Smart Storage Scanning for mobile apps - Attacks and exploit

OWASP

The Open Web Application Security Project

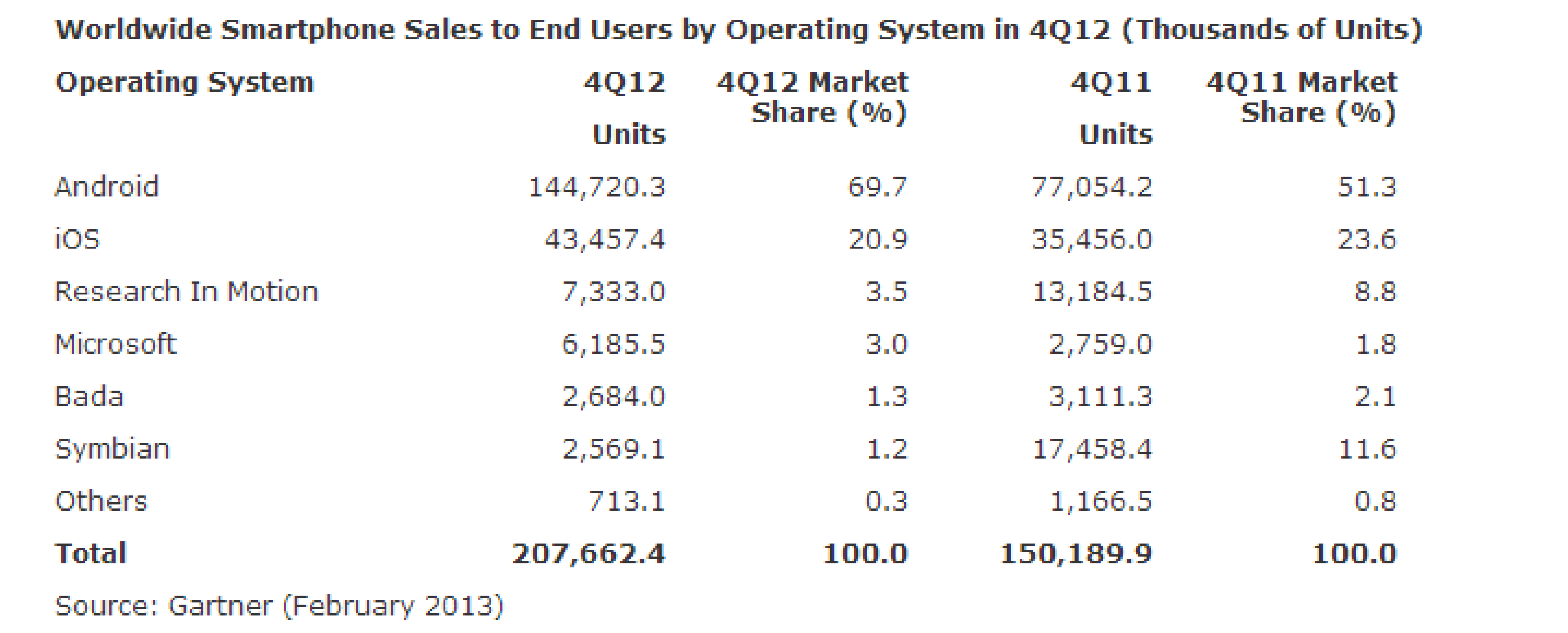
About Me

- **Hemil Shah – hemil@espheresecurity.net**
- **Twitter -** @espheresecurity
- **Past experience**
  - HBO, KPMG, IL&FS, Net Square
- **Interest**
  - Application security research (Web & Mobile)
- **Published research**
  - Articles / Papers – Packstroem, etc.
  - Tools – DumpDroid, CheckDebugable, FSDroid, iAppliScan, wsScanner, scanweb2.0, AppMap, AppCodeScan, AppPrint etc.

Mobile Apps

Gmail +talk BETA
Google
Wikipedia The Free Encyclopedia
Google Maps
digg
del.icio.us
flickr BETA
YouTube
Google Earth
netvibes
(beta) writely
WordPress
Technorati
skype
Techcrunch
last.fm
PANDORA
Google Calendar BETA
BitTorrent
amazon.com
meebo alpha
Bloglines
FeedBurner
DealsPlus BETA
SQUIDOO BETA The Power of Recommendation
blinklist beta

Gartner Statistics



Worldwide Smartphone Sales to End Users by Operating System in 4Q12 (Thousands of Units)

Operating System	4Q12 Units	4Q12 Market Share (%)	4Q11 Units	4Q11 Market Share (%)
Android	144,720.3	69.7	77,054.2	51.3
iOS	43,457.4	20.9	35,456.0	23.6
Research In Motion	7,333.0	3.5	13,184.5	8.8
Microsoft	6,185.5	3.0	2,759.0	1.8
Bada	2,684.0	1.3	3,111.3	2.1
Symbian	2,569.1	1.2	17,458.4	11.6
Others	713.1	0.3	1,166.5	0.8
Total	**207,662.4**	**100.0**	**150,189.9**	**100.0**

Source: Gartner (February 2013)

Frequency of updates

- Very High compare to Web Applications
- Usually, 4-5 updates in a year for web applications or even less at times
- Usually, 10-12 updates in mobile applications or even more in some cases
- We all have accepted that application needs to be reviewed before going to production – DID WE???

Frequency of Updates

Application Name	Number of Releases in iOS	Number of Releases in Android
Facebook	19	34
Twitter	22	25
Chase Bank	9	2
eBay	9	4
Amazon	10	3
Temple Run 2	12	10
FB Messenger	12	10
Whatsapp	4	154
skype	8	6

Mobile Attacks

- So What attacks are we talking about?
- Privacy becomes important along with the Security in mobile space
- It is MOBILE so chances of loosing device or someone getting physical access to it is MUCH MUCH higher than the other devices

Mobile Top 10 - OWASP

OWASP
The Open Web Application Security Project

- **Insecure Data Storage**
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- **Security Decisions Via Untrusted Inputs**
- Side Channel Data Leakage
- **Broken Cryptography**
- **Sensitive Information Disclosure**

OWASP
The Open Web Application Security Project

Enterprise Mobile Cases

Banking Application

- Scanning application for vulnerabilities
- Typical banking running with middleware
- Vulnerabilities – Mobile interface
  - **Poor encoding to store SSN and PII information locally**
  - **Very sensitive transaction information stored locally**
  - Profile manipulation (Logical and Hidden values)
  - Authentication submitted in GET request

E-commerce

OWASP
The Open Web Application Security Project

- Typical application making server side calls
- Server side scan with tools/products **failed**
- Security issues and hacks
  - **Storage issues with PII information**
  - SQLite hacks
  - SQL injection over XML
  - Ajax driven XSS
  - Several XSS with Blog component
  - Several information leaks through JSON fuzzing
  - CSRF on both XML and JSON

Large Telecom

- Large Telecom company
  - Source code review was done
  - Application is distributed running in browser, PDA and Mobile phones
  - Payment system was involved
  - Vulnerable
    - **Keys/session stored in keychain file**
    - **Screenshot revealing sensitive information**
    - **Default OS Behavior leaking information**
    - Presentation layer (XSS and CSRF)

Postmortem

- One pattern in all the reviews are **SOME INFORMATION WAS STORED LOCALLY**
- More than 99% of the application review has the LOCAL STORAGE issue
- Fair to say LOCAL STORAGE has been the biggest issue on the Mobile front

Local Storage

- Why application needs to store data
  - Ease of use for the user
  - Popularity
  - Competition
  - Activity with single click
  - Decrease Transaction time
  - Post/Get information to/from Social Sites

Local Storage

- How does attacker can gain access
  - Either in same Wifi
  - Default password after jail breaking (alpine)
  - ADB over wifi/3G/4G
  - Physical Theft
  - Temporary access to device

- **JailBreak/Rooting is not REQUIRED**

Local Storage

- What information we usually find
  - Authentication Credentials
  - Authorization tokens
  - Financial Statements
  - Credit card numbers
  - Owner’s Information – Physical Address, Name, Phone number
  - Social Engineering Sites profile/habbits
  - All the request/response to the server including login request

Type of Media

- XML File
- Text File
- Database File (db file)
- Images
- WebView Control or cache files
- Logs

Android – Local Storage

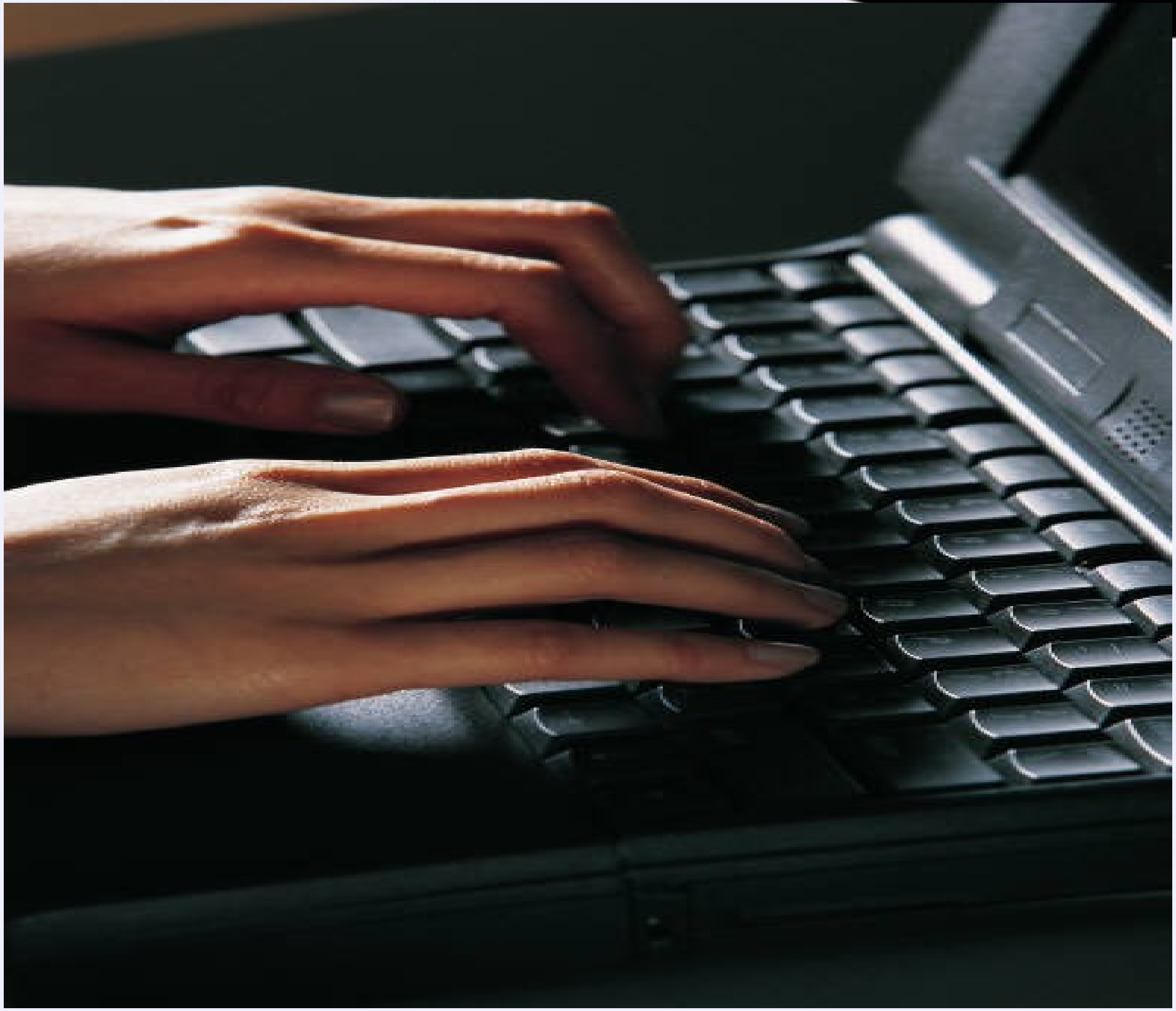
Type of Storage supported

- Android OS supports three type of storage
  - Internal Storage – As part of the application directory, typically under /data/data/PACKAGENAME directory
  - External Storage – Storage in any external storage i.e. SDCard
  - Storage in Shared preferences – Storage under shared_prefs directory, Information CAN be accessed by other applications if ALLOWED

How to test

- Very hard to test – REALLY???
- Very time consuming as one needs to go through each file under all directory of the application
- At times, one need to review files more than once to actually find out what has been stored before login, after login and after logoff

Demo - How to test



Manual Review

- Looking for information in local storage manually is really –
  - Time Consuming
  - Tedious
  - Prone to be false negatives (how accurately you can check files more than once in an hour and file formats are different)

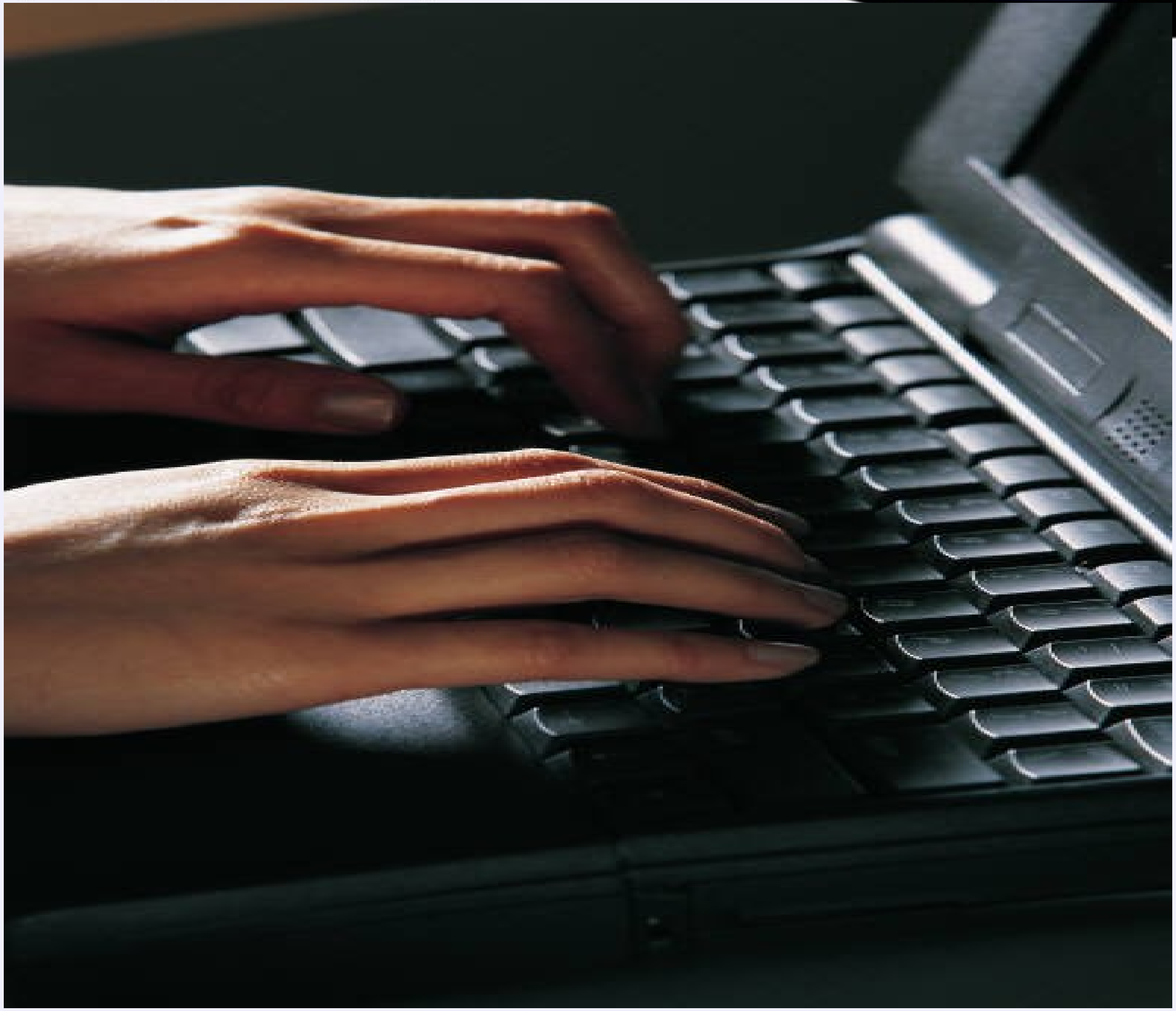
Automation

- Can we automate it?
- Is it possible to know what files/directories my application have accessed when I open it or performed any particular functionality???
- Can I monitor file system as I can do it on windows box or one can monitor network traffic???

FSDroid

- Leverages SDK Class – No hacks in here!!!
- FSDroid can –
  - Monitor file system
  - Can write filter to monitor particular directory
  - Can save last 5 reports for future use
  - Does not need mobile device – can run on Emulator smoothly
  - Easy to run (As easy as giving directory name and pressing start button)

FSDroid - Demo

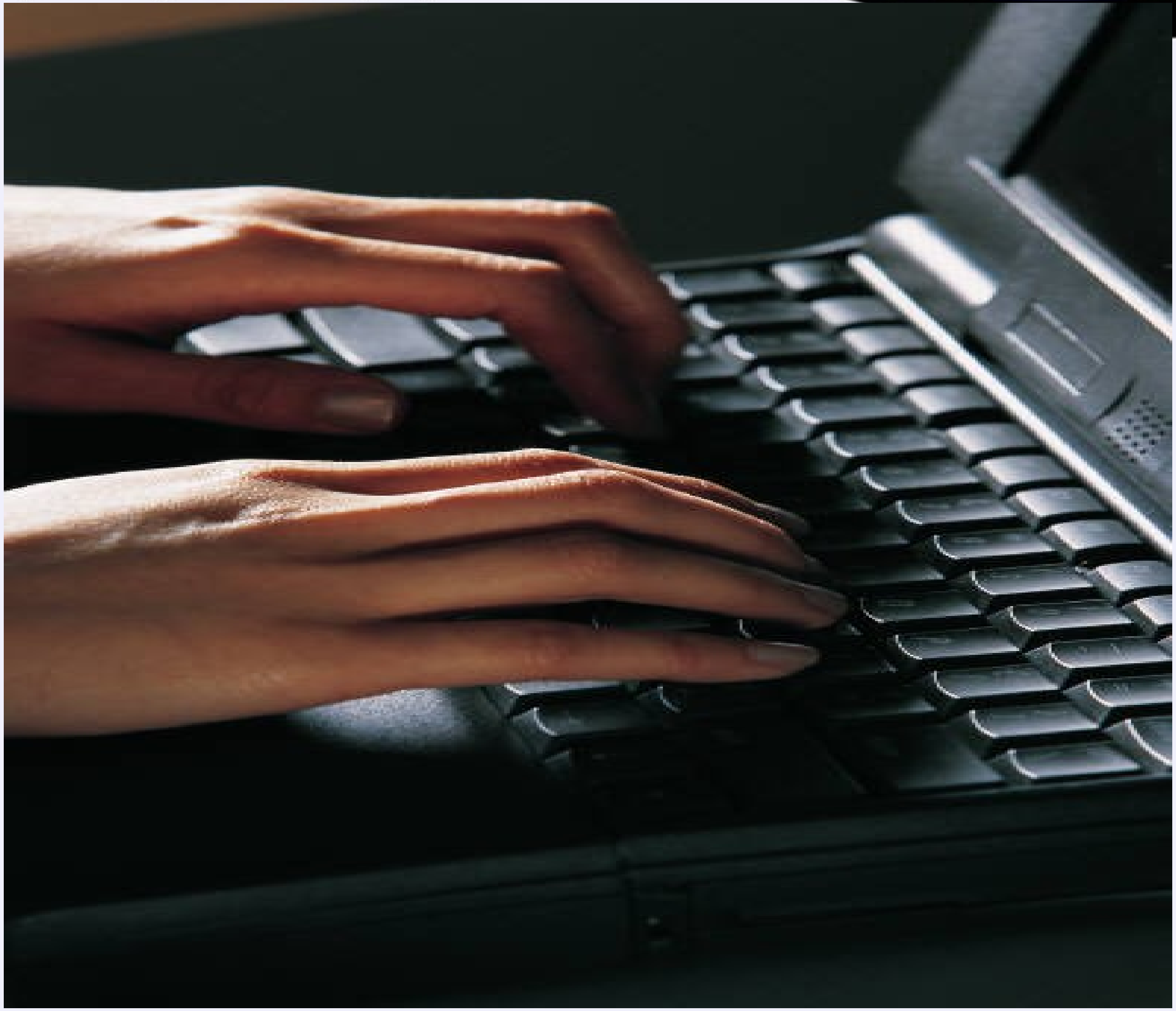


FSDroid v0.2

- What New version bring on the table???
  - Recursive Monitoring
    - Previous version does not monitor if new directory is created at runtime by the application
  - Assign permission from FSDroid
    - Permissions to monitored had to be given manually in previous version

Demo

The Open Web Application Security Project



Android – Interesting Locations

System Information

Detail	Location
Applications	/data/data/(package name)
Etc	/system/etc/
Provisioning Profile	/system/etc/security/cacerts.bks
Wifi Settings	/system/etc/wifi
GPS configuration file	/system/etc/gps.conf /system/etc/gpsconfig.xml
Host file (DNS entries)	/system/etc/hosts
Device information, Firmware Information, Manufacturer information	/system/build.prop
Framework files	/system/framework
Bin directory	/system/bin
Apk files of installed applications	/system/app
Tmp	/private/var/tmp

Application Information

Detail	Location
Address Book	**/ data/data/com.android.providers.contacts/databases/contacts2.db**
User Dictionary	/ data/data/com.android.providers.userdictionary/databases/user_dict.db
Google Map History Information	/ data/data/com.google.android.apps.maps/databases/search_history.db
Calendar	/ data/data/com.android.providers.calendar/databases
Photos	/sdcard/dcim/Camera

Default Services Information

Detail	Location
SMS (Odd number is for Outgoing calls, Even number is for Incoming calls)	/data/data/com.android.providers.telephony/databases/mmssms.db
System provided applications, ringtons and wallpapers	/system/media

User Installed Application

OWASP
The Open Web Application Security Project

Detail	Location
Application permissions, Certificate, Package Name	/data/system.packages.xml
Installed Applications	/data/data/
Application Directory	/data/data/(package name)
Applications documents i.e. images, PDF, text files	/data/data/(package name)/files
Application Preferences	/data/data/(package name)/shared_prefs
Application temporary storage	/data/data/(package name)/files

Browser information

Detail	Location
Browser Cookie	/data/data/com.android.browser/webview.db
Browser favorites (Book marks)	/data/data/com.android.browser/browser.db
Browser History	/data/data/com.android.browser/history.db
Browser Settings	/data/data/com.android.browser/shared_prefs
Browser Cache	/data/data/com.android.browser/app_databases

iOS – Local Storage

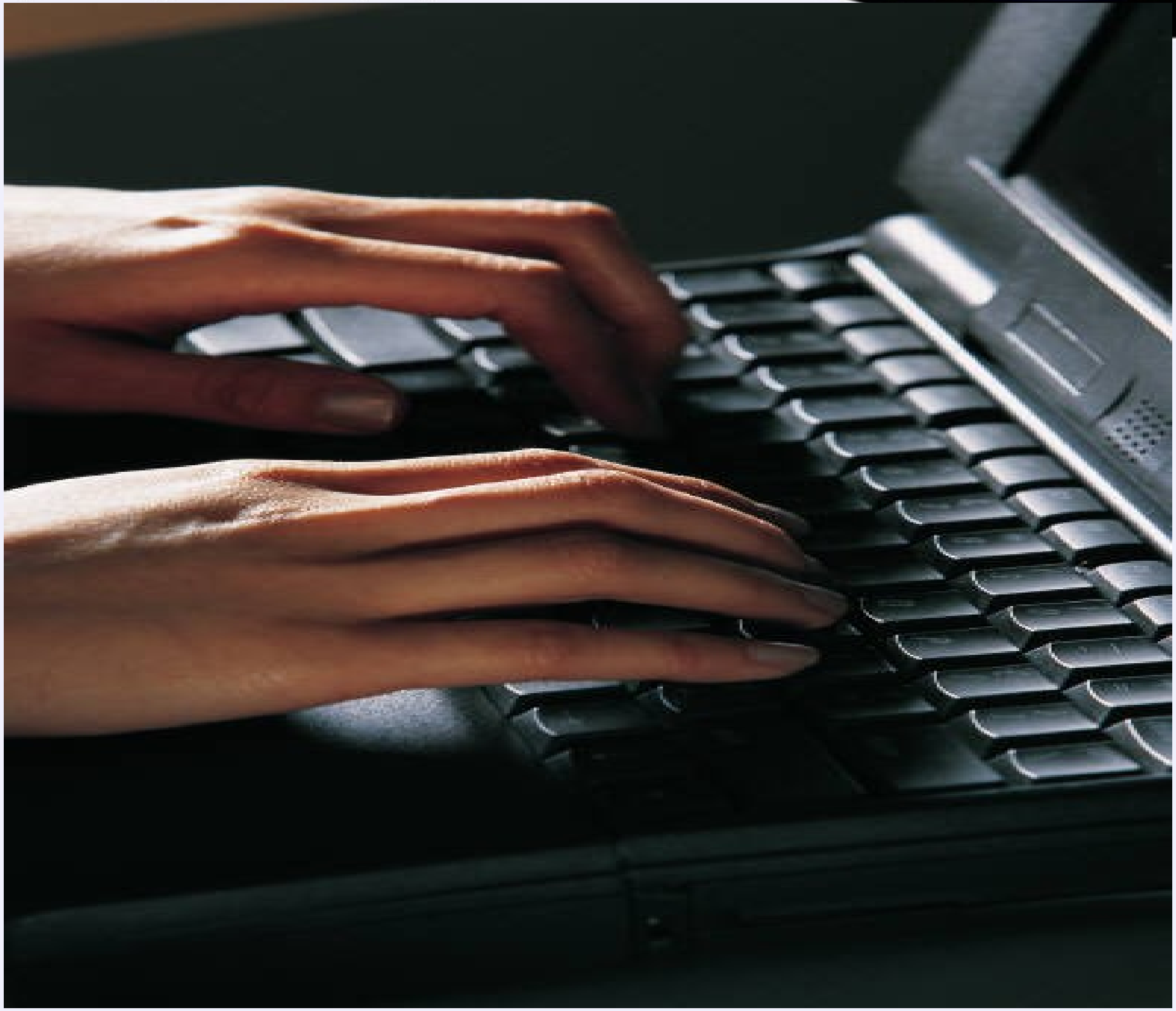
Type of Storage supported

- iOS supports two types of storage
  - Internal Storage – As part of the application directory, typically under / “/private/var/mobile/Applications/<GUID>" directory – Information can be in PLIST file, binary cookie file or cached
  - Keychain file – an encrypted file shared between all the applications but have permission model like /etc/shadow

How to test

- Nothing new than android
- Go through each file and directory multiple times.
- Can this be easy???

Demo – Manual Testing



Automation with iAppliScan

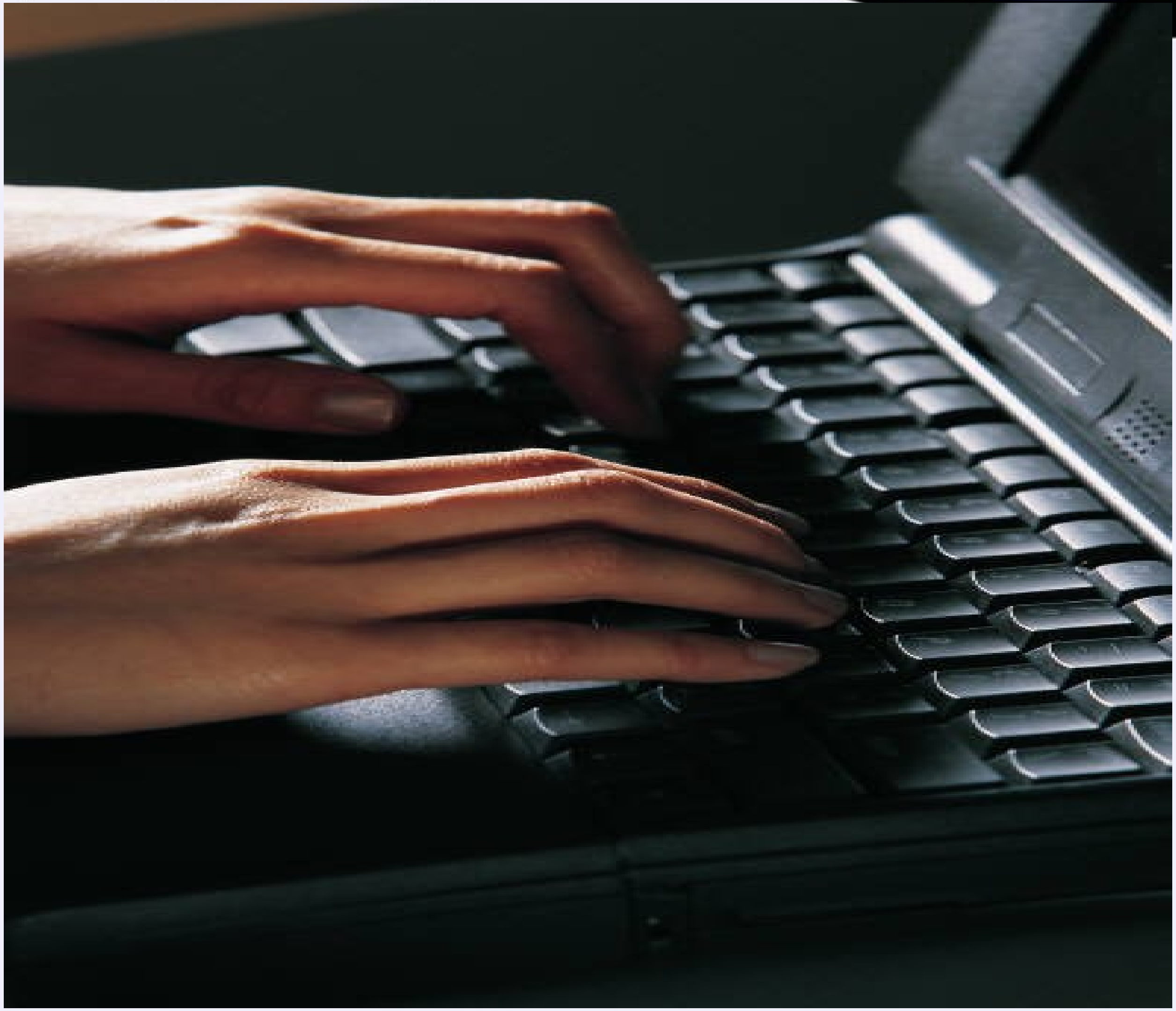
- Can we automate it? - YES
- Using iAppliScan
- Current version requires JailBroken Device and SSH access to it

- Existing Features
  - Look for Sensitive information
  - File or type of file exist is application directory
  - Download file for further analysis
  - Run external binary

Demo

OWASP

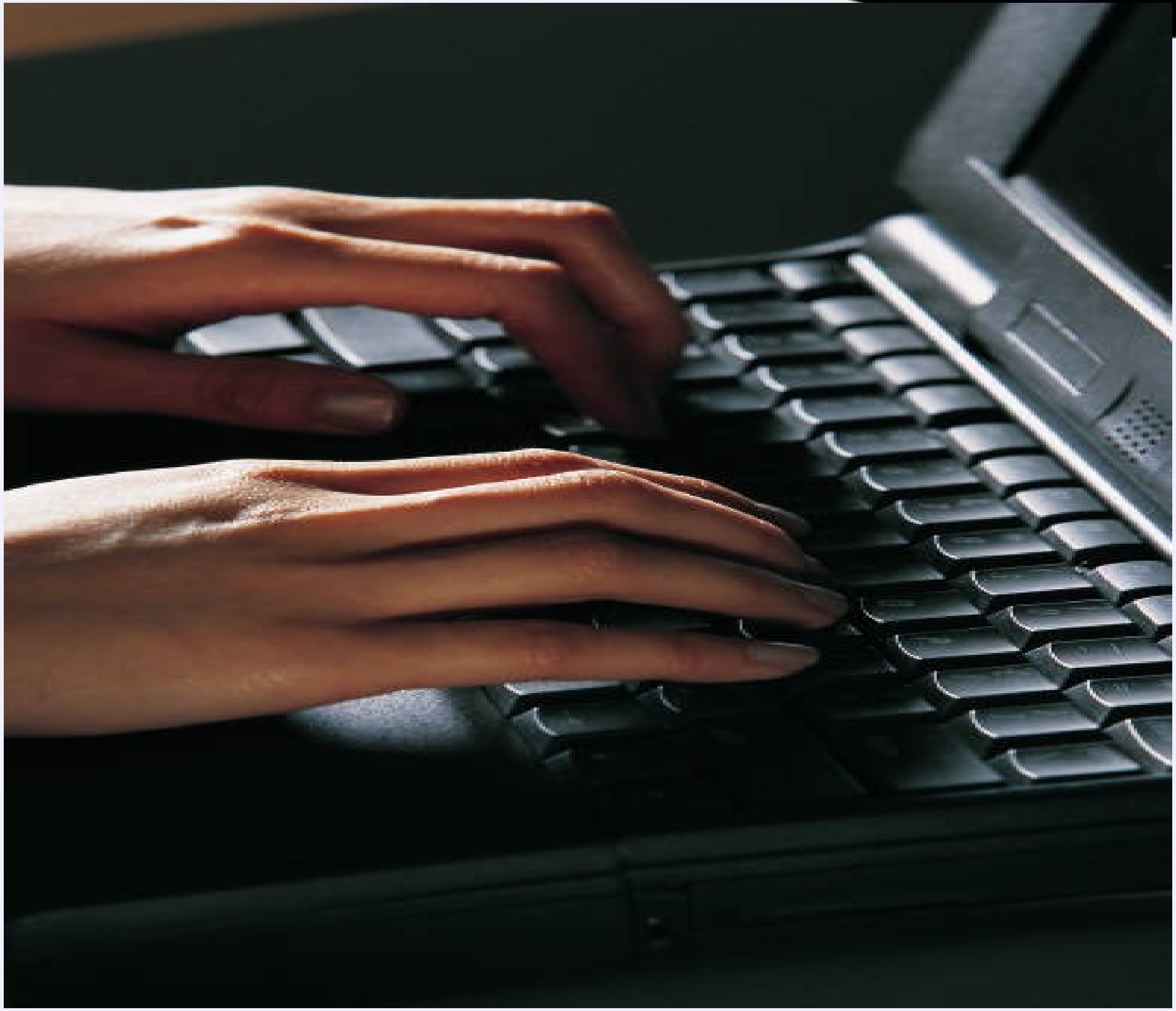
The Open Web Application Security Project



iAppliScan v0.2

- What New version bring on the table???
  - Poor cryptography detection
    - Encoding - Base64, Hex, URL, HTML, Gzip
    - Hashing - MD5, SHA256, SHA384, SHA512
  - Load/Save configuration for future use

Demo



Where To Get Tools

http://espheresecurity.com/resourcestools.html

- FSDroid
- iAppliScan
- Other Available Tools
  - DumpDroid
  - CheckDebugable
  - AppCodeScan Mobile Rules

iOS – Interesting Locations

System Information

Detail	Location
Applications	/var/stash/Applications
Etc	/private/etc
Var	/private/var
User	/var/mobile
Provisioning Profile	/var/mobileDevice/ProvisioningProfiles
Logs	/var/log, /var/logs /var/mobile/Library/Logs
Network Settings	/var/preferences/SystemConfiguration/com.apple.network.identification.plist
Wifi Settings	/var/preferences/SystemConfiguration/com.apple.wifi.plist
	/var/preferences/SystemConfiguration/preferences.plist
Apple ID, Owner information and Firmware Information	/root/Library/Lockdown/data_ark.plist

Application Information

Detail	Location
Address Book	/var/mobile/Library/AddressBook/AddressBook.sqlitedb /var/mobile/Library/AddressBook/AddressBookImages.sqlitedb
Last searched Google maps	/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb
Google Map History Information	/var/mobile/Library/Maps/History.plist /var/mobile/Library/Maps/Directions.plist
Calendar	/var/mobile/Library/Calendar/Calendar.sqlitedb
Data under notes application	/var/mobile/Library/Notes/notes.sqlite
Configuration file for Applications	/var/mobile/Library/Preferences
Photos	/var/mobile/Media/DCIM/
Application Pictures when HOME button is pressed (Each application has its own directory - Default applications)	/User/Library/Caches/Snapshots

Default Services Information

OWASP
The Open Web Application Security Project

Detail	Location
Call History (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/Callhistory/call_history.db
SMS (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/SMS/sms.db
Voicemail	/var/mobile/Library/Voicemail/voicemail.db
Voice mail recording	/var/mobile/Library/Voicemail/
System provided applications, ringtons and wallpapers	/var/stash
Call History	/var/wireless/Library/CallHistory
Call Log	/var/wireless/Library/logs
Call Preferences	/var/wireless/Library/Preferences

User Installed Application

OWASP
The Open Web Application Security Project

Detail	Location
Installed Applications	/User/Applications or /private/var/mobile/Applications
Application Directory (Binary, supporting files	/User/Applications/<app GUID>/<appname.app> or /private/var/mobile/Applications/<app GUID>/<appname.app>
Applications documents i.e. images, PDF, text files	/User/Applications/<app GUID>/Documents
Application cookies	/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies
Application Preferences (plist files)	/User/Applications/<app GUID>/Library/Preferences
Application temporary storage	/User/Applications/<app GUID>/tmp
Application crash report	/User/Library/Logs/CrashReporter
Application Screens when pressed HOME button	/User/Applications/<app GUID>/Library/Caches/Snapshots

Browser information

OWASP
The Open Web Application Security Project

Detail	Location
Browser Cookie	/var/mobile/Library/Cookies/Cookies.binarycookies
Browser favorites (Book marks)	/var/mobile/Library/Safari/Bookmarks.db
Browser History	/var/mobile/Library/Safari/History.plist
Browser Settings	/var/mobile/Library/Preferences/com.apple.mobilesafari.plist
Browser Cache	/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db

Conclusion – Questions?