經濟部106年度
《資策會創新前瞻技術研究計畫》
合作研究計畫

《程序記憶體分析與金鑰擷取技術》

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 18 日

106年度合作研究計畫建議書徵求文件

一、 簡介

惡意軟體的偵測與預防為資安領域中持續存在的挑戰，惡意軟體近幾年數量暴增、行為複雜度不斷增高，造成之危害亦日漸嚴重。現有的防毒軟體已無法保證能夠偵測惡意軟體，其通常只能針對已知且常見的惡意軟體做出防堵。因此，資安服務提供者急需一個針對惡意軟體感染行為所設計的特徵萃取與早期偵測機制，以即時在惡意軟體產生危害前將之隔離與移除。此外，惡意軟體使用加密通道以隱藏其通訊行為之比例亦呈現增加之趨勢，將使得分析難度增加。因此，本計畫預計針對具加密通訊機制之惡意軟體，瞭解其感染主機端之記憶體資訊，從中取出加密通道金鑰，以解開受感染主機端與惡意軟體中繼站間通訊之資訊。

本分包合作研究案因應主計畫之目標，在動態記憶體通道金鑰萃取與情資挖掘機制方面，預計實作SSL/TLS主金鑰破解於Windows系統中，嘗試解開惡意軟體之加密通道，從中取出惡意軟體通訊行為。

二、 計畫目標

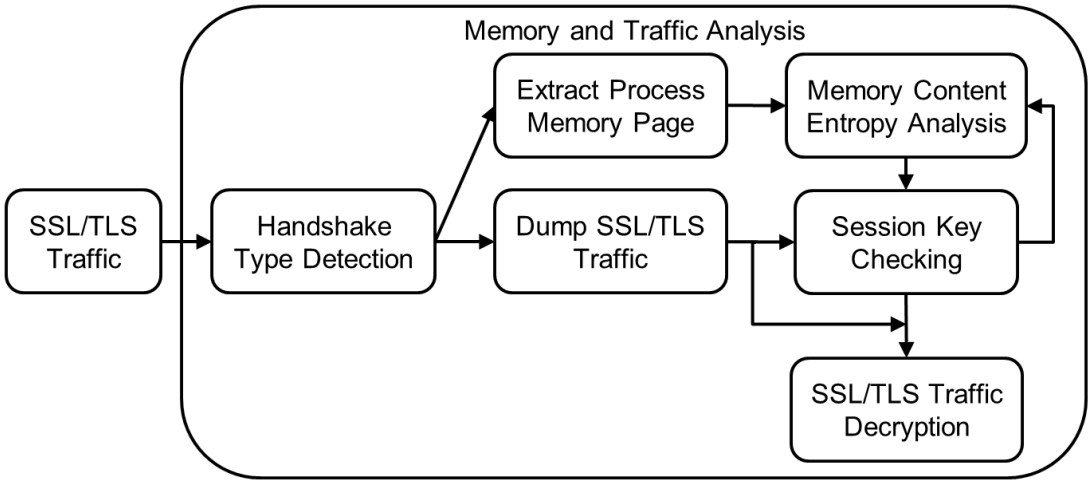
通道加密協定的研究與解析將以SSL/TLS協定作為研究目標，此研究項目將剖析Client端與Server之通訊流程，判斷通道加密金鑰的產生時機，並於適當的時機進行流量的擷取，以作後續金鑰正確性之判斷。另外，針對程序記憶體於作業系統中的配置與剖析方面，將深入程序記憶體結構，取出程序記憶體區塊，搭配金鑰亂度等技術以解出通道加密金鑰。

三、 計畫範圍

本計畫預期工作項目包括:

A) 提供 Windows 程序之分析程式(包含記憶體擷取、封包監控與分析等)。
其中，分析程式規格至少需滿足下列低標:

i. 至少能擷取指定程序之記憶體內容與通訊流量。
ii. 至少能在常見之 Windows 版本中運行，如 Windows 7、Windows 8 或 Windows 10 等。
iii. 針對自製之 SSL/TLS Client 程序，能夠 100%將其通訊流量解密成功。
iv. 針對正常使用 SSL/TLS 之程序，分析至少 5 支程序，以評估此解析程式之效能。



圖、加密通道解析流程

B) 規劃並應用上述程式於分析至少 3 支使用加密通道之惡意程式。
C) 將上述程式實作為模組或封裝成 API 供其它程式或系統介接。
D) 評估與分析此技術於勒索軟體之可行性。
E) 設計、實作並交付工作項目 A)、B)、C)及 D)所需的程式、文件及系統。

四、 預期成果

本計畫預期成果包括以下項目:

A) 協助主計畫人員探求惡意程式與後端 C&C 伺服器之通訊內容，提供主計畫技術研發之參考。
B) 建立情資挖崛技術，尋求後續技術研發與創新研究之可能性。
C) 建立系統化效能評估方式，提供本主計畫產出解析程式於真實環境下之效能測試，並建立團隊後續相關技術的評估標準流程。

※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

本計畫運用業界的研發能量，搭配本團隊收容之惡意程式樣本資料，配合主計畫「動態記憶體金鑰萃取技術於惡意軟體通訊之分析與偵測計畫」進行惡意程式加密通道之解析與研究，並完成如「計畫範圍」所定義實驗與分析。

預計將結合業界在實務面以及產品效能調校經驗，回饋給主計畫提升技術層面，並創造其它研發方向，合作方式採雙方相互討論進行。本合作研究計畫亦需提供相關系統之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. 剖析 Client 端與 Server 端之通訊流程與程序記憶體結構，判斷通道加密金鑰之產生時機，並適時進行流量與記憶體內容之擷取。
2. 實作加密通道解析程式，於真實 Windows 環境下運行並解析加密通訊。
3. 搜集具加密連線之惡意程式樣本，透過解析程式解開其通訊行為。
4. 完成成效評估實驗及對應結案報告，驗證本主計畫產出系統的有效性、效率成果品質，以及相關配合施作系統教育訓練分享。

六、 計畫期程及預估計畫總經費

計畫執行區間： 106 年 5 月 1 日 至 106 年 12 月 15 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 106 年 9 月 01 日與 106 年 12 月 01 日完成期中與期末報告。
2. 期中報告的內容包含：加密流量與程序記憶體擷取實作規劃報告。
3. 期末報告的內容包含：應用加密通道解析程式於分析惡意程式之成效報告。
4. 提供教育訓練：針對計畫成果移交、相關系統運作機制及操作說明等提供教育訓練。
5. 進度討論會議：每月至少一次召開進度研討會議。

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。包含 1. 資訊安全相關知識; 2. 程序記憶體與加密流量擷取經驗：Python、C/C++等語言的相關開發套件，開發出之程式須能在常見之Windows版本中運行 3. 相關計畫參與經驗 及 4. 其他：如熟悉密碼學相關知識等。

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