Things Your Smartphone Does When Nobody's Looking

Chris Eng
VP Research, Veracode
July 12, 2012

Mobile Risks at Every Layer

- NETWORK: Interception of data over the air
- HARDWARE: Baseband layer attacks
- OPERATING SYSTEM: Defects in kernel code or vendor supplied system code
- APPLICATION: Third-party apps with vulnerabilities and malicious code

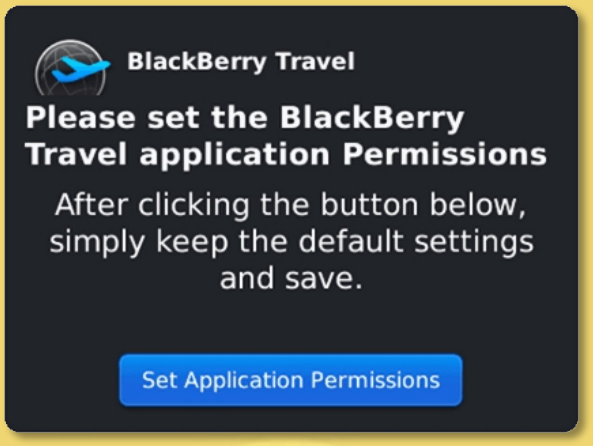
10.9 billion mobile apps downloaded in 2010, according to IDC

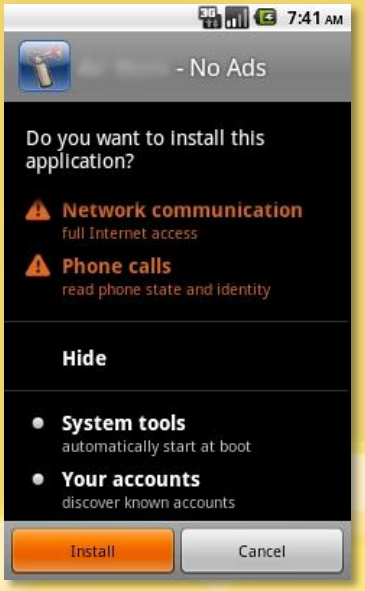
Expected to rise to 76.9 billion apps by 2014

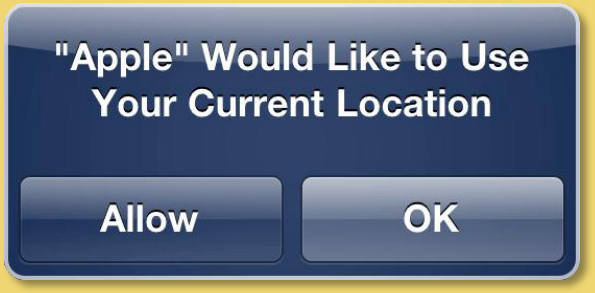
So What?

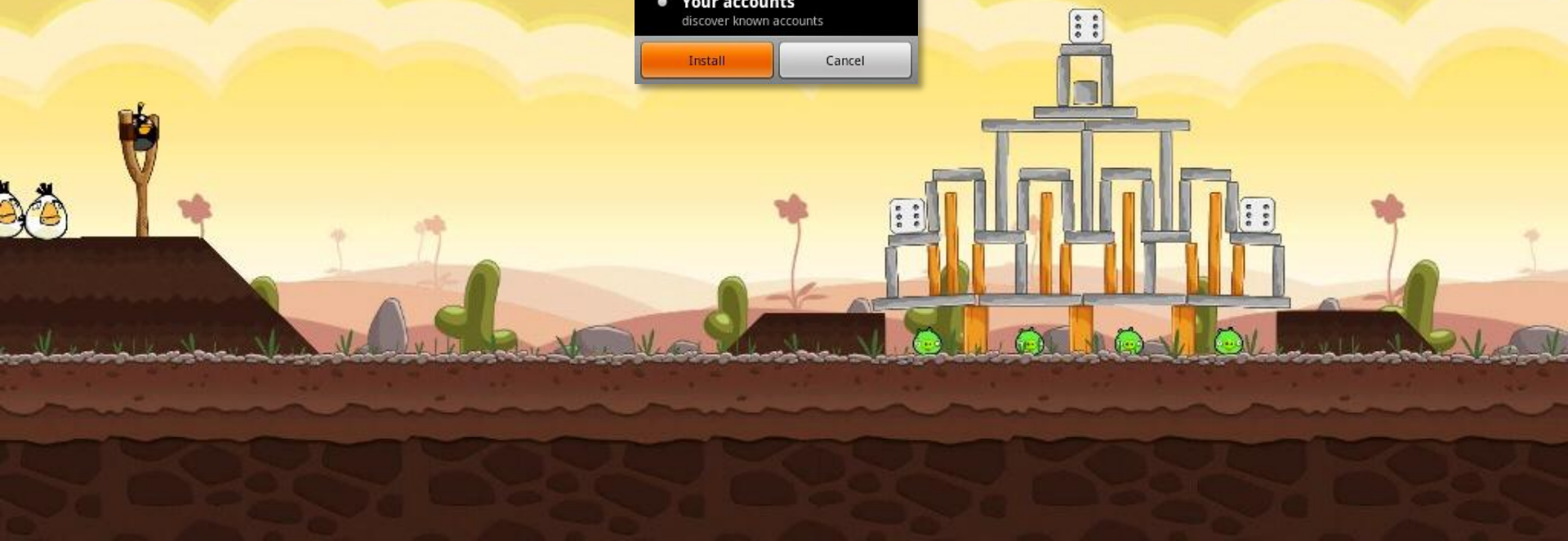
Back to the ’90s

Just Let Me Fling Birds at Pigs Already!









Mobile Top 10

- Malicious Code
  - Activity Monitoring and Data Retrieval
  - Unauthorized Dialing, SMS, and Payments
  - Unauthorized Network Connectivity (Exfiltration of Command & Control)
  - UI Impersonation
  - System Modification (Rootkit, APN Proxy Configuration)
  - Logic or Time Bombs
- Coding Vulnerabilities
  - Sensitive Data Leakage (Inadvertent or Side Channel)
  - Unsafe Sensitive Data Storage
  - Unsafe Sensitive Data Transmission
  - Hardcoded Passwords / Hardcoded Crypto Keys

OWASP Mobile Top Ten

(for reference, not discussing today)

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

Part 1: Malicious Code

- Activity monitoring and data retrieval
- Unauthorized dialing, SMS, and payments
- Unauthorized network connectivity (exfiltration or command & control)
- UI impersonation
- System modification (rootkit, APN proxy config)
- Logic or time bomb

Activity Monitoring and Data Retrieval

- Attackers can monitor and intercept lots of information
  - Sending each email sent on the device to a hidden 3rd party address
  - Listening in on phone calls or simply open microphone recording
  - Stored data, contact list or saved email messages retrieved

Secret SMS Replicator

- Covertly forwards text messages to another phone
- No visible icon; once installed, will continue to monitor without revealing itself
- Pulled from Android Marketplace after 18 hours

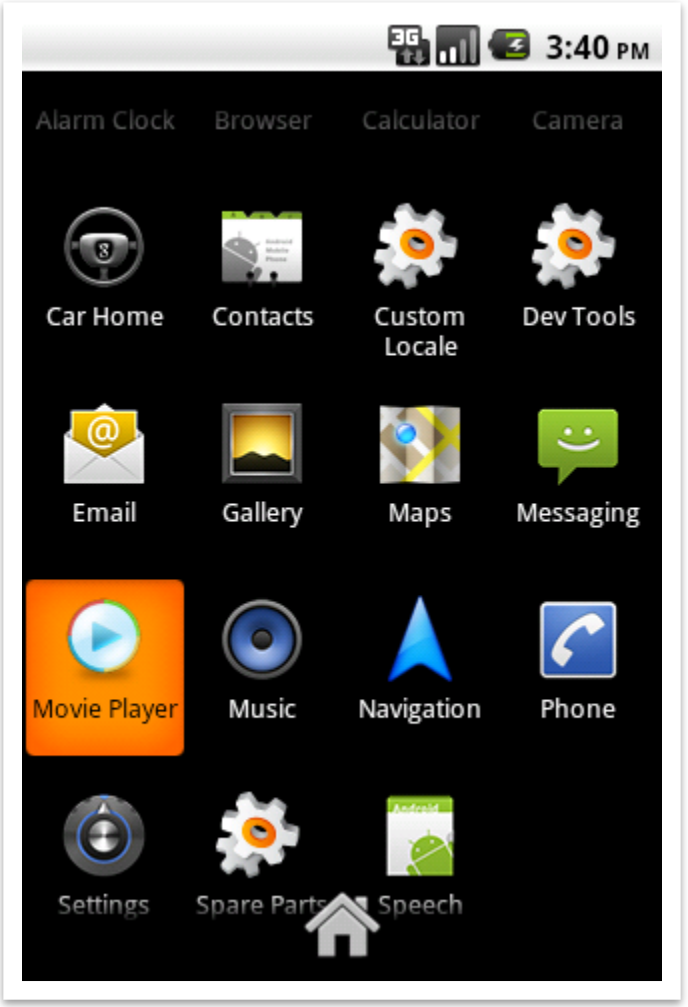
1. "Spy App Forwards Cheating Partner's Texts, Gets Banned From Android Store" http://www.switched.com/2010/10/28/sms-replicator-forwards-texts-banned-android/

Unauthorized Dialing, SMS, and Payments

- Directly monetize a compromised device
  - Premium rate phone calls
  - Premium rate SMS texts
  - Mobile payments
- SMS text message as a vector for worms

AndroidOS/FakePlayer.B

- Secretly sent SMS messages (Short Message Service) to a premium rate number presumably belonging to the hackers who created it
- End user does have to grant the application access to use SMS



1. "First Android SMS Trojan Found in the Wild" http://blog.mylookout.com/2010/08/security-alert-first-android-sms-trojan-found-in-the-wild/

Android.Qicsomos

- Detects whether CarrierIQ software is present
- When the user presses the "Déinstaller" button, four premium rate SMS messages are sent
- Icon on home screen looks exactly like the logo of a European telecom provider

1. "The Day After the Year in Mobile Malware?" http://www.symantec.com/connect/blogs/day-after-year-mobile-malware

Are You Ready For Some Football?

- Found in Android Market two weeks before Super Bowl
- Sends SMS to premium rate numbers
- Attempts to root the device using an executable disguised as an image file
- Attempts to install an IRC bot

1. "Are You Ready For Some Football? "http://www.symantec.com/connect/blogs/are-you-ready-some-football

Unauthorized Network Connectivity

- Spyware or other malicious functionality typically requires exfiltration to be of benefit to an attacker

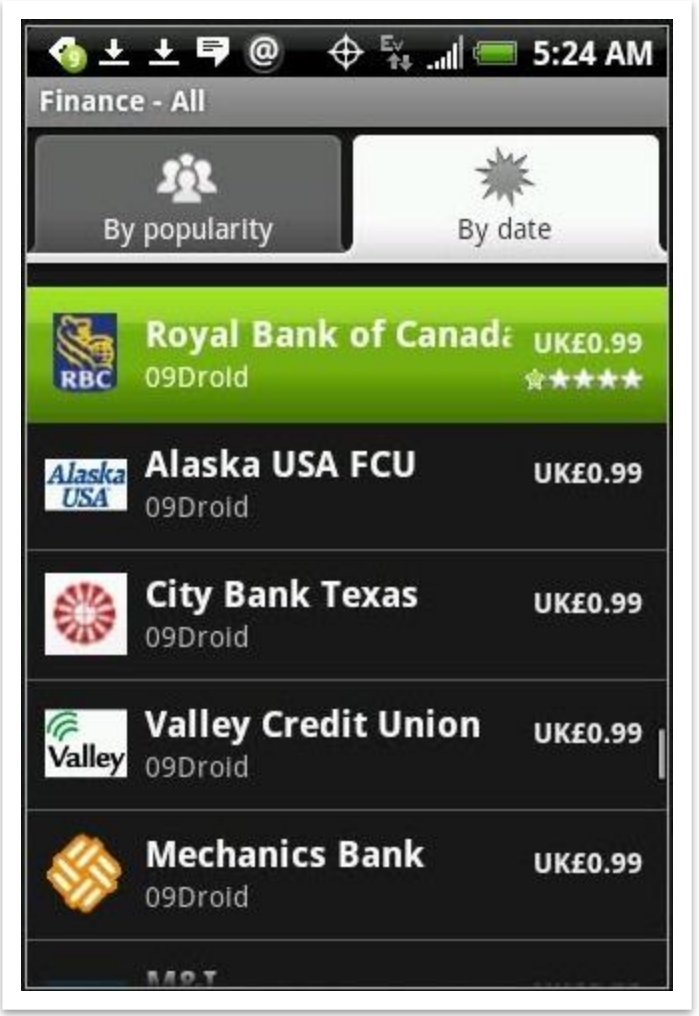
- Many potential vectors that a malicious application can use to transmit data
  - Email
  - SMS
  - HTTP
  - Raw TCP/UDP
  - DNS
  - Bluetooth
  - Blackberry Messenger
  - IRC
  - etc.

UI Impersonation

- Similar to phishing attacks
- Web view applications on the mobile device can proxy to legitimate website
- Could also impersonate the phone's native UI or the UI of a legit application

09Droid

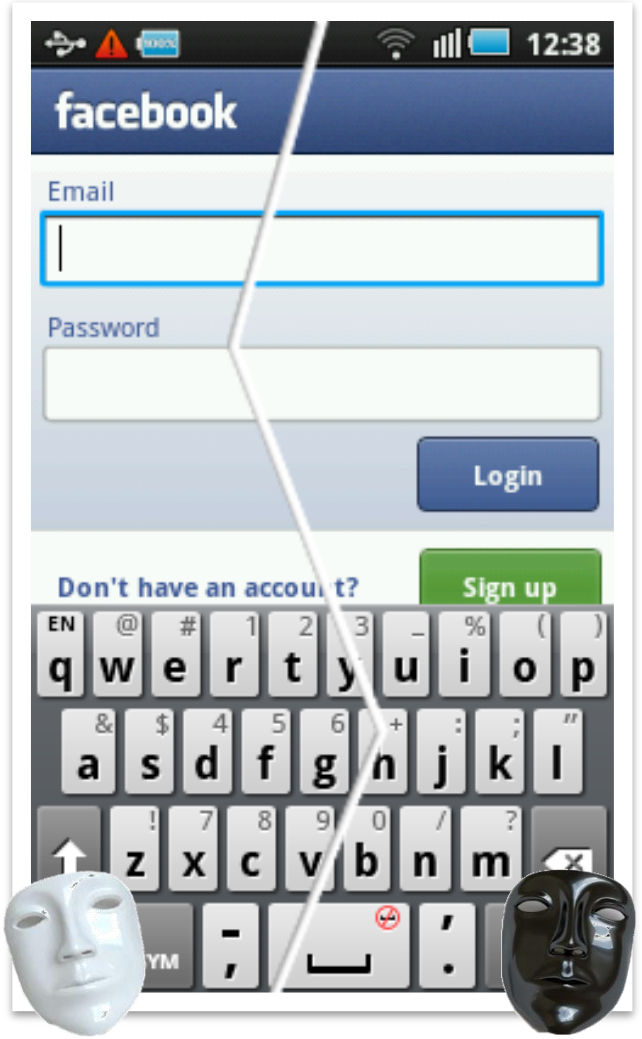
- Abbey Bank
- Alaska USA FCU
- Alliance & Leicester (v. 1.1)
- Bank Atlantic
- Bank of America
- Bank of Queensland
- Barclaycard (v. 1.1)
- Barclays Bank (v. 1.2)
- BB&T
- Chase
- City Bank Texas
- Commerce Bank
- Compass Bank
- Deutsche Bank
- Fifty Third Bank v.1.1
- First Republic Bank v.1.1
- Great Florida Bank
- Grupo Banco Popular
- HSBC US (v. 1.2)
- ING DiBa v.1.1
- Key Bank
- LloydsTSB
- M&I
- Mechanics Bank v.1.1
- MFFCU v.1.1
- Midwest
- Nationwide (v. 1.1)
- NatWest (v. 1.1)
- Navy Federal Credit Union (v. 1.1)
- PNC
- Royal Bank of Canada
- RBS v.1.1
- SunTrust
- TD Bank v.1.1
- US Bank v.1.2
- USAA v.1.1
- Valley Credit Union
- Wachovia Corp (v. 1.2)
- Wells Fargo (v. 1.1)



1. "Phone Phishing: A look at seemingly legitimate applications on mobile phones" http://blog.mylookout.com/2010/01/phone-phishing-a-look-at-seemingly-legitimate-applications-on-mobile-phones/

UI Impersonation via Focus Stealing

- Can you tell the difference between the real Facebook login screen and the fake one?
- It's a feature not a bug!



1. "Android could allow mobile ad or phishing pop-ups" http://news.cnet.com/8301-27080_3-20089123-245/android-could-allow-mobile-ad-or-phishing-pop-ups/

System Modification

- Malicious applications will often attempt to modify the system configuration to hide their presence
  - Modifying the device proxy configuration
  - Modifying the Access Point Name (APN)
- Rootkit behavior
  - Fine line between application layer and OS layer
  - Hiding exploits and rootkits inside legitimate JPG files (e.g. GingerBreak embedded in "Angry Birds Space" malware edition

1. "Security Alert: New Variants of Legacy Native (LeNa) Identified", http://blog.mylookout.com/blog/2012/04/03/security-alert-new-variants-of-legacy-native-lena-identified/

DroidDream

- Exploit breaks out of application sandbox and roots the device, then sets up C&C channel
- More than 50 applications from 3 publishers, including:
  - Falling Down
  - Super Guitar Solo
  - Super History Eraser
  - Photo Editor
  - Super Ringtone Maker
  - Super Sex Positions
  - Hot Sexy Videos
  - Chess
  - Hilton Sex Sound
  - Screaming Sexy Japanese Girls
  - Falling Ball Dodge
  - Scientific Calculator
  - Dice Roller
  - Advanced Currency Converter
  - App Uninstaller
  - Funny Paint
  - Spider Man
  - Bowling Time
  - Advanced Barcode Scanner
  - Supre Bluetooth Transfer
  - Task Killer Pro
  - Music Box
  - Sexy Girls: Japanese
  - Sexy Legs
  - Advanced File Manager
  - Magic Strobe Light
  - Advanced App to SD
  - Super Stopwatch & Timer
  - Advanced Compass Leveler
  - Best password safe
  - Finger Race
  - Piano
  - Bubble Shoot
  - Advanced Sound Manager
  - Magic Hypnotic Spiral
  - Funny Face
  - Color Blindness Test
  - Tie a Tie
  - Quick Notes
  - Basketball Shot Now
  - Quick Delete Contacts
  - Omok Five in a Row
  - Super Sexy Ringtones

1. "Security Alert: DroidDream Malware Found in Official Android Market" http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/

Logic or Time Bomb

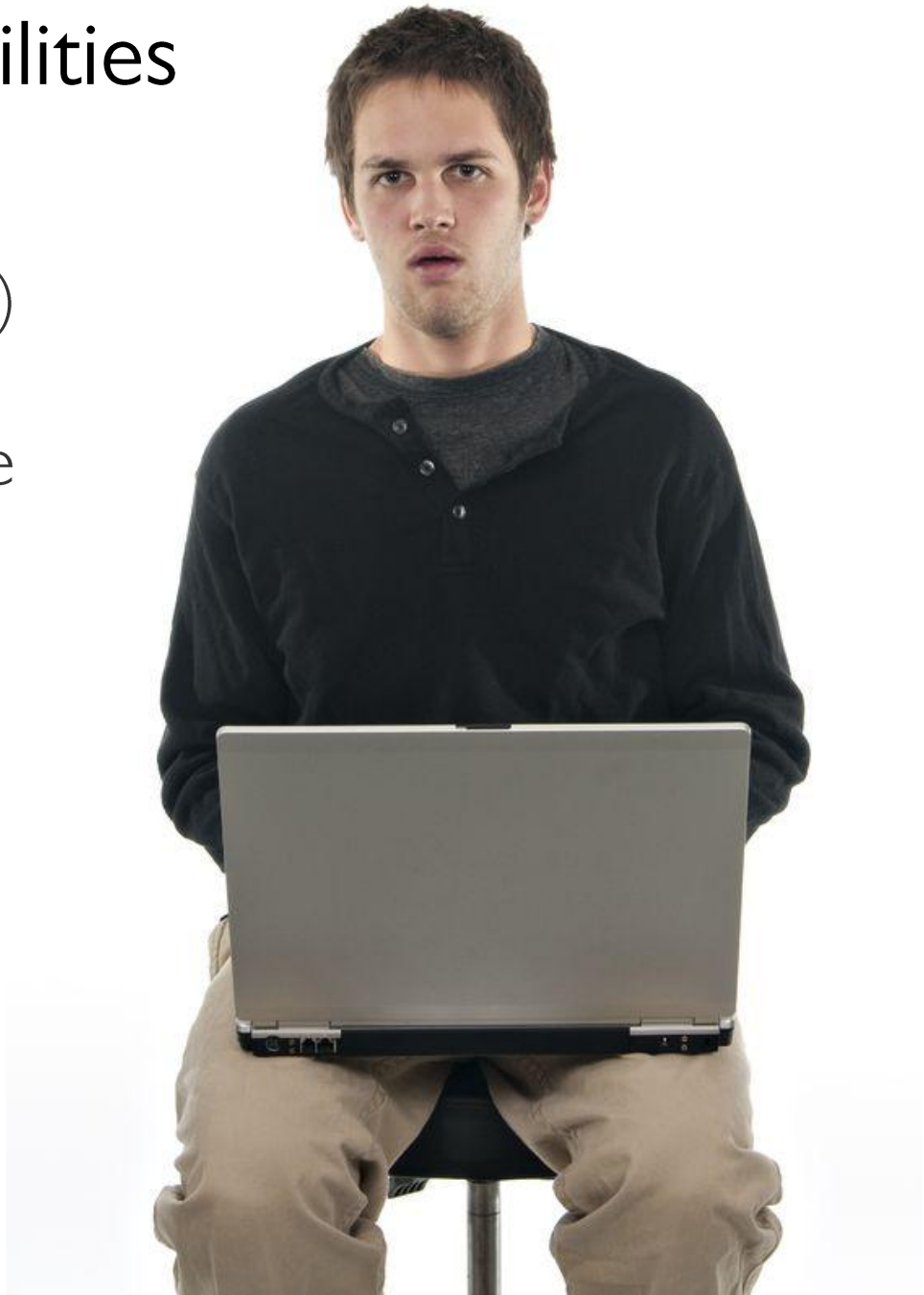
CWE 511

- Classic backdoor techniques that trigger malicious activity based on a specific event, device usage or time
  - Certain hours of the day or days of the week
  - Upon receipt of an email or SMS from a particular sender
  - When a phone call is made

- DroidDream had time-based component: run overnight to accept commands only between 11pm and 8am

Part 2: Code Vulnerabilities

- Sensitive data leakage (inadvertent or side channel)
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Hardcoded password/keys



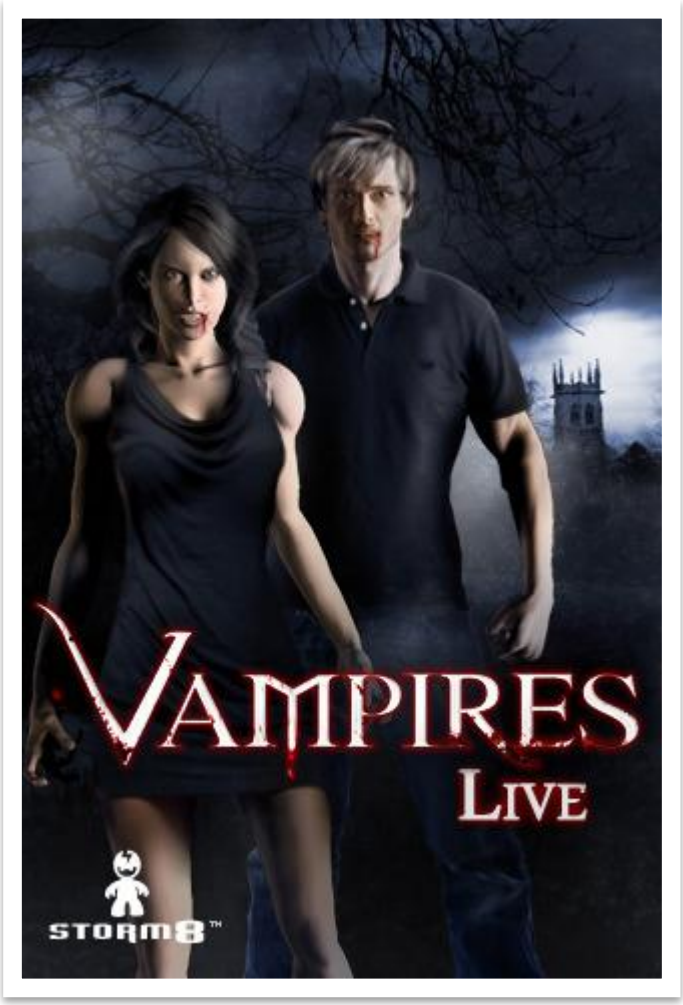
Sensitive Data Leakage

CWE 200

- Sensitive data leakage can be either inadvertent or side channel
- A legitimate apps usage of device information and authentication credentials can be poorly implemented thereby exposing this sensitive data to third parties
  - Location
  - Owner info: name, number, device ID
  - Authentication credentials
  - Authorization tokens

Storm8

- Automatically transmitted the wireless telephone number of each iPhone user who downloaded any Storm8 game

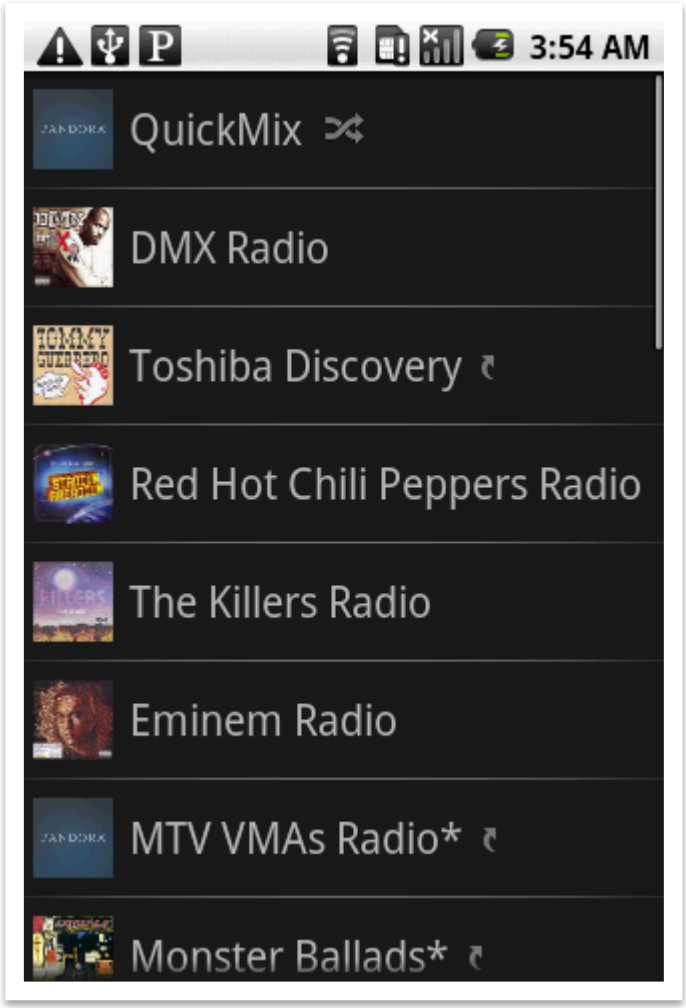


1. "iPhone game dev accused of stealing players' phone numbers" http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html

Pandora

- Embedded advertising libraries access information such as GPS location, device identifiers, gender, and age
  - AdMarvel, AdMob, comScore, Google.Ads, and Medialets

- Ad libraries "piggyback" on permissions of the host application



1. "Mobile Apps Invading Your Privacy" http://www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy/

POSTED: APRIL 15, 2:32 PM ET | *By* SCOTT STEINBERG

Pandora Responds to Claims That Its Online Service Violates User Privacy

Recommend | 2 recommendations. Sign Up to see what your friends recommend.

As discussed in an earlier post, security firm Veracode alleges that online streaming music service provider Pandora has been secretly sharing users' information, including age, gender and location, with digital advertising firms.

In response to these accusations, the popular Internet radio service is removing third-party advertising platforms, including Google, AdMeld and Medialets. Despite insisting it has found zero evidence to support the charge that these companies acted beyond the confines of its ad policy, the company hopes to mollify fans by taking a proactive stance. New versions of its smartphone and mobile device apps lacking support for these services are planned for free download via the Android Market and the Apple App Store soon.

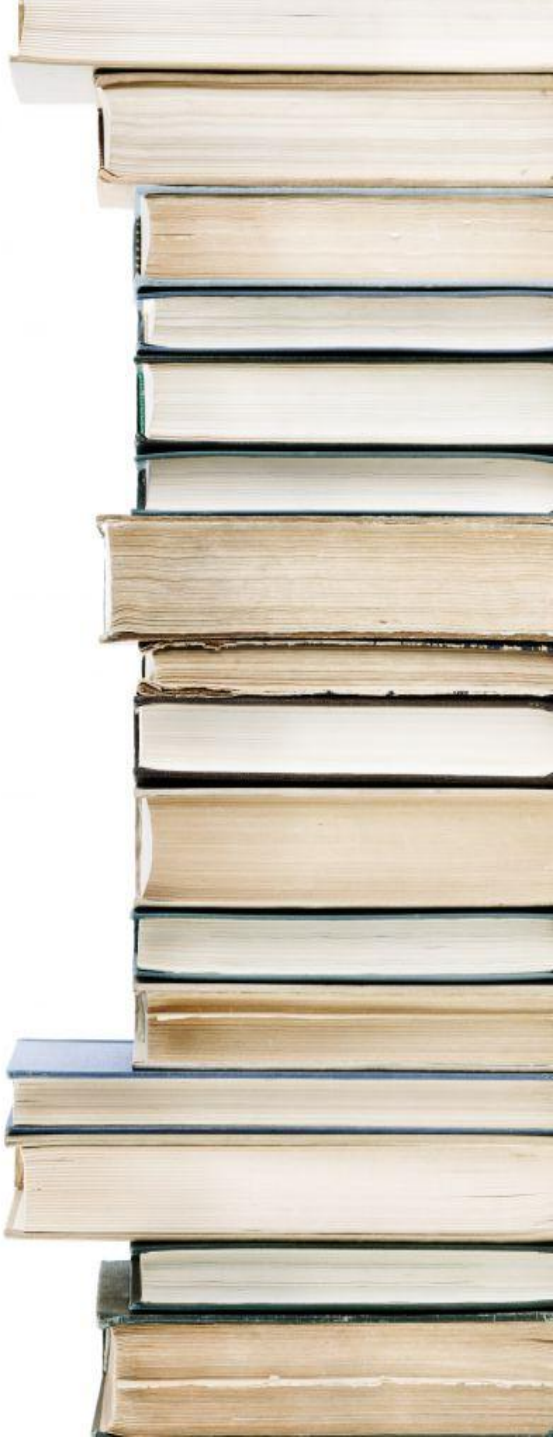
Share Tweet 17

One week later...

1. http://www.rollingstone.com/culture/blogs/gear-up/pandora-responds-to-claims-that-its-online-service-violates-user-privacy-20110415

Shared Library Use

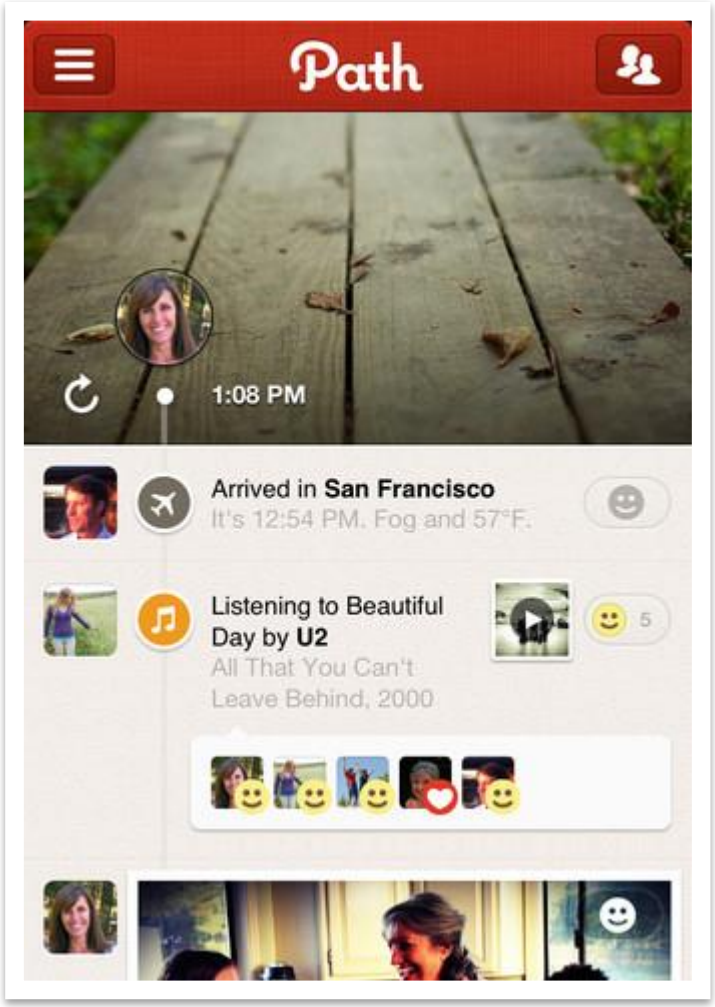
- 53,000 apps analyzed
  - Android Market: ~48,000
  - Third-Party Markets: ~5,000
- Total third-party libraries: ~83,000
- Top shared libraries
  - com.admob: 38%
  - org.apache: 8%
  - com.google.android: 6%
  - com.google.ads: 6%
  - com.flurry: 6%
  - com.mobcity: 4%
  - com.millennialmedia: 4%
  - com.facebook: 4%



1. http://www.slideshare.net/praetorianlabs/staaf-an-efficient-distributed-framework-for-performing-largescale-android-application-analysis

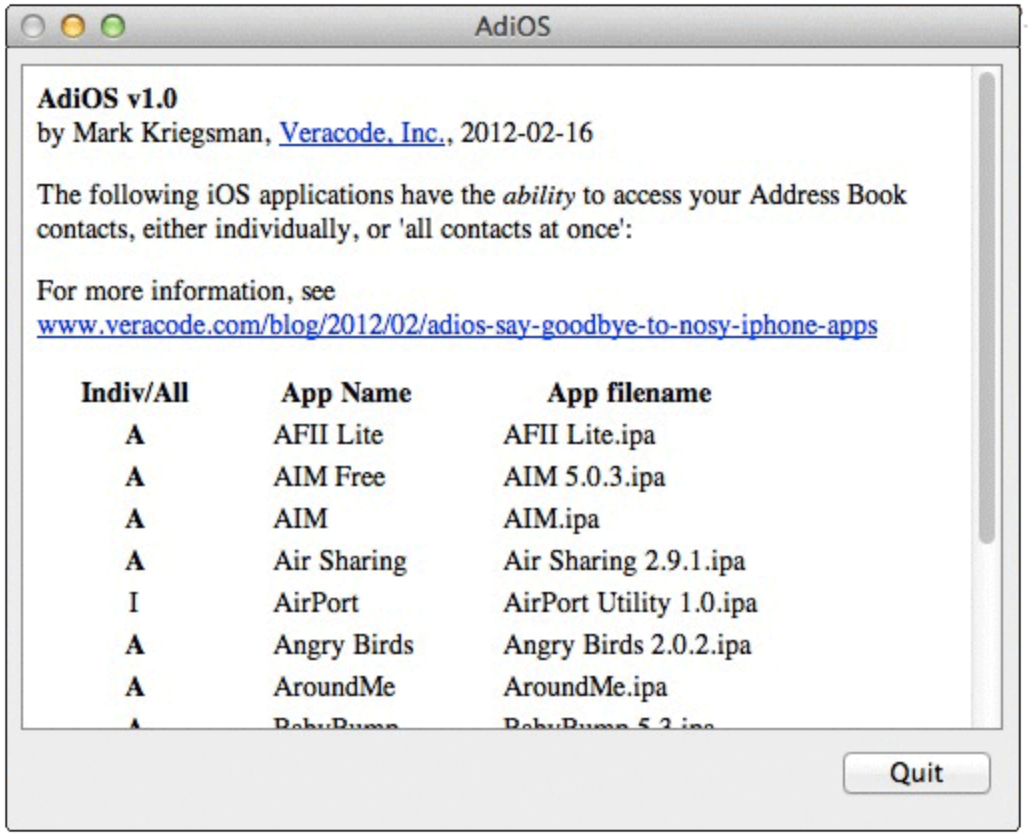
What Constitutes a Privacy Leak?

- Sends entire address book (including full names, emails and phone numbers) to Path
- Full apology on Path blog, and new iOS version within days with an opt-in prompt
- New Apple policy
  - "Apps that collect or transmit a user's contact data without their prior permission are in violation of our guidelines"



1. "Path uploads your entire iPhone address book to its servers", http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html

iPhone Apps are Nosy



1. "AdiOS: Say Goodbye to Nosy iPhone Apps",
   http://www.veracode.com/blog/2012/02/adios-say-goodbye-to-nosy-iphone-apps/

Unsafe Sensitive Data Storage

CWE 312

- Mobile apps often store sensitive data
  - Banking and payment system PIN numbers, credit card numbers, or online service passwords
- Sensitive data should always be stored encrypted
  - Make use of strong cryptography to prevent data being stored in a manner that allows retrieval
  - Storing sensitive data without encryption on removable media such as a micro SD card is especially risky

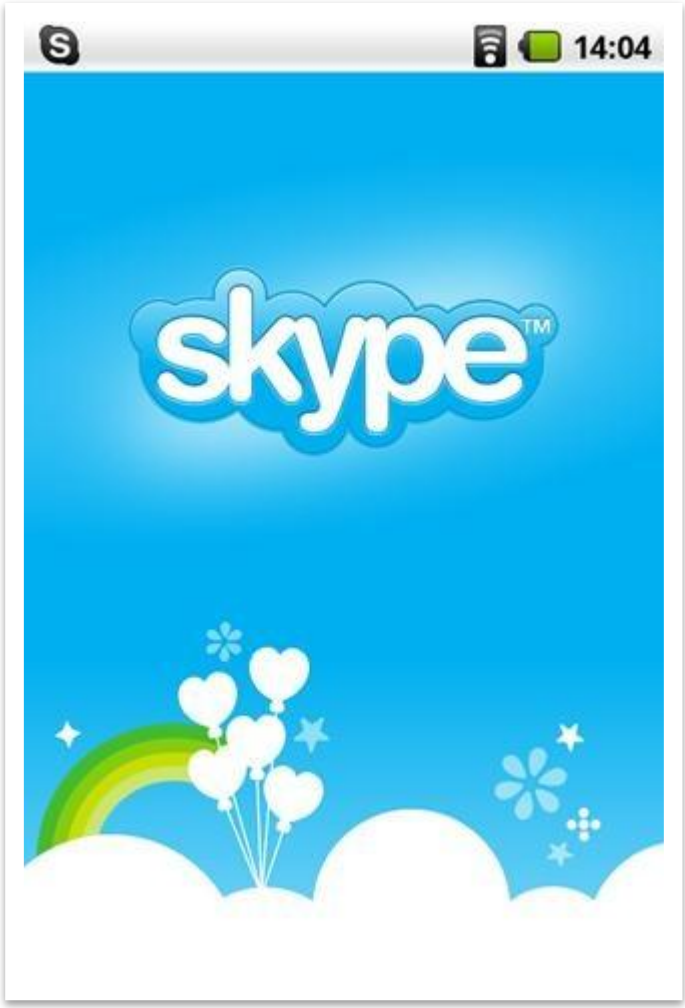
CitiGroup

- Account numbers, bill payments and security access codes are stored on the iPhone where they could be accessed later by attackers or other unauthorized users

1. "Citi iPhone App Flaw Raises Questions of Mobile Security" http://www.pcworld.com/businesscenter/article/201994/citi_iphone_app_flaw_raises_questions_of_mobile_security.html

Skype

- Uses SQLite3 databases to store contact list and chat logs
  - Files are not encrypted
  - Can be read by any app on the phone
- Skype responds the following day announcing they are working on a fix



1. "Exclusive: Vulnerability In Skype For Android Is Exposing Your Name, Phone Number, Chat Logs, And A Lot More" http://www.androidpolice.com/2011/04/14/exclusive-vulnerability-in-skype-for-android-is-exposing-your-name-phone-number-chat-logs-and-a-lot-more/

Unsafe Sensitive Data Transmission

CWE 319

- It is important that sensitive data is encrypted in transmission lest it be eavesdropped by attackers
- Mobile devices are especially susceptible because they use wireless communications exclusively and often public WiFi
- SSL is one of the best ways to secure sensitive data in transit
  - Beware of downgrade attack if it allows degrading HTTPS to HTTP
  - Beware of not failing on invalid certificates; this would enable that a man-in-the-middle attack

Hardcoded Password/Keys

CWE 798

- Used as a shortcut by developers to make the application easier to implement, support, or debug
- Once the hardcoded password is discovered through reverse engineering or other means:
  - Everybody has it (e.g. backdoor passwords for router maintenance)
  - The security of the application is rendered ineffective
  - The system(s) being authenticated to may also suffer due to trust assumptions

MasterCard Payments API

- In this snippet from their reference code, they suggest hardcoding your companyID and companyPassword in plaintext string format:


```
final double amount = Float.valueOf(amountInput.getText().toString());
final String currency = "USD";
final String companyId = "your-company-id-here";
final String companyPassword = "your-company-password-here";
final String messageId = "your-message-id-here";
final String settlementId = "your-settlement-id-here";
```

1. "Scary, Scary Mobile Banking" http://jack-mannino.blogspot.com/2011/02/scary-scary-mobile-banking.html

What Can Be Reliably Detected?

- Unintentional vulnerabilities are straightforward; always scan for these
  - We see lots of information leakage and cryptographic issues
- The challenge with detecting malicious behavior is determining ***intent***
- FP/FN tradeoffs with "unauthorized" behaviors
  - e.g. Is it good or bad that the app uses GPS?
- Think differently – behavioral profiling?

What We're Seeing So Far

CWE Category	CWE	Percent Applications Affected
Insufficient Entropy	331	61%
Use of Hard-coded Cryptographic Key	321	42%
Information Exposure Through Sent Data	201	39%
Information Exposure Through Error Message	209	6%

Questions?

ceng@veracode.com
@chriseng