Mobile device security

February 21, 2014

Overview

We'll talk about iOS and Android

But the same concepts apply to other "smart" mobile OSes

- Windows
- BlackBerry

The landscape

So-called “smart” phones, media players, and tablets are computers

Some have more horsepower than laptops from 5 years ago

Many of the threats are similar to those of any personal computer

Problem is, mobile devices don’t come with the tools required to analyze what’s happening

Security execution model

Android, iOS both use a “sandbox” concept.

Each process is run it a partitioned environment

Not allowed to interact directly with other Apps or their data

No direct access to OS resources

- iOS: strict API, SDK enforces restrictions
- Android uses a different model (Dalvik VM)

Additionally, apps must be signed and can only be deployed from a single, trusted source [1]

[1] In the case of Android, applications from “unknown sources” can be installed

Risk

The usual suspects: virus, malware, buffer overflow, password theft, keylogging, . . .

They are computers!

- Android may have a slight disadvantage [2]
- Java VM means it's unlikely the base OS will be compromised

Does it matter ?

[2] http://www.kansascity.com/2011/11/15/3267279/android-more-virus-prone-than.html

Risk (2)

Malware don't need to be viruses

Malicious intent is not something you can automate the detection of, even if there are patterns

Risk (3)

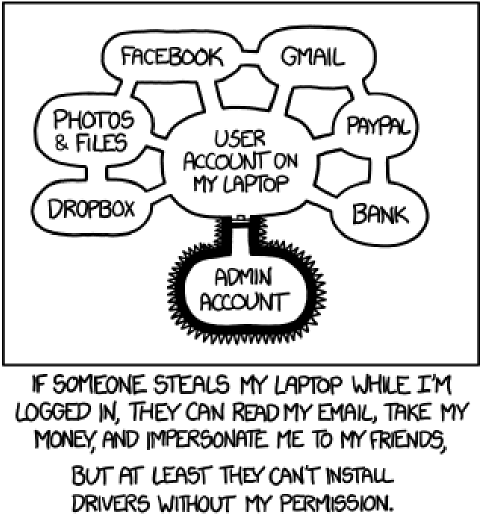

FACEBOOK
GMAIL
PHOTOS & FILES
PAYPAL
USER ACCOUNT ON MY LAPTOP
DROPBOX
BANK
ADMIN ACCOUNT
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Figure : http://xkcd.com/1200/

Threat models

Mobile devices tend to be less infested by viruses

The sandboxing makes it more difficult to exploit, but...

There are some weaknesses

- USB ports: malicious charger can compromise iPhone [3]

[3] http://www.technewsdaily.com/18241-iphone-malicious-charger.html

Jailbreaking (or rooting)

Self inflicted weakening of the restrictions

Usually used to allow installing third party software

Grounds may be commercial

- Install paying Apps not on official store
- Install malware

Often used (and required) for carrier unlocking as well

Case story

Jailbroke my phone (wanted WiFi Analyzer)

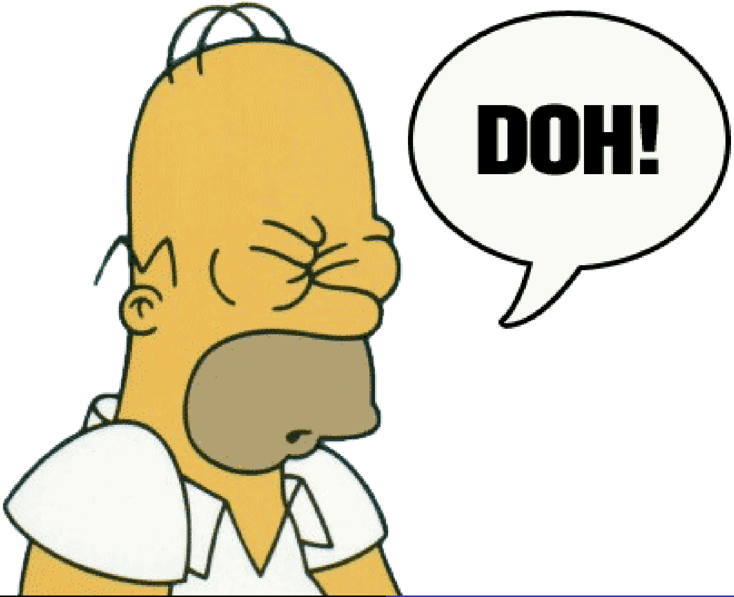
Installed OpenSSH (Because I Can!)

Forgot to change the default root password (`alpine`)

Weeks later, I realize something is port scanning

FROM my network TO the internet

Case story (2)



Case story (3)

Logging in, I found

- Python process running
- Attempting to find other jailbroken iOS devices with default user/pwd

Luckily I found some data about this [4] [5]

I was able to clean up, but. . .

- I use Lockbox to store credit card numbers and some application passwords

(I use SSH keys, so I wasn't too worried there)

How much was compromised ?

[4] http://www.redmondpie.com/how-to-secure-your-jailbroken-iphone-from-ssh-hack-9140084/

[5] http://www.researchgate.net/profile/Dimitrios_Damopoulos/publication/22580962

When the OS is compromised. . .

How do I know what was compromised ?

No tripwire or AIDE to compare

Root access on iOS:

- The device is entirely under the evil process' control
- keystroke logging is possible
- making calls ($), sending SMS
- turning on the microphone & camera (stealth recording)

. . . wipe, reinstall, restore from backup

You have backups, right ?

When the OS is compromised. . . (2)

On Android, unlocking the bootloader and “rooting” is not explicitly forbidden.

In fact, it’s the way one installs alternate operating systems [6]

Some carriers may prevent it.

[6] or community built versions of Android, like CyanogenMod

Location services

Every smart phone has a GPS or other ways of locating where you are.

This information is sometimes passed on to third parties without your knowledge. [7] [8]

Apps use this (Facebook, Maps (!), . . .)

This may be for debugging/statistical purposes

[7] http://www.foxnews.com/tech/2011/04/20/apple-iphone-users-beware-location-tracking/

[8] http://www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to/

iCloud

iCloud and other Internet based storage/backup services make sense for small devices

- Not always near computer
- Make backup of device data, media
- Contact synchronization, etc.

But how is your data stored ?

Apple has admitted it uses Amazon S3 to store your data, encrypted

- Apple can probably recover your data - how many keys are there, really ?

Additional “from the cloud” features

Remote wipe is a great feature, but think twice before enabling it [9]

Auto-wipe on a number of failed unlock attemps may be better

[9] http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

Google and Android

Android has similar feature (forgot pattern or passocde ? Email can be sent Gmail account to reset/unlock.

But don't be fooled: anyone with physical access to the device can most likely access the data.

That's how data recovery companies get data out of your damaged device.

Passcode is meant to protect from casual inspection.

How much is really encrypted ?

- Email notifications show up after a cold start, even when no password has been entered

Trusting applications

Signed vs unsigned applications

Android allows the installation of unsigned apps

- “Unknown Sources” in Security Setting

Both Google Play Market and App Store review code

Google has automated some of the process [10] [11]

[10] http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-google-bouncer/

[11] http://www.webpronews.com/google-integrates-its-app-verification-tool-directly-into-google-play-2013-07

Application trust

It won't protect against fraudulent behaviour [12]

- A computer tied to a modem, controlled by hostiles = $

[12] http://venturebeat.com/2012/09/06/toll-fraud-lookout-mobile/

Abusing Enterprise Distribution

Possible to bypass the App Store and install applications directly over the network

Web server with the right Enterprise Certificate

Lure users into downloading malicious apps [13]

[13] http://www.iphonehacks.com/2013/07/apple-revokes-gba4ios-signing-certificate.html

Application Permissions

In iOS, not much control over what an App may or may do

- The default permissions are pretty strict
- Location Services can be set per application
- User is prompted if an application wants to access contacts, photos, etc. . .

Who says no ?

Application Permissions (2)

Android apps displays which permissions the application requests, at install time.

- All or nothing proposition

Before Android 4.4

- Possible to override permissions requested by an App

Not anymore

Is the latest Facebook App just spyware ? [14]

[14] http://www.redflagnews.com/headlines/facebook-app-requires-users-agree-to-be-monitored-by-microphone-at-any-time-without-their-permission

BYOD - Bring Your Own Destruction

Mobile devices are the ideal trojan hosts

- Sniffer
- Wireless access point
- 3G router
- Wifi analyzer, scanner
- Exfiltration device (upload later)

This is why the concept of a perimeter firewall as first line of defense is long gone.

The Maginot line of the 00s.

BYOD (2)

Mobile Device Management tools

- iPhone configurator
- Various Android solutions

Wireless compromise

iMutual authentication - we discussed this!

- How do you know you're connecting to the right server ?

Other attacks

Bluetooth

- Device is not discoverable all the time
- When pairing with an accessory, make sure you pair with the right one (rogue bluetooth calls, microphone activation, etc.)

Securing your device

Use a passcode!

These are single user devices

- Android allows multi user to some extent
- Do Not Share

Use encryption

- This is automatic on iOS
- Android: you can turn it on, but if there's no HW support -> slow!

Set autoerase on

- Too many failed attempts will lock down or erase the device
- Use backups!
- Android: not a built-in function, need an app

Securing your device (2)

Pay attention where you use the device

- Be aware of your surroundings
- We use our mobile devices in many places
- Cameras ?
- Someone looking over the shoulder ?

Biometrics

- Not specific to mobile devices, but not widespread
- Beware - some are easily spoofable (Android face)
- Fingerprint - something you have... 10 of.

You can replace passwords, not fingers [15]

[15] https://www.schneier.com/blog/archives/2013/09/apples_iphone_f.html

Securing your device (3)

Level of trust

- What is it safe to store on the device ?
- Is it safer to use paper ?

Antivirus

- No clear-cut opinion that antivirus are very helpful
- Many don't have the necessary privileges to inspect the system at a low enough level
- . . . they are just apps after all [16] [17]

[16] http://www.digitaltrends.com/mobile/top-android-security-apps/

[17] http://lifehacker.com/5861757/do-android-antivirus-apps-actually-do-anything

Questions ?