Technology Overview

Smartphones are ubiquitous items these days. The amount of code is burgeoning on the Smartphone platforms. As a result of ever shrinking time-to-market rush, a lot of software defects are being shipped to the user; many of them could have potential vulnerabilities leading to security implications. To find vulnerabilities before the attackers do, this automated system uses techniques such as fuzzing to find software vulnerabilities on the mobile phones. STAMP is a distributed platform based on the fat server and thin client model. The web application can be deployed on physical, virtual and cloud instances. Through this architecture, we are able to integrate various fuzz engines, scale on demand while making it easy to move to different client platforms. STAMP is currently used to expose software vulnerabilities in smartphones but can be extended to other targets with ease.

Technology Features

- Distributed system architecture with fat server and thin client model – scalable to cloud and multiple client platforms
- Compatible with Android, iOS, Symbian and all major browsers (with plans of extension of support to BB10 and WP8)
- Automatic management of SUTs (System Under Test)
- User-friendly secure web interface for job dispatch and results visualisation
- Extensible to 3rd party fuzzing engines, newer mobile/embedded platforms and proprietary protocols

Potential Applications

- Security testing for discovering unknown software vulnerabilities on smartphones and other programmable embedded devices
- Security testing of web-enabled embedded devices also known as the Internet-of-Things i.e., kiosks, tablets, Point-Of-Sales systems

Benefits

- Highly scalable platform that can be deployed in physical, virtual and cloud-based infrastructures
- Compatible across multiple client platforms - tested with iOS, Android, Blackberry and Symbian
- Capability to discover zero-day software vulnerabilities in proprietary and open-source software and platforms
- Extensible to include 3rd party fuzzers
- Automatic management of client devices, with visualisation of results across various platforms from one centralised secure web-based dashboard and management console