經濟部 107 年度
物聯網系統檢測與驗證計畫
合作研究計畫

《AI 資安模糊測試核心技術》

建議書徵求文件

財團法人資訊工業策進會

中華民國 107 年 3 月 6 日

107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，如何有效率地針對現有的軟體和系統進行自動化地安全測試，以識別系統潛在的缺陷和風險，便成為一個重要的議題。

現有大多數的資安事件都是針對連網設備發動攻擊。而隨著IoT裝置的盛行和連網裝置的多樣化，各種新興的網路協定和實作也依其應用場域的需求而被開發出來。為了確保網路通訊協定的設計和實作可以免於有心人士的攻擊，本合作計畫（以下簡稱本計畫）著重於研發通訊協定實作缺陷自動化檢測所需之核心技術。如此不僅可以有效了解連網系統通訊協定的設計和行為，更可用於評估待測系統是否潛藏需要修補的系統弱點和風險，以提升研發資安弱點測試平台的檢測能力。

二、 計畫目標

本計畫目標針對連網裝置所使用的網路通訊協定進行自動化的識別和測試，以偵測可能的系統弱點和風險。具體而言，通訊協定的自動化識別旨在透過已搜集的網路流量資料，找出可能利用於測試的有效協定欄位（protocol field）。而通訊協定實作測試的進行則利用模糊測試（fuzz testing）相關技術進行。本計畫預期研發的技術將可以針對已知或未知網路協定的封包進行分析並產生測試資料，以提供模糊測試使用。利用上述流程，以其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

本計畫範圍以建構一通訊協定安全檢測模組為主，本計畫所產出之模組需提供界面與主計畫所研發之資安弱點測試平台界接。預計將提供制式的使用者或系統界接界面，接收來自主系統遞交的網路流量封包側錄資料檔，進行分析和測試後，再產出分析結果以及測試資料。分析結果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，應可針對網路流量封包側錄資料檔案進行處理，並利用人工智慧相關技術進行分析，供研發人員或測試人員了解資料傳輸通訊協定的可能結構，並產生適用於模糊測試的測試資料。本計畫的預期成果應包含以下三項：

1. 通訊協定實作弱點分析檢測系統，包含：
   - 通訊協定分析模組:讀取網路流量封包側錄資料,分析封包內容並進行協定欄位識別。
   - 測試資料生成模組：依據分析封包內容，產生測試資料。
   - 模糊測試系統模組：依據測試資料對通訊協定實作進行測試的系統模組。
2. 利用本計畫所產出系統，針對 3 個 IoT 相關網路協定進行測試以作為實證。
3. 期中期末報告各一份（含教育訓練）
4. 本計畫預期撰寫國際或國內知名研討會或期刊論文一篇

※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

本計畫預計將結合學界在理論面以及本會在資安弱點測試平台建置的實務面經驗，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. 完成通訊協定安全檢測模組系統架構規劃及架構程式編寫
3. 完成通訊協定安全檢測模組雛形系統，並完成系統功能測試
4. 完成結案報告，驗證分析系統的正確性、成果品質以及教育訓練分享

六、 計畫期程及預估計畫總經費

計畫執行區間：107年01月01日至107年12月7日

總經費：800,000元

七、 驗收標準(含教育訓練)

1. 期中、期末報告：分別預計於 107 年 8 月 30 日與 107 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：系統操作行為檢測模組的研究成果、相關的功能驗證報告以及雛形展示
2. 雛形系統：期末完成通訊協定封包識別及測試檢測模組，包含執行檔、程式原始碼及檢測功能驗證。
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。
5. 國內外知名研討會或期刊論文一篇。

八、 技術能力需求

本計畫執行人員須具備資訊領域相關基礎知識背景外，尚須對網路及系統行為測試及監控手法擁有一定瞭解。

1. 資訊安全相關背景：須瞭解網路系統運作原理，惡意程式偵防技術，網路攻防技術，惡意程式分析等各項技術，並熟悉相關資安分析工具的使用，能掌控本計畫研發所需核心技術。
2. 相關計畫參與經驗：熟悉模糊測試運作原理，了解編譯器運作原理，了解虛擬機運作原理，並具相關研究論文發表及計畫執行參與經驗。
3. 其他：如熟悉 C/C++、Python、Shell programming、虛擬機器（Virtual Machine）、一般網路服務軟體如 Apache 等系統程式的運作。

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