經濟部 106 年度

《先進通訊實驗環境建置與技術研發計畫》

合作研究計畫

《4G 端點防護之關鍵檔案隔離技術》

建議書徵求文件

財團法人資訊工業策進會

中華民國 106 年 05 月 17 日

106年度合作研究計畫建議書徵求文件

一、 簡介

4G LTE顛覆傳統電信(Telecom)網路架構，採用全IP網路直接與網際網路(Internet)介接，以加速電信網路的普及，此一創舉使得電信網路同樣面臨網際網路世界的安全威脅，駭客只要透過上行鏈路(backhaul link)此一著力點，4G LTE網路即曝露在傳統網路的資安威脅下，可行的網路攻擊像是竊聽(sniffing)、弱點掃描(vulnerability scan)、偽裝(Masquerade)等，除此之外，LTE本身也存在高風險之資安漏洞，例如：S1AP的first network contact協定漏洞、IMSI遭偽基站竊取、利用UE連網訊息引發之MME分散式阻斷攻擊(DDoS)等，尤其在人們相當仰賴行動網路的現在，強化電信網路資安是刻不容緩的。

本計畫之主計畫為4G通訊系統軟體資安檢測技術，因應國內外電信商及4G應用服務商(例如:金融、醫療、交通等)針對通訊設備第三方資安檢測要求，涵蓋前端UE設備、接取端小型基站及後端伺服器設備之4G應用服務E2E整體資檢測技術。本計畫將與學界合作研究4G LTE端點防護之關鍵檔案隔離技術，意在提供4G應用服務E2E(End-to-End)資安解決方案。期望透過此一合作研究計畫，單一端點的資安可以獲得關鍵強化，促使全面提升4G應用服務的資安品質。

二、 計畫目標

本計畫將與學界合作研發4G端點防護之關鍵檔案隔離技術，由於4G設備存在相當多的關鍵資料，這些資料包括CSG List、ACL(Accest Control List)、4G組態設定檔、系統組態設定檔等，甚至是資安防護軟體最常使用到的黑、白名單等，都需要嚴加保護及控管其存取權限，避免駭客利用這些資訊發動進一步的攻擊；除此之外，4G網路的傳輸對於延遲(latency)，比起傳統的電腦網路有較高的要求，因此所研發的隔離保護及權限控管之端點防護技術必須兼具時效性；最後此端點防護需具備自我保衛能力，以因應駭客利用系統提權手法，操弄甚至移除此端點防護功能。

研發此技術可加值予既有之4G端點設備，使其完善機敏資料的儲存保護能力，並鞏固4G端點的資安質量，透過此項技術可達成之防護目標如下：

1. 研發一可信賴的軟體層4G安全區塊(Trust Environment,TrE)，提供關鍵檔案(e.g. configure file、white list)之隔離儲存區域。
2. 可偵測關鍵檔案的非預期寫入行為，並滿足高效率防止駭客存取機敏資訊之需求。
3. 強化防護模組之自我保護技術，即使是系統之超級使用者(super user)也不能任意操作。

三、 計畫範圍

本計畫以Linux based之4G端點設備為研究對象，設計一可供4G端點設備(一體適用前端、接取端及後端)管控其關鍵檔案存取權限之雛型系統。此雛型系統可用於提升4G單一端點之資安防護能力，徹底秉除因4G相關機敏資訊之外洩，或者單一端點被駭客入侵，所引發之阻絕服務(DoS)或偽基站等4G LTE資安攻擊。其實作內容包含下列項目:

1. 為提高此雛型系統之擴展性，捨棄傳統所採用之邏輯隔離實體技術，利用Linux內建之功能，於軟體層開發一4G TrE安全隔離區塊。
2. 改善現行之whitelisting技術，設計一高效率之關鍵檔案存取控制機制。
3. 設計一保護機制，迫使任何身分之使用者皆無權限存取此端點防護功能，或者隱蔽此端點防護功能不被任何身分之使用者察覺。

四、 預期成果

為提供4G LTE應用服務商與設備商資安解決方案，研發用以確保端點設備之關鍵檔案防護能力，經由主計畫提供4G應用服務商檢知其整體上的關鍵脆弱點後，為進一步協助4G應用服務商補強其資安品質，同時促進4G應用服務的普及，本計畫預期成果為建立一Linux based之4G端點設備防護之4G關鍵檔案隔離技術。內容包括：

1. 4G端點設備之關鍵檔案保護隔離方法。
2. 4G端點設備之高效率關鍵檔案非預期存取偵測及阻絕方法。
3. 期中期末報告各一份(含系統功能展示、說明及相關技術資料)。
4. 提出研發相關專利構想一案。
5. 投稿國際或國內研討會或期刊論文並被接受共2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

本計畫將整合資策會與合作對象的專長和資源，透過雙方相互合作討論的方式進行，同時由合作對象負責執行和完成相關產出。相關執行方式步驟如下：

1. 完成相關文獻蒐集與4G各端點設備所內含之關鍵檔案的整理。
2. 完成4G端點設備防護之關鍵檔案隔離的雛型規劃設計與實作。
3. 完成4G端點設備防護之關鍵檔案隔離雛型系統，包含基本驗證與案例測試。
4. 完成期中期末報告並驗證分析系統的正確性。
5. 進度討論會議：
   - 每2週以con-call召開工作會議，以管控專案進度及問題排除等。
   - 每月參與實驗室會議，進行論文及研發技術之討論。
   - 每季一次實機功能展示，確保專案技術之實現。

六、 計畫期程及預估計畫總經費

計畫執行區間： 106 年 05 月 01 日 至 106 年 12 月 15 日

總經費：600,000元

七、 驗收標準(含教育訓練)

1. 提交期中、期末報告：
   -期中報告的內容包含：4G端點設備防護之關鍵檔案隔離雛型系統的規劃，及4G端點設備相關之關鍵檔案的整理。
   -期末報告的內容包含：4G端點設備防護之關鍵檔案隔離雛型系統的實際應用案例、測試結果說明及展示。
2. 4G端點設備防護之關鍵檔案隔離雛形系統(包含執行檔、測試程式與相關程式原始碼)。
3. 提供教育訓練：針對計畫成果移交，雛型系統運作機制與操作說明等提供教育訓練。
4. 期末交付已被研討會接受之學術論文兩篇。
5. 研發相關專利提案構想一案。

八、 技術能力需求

本計畫執行人員需具備資訊安全相關基礎知識背景外，尚須對4G LTE的系統架構、運作機制及不同應用層面所使用到的函式庫對應有一定的了解。

1. Linux kernel module開發技術：熟悉Linux平台架構與核心模組開發技術、Linux container、Linux system call hooking，並具備通訊與檔案存取異常行為分析之經驗。
2. 熟悉4G LTE通訊協定、TrE(Trust Environment) 等4G相關安全防護知識、且有白名單防護開發經驗，或實際滲透測試操作的技術人員。

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