經濟部 109 年度
《5G+系統暨應用淬煉計畫》
合作研究計畫

《5G 網路偽造 SIB 攻擊設計與偵測》

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年 3 月 24 日

一、簡介

為了研究未來 5G NR 上面可能的攻擊，本計畫將利用了 4G/5G 協定上著名的弱點：SIB 偽造攻擊，在手機與基地台進行相互認證之前的所有交換的信令都是明文。我們特別著重在由基地台廣播的系統資訊區塊（system information block; SIB）訊息必且檢查透過惡意基地台廣播的偽造的 SIB 訊息是否會對受害者手機有負面的影響。

本計劃著重在 SIB 的相關資訊，取得 SIB 訊息為 UE 在選定基地台時的必要流程，得到實體層資料的基本資訊後會解碼基站建立之廣播通道以取得 MIB 與 SIB。而 MIB 因傳輸的次數非常頻繁，所以在無線電資源有限的情況下，MIB 只會帶有最重要且接收其他訊息前的必要資訊。而 SIB 所包含的資訊類型比 MIB 廣泛，如 PLMN 相關的資訊，用戶端裝置駐留在某一個基地台之前所需要的資訊、駐留期間需要的資訊等等。SIB 透過下行分享通道（即 PDSCH）動態傳輸，用戶端裝置必須利用系統資訊-無線電網路暫時身分（SI-RNTI）來取得這些系統資訊，SIB1 也具有固定的排程時間，每 80 毫秒會發送一道新的 SIB1 訊息，其餘的 SIB 會被包含在系統資訊訊息中且動態的被排程在一時間區段中（SI-window），詳細的排程資訊如各 SI 訊息的週期以及上述的 SI-window 長度會在 SIB1 中被定義。

本計畫也希望能夠探討 4G 的開源軟體實作的經驗如何延續至未來 5G 的開源軟體上，如此一來，開發相關的攻擊才能夠實際應用在未來的 5G 環境中。此外，也著重在防禦面，透過觀察這些 SIB 攻擊的封包，期待能夠設計出在 4G 中偽造 SIB 攻擊的偵測機制，使這樣的機制可以應用到 5G 中。

二、計畫目標

本計畫將委託大學專科院校執行相關作業，希望借重學術研發能量來產生具完整性、前瞻性及專業性之成果，包含測試環境建置、攻擊工具研發、程式代碼開發、偵測樣態解析等，本計畫需完成開發四種類型的攻擊，包含偽造「警急警示訊息」、「黑名單」、「傳輸電力資訊」與「GPS 訊息」，並且產生攻擊的封包、工具、執行代碼及樣態。

議題一：執行 LTE SIB 資訊偽造攻擊，產生攻擊流量封包、工具、執行代碼及樣態，以作為威脅偵測分析之效益

LTE SIB 與 5G SIB 的有部分重複，因此 LTE 上的 SIB 偽造攻擊可以沿用至 5G，如下所示：

偽造緊急警訊

偽造黑名單

偽造電力協調資訊

偽造 GPS 資訊

議題二：研究偵測此偽造 SIB 攻擊的機制

透過研究這些攻擊的樣式，我們可以搜集相關的攻擊 payload 與 pattern，嘗試偵測出這樣的攻擊模式。針對某些攻擊完就消失的我們可能比較難處理，但是如果某些 SIB 攻擊需要持續廣播的，那我們可以透過開發一個 srsLTE 的 UE 端來偵測這類的攻擊。

三、計畫範圍

本計畫範圍需建構 LTE 實驗環境平台，並於平台中產生 SIB 封包，主要研究範圍如下:

1. 產生 SIB 封包，包含「偽造緊急警訊」、「偽造黑名單」、「偽造電力協調資訊」及「偽造 GPS 資訊」 類型。
2. 探討 4G 網路上的開源軟體與 5G 上的差異與相關機制如何轉移，完成 1 篇報告
3. 研究偽造緊急警訊攻擊之研究與實證與 SIB 攻擊之實作與偵測，完成 2 篇國外會議論文投稿。

四、預期成果

1. 建置包含受害者 UE 與惡意基地台的實驗平台環境與監控模組

2. 研究 4G 開源軟體進展到 5G 所需實作之改變

3. 實現偽造緊急警訊達到恐慌攻擊與詐騙（利用 LTE SIB 10-12）。產生流量封包、工具、執行代 碼及樣態(snort rule 格式)。

4. 實現偽造黑名單來達到阻斷式攻擊（利用 LTE SIB 4），產生流量封包、工具、執行代 碼及樣態(snort rule 格式)。

5. 實現偽造電力協調資訊來達到消耗電力攻擊（利用 LTE SIB 6），產生流量封包、工具、執行代 碼及樣態(snort rule 格式)。

6. 實現偽造 GPS 資訊來達到時間同步失敗攻擊（利用 LTE SIB 16），產生流量封包、工具、執行代 碼及樣態(snort rule 格式)。

7. 設計偵測偽造 SIB 攻擊的機制，產生流量封包、工具、執行代 碼及樣態(snort rule 格式)。

8. 完成 2 篇國內外會議論文投稿。

※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 LTE 環境及資安研究之理論與實作經驗，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，相關執行方式如下:

(1) 完成相關文獻蒐集等先前技術整理

(2) 完成功能設計及系統架構規劃

(3) 實現產生 SIB 之流量封包、開發程式、執行工具、執行代碼(payload)及樣態(snort rule)

(4) 完成結案報告，評量與驗證測試效果，及產生實驗數據

(5) 計畫執行期間，每 2-3 週至少召開 1 次進度追蹤與討論會議。

預計時程與驗收查核點:

時程 / 工作項目	109 年							
	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月
1. 建置多 UE 連接的 LTE 實驗與監控平台（109/5/31 完成驗收）	—	—						
2. 研究 4G 開源軟體進展到 5G 所需實作之改變。	—	—						
3. 利用 LTE SIB 10-12 實現偽造緊急警訊達到恐慌攻擊與詐騙，產生流量封包、執行軟體、執行代碼及樣態（109/6/30 完成驗收）		—	—					
4. 利用 LTE SIB4 實現偽造黑名單來達到阻斷式攻擊，產生流量封包、執行軟體、執行代碼及樣態（109/7/31 完成驗收）			—	—				
5. 期中報告 (109/7/31 完成驗收)				—				
6. 利用 LTE SIB 6 實現偽造電力協調資訊來達到消耗電力攻擊，產生流量封包、執行軟體、執行代碼及樣態（109/9/30 完成驗收）					—	—		
7. 利用 LTE SIB 16 實現偽造 GPS 資訊來達到時間同步失敗攻擊，產生流量封包、執行軟體、執行代碼及樣態（109/10/31 驗收）						—	—	
8. 設計偵測偽造 SIB 攻擊的機制（109/11/30 完成驗收）						—	—	—
9.國內外會議論文投稿（題目暫定：偽造緊急警訊攻擊之研究與實證，109/6/30 完成驗收）		—	—					
10. 國內外會議論文投稿（題目暫定：偽造 SIB 攻擊之實作與偵測，109/11/30 完成驗收）							—	—
11. 期末報告 (109/11/30 完成驗收)								—

六、計畫期程及預估計畫總經費

計畫執行區間: 109 年 04 月 01 日 至 109 年 12 月 10 日

總經費: 700,000 元

七、 驗收標準

完成並產出下列 8 項成果，具體成果之驗收條件如下：

1. 建置多 UE 連接的 LTE 實驗與監控平台。
2. 研究 4G 開源軟體進展到 5G 所需實作之改變，並將成果併入期中報告。
3. 利用 LTE SIB 10-12，實現偽造緊急警訊達到恐慌攻擊與詐騙，產生流量封包、執行軟體、執行代碼及樣態，並以光碟交付相關產出。
4. 利用 LTE SIB 4，實現偽造黑名單來達到阻斷式攻擊，產生流量封包、執行軟體、執行代碼及樣態，並以光碟交付相關產出。
5. 利用 LTE SIB 6，實現偽造電力協調資訊來達到消耗電力攻擊，產生流量封包、執行軟體、執行代碼及樣態，並以光碟交付相關產出。
6. 利用 LTE SIB 16，實現偽造 GPS 資訊來達到時間同步失敗攻擊，產生流量封包、執行軟體、執行代碼及樣態，並以光碟交付相關產出。
7. 設計偵測偽造 SIB 攻擊的機制，並將成果併入期末報告。
8. 完成 2 篇國內外會議論文投稿。
9. 期末報告書一份

八、 技術能力需求(請詳述所需要之技術能力或專長)

本案需要技術研發能力與相關專案執行經驗如下，如下:

1. 具備 4G /5G 實驗環境、核心元件、執行流程之部署與設計能力。
2. 熟悉基站實驗環境、核心元件、架構相關知識。
3. 具相關研究論文發表及計畫執行參與經驗 ，且有 C/C++ 等程式開發能力。
4. 至少每 2-3 週召開進度檢視會議。

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