SecureState®

Your Security Team

Android vs. Apple iOS Security Showdown

Tom Eston

About Your Presenter

- Tom Eston CISSP, GWAPT
- Manger of the SecureState Profiling & Penetration Team
- Specializing in Attack & Penetration, Mobile Security
- Founder of SocialMediaSecurity.com
- Facebook Privacy & Security Guide
- Security Blogger – SpyLogic.net
- Co-host of Social Media Security Podcast
- Former Founder and Co-host of the Security Justice Podcast
- National Presenter
  (Black Hat USA, DEFCON, ShmooCon, SANS, OWASP)

Agenda

- The Latest Statistics on Android vs. Apple iOS
- Android and Apple iOS Overview – Versions & Features
- What are the issues, what are the security concerns?
- The "**SHOWDOWN**"!
  - Each feature compared between Android and Apple iOS…who will win??
- Mobile Device Best Practices

Android?

Apple?

It’s a SHOWDOWN!

Image: PinoyTutorial.com

Android - Latest Statistics

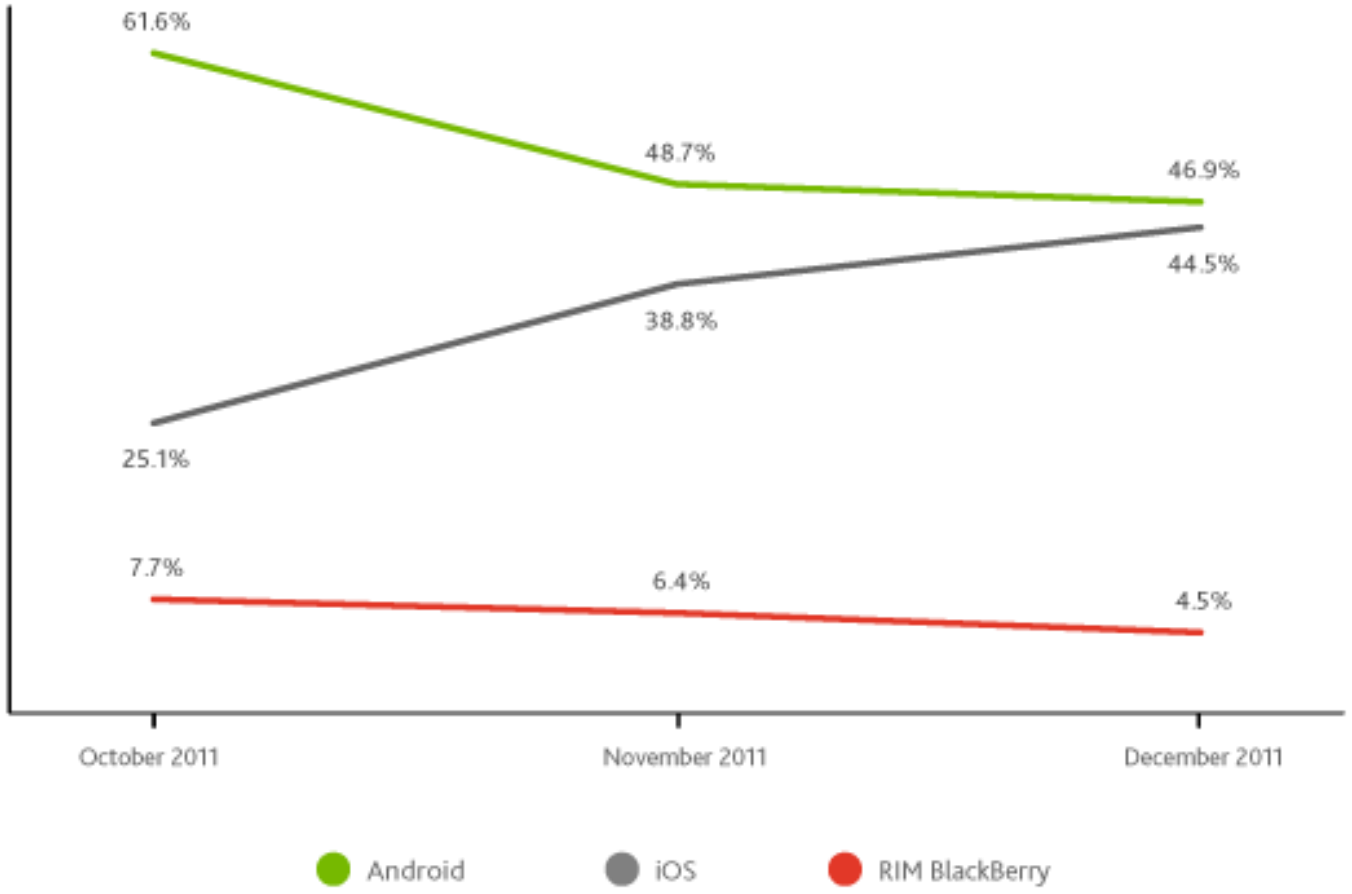
- 300 Million Devices Sold
  (as of February 2012)
- 450,000 apps in the Android Market

Apple iOS - Latest Statistics

- 316 Million iOS Devices Sold (as of February 2012)
- Mostly due to Verizon/Sprint now selling Apple devices
- 500,000 apps in the Apple App Store

Smartphone Operating System Share – Recent Smartphone Acquirers

Oct - Dec 2011, Nielsen Mobile Insights

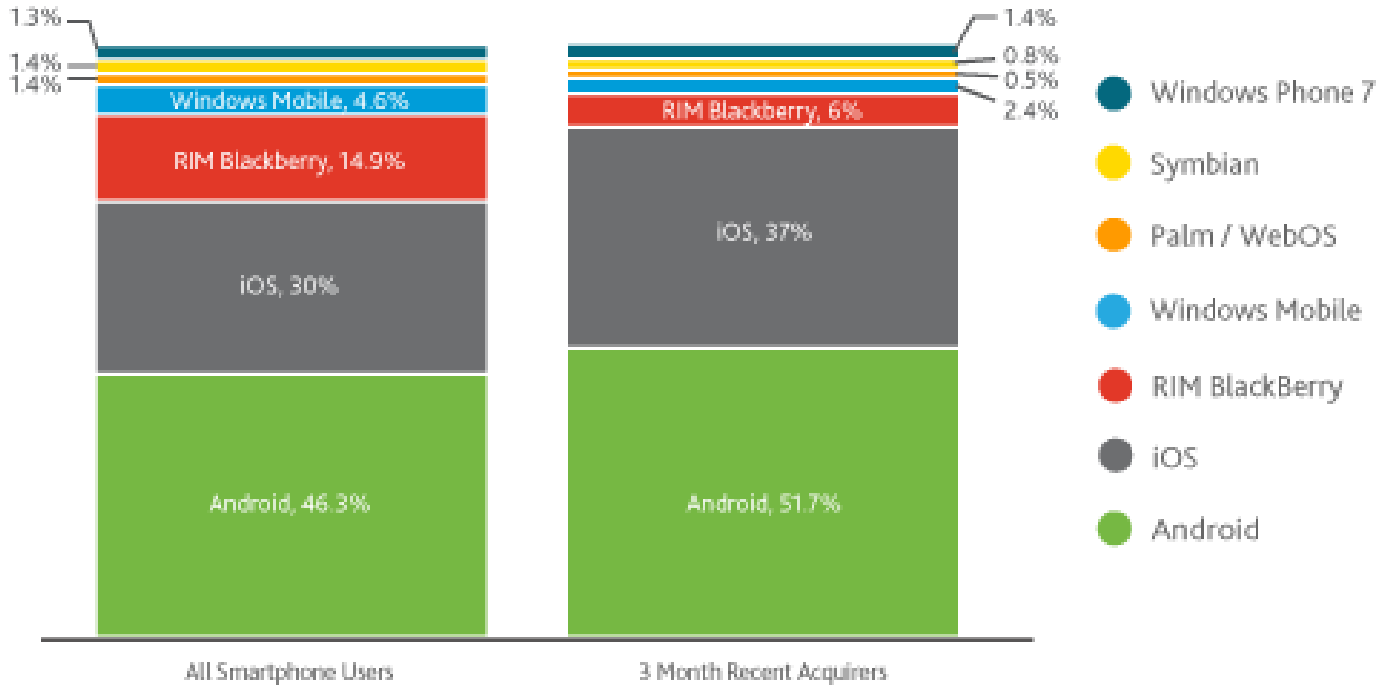


Source: Nielsen

nielsen

Operating System Share – All Smartphone Consumers vs. Recent Smartphone Acquirers (3Mo).

Q4 2011, Nielsen Mobile Insights



Source: Nielsen

nielsen

What Do We See?

- Apple iOS is the most talked about, more widely deployed
  - iPad's are hot!
- Android a close second
- BlackBerry third
- Windows Mobile fourth
- webOS or Symbian OS?

Android: Current Versions

- Ice Cream Sandwich 4.0.4
  - Tablet and Phone
- Honeycomb 3.2.6
  - Tablet only (Motorola Xoom)

- Updates are periodic. No set schedule by Google.
- Updates depend on the hardware manufacturer and the cell carrier
- Samsung Galaxy Nexus gets updates immediately from Google (this is the 'Google Phone')

Apple iOS: Current Versions

- Not to be confused with Cisco "IOS"
- Apple changed the name to "iOS" in June 2010
- Updated at least once a quarter, mostly minor revisions
- Current version(s):
  - AT&T (GSM) = 5.1
  - Verizon (CDMA) = 5.1
- iOS 5 fully supports iPhone 4, iPhone 3GS, iPod Touch 3/4 gen, iPad 1-3

Mobile Security Concerns

- App Store and Mobile Malware
- App Sandboxing
- Remote Wipe and Policy Enforcement
- Device and App Encryption
- Cloud Storage
- OS Updates
- Jailbreaking and Rooting
- New(er) Technology

App Stores and Mobile Malware

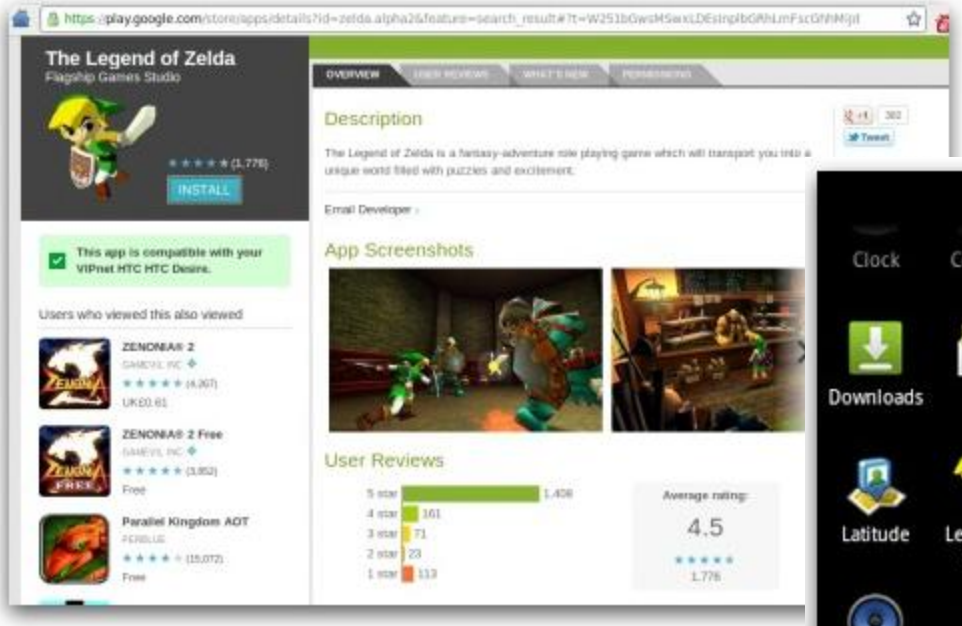
- Android Marketplace (now Google Play)
  - Very little application vetting, previous issues with Malware in the Marketplace (working on improving this)
  - Hot target for malware and malicious apps
  - Easy to get users to install popular “fake” apps *outside* Google Play

Recent Mobile Malware Statistics

- Juniper Networks' 2011 Mobile Malware Threats Report
  - **13,302** samples of malware found targeting Android from June to December 2011
  - **"0"** samples of malware found targeting Apple iOS

Source: http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

Legend of Zelda on Android?

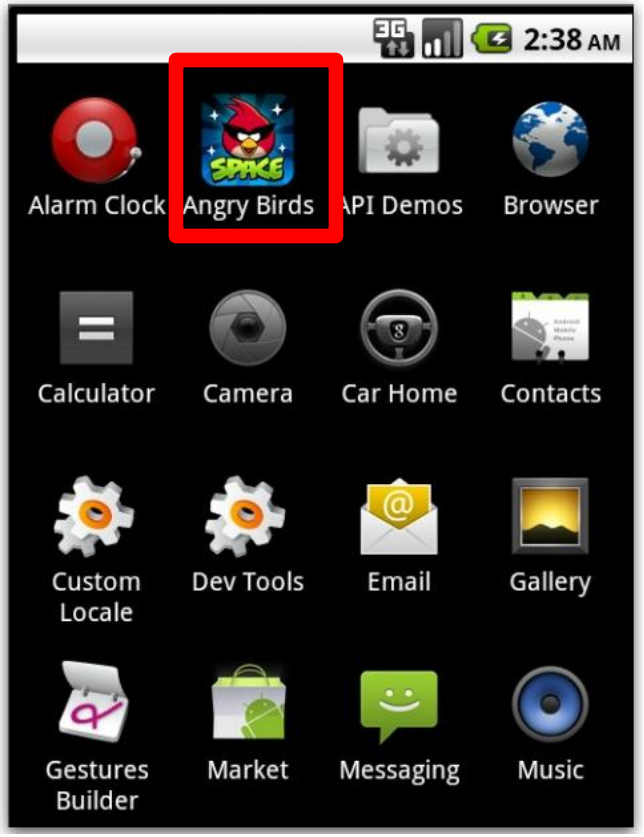


This would be awesome if true! ☺

http://nakedsecurity.sophos.com/2012/04/26/dirty-tricks-android-apps/

Angry Birds from Unofficial App Stores

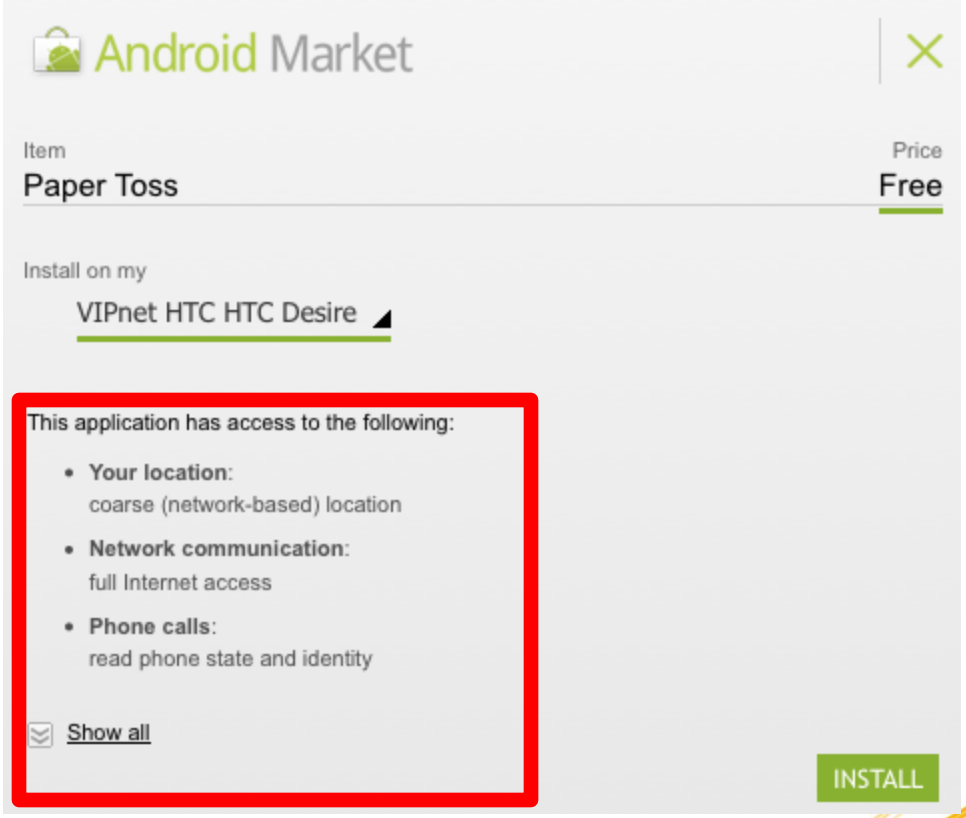
- Disguised as a Trojan horse
- Uses the “GingerBreak” exploit to root the device
- Your device becomes part of a botnet



http://nakedsecurity.sophos.com/2012/04/12/android-malware-angry-birds-space-game/

Easy to Ignore Android App Permissions

- Reminder: Some apps can do things you didn't know about
  - Example: Launching the web browser



Example: Fake Instagram App

App Stores and Mobile Malware

- Apple App Store
  - Developers must pay $99
  - Submit identifying documents (SSN or articles of incorporation for a company)
- Google Play
  - Developers must pay $25
  - Agree to a “Developers Distribution Agreement”
  - Easy to upload lots of apps and resign if apps get rejected or banned

App Stores and Mobile Malware

- Apple App Store
  - Vetting process for each app in the store
  - Must pass Apple's "checks" (static analysis of binaries)
  - Code for each app is digitally signed by Apple, not the developer
- Process was exploited by Charlie Miller in November of 2011
  - Created an "approved" app which was digitally signed
  - The app later downloaded unsigned code which could modify the OS dynamically
  - Was a bug in iOS 4.3/5.0

Apple's Problem? Questionable Apps

- 90% of submissions to the Apple App Store are denied because the app doesn't do what it says it does
- Spammy apps…mainly privacy issues such as UDID usage
- Jailbroken device? More susceptible to malware from unauthorized app repositories (Cydia)
- Apps that look like legitimate apps:
  - **Temple Run** -> *Temple Guns* -> *Temple Jump*
  - **Angry Birds** -> *Angry Ninja Birds* -> *Angry Zombie Birds*
  - **Zombie Highway** -> *Zombie Air Highway*

Angry Zombie Birds is Real!

…and it's horrible!

Customer Reviews

Are you kidding me? ★
by Irelee

I would have rather burned a dollar than spent it on this crap!!! Don't waste your money!!! This game should be taken off... Ridiculous!!!!

Total rip off ★
by Candy/man

This should not be allowed out there! Now I'm angry.

FAIL!

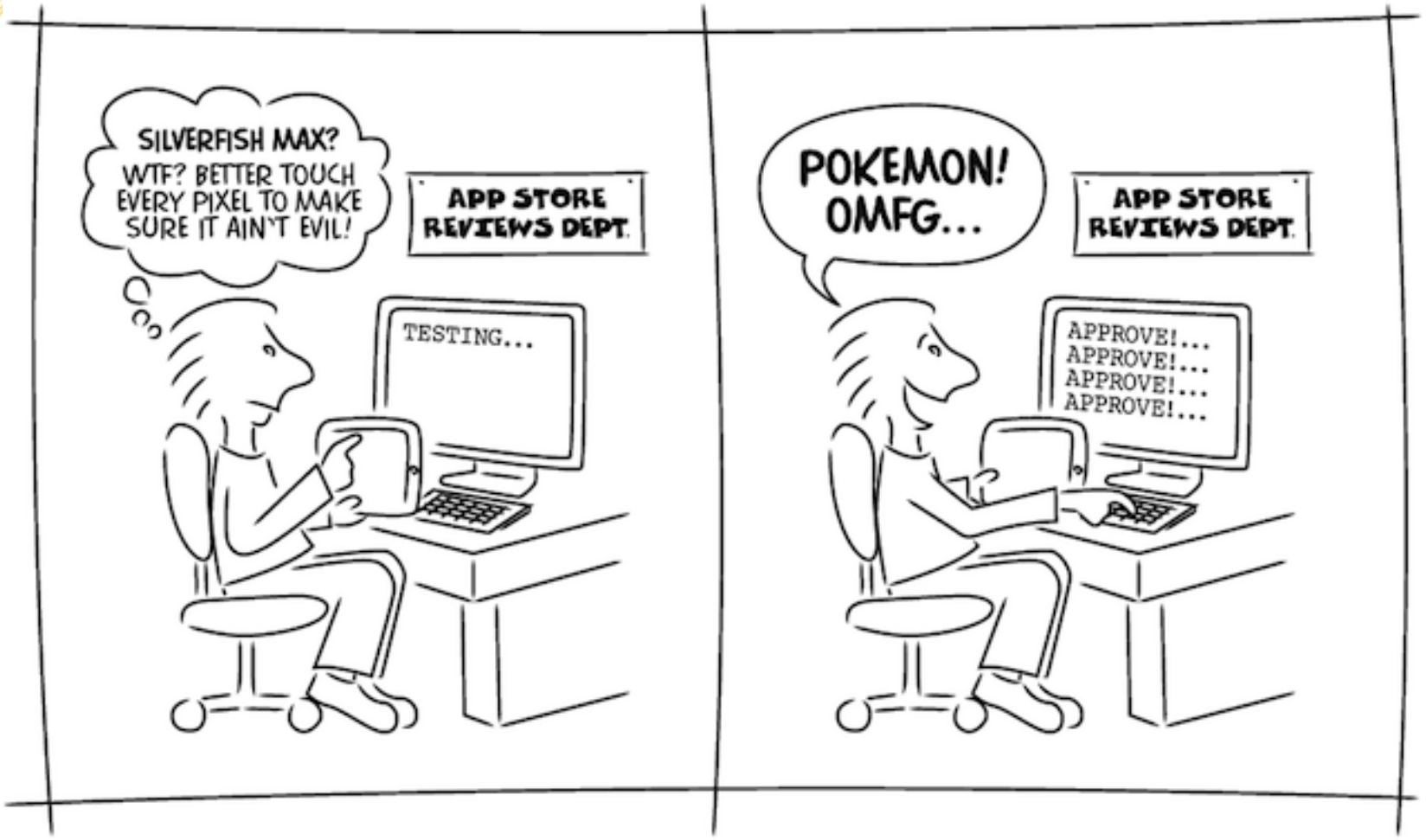


Image: http://mashable.com/2012/03/01/app-store-security-risks/

Apple: Very Little App Permissions Shown To Users

- Mainly for privacy
- Apps are limited to what they can do
- Apps can access contact data without permission (will be fixed in future release)

Winner: Apple iOS

- Apple's "walled garden" works better then Android's "open garden" (at least for now)
- However, still not immune from spammy, fake or potentially malicious apps (or really bad games)!

Android: App Sandboxing

- Privileged-Separated Operating System
  - Each app runs with a distinct system identity
    - Unique Linux user ID and group ID for each app
    - No app, by default, has permissions to perform operations that would impact other apps, the OS, or the user (Android Developer Docs)
  - The app grants permissions outside the default "sandbox"
    - Location based services can only be disabled globally, not on a per app basis
  - Apps are "signed" by the developer (not Google) and can be self-signed certificates (not a security feature)

Android: App Sandboxing

- Google "community based" enforcement
  - If the app is malicious or not working correctly the App community will correct the problem (in theory)
- Rooted device? Too bad…root can access the keystore!

- Apps can write to the SD Card (removable storage)
  - Files written to external storage are globally readable and writable

Apple iOS: App Sandboxing

- Each app is installed in its own container
- If the app is compromised via exploit, the attacker is limited to that container
- Jailbroken device? Ignore the last bullet point…

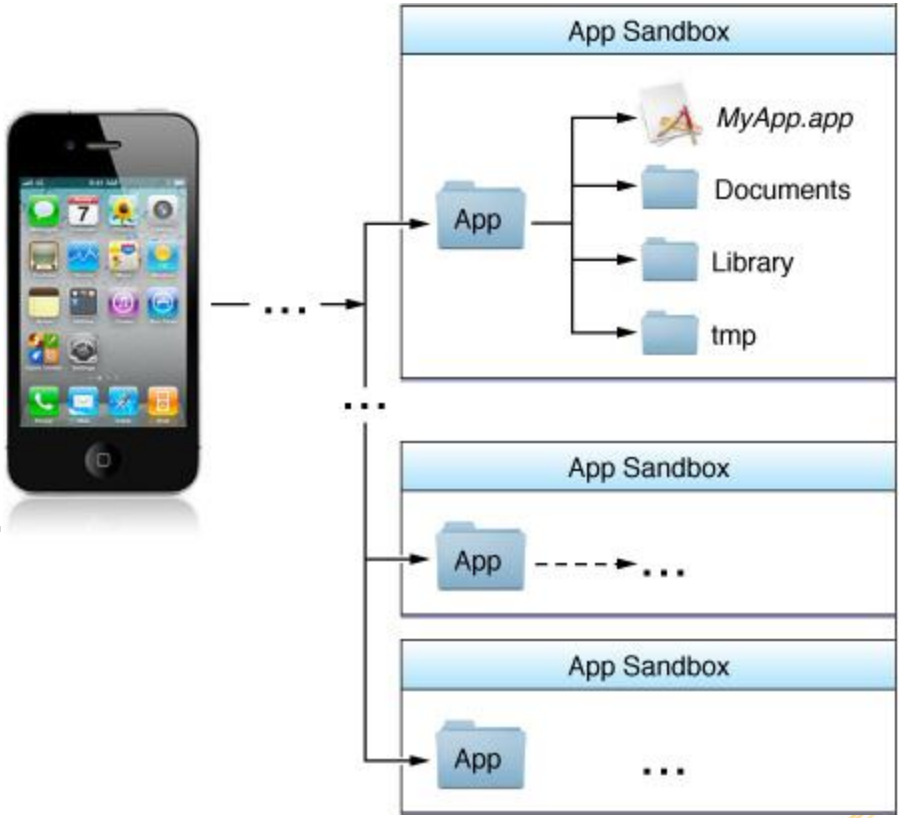


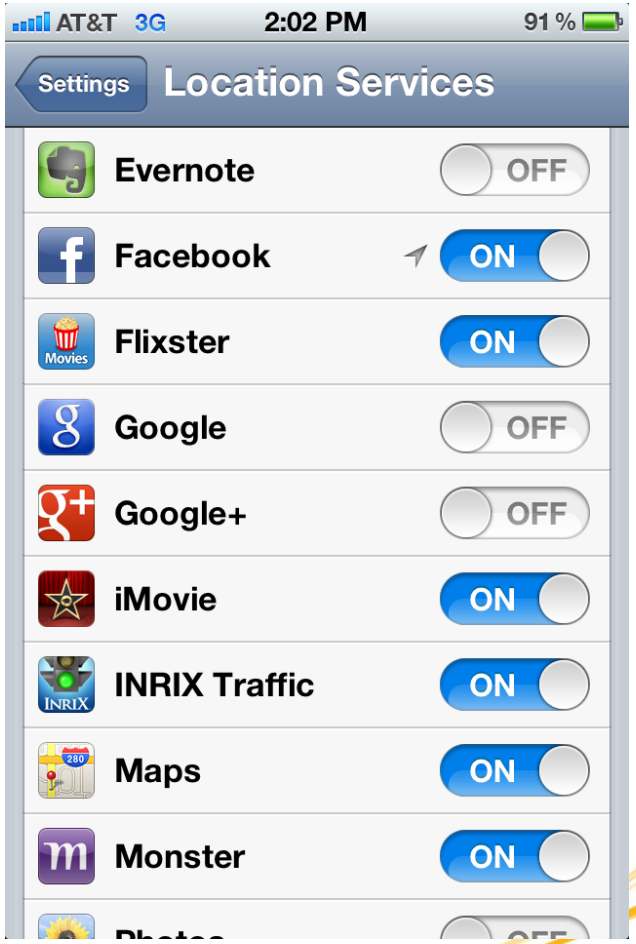
Image: iOS Developer Library (developer.apple.com)

Apple iOS: App Sandboxing

- Each app is signed by Apple (not the developer)
- Apps run as the "mobile" user
- The Keychain is provided by Apple outside the sandbox for password or sensitive data storage
- Apps can only access Keychain content for the application
  - Also a "device protection" API is used by developers
  - Note: There are tools to dump the Keychain but the device has to be Jailbroken
- Apple does not use external storage devices (SD Cards)

Winner: Apple iOS (by a nose)

- Apple signs all applications
- Limited areas to store app data
- Permissions system is simpler for users
  - Example: More granular control of location based settings
- Keychain and device protection APIs help
  (if developers use them)

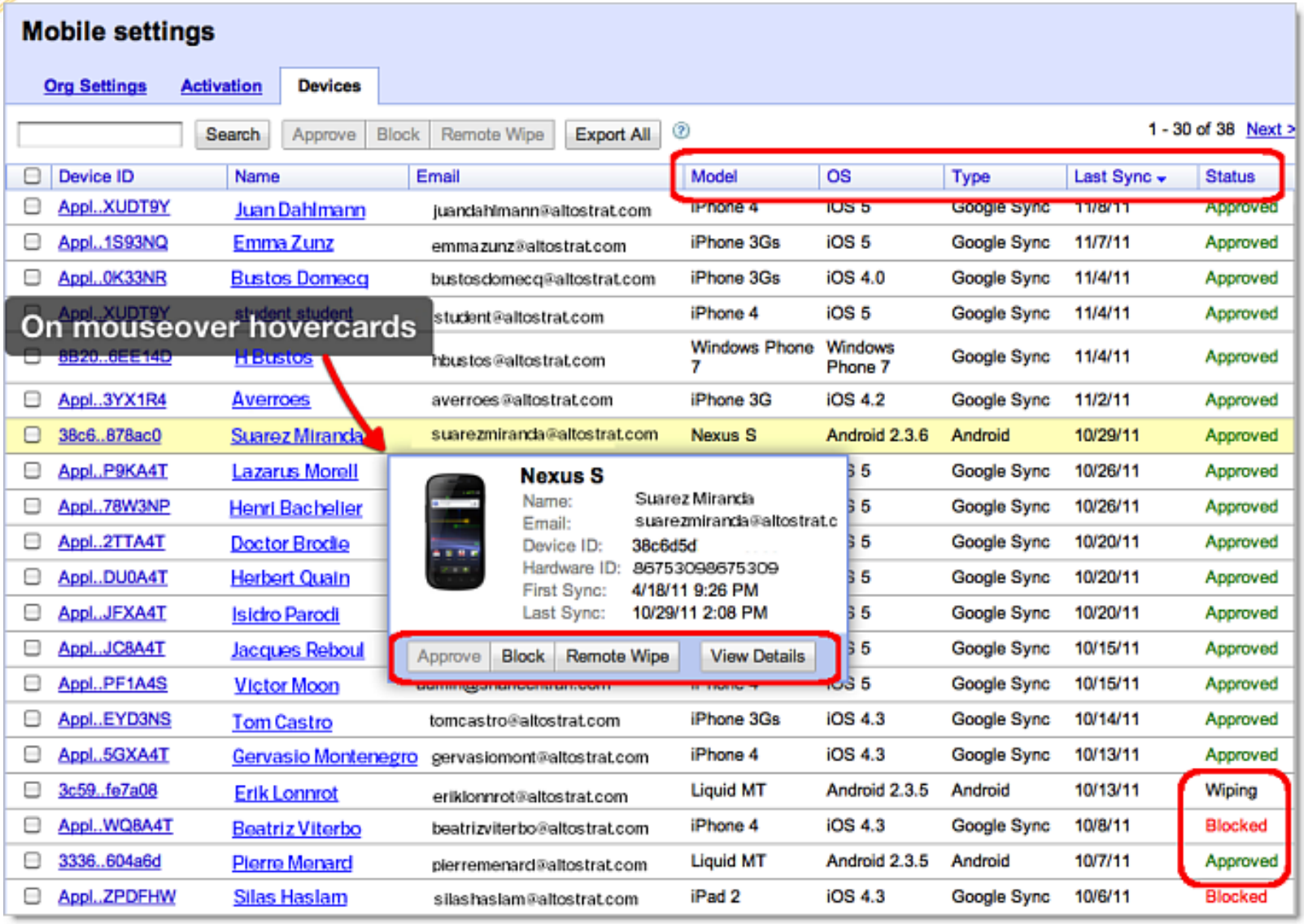


Remote Wipe and Policy Enforcement

- Android
  - Google Apps Device Policy ($$)
  - Third-Party App ($$)
  - Third-Party MDM (Mobile Device Management) ($$)
  - Microsoft Exchange ActiveSynch
- Apple iOS
  - Google Apps Device Policy ($$)
  - FindMyPhone (Free)
  - iPhone Configuration Utility (Free)
  - Third-Party MDM ($$)
  - Microsoft Exchange ActiveSynch

Android: Remote Wipe

- Google Apps Device Policy (Full MDM)
  - Need a Google Apps Business Account
  - Can manage multiple devices
    - iOS, Windows Mobile and Android


Mobile settings
Org Settings
Activation
Devices
Search
Approve
Block
Remote Wipe
Export All
1 - 30 of 38
Next >
Device ID
Name
Email
Model
OS
Type
Last Sync
Status
Appl..XUDT9Y
Juan Dahlmann
juandahlmann@altostrat.com
iPhone 4
iOS 5
Google Sync
11/8/11
Approved
Appl..1S93NQ
Emma Zunz
emmazunz@altostrat.com
iPhone 3Gs
iOS 5
Google Sync
11/7/11
Approved
Appl..0K33NR
Bustos Domecq
bustosdomecq@altostrat.com
iPhone 3Gs
iOS 4.0
Google Sync
11/4/11
Approved
Appl..XUDT9Y
student student
student@altostrat.com
iPhone 4
iOS 5
Google Sync
11/4/11
Approved
On mouseover hovercards
8B20..6EE14D
H Bustos
hbustos@altostrat.com
Windows Phone 7
Windows Phone 7
Google Sync
11/4/11
Approved
Appl..3YX1R4
Averroes
averroes@altostrat.com
iPhone 3G
iOS 4.2
Google Sync
11/2/11
Approved
38c6..878ac0
Suarez Miranda
suarezmiranda@altostrat.com
Nexus S
Android 2.3.6
Android
10/29/11
Approved
Appl..P9KA4T
Lazarus Morell
Google Sync
10/26/11
Approved
Appl..78W3NP
Henri Bachelier
Google Sync
10/26/11
Approved
Appl..2TTA4T
Doctor Brodie
Google Sync
10/20/11
Approved
Appl..DU0A4T
Herbert Quain
Google Sync
10/20/11
Approved
Appl..JFXA4T
Isidro Parodi
Google Sync
10/20/11
Approved
Appl..JC8A4T
Jacques Reboul
Google Sync
10/15/11
Approved
Appl..PF1A4S
Victor Moon
Google Sync
10/15/11
Approved
Appl..EYD3NS
Tom Castro
tomcastro@altostrat.com
iPhone 3Gs
iOS 4.3
Google Sync
10/14/11
Approved
Appl..5GXA4T
Gervasio Montenegro
gervasiomont@altostrat.com
iPhone 4
iOS 4.3
Google Sync
10/13/11
Approved
3c59..fe7a08
Erik Lonnrot
eriklonnrot@altostrat.com
Liquid MT
Android 2.3.5
Android
10/13/11
Wiping
Appl..WQ8A4T
Beatriz Viterbo
beatrizviterbo@altostrat.com
iPhone 4
iOS 4.3
Google Sync
10/8/11
Blocked
3336..604a6d
Pierre Menard
pierremenard@altostrat.com
Liquid MT
Android 2.3.5
Android
10/7/11
Approved
Appl..ZPDFHW
Silas Haslam
silashaslam@altostrat.com
iPad 2
iOS 4.3
Google Sync
10/6/11
Blocked
Nexus S
Name:
Suarez Miranda
Email:
suarezmiranda@altostrat.c
Device ID:
38c6d5d
Hardware ID:
86753098675309
First Sync:
4/18/11 9:26 PM
Last Sync:
10/29/11 2:08 PM
Approve
Block
Remote Wipe
View Details

Apple iOS: FindMyPhone

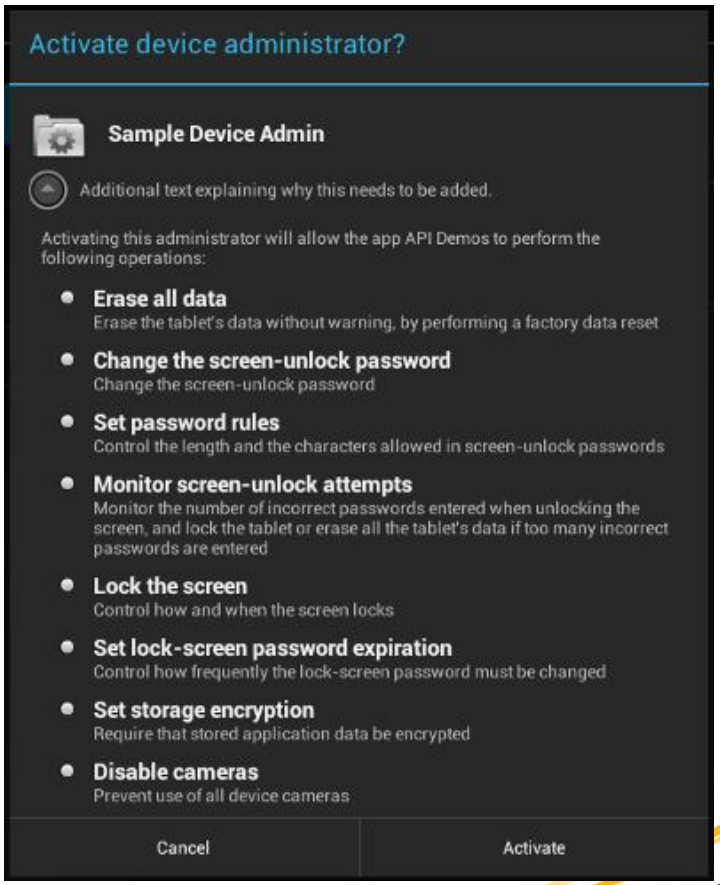
- Free and easy way to remote wipe or find a lost or stolen device
- Accessible via icloud.com

Android: Policy Enforcement

- Android Device Administration API
  - Encrypt data stored locally
  - Require password
  - Password strength
  - Minimum characters
  - Password expiration
  - Block previous passwords
  - Device auto lock
  - Device auto wipe after failed password attempts
  - Allow camera (not supported on Android, only iOS)
  - Encrypt device (whole disk)
  - Remote wipe/lock

Android Policy Enforcement

- No free utility to provision or create profiles
- Need to create an app to install specific settings
- Android provides little guidance on how to deploy this app
- Users must activate the app for policies to take effect



Apple iOS: Policy Enforcement

- Very detailed settings available:
  - Passcode
  - Wi-Fi
  - VPN
  - Proxy
  - LDAP
  - Exchange ActiveSynch
  - App/Camera and other Restrictions
  - …and more!

iPhone Configuration Utility

Winner: Apple iOS

- Free remote wipe utility (FindMyPhone)
- Much more granular enterprise controls
- Free small scale MDM (iPhone Configuration Utility)
- Easier to implement policies

Device and App Encryption

- Android
  - No device encryption on Android < 3.0
  - Device encryption API released in “Ice Cream Sandwich – 4.0”
  - Based on dm-crypt (disk encryption)
  - API available since 3.0 for app level encryption

Device and App Encryption

- Apple iOS Hardware Encryption
  - Hardware encryption was introduced with the iPhone 3GS
  - Secures all data “at rest”
  - Hardware encryption is meant to allow remote wipe by removing the encryption key for the device
  - Once the hardware key is removed, the device is useless
  - Full MDM API’s available

Device and App Encryption

- Apple iOS Device Protection
  - "Device Protection" different than "Hardware Encryption"
  - This is Apple's attempt at layered security
    - Adds another encryption layer by encrypting application data
    - Key is based off of the user's Passcode.
  - Only Mail.app currently supports this
  - Many developers are not using the APIs
  - Often confused with Hardware Encryption

Winner: Apple iOS

- Slight edge to Apple for having hardware based encryption
- Device Protection API more robust than Android
- Developer documentation +1 for Apple

Cloud Storage

- Android
  - Lots of third-party apps for storage and backup
  - Google provides backups of Gmail, calendar and Wi-Fi settings (apps) on Android
  - Google Drive will change this
- Apple iOS
  - iCloud
  - New with iOS 5
  - Takes the centralized approach (API based)
  - Backups, documents, music and photos

Winner: Android and Apple iOS

- Slight edge to Apple for allowing full native backups of data
- Many third-party solutions available
- You need a policy regardless of what device you use
- Some MDMs can provide backup solutions

OS Updates

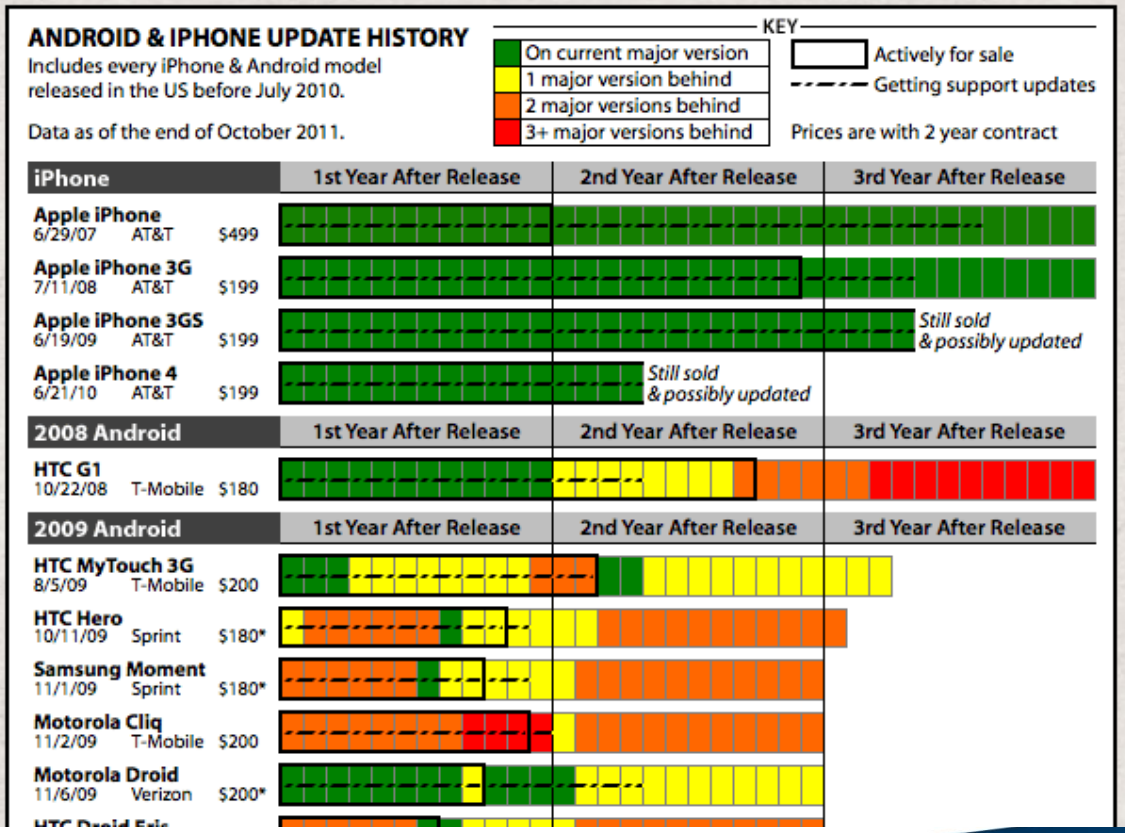
- Android
  - Slow patching, if at all!
  - OTA updates
  - A lot depends on forces outside of Google
  - Some devices will not support 4.0
  - Google releases the update or patch, device maker customizes it, then carrier customizes it as well…

October 26, 2011 2,528 notes

Android Orphans: Visualizing a Sad History of Support

The announcement that Nexus One users won't be getting upgraded to Android 4.0 Ice Cream Sandwich led some to justifiably question Google's support of their devices. I look at it a little differently: Nexus One owners are lucky. I've been researching the history of OS updates on Android phones and Nexus One users have fared much, much better than most Android buyers.

I went back and found every Android phone shipped in the United States[1] up through the middle of last year. I then tracked down every update that was released for each device - be it a major OS upgrade or a minor support patch - as well as prices and release & discontinuation dates. I compared these dates & versions to the currently shipping version of Android at the time. The resulting picture isn't pretty - well, not for Android users:



TWITTER
RSS FEED
EMAIL
ARCHIVE

POPULAR CHARTS
Android's Fragmented Update History
Google Management Isn't Using Google+
Amazon's 14 Kindles vs. Apple's 18 iPads
NY Times' Crazy Digital Pricing
US Wealth Distribution
The Collapse of the Newspaper Business
The Collapse of the Recording Industry

OS Updates

- Apple iOS
  - Frequent updates (at least once a quarter)
  - Easier for Apple because the hardware is the same, not device manufacturer or carrier dependent
  - iOS 5 brings OTA updates

Winner: Apple iOS

- Same hardware, updates from one source = easier and faster to update
- Track record of quickly addressing security issues

Jailbreaking and Rooting

"Jailbreaking essentially reduces iOS security to the level of Android..."

– Dino Dai Zovi, iOS Hacker

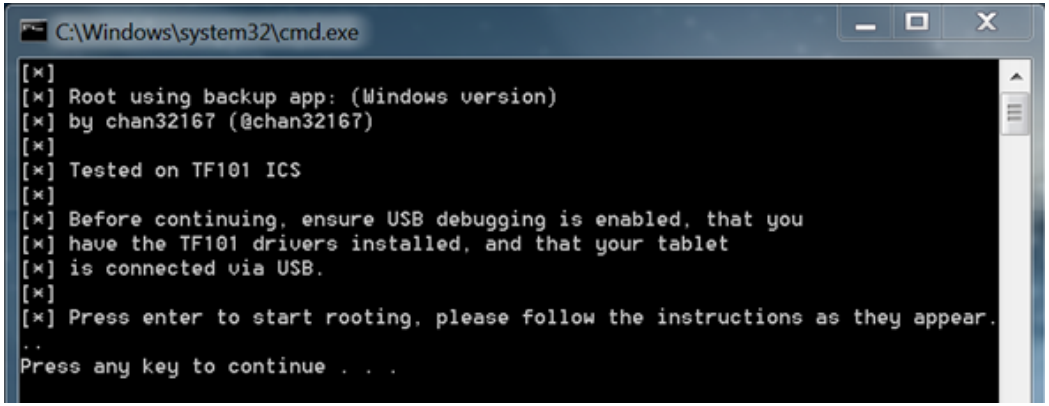
Rooting on Android

- Allows “root” access (super user) to the device
- Why do people “root”?
  - Access the flash memory chip (modify or install a custom ROM)
  - Make apps run faster
  - Remove device or carrier apps
  - Turn the phone into a WiFi hotspot to avoid carrier fees
  - Allows “Unlocking” so the device can be used with another cell provider

- Rooting is **LEGAL** in the United States
  - Digital Millennium Copyright Act (DMCA 2010)

Rooting Process on Android

Google



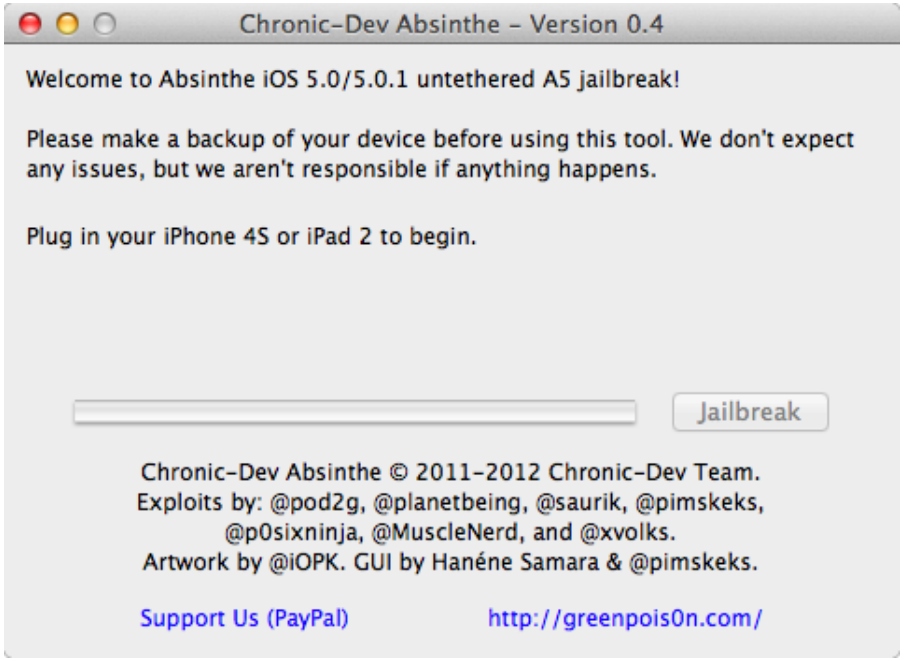
Jailbreaking on Apple iOS

- Full access to the OS and file system
- Install applications and themes not approved by Apple (via installers like Cydia)
- Tether their iOS device to bypass carrier restrictions
- They hate Apple's communist and elitist restrictions

- Jailbreaking is **LEGAL** in the United States
  - Digital Millennium Copyright Act (DMCA 2010)

Jailbreaking Tools

- Pwnage Tool*
- **Redsn0w***
- Sn0wbreeze*
- **GreenPois0n Absinthe**
- **Jailbreakme.com**
- LimeRa1n exploit used for most Jailbreaks

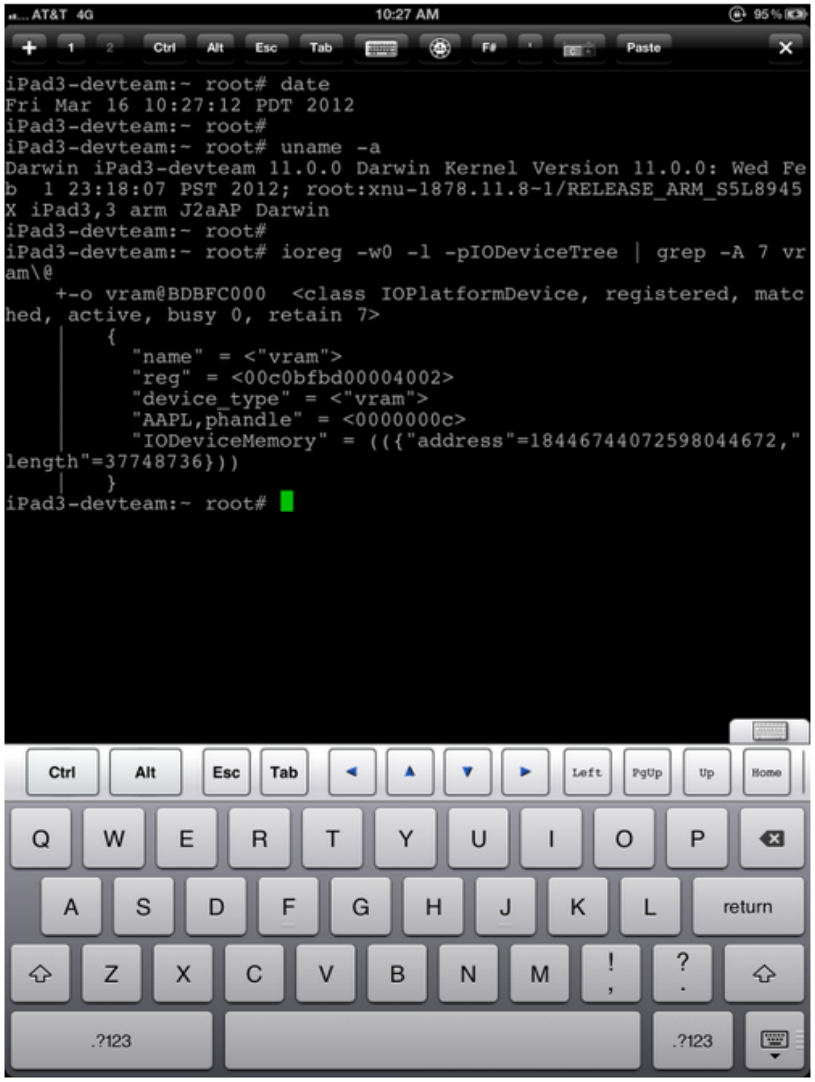


* Require the IPSW (firmware) in some form…

MuscleNerd
@MuscleNerd

Follow

jailbroken iPad3: twitpic.com/8x48rt twitpic.com/8x48xg (Just a first step, still lots of work to do! No ETA!)



TwitPic

Winner? None!

- Rooting and jailbreaking are **bad** for the security of the device!
- Malware for Android takes advantage of this…and in some cases roots the device for you
- Previous iOS "worm's" that look for SSH ports from jailbroken devices
- Removes built in sandbox restrictions

- MDM needs to prevent and/or detect rooted and jailbroken devices!
  (you should also have a policy!)

New(er) Mobile Technology

- Both devices are coming out with more innovative features which have interesting security considerations
- Android 4.0 has facial recognition to unlock the device
  - Potential issue with the “swipe pattern” feature vs. standard passcode unlock
- ASLR (Address Space Layout Randomization)
  - New in Android 4.0
  - Support since iOS 4.3
  - Developers have to take advantage of this!

New(er) Mobile Technology

- Android: NFC
  - Android Beam

Android Beam

Share contacts, web pages, YouTube videos, directions, and apps—just by touching two NFC-enabled Android phones back to back. Tap to beam what's on your phone to your friend.

Watch a video

New(er) Mobile Technology

- Android: NFC
  - Google Wallet

New(er) Mobile Technology

- Apple iPhone 4S – Siri Voice Control
- Allows commands by default on a locked device
- Send emails/text's and more…

Image: Sophos

Mobile Device Best Practices (for Android or Apple iOS)

The Passcode

- You should always have a passcode
- You should require it immediately
- It should be > 4 characters, 6 is recommended
- It should be complex
- Enable lockout/wipe feature after 10 attempts

Enable Remote Management

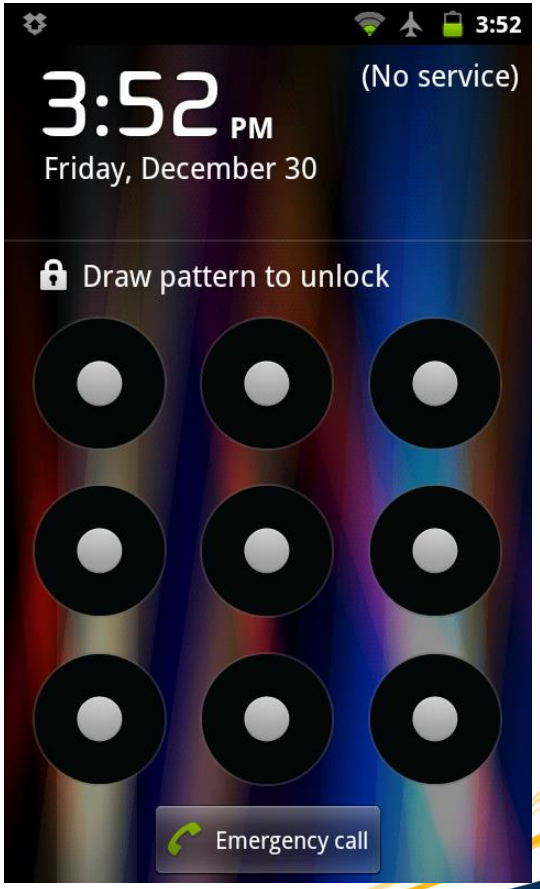
- For true Enterprise level management you must use a third-party MDM
  - Decide which type of enrollment is best for you
  - Whitelist approach may be best
    - Allow only devices you have authorized
    - BYOD: policy sign-off?

Don’t Allow Rooting or Jailbreaking

- Removes some built-in security features and sandboxing
- Can leave you vulnerable to malicious applications
- Ensure third-party MDM solutions prevent or detect rooting/jailbreaking
- Address this in your mobile device policy

Android Specific Best Practices

- Enable Password Lock Screen vs. Face Unlock or Pattern
- Disable USB Debugging
- Enable Full Disk Encryption
- Download apps only from official app stores
  - Google Play
  - Amazon



Where to Find More Information

- Links to all the tools and articles mentioned in this presentation:

  http://MobileDeviceSecurity.info

- My presentations:

  http://SpyLogic.net

Thank you for your time!

Email: teston@securestate.com

Twitter: agent0x0