INTRODUCING..... A S E F
Android Security Evaluation Framework

- Parth Patel
$ whoami_
Agenda

Manual Research

Automation - A S E F

Let’s solve problems

Conclusion
Security Evaluation of Android Apps
Android APP Store

Developer

Attacker

Bouncer

Developer

Attacker
Permissions
Manual Research
“Behavioral Analysis” of Apps
Utilities for Behavioral Analysis

Android SDK
- Emulator (Android Virtual Device - AVD)
- Android Debug Bridge - adb
- Android Asset Packaging Tool - aapt

Wireshark

dex2jar

IDE - eclipse
Limitations
of
‘Manual Research’
Introducing .....
A S E F as a Black Box

- Malware
- Aggressive Adware
- Bandwidth
- Vulnerabilities
Phase 1: Passive

**Initialization Mode**

- **Configurator**
  - Default Virtual Device = Google Safe Browsing API = Host IP = interface =
  - Creates Virtual Device
- **adb refresh**
  - Session cleanup
- **Device Detect (virtual/physical)**
  - Enable USB debugging
%HAPK->{$apk} =
( { pkgnm => $PKGNM,
    launchact => $LAUNCHACT,
    vercode => $VERCODE,
    vername => $VERNAME,
    applable => $APPLABLE,
    adbstart => "",
    adbstop => ""}, );
ASEF
Phase II: Active
Launch Mode

Virtual Device Launcher

- Running
- Not Running

Boot
Boot check
Display unlock
Statistics & Results
Apps leaking private information
Total Apps = 80

6 Apps - Leaking private data

Safe Apps = 74
IMIE number

sp_k_test.apk accessed --> "time.apple.com"

inside parser module ......

Time when adb log started for the app sp_mtm.apk:

Time when adb log ended for the app sp_mtm.apk:

sp_mtm.apk accessed --> "file:///sdcard/tmp/sp_mtm.apk"

sp_mtm.apk accessed --> "http://14243444.com/send.php?a_id=0000000000000000&telno=1555215554&m_addr="

sp_mtm.apk accessed --> "http://14243444.com/send.php?a_id=0000000000000000&telno=1555215554&m_addr="

sp_mtm.apk accessed --> "http://14243444.com/play2.php"

sp_mtm.apk accessed --> "http://14243444.com/rgst5.php?gpsx=0.0&gpsy=0.0"

sp_mtm.apk accessed --> "http://14243444.com/rgst5.php?gpsx=0.0&gpsy=0.0"

sp_mtm.apk accessed --> "http://14243444.com/rgst5.php?gpsx=0.0&gpsy=0.0"

sp_mtm.apk accessed --> "http://14243444.com/rgst5.php?gpsx=0.0&gpsy=0.0"

sp_mtm.apk accessed --> "http://dfltweb1.onamae.com/"

sp_mtm.apk accessed --> "http://dfltweb1.onamae.com/"

sp_mtm.apk accessed --> "http://dfltweb1.onamae.com/"

sp_mtm.apk accessed --> "224.0.0"

sp_mtm.apk accessed --> "bas1.us01.qualys.com"

sp_mtm.apk accessed --> "dfltweb1.onamae.com"

sp_mtm.apk accessed --> "dhcp-41.vuln.qa.qualys.com"

sp_mtm.apk accessed --> "nuq04s06-in-f8.1e100.net"

sp_mtm.apk accessed --> "nuq04s07-in-f0.1e100.net"
Lovetrap.apk accessed --> " file:///sdcard/tmp/Lovetrap.apk "
Lovetrap.apk accessed --> " file:///sdcard/tmp/Lovetrap.apk "
Bandwidth Usage
Aggressive Adware
(No of Servers accessed) / App

3 min Test Cycle
(Access-rate) / App
3 min Test Cycle
Ad Requests @ 1.333 req/sec

Aggressive Adware
Permission mapping
Permission distribution - 1000 game apps
Vulnerability Scanning
Non-updated Android Apps

- No of total Apps: 75
- No of Vulnerable Apps: 0
ASEF Scan - Before updates

No of total Apps: 75
No of Vulnerable Apps: 12

- Adobe Flash Player
- Mozilla Firefox
A S E F Scan - After updates

- No of total Apps: 75
- No of Vulnerable Apps: 6
Vulnerability Summary for CVE-2012-1483

**Original release date:** 03/15/2012  
**Last revised:** 03/16/2012  
**Source:** US-CERT/NIST

**Overview**
Unspecified vulnerability in the Message Forwarder (com.gmail.zbnetium) application 1.12.20110409.1 for Android has unknown Impact and attack vectors.

**Impact**

**CVSS Severity (version 2.0):**

**CVSS v2 Base Score:** 10.0 (HIGH) *(AV:N/AC:L/Au:N/C:C/I:C/A:C)* *(legend)*

**Impact Subscore:** 10.0

**Exploitability Subscore:** 10.0

**CVSS Version 2 Metrics:**

**Access Vector:** Network exploitable
Extending the Framework
Command line tools

- start - cmd line tool
- start - adb log
- start - tcpdump

Installation mode
- start-timestamp

Launch mode

Activity mode

Uninstallation mode
- stop - adb logcat
- stop - tcpdump
- stop - cmd line tool
- stop-timestamp
Extending the Framework
Let’s solve problems....
ASEF to scan an APP STORE

Protect & Promote
ASEF in Large Organizations
Android APP

THE NIGHT PHOENIX
NIGHT PHOENIX & ASEF

Package Manager ↔ Extractor of ASEF

NIGHT PHOENIX

apkzip

ASEF Server

unzip

@ of .apk path

ANDROID
NIGHT PHOENIX ??

Alarm Manager
Who watches THE WATCHMEN
THE NIGHT PHOENIX

Internet

Write external storage
THE DARK PHOENIX
It is just the beginning ........
Next Generation of ASEF

Scalability - Load balancer module

Automated/Custom signature generation

Distinguishing updates - Security Fixes

UI reporting with correlated results and statistics

ASEF in cloud

Offline scanning - Crawler module
Conclusion ?
Thank You

Twitter : @parth_84

e-mail : pdpatel@qualys.com

http://code.google.com/p/asef/

https://community.qualys.com/blogs/securitylabs/2012/07/25/
android-security-evaluation-framework--a-s-e-f