Royal Holloway
University of London

Google Android vs. Windows Phone 7.0

A Comparative Analysis of Smartphone Security with Respect to a Range of Practical Tests and Conditions

Smart Card Centre
Royal Holloway

Nigel Stanley
Supervisor: Prof. Keith Mayes

ABSTRACT

Smartphones are the most intimate form of computing we have ever had, and permeate many people's lives day in and day out.

Securing these devices is now more important than ever, as a compromised device can lead to the loss of personal and professional data.

This project compares the security posture of Google Android and Windows Phone 7.0 smartphones against each other using a set of practical experiments and then provides recommendations for users and network operators to help improve device security.

PROBLEM

Users want to know what is the most secure platform to protect themselves from smartphone security threats – Google Android or Windows Phone 7.0?

SOLUTION

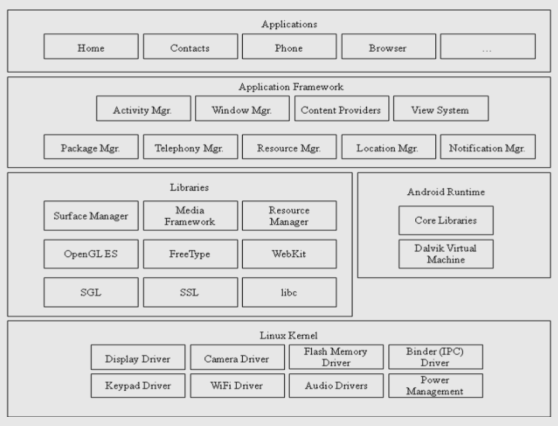
Both users and network operators can take a number of measures to secure Google Android and Windows Phone 7 devices

Project Objectives

- Compare and contrast Google Android security with Windows Phone 7.0 security in detail
- Undertake practical experiments with the generic threats identified in the ENISA (European Network and Information Security Agency) paper "*Smartphones: Information security risks, opportunities and recommendations for users*" to see how they can be realised on these platforms
- Provide a set of actionable recommendations for users and network operators

Google Android

- Android is an application execution environment for mobile devices that includes an operating system, application framework and some core applications
- The Android architecture comprises a number of layers and at the core of the Android operating system is a kernel based on Linux version 2.6.
- Android applications run in their own process space with their own instance of a Dalvik virtual machine (DVM)



Applications: Home, Contacts, Phone, Browser, ...

Application Framework: Activity Mgr., Window Mgr., Content Providers, View System, Package Mgr., Telephony Mgr., Resource Mgr., Location Mgr., Notification Mgr.

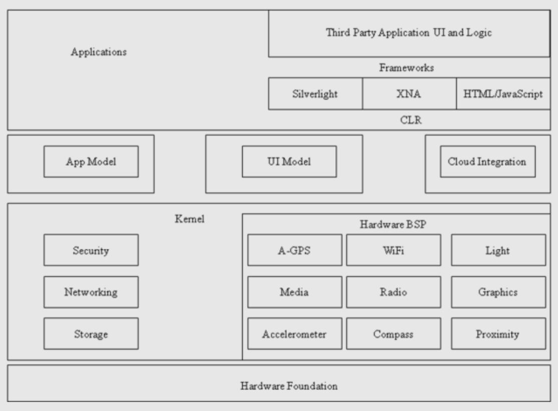
Libraries: Surface Manager, Media Framework, Resource Manager, OpenGL ES, FreeType, WebKit, SGL, SSL, libc

Android Runtime: Core Libraries, Dalvik Virtual Machine

Linux Kernel: Display Driver, Camera Driver, Flash Memory Driver, Binder (IPC) Driver, Keypad Driver, WiFi Driver, Audio Drivers, Power Management

Windows Phone 7.0

- Windows Phone 7.0 is a layered architecture that can run across multiple different devices
- Windows Phone OS 7.0 uses a security model similar to the Android platform, in that least privileges and isolation techniques are used to sandbox processes



Applications: Third Party Application UI and Logic

Frameworks: Silverlight, XNA, HTML/JavaScript

CLR

App Model, UI Model, Cloud Integration

Kernel: Security, Networking, Storage

Hardware BSP: A-GPS, WiFi, Light, Media, Radio, Graphics, Accelerometer, Compass, Proximity

Hardware Foundation

Generic Risks

- Data loss/leakage
- Poor disposal
- Unintentional data disclosure
- Phishing
- Spyware
- Network spoofing attacks
- Surveillance
- Diallerware
- Financial malware
- Network congestion

Comparative Experiments

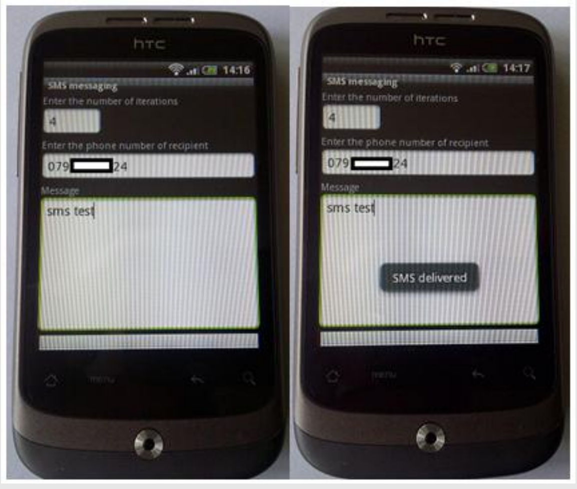
1. Data loss and data leakage – examining the possibility that physical access to a device could result in data being accessed or retrieved
2. Unintentional data disclosure – exploring the way in which each device manages downloaded applications and prevents private data such as location data being inadvertently disclosed
3. Detecting phishing emails – how does each platform provide protection to the user from phishing emails
4. Network spoofing attacks - how a device can be spoofed into connecting to a fake mobile phone network
5. SMS message attacks – how easy is it to configure each device to send automatic SMS messages, mimicking the action of some smartphone malware.

Network Spoofing Attack

- Both devices were able to pick up the presence of an AT&T network in their list of available mobile networks.
- Neither device was able to connect to OpenBTS in this instance to demonstrate the sending of a spoof SMS message.

SMS Message Attack

```
// ---sends a SMS message to another device---
          private void sendSMS(String
phoneNumber, String message) {
                    /*
                     * PendingIntent pi =
PendingIntent.getActivity(this, 0, new
                     * Intent(this,
test.class), 0); SmsManager sms =
                     *
SmsManager.getDefault();
sms.sendTextMessage(phoneNumber, null,
                     * message, pi, null);
                     */
```



SMS messaging
Enter the number of iterations
4
Enter the phone number of recipient
079[redacted]24
Message
sms test

SMS messaging
Enter the number of iterations
4
Enter the phone number of recipient
079[redacted]24
Message
sms test
SMS delivered

Conclusions

- Users should prevent others having physical access to their smartphone device
- Applications should only be obtained from official marketplaces and the offer of a cheap or free version of a paid for application should be treated with suspicion
- Network providers should investigate how email data is presented to users and maybe evaluate an email scanning application
- High security users and those that need to protect the integrity of their data and voice traffic should consider selecting to use a 3G signals only
- Network providers could consider monitoring sudden surges of calls to transient premium rate numbers indicating a possible Trojan infection
- … and finally if both devices are secured and used based on the recommendations in this report they would both achieve the same approximate level of security.

Unintentional Data Disclosure (Android)

```
•GET /b/ss/yelliphone/0/JAN-
1.0/s58415352?AQB=1&ndh=1&t=8%2F7%2F2011+11%3A21%3A4+1+0&ce=UTF-
8&pageName=%2FAndroid%2FYellSearch%2Fhome&cc=GBP&ch=Android%2FYellS
earch&c5=f182bb77e88dc2de&c13=51.XXXXX%2C-
0.2XXXXX&c14=XXXXX%2C+Epsom%2C+Surrey&c39=08082011+11%3A21&v12=andr
oid2.2.1&v13=HTC+Wildfire&v15=2.0.59.404&v16=-&s=240x320&AQE=1
HTTP/1.1
```