ISS-P-306

MCSTRP における スマートフォン安全化技術に関する研究

山田　淳司†　安田　浩††
† 東京電機大学未来科学部情報メディア学科　　†† 東京電機大学応用情報工学研究室

1. はじめに

東京電機大学では,複合領域サイバーセキュリティプロジェクト(Multi-disciplinary Cyber Security Technology Research Project :MCSTRP) (代表:安田浩教授)を発足し,MCSTRP は,キュリティ高度専門家育成のためのグローバルサイバーセキュリティマスターコース,サイバーセキュリティ研究所の 2 機関によって構成される.

そして私は,サイバーセキュリティ研究所のスマホ安全化技術の研究開発に携わった.スマートフォンにおける悪意のあるソフト,個人情報を通信するアプリの実態を知り,スマートフォン安全化を研究することへ繋がった.

本研究では,スマートフォンアプリにおける個人情報通信の中で,端末の位置情報に関する通信を研究した.

スマートフォンの地図アプリを使用した際の端末から送信される情報をパケットキャプチャし,キャプチャしたパケットから位置情報が解読できるか試みた.また,情報漏洩を起こせるかどうか実験,その対策を検討した.

2. 研究内容

iPhone にて,Google Maps アプリを起動した際の通信をパケットキャプチャした.Man In The Middle と呼ばれる「第三者介入」方式によって,スマートフォン端末から位置情報がどういった形で Google Maps のサーバへ送信されているかパケットキャプチャを行った.

3. 実験方法

使用機材においては,以下のものを使用した.

- ・Apple iPhone5 バージョン 7.0.4
- ・Panasonic CF-S9
- ・PLANEX USB GW-USWEXTREME
- ・Mobile WiMAX Aterm WM3500R

使用したソフトにおいては以下のものを使用した.

- ・iPhone 構成ユーティリティ 3.6.2 – Windows 用
- ・Burp Suite(Free Edition) 1.5

手順として,以下の通りに行った.

(1)iPhone では PC をプロキシとして設定.

(2)PC は iPhone からの SSL セッションの暗号化を一旦解除し,更に SSL クライアントとしてリクエストをターゲットサイトへ転送する.

(3)ターゲットサイトはレスポンスを PC へ返答し更に PC はターゲットサイトに成り代わり iPhone へレスポンス.

(4)PC にてキャプチャ.

(5)各 6 地点にて複数回ずつこの実験を実施.

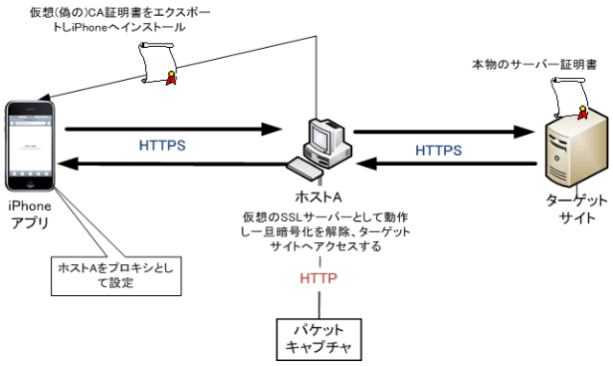

図1. 実験システム

4. 実験結果・考察

(1)　6 地点で実験を行った結果,パケット内のデータ配列において実験を行った各地点それぞれに特徴的のある 16 進数の配列があった.

□b4:c7:99:ae　□d0:c7:89:49
□c4:a:cb:5c:ca

図 2. 東京駅での配列データ

(2) (1)で述べた配列は,位置情報を特定のデータ配列で送信しているのではと推定できる.

(3) (1)で述べた配列から,端末が送信している位置情報を経緯度などの実数値には変換することは出来なかった.端末から送信される位置情報のデータはさらに暗号化されていたと考えられる.

(4) 実験により通信は暗号化はされているが,一部のデータ配列は端末の位置に依存していることが推定でき,完全ではなかったと考えられる.この通信の更なる安全化のためには,データ配列を乱数などによって変化をつけることによって,位置情報として推定できないようにすることを提案する.

5. まとめ

実験結果より iPhone のパケット内での位置情報データを推測できた.暗号化されていたが更なる安全化が必要と考えられる.

参考文献

[1] 博報堂 DY グループ・スマート・デバイス・ビジネスセンター”全国スマートフォンユーザー1000 人定期調査” (2013).