



Time to Move into High Gear!

MOBILE DEVICE SECURITY

Karen McDowell, Ph.D., GCIH
Information Security, Policy, and Records Office
University of Virginia

Varieties of Devices at Risk

- Laptops and Netbooks
- External storage devices like USB drives
- Smart phones
 - BlackBerry (RIM Operating System)
 - Windows Mobile Operating System
 - Palm Operating System (WebOS)
 - iPhones / iPod touch
 - Android System
 - Symbian System

Focus on Smart Phones



Smart Phone Growth

- Total smart phone sales grew by 8 million units in Q209¹
- Four things driving growth –
 - Increasing amount of time we spend online whether business or pleasure
 - Convenience and efficiency
 - Instant gratification - hard to wait to check messages or update status
 - Desire to look good while going online²

¹<gartner.com>

²<cnet.com> March 2008 Tom Krazit

Smart Phone Security 2009

- Proliferation of mobile devices with powerful computing resources
- No massive malware outbreak to date = no panic about security
- Little incentive for hackers to develop malware because limited vectors to scam
 - Texting, premium rate numbers, vishing
- Encryption and protection options not well known

Users Oblivious to Threats

- Mistaken sense smart phones immune to security threats
- “Smartphone owners remain oblivious to security risks despite using their handhelds for a growing range of applications that introduce potential problems, such as web surfing”
- Concomitantly we are witnessing an explosive growth in social networking

Smart Phone Security 2010

- Smart phones especially difficult to protect
- Many types of smart phones & BYOphone = Less IT control
- Smart phones let us surf the Internet, shop and *bank* online
- We are socially and technically conditioned to enter data from a smart phone
- Fertile market for malware vendors to attack

Smart Phone Architecture

- Early versions had default-deny security model with no running extraneous services
- Every feature added from ground up
- Portability and customer convenience are now design goals
- Code base has
 - many communications services
 - data handling hooks
- Security model is currently default-allow

Smart Phone Security Caveats

- Good security is built-in, not added on
- Phone and application developers must build-in security, while this technology is *relatively new*
 - Developers must ensure unused code is removed or disabled where appropriate

Early Warnings

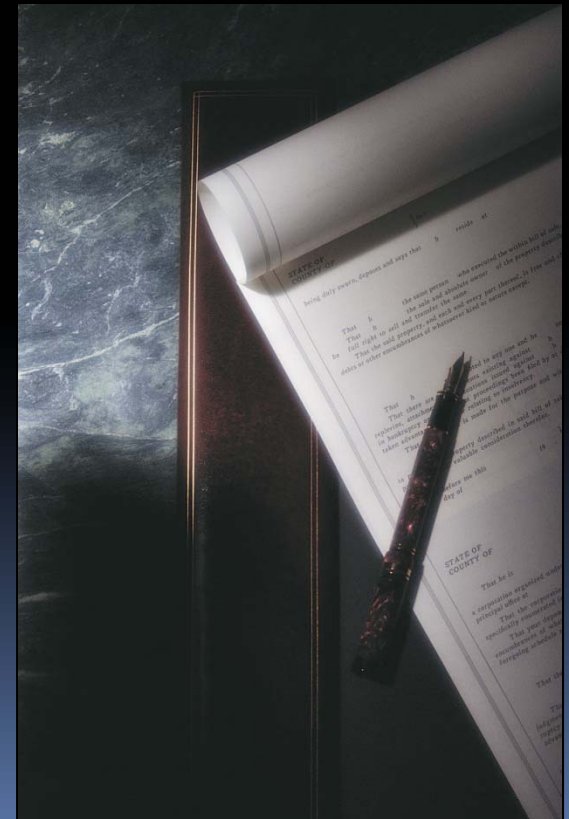
- "The smartphone will become a major security target... Personally I think this will become an epiphany to malware authors."¹
- "At this point, *mobile device capability is far ahead of security*... We'll start to see the botnet problem infiltrate the mobile world in 2009."²

¹Rich Cannings Google's Android Security Team <independent.co.uk> 10/2009

²Patrick Traynor School of Computer Science Georgia Tech Information Security Center <gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>

Security Policies Essential

- Policies are a necessity - not a luxury
 - Auditing and Authentication
 - Centralized security management
 - Data loss prevention
 - Encryption
 - Unauthorized access
 - User training



Corporate Smart Phone Policy

- Corporate policy must strictly enforce remote delete, password, and encryption policies
- Passcode-lock enhances auto-lock
- Exceeding the number of allowed password attempts deletes all data
- Enable at least 4 digits – depends upon IT policies
 - Configure pre-set time period to less than one hour

Non-Business Smart Phone Use

- Non-business users can rely on features common to most smart phones
 - User sets auto-lock to lock the screen after a pre-set time period of non-use
- Connect only to WPA-secured Wi-Fi networks in any case!

Secure a BlackBerry (BES)

- If you connect to the BlackBerry Enterprise Server (BES) on a corporate intranet, ask the BlackBerry server admin to enforce these options and test them
 - Password or passcode (PIN) protection
 - Remote Delete
 - Encryption
- If you connect to the BlackBerry Internet Service (BIS), use POP3s over SSL to increase security from the BIS server back to your mail server.
 - The data is secure from your device back to the BIS servers, because it uses SSL over a secure network

Secure Windows Smart Phone

- If you connect to a Windows Exchange Server on a corporate intranet, ask the IT folks to enforce the password protection, remote delete, and encryption options, and *test* them
 - Remote Delete through Outlook Web Access
 - Encryption may only be possible if you use a removable flash storage card, even if you connect to an Exchange server
- If you are a non-business user, encrypt with removable flash memory storage card
- Antivirus protection is available from third-parties.
- Remote delete is available as long as GPS installed

Secure an iPhone

- The Erase Data function lets you completely wipe your iPhone after 10 failed passcode attempts
- Enable the iPhone “Ask to Join Networks” function
- Non-business users
 - Use POP3s over SSL to increase security
 - Center for Internet Security (CIS) released free [guidelines](#) to help organizations develop custom policies related to iPhone use

Secure a Palm Pre (WebOS)

- Original PalmOS does not allow for encryption or timed auto-lock
- New Palm webOS enables these features
- Both operating systems can connect to an Exchange server through ActiveSync
 - Remote Delete is available through Outlook Web Access
 - Encryption may only be possible if you use a removable flash storage card and a third-party provider
- Non-business users --
 - Use POP3s over SSL to increase security

Palm Pre Phones Home!

- Palm Pre webOS sends back to Palm
 - Your location via GPS
 - Which webOS apps you use
 - How long you use them
- Location data for LBS (location based services) apps like Google Maps are OK
- Palm response is turn it off, but no one knows how to do it

<http://www.mobilecrunch.com/2009/08/12/oh-by-the-way-the-palm-pre-phones-home-with-your-location/>

Bluetooth Threat Vectors

- Bluejacking - sending unsolicited messages over Bluetooth (BT) to BT-enabled devices
 - Limited range, usually around 33 ft on mobile phones
- Laptops can reach up to 328 ft with powerful transmitter
- Bluesnarfing - unauthorized access of information from a wireless device through a BT connection
 - Allows access to a calendar, contact list, emails and text messages, and on some phones users can copy pictures and private videos
 - Possible on any BT-enabled device
 - Either can do serious harm - Bluesnarfing copies info from victim's device and is more dangerous

Lock Down Bluetooth!

- Bluetooth is default-on
 - Wastes your battery
 - Leaves you open to Bluetooth-based attacks

Twitter on Smart Phones

- Two Security Issues
 - Link shorteners like TinyURL lead users to unknown destinations
 - Single login system
- Phishers use Twitter in attack May 2009¹
 - Bogus accounts of “hot” women
 - Tiny URLs obfuscated real sites
- Clicking on Twitter-delivered video installs rogue antivirus, which demands payment²

<¹gadgetwise.blogs.nytimes.com> 5/2009

<²internetnews.com> 6/3/2009

Viruses and Smart Phones

- Viral Epidemics – highly fragmented smart phone market share has inhibited outbreaks
- Only smart phones susceptible to viruses
- Once a single mobile operating system market share grows large enough...
- Smart phone annual growth rate = 150%
 - Bluetooth virus (short range)
 - Multimedia Messaging System (MMS) virus spreads using the device address book

Social Engineering Threats

- The best security in the world will *not* help you if --
 - you click on an phishing email and give your personal information
 - you respond to a vishing phone call
- Never give information via email or by phone or on the web, unless you initiate the exchange, and then only if you employ best security practices

Threats to Smart Phones 2009

- Attackers will exploit our social conditioning entering personally identifiable information (PI), while interacting with phone voice response to commit vishing and identity theft.¹
- We demand more and better availability from phone service than we would from an ISP, "so the threat of a DoS attack might compel carriers to pay out on a blackmail scam."¹

Broader Issues

- Sensitive data storage on smart phones
- Users still clicking on phishing email
- RIM BlackBerry phishing hole fixed - if you download the patch
- Transferring files from a computer
- China's 3G revolution may drive threats
- Malware threat from spoofed cell phone texts sent to GSM networks

Mobile Security Basics

1. Install anti-virus and at least 2 anti-malware
2. Encrypt, especially if you handle sensitive data
3. Turn on firewall [speed bump to attackers yet it's *layered security*]
4. Install covert data deletion software
5. Create long password Best >15 characters [First line of defense – strength in length]
6. Secure devices physically with physical locks
7. Encrypt all USB drives*
8. Connect NOT to insecure wireless hotspots!

*IT can disable USB drive access

Mobile Devices & Best Practices

- Maintain *situational awareness* when carrying electronic devices
- Do not make mobile device obvious target
 - Disguise your laptop by carrying it in a non-laptop bag
 - Hide it in the trunk if you *must* store it in a vehicle but do not let anyone see you hide it
 - Never carry more information in your mobile device than you absolutely need

Best Practices II

- Backup data frequently to mitigate data loss in a worst-case scenario
- Carry your laptop on board flights
 - Store under the seat in front of you
- Watch your mobile device as you go through airport security
 - *Known bad location for device theft*
- Do not use insecure wireless hotspots
 - Save important transmissions until you can connect to a secure environment

Mobile Device Data Losses



Mobile Device Data Losses

- Mobile device theft occurs every 12 seconds
- Theft or loss of a computer or other data-storage devices accounted for 48 percent of data breaches that could lead to identity theft and for 66 percent of the identities exposed in 2008¹
- 196 data breaches involving personally identifiable information (PI) publicly reported in 2009 affecting 3,943,522 records²
- Costs already calculated in millions of dollars, to say nothing of collateral damage

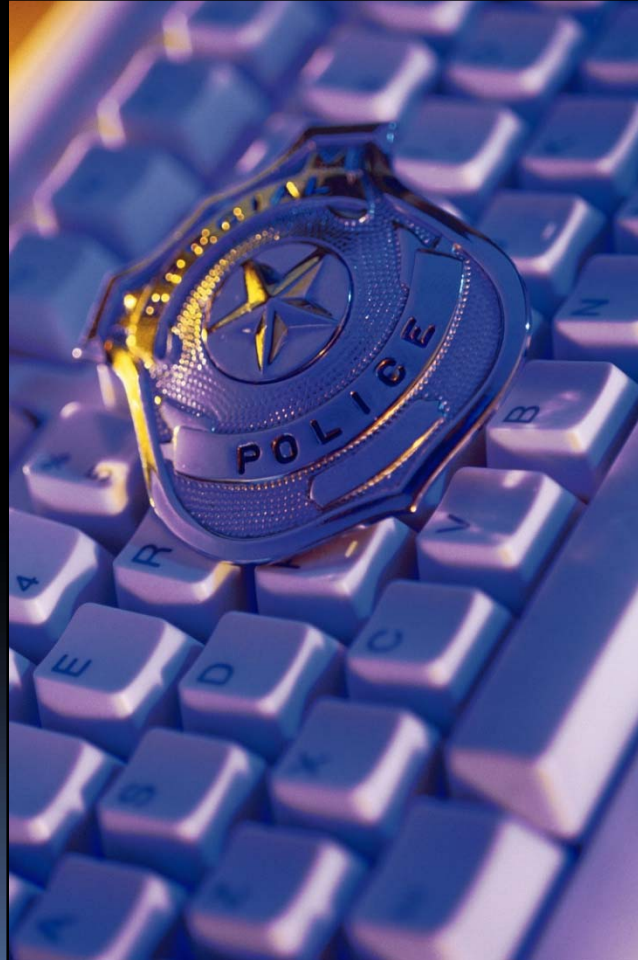
¹ Symantec Global Internet Security Threat Report Trends for 2008 Volume XIV, April 2009

² Open Security Foundation <datalossdb.org>

Cost of a Security Breach

- \$202 USD per stolen database record
 - Forensics cost
 - IT staff not productive because of breach
 - Legal and compliance fees
 - Loss of customers – Disastrous PR
 - Attackers may extort millions of dollars
 - Nothing good about it
 - 10,000 sensitive database records = \$2M breach

Mobility = Higher Risk Agility



Mobility = Higher Risk Agility

- Business travelers lose more than 12,000 laptops per week in U.S. airports¹
- One in 10 people have lost a laptop, smart phone, or USB flash drive with stored corporate information
- 79% frequently or sometimes leave their workplace with a mobile device such as a laptop, smart phone, or USB flash drive containing sensitive information²

¹ <aviationweek.com> July 3, 2008

² RSA, Security Division of EMC, Insider Threat 2008 Survey <rsa.com>

Avoid Maginot Line Security

- Think “Layered Security” or “Defense in Depth”
- Attackers penetrate our computers daily
- Smart phones are unusually vulnerable
- We can and must make it difficult for them
- “Systemic, cascading risk...” given any user who does not follow best practices
- We all have a responsibility to employ proactively, not reactively, best security practices