

Mobile Security

The evolution of a new challenge

Christopher Triplett
viaForensics
May 18, 2011





Agenda

Mobile Insecurity

Ramifications of insufficient action

Solutions to securing your mobile network

Implementation costs

Forensics as a proactive solution to security



About viaForensics

- viaForensics is the leading proactive forensics solutions firm, specializing in security consulting, data recovery, mobile forensics training, and server surveillance.



Mobile insecurity

- We are facing a perfect storm
 - Technical
 - Business / regulatory
 - Maturity of technology and processes



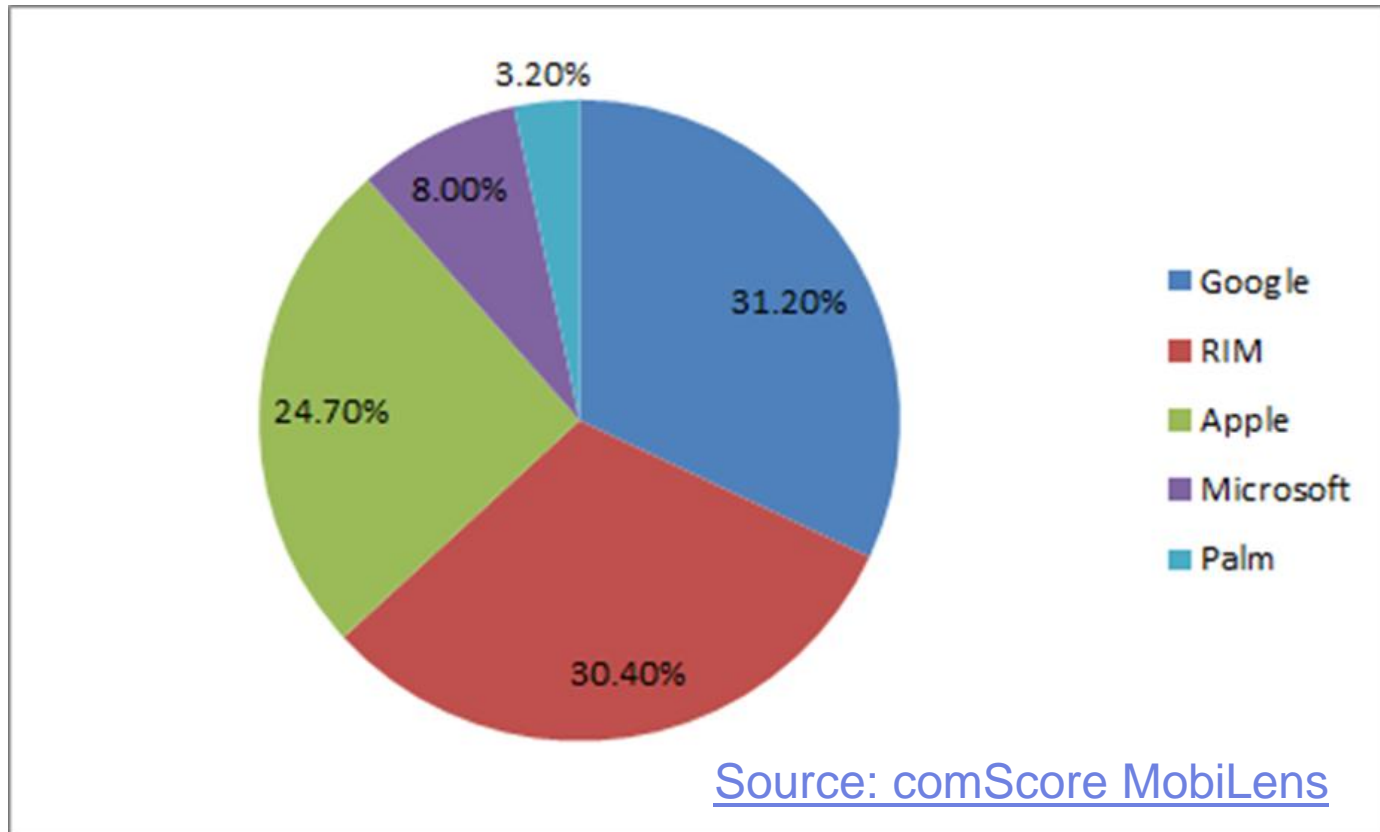
Mobile insecurity

- Lack of control / auditability
- Rapid migration to immature platforms
- “Consumerization” of devices
 - Apps
 - Personal and enterprise combined
 - Who owns the data?
- Portability = easily lost or stolen
 - Short life cycle
- Growing threats
 - Wi-Fi attacks, lost devices, malware



Mobile insecurity

- Enterprise friendly mobile market losing ground





Mobile insecurity

- Blackberry offers extensive enterprise controls
 - Secure platform through BES
- Currently Apple, Android, WebOS built in policy through ActiveSync
 - Password enforcement options
 - Attachment options
 - File access (UNC or MSS file access)
 - Remote wipe
 - Prohibited use of camera
- ActiveSync policies similar to Lotus Notes Traveler



Mobile Insecurity

- Blackberry security
 - Not possible to image
 - Backup file, BES
 - Effective remote wipe
 - Sensitive information protected
- WebOS
 - Easily imaged
 - Cached data includes emails, attachments, and more
 - Backup on Palm Cloud



Mobile Insecurity

- iOS Security
 - Imaging requires special tools, iOS 4 encrypted
 - Can bypass passcode in 6 minutes
 - Backup file can contain sensitive info
 - Opened PDF and other docs
 - Voice Recordings
 - Voicemails
 - Emails*
 - More
 - 4 digit pin insignificant
 - No encryption on 3.x
 - Jailbreaking easy and puts phone and enterprise network at risk



Mobile Insecurity

- iOS keychain.db

```
==== GENERIC PASSWORDS ====
```

```
AirPort (faiv-wireless)
```

```
Service:           AirPort
Account:           viaforensics
Data:              5238675309123
Access Group:     apple
```

```
viaForensics\ctriplett
```

```
Account:          ctriPLETT
Data:            P@55w0rd
Server:          via.exchange.server
Service:         TCP
Port:            443
```



Mobile Insecurity

- iOS keylogger

DynamicDictionary-4

[test mail test test golf clubs hey what
type of clubs would your first choice
calloway mail how am supposed to get
into the store after hours check out
sure is nice day out what're you doing
today dinner at great may need to
head out around but that should give
us plenty of time lake oak park oak
park il lake oak park il piece of cake
can't wait to try out on sunday test to
brad test to brad will you go get me
coffee guess you'll never know

viaforensics gmail golfsmith
ctriplett taylormade sbcglobal sarpinos
mccalister em



Mobile Insecurity

- Android security
 - Imaging possible
 - SD card
 - Backup file
 - Passwords in plain text
 - No encryption
 - Some versions resistant to remote wipe
 - Apps can be downloaded from non-trusted sources



Mobile Insecurity

- Android data examples
 - Accounts.db

The screenshot shows the SQLite Database Browser interface. The title bar indicates the file path: E:\Laptop Cleanup\Various-Case-Nand-Images\Teds... The application has a menu bar (File, Edit, View, Help) and a toolbar with various icons. Below the toolbar are three tabs: Database Structure, Browse Data (selected), and Execute SQL. The 'Table:' dropdown is set to 'accounts'. There are 'New Record' and 'Delete Record' buttons. The main area displays a table with the following data:

	id	name	type	password
1	1	Weather	com.htc.sync.provic	
2	2	teull@viaforensics.com	com.htc.android.ma	p@55w0rd!
3	3	ted.eull@gmail.com	com.google	AFcb4KRCVdVdcahYtZZg4Qupc5r

At the bottom, there are navigation buttons: '<' (previous), '1 - 3 of 3', '>' (next), 'Go to:', and a text input field containing '0'.



Mobile Insecurity

- Android data examples
 - WPA_supplicant.conf

```
ctrl_interface=tiwlan0update_config=1
network={
    ssid="home_network"
    psk="Redhound"
    priority=1}network={
    ssid="Romus"
    psk="basket111" priority=2}
```



Mobile Insecurity

- Android data examples
 - Email account and attachment paths

SQLite Database Browser - E:\Laptop Cleanup\Various-Case-Nand-Images\Teds Eris data\data\com.google...

File Edit View Help

Database Structure Browse Data Execute SQL

Table: messages

New Record Delete Record

	snippet	listInfo	personalLevel	body	bodyEmbedsExt	joinedAttachme	s
1	- FAX offer and HUD			1 <div><div style="fr	0		
2	4] Things are shaping u			0 <div>Things are sha	0	0.1 332.gif image/g	
3	on We will be at your h			0 We will be at your	0	0.1 332.gif image/g	
4	on send an invite to mir			0 send an invite to mir	0	0.1 332.gif image/g	
5	on Do they see these e			0 Do they see these	0	0.1 332.gif image/g	
6	on From: tricia.jacobs@			0 <p><font color=#5	0	0.1 332.gif image/g	
7	01 Paula ma 1 I dr			0 Paula ma 	0		

1 - 18 of 18

Go to: 0



Mobile Insecurity

- Is your current posture enough?
- Many consumers and corporate entities unaware that this data exists.



Ramifications

- What happens if my MDM solution or mobile policy is insufficient or not effective?



Ramifications

- Sony
 - SQL injection attack
 - 100 million customers data exposed
 - Damaged brand image
 - Estimated \$2.74B damages



Ramifications

- Malware infections can be sophisticated and insidious
- Corporate knowledge of exploits
- Exponential increase in recent threats



Ramifications

- McAfee CEO David Dewalt on malware
 - “When I first arrived, we were seeing somewhere in the neighborhood of about **three million bad pieces of content a year**. “...” We’ve literally seen an exponential increase in that in the last four years. **We’re now tracking somewhere in the neighborhood of 48 million bad pieces of malware** now. The cost of offense remains very low, and the cost of defense is very high.”



Ramifications

- Malware in the mobile environment
 - Embedded in applications, emails, text messages
 - Denial of service
 - Cross infect enterprise network
 - Key loggers
 - PII collection



Solutions

- Many factors to consider
 - Time
 - Resources
 - Knowledge



Solutions

- Good solutions
 - Blackberry only
 - Don't allow mobile devices



Solutions

- Better solutions
 - Restrict device choices
 - Ensure security through appropriate auditing techniques
 - Use inherent device management features
 - Use policies to enforce passcodes, wipe devices



Solutions

- Best solutions
 - Everything in the previous slide
 - Revise policies and procedures to deal with mobiles comprehensively
 - Again, use an effective device audit to determine risks
 - Training
 - Evaluate and implement MDM solution
 - Remember that 80% of security products fail to work as intended
 - Restrict apps if possible
 - Use a more secure email client
 - Audit your systems and procedures frequently



Implementation costs

- Planning
 - Mobile device risk study
- Software
 - MDM solution
- Training
 - Both end users and IT/Security staff
- Ongoing management, auditing
 - Ensuring version compliance
- Other – time invested and complexities



Implementation costs

- Cost vs. risk – is it worth it?
 - Average data breach \$202 per record
 - May 2011 Reid Hospital computer stolen containing information from patients who visited the hospital between 1999-2008 (estimated 20,000 records = > \$4mil)
 - September 2010 SunBridge Health Care Blackberry mobile device stolen containing patient information from eight different nursing and rehab centers. Device contained more than 1000 patient records = > \$200K



Implementation costs

- Mobile application auditing – cost vs. risk
 - Average cost of a comprehensive application audit ~ \$20k
 - July 2010 Citigroup announced that iPhone app contained a security flaw that cached data to the device. 117,600 devices affected resulting in confidential consumer info being cached on local device.
 - November 2010 PayPal and Wells Fargo mobile app issues
 - Is your app secure?



Forensics as a solution

- Completely new way to approach security
- Traditional forensics are used as an investigative tool (reactive)
- Extremely useful tool when used proactively
 - Determine security vulnerabilities before implementing solution
 - Very low cost in comparison to data breach
 - App development community slowly starting to embrace as an essential tool



Forensics as a solution

- Key elements of mobile device security audit
 - Connect to enterprise domain via MDM and simulate real-world use
 - Forensically examine data
 - Analyze Wi-Fi network transmissions
 - Test the implementation of corporate security
 - Test the efficacy of erasing methods



Forensics as a solution

- Key elements of mobile application security audit
 - Network monitoring
 - Enforce SSL
 - Multiple MITM – ARP poisoning, fuzzing, etc.
 - PCAP analysis
 - Live memory investigation
 - Web service (webkit)
 - Hosts attack, framebusting,
 - Logical memory analysis
 - Physical memory analysis
 - Backup file analysis
 - Reverse engineer application



Contact us

Andrew Hoog

Chief investigative Officer

ahoog@viaforensics.com

<http://viaforensics.com>

Main Office:

1000 Lake Street, Suite 203

Oak Park, IL 60301

Tel: 312-878-1100 | Fax: 312-268-7281



Questions?

Closing comments

