1 式	電子檔	109 年 10 月 31 日
4	介接 SecBuzzer ESM，並佈署於資安所所提供的重直應用場域	• 介接 SecBuzzer ESM 之系統說明書，本開發系統將處理從醫院 mirror 的流量。	1 份	紙本及電子檔	109 年 10 月 31 日
5	期末研究報告一份	• 可識化研究細節陳述及系統說明 • 場域測試報告書	1 件	紙本及電子檔	109 年 12 月 15 日

六、 計畫期程及預估計畫總經費

計畫執行區間： 109 年 01 月 01 日 至 109 年 12 月 31 日

總經費：1,400,000元

七、 驗收標準(含教育訓練)

- 依本建議書徵求文件第四章「預期成果」規定，如期繳交相關成果。

八、 技術能力需求

本計畫執行人員須具備電信網路研究背景外，尚須對網路安全、網路流量分析和網路系統性能評估擁有相關經驗背景。

- 具行動通訊網路研究經驗之學界研究人員
- 具備且熟悉無線網路與 TCP/IP 協定技術之學界研究人員

附件1：契約書格式
1-1：計畫書格式
1-2：經費動支報表
1-3：成果報告撰寫須知
1-4：報告格式
1-5：論文格式
1-6：保密聲明書
1-7：委託匯款同意書