

Mobile Device Security—How to Secure Mobile Platforms

Speaker: Mr. Loras Even, Principal, Regional
Leader Security and Privacy Services

Institution: McGladrey LLP

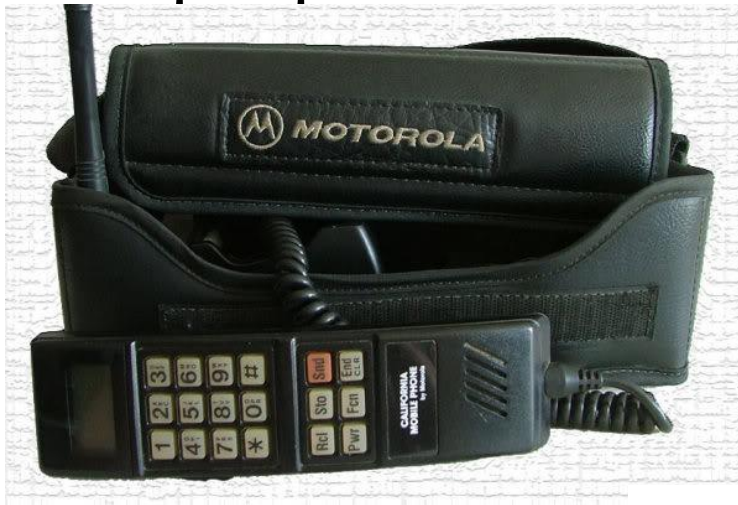
Date: October 7, 2014

Agenda

- * Brief history of mobile devices
- * Current risks
- * Securing Mobile Devices
- * References
- * Q&A

Brief History of Mobile Devices

- * Few people remember this:



- * Or this:



Brief History of Mobile Devices

The iPhone, costing \$200 today, replaces 13 separate devices listed in a 1991 Radio Shack advertisement costing over \$5,000.

Radio Shack
AMERICA'S TECHNOLOGY STORE

PRESIDENTS' BIRTHDAY SALE!

AM-FM Clock Radio: **30% OFF \$1399** HALF PRICE! 799

In-Car Stereo Phones: **30% OFF \$799**

Micro-Timer Calculator: **30% OFF \$499**

3-DAY SPECIALS ABOVE GOOD SATURDAY THRU MONDAY ONLY!

0% \$5,225 in 2013 dollars for 13 products in this ad

TRY! OFFER IS TUESDAY FEBRUARY 19

COME IN AND TAKE ADVANTAGE OF THESE OTHER FANTASTIC VALUES!

INTRODUCTORY SPECIAL!
SMART! 1000 TL12 Computer System: **Save \$670 \$1599**

BONUS PACKAGE
\$1999

VHS Camcorder
Save \$100 \$799

3-Way Speaker With Massive 15" Woofer
Save \$110 \$14995

Mobile Cellular Telephone
Save \$100 \$199

Deluxe Portable CD Player
Save \$40 \$15995

Tiny Dual-Superhet Radar Detector
Save \$80 \$7995

Compact 10-Channel Desktop Scanner
Save \$30 \$995

Mobile CB With Channel Controls on Mike
HALF PRICE! \$4995

Our Easiest-to-Use Phone Answerer
Cut 17% \$4995

20-Memory Speed-Dial Phone
Cut 33% \$2995

Handheld Voice-Activated Cassette Tape Recorder
30% OFF \$2995

Check Your Phone Book for the Radio Shack Store or Dealer nearest you.

Meet Major Credit Cards Welcome

Current Risk—Consumerization

- * Bring Your Own Device (BYOD) push from all employee levels across departments
- * Huge variety of devices and OSs
- * Need to mobilize business in a secure, manageable, scalable fashion... cost effectively!



Current Risks—Support Problems

- * Mobile devices are not typically connected to the “local area network” like workstations, which poses management issues. Most mobile devices have no wired-network provisioned.
 - Data charges for pushing updates to the devices can be expensive.
 - The solution is most commonly a separate WI-FI network in the offices for ONLY these mobile devices.

Current Risks—Support Problems

- * Mobile devices contain more sensitive information per pound than traditional systems.
 - Emails
 - Calendars
 - Local file storage
 - “Secure” management of user IDs/passwords

Current Risks—Support Problems

- * Support staff will have to learn new tools and methods.
 - Mobile device management tools
 - Implementing traditional desktop technologies, such as Citrix on mobile devices
 - Myriad of other considerations
 - Encryption method
 - Alerts
 - Etc.

Current Risks—Support Problems

- * There is a need for flexibility while both parties recognize the need and responsibility to secure them.
 - The devices need to be secured, but they have to be useable.
 - The users need to be responsible for physical security of the device.
 - Users also have to comply security policies.
 - IT management also has to have systems in place for if/when the users disable settings.

Current Risks—Data Leakage Threats

- * Lost devices
 - Will users tell us when they lost it?
 - Does IT have mechanisms in place to be notified when a device may be lost?
 - Best practice would include at least weekly report review for mobile devices that haven't "checked in" for a week or more.
 - GPS should be enabled so that if needed the system can be located when lost.

Current Risks—Data Leakage Threats

- * Bluetooth/USB attacks
 - Every mobile device has Bluetooth some have USB
 - BTScanner—scans for bluetooth system
 - BlueSnarfer—downloads the phonebook
 - BTCrack—breaks the keys used for pairing exchange so attacker can decrypt communications between the mobile device and bluetooth accessories
 - Flash drives, hard drives, etc.

Current Risks—Third-Party Applications

- * Third-party applications
 - The users of mobile devices tend to accumulate a lot of “apps.”
 - A lot of “Free” ones with lots of malware possibly in them.
 - Sometimes the free ones are the bait and then during an upgrade they insert malicious code into the app.
 - Need to be able to monitor and control what they have installed.

Current Risks—By-The-Numbers



How to Secure Mobile Devices

- * **NIST Special Publication 800-124**

<http://csrc.nist.gov/publications/PubsSPs.html#800-124>

Uses standard CIA approach as security objective

Confidentiality—ensure that transmitted and stored data cannot be read by unauthorized parties

How to Secure Mobile Devices

- * **NIST Special Publication 800-124**

Integrity—detect any intentional or unintentional changes to transmitted and stored data

Availability—ensure that users can access resources using mobile devices whenever needed.

Securing Mobile Devices

- * Organization Policies—BYOD Policy
 - Password settings
 - Device wipe
 - Data encryption
 - Appropriate use guidelines
 - Data ownership
 - Approved app list
 - Approved device list
 - User training

Securing Mobile Devices

- * Mobile Device Manager (MDM)
 - There are several solutions available, including:
 - MobileIron, AirWatch, MaaS360, Good Technology and several others.
 - They have many of the reporting, alerting and other capabilities.
 - There are many reports available comparing features, a client sent me this one which I like:
 - <http://tinyurl.com/of3m3f8>

Securing Mobile Devices

- * Mobile Device Manager (MDM)
 - Just like any other security tool, training, and care and feeding of the MDM solution is essential.
 - If you want to host it on-premise, consider training for the administrators that need to support it.
 - If you want to subscribe to a SaaS cloud offering, almost all vendors of MDM offer that option too.

Securing Mobile Devices

- * Incidental cloud usage—Data leakage
 - It is getting more common to see “Clouds” for storage used by apps getting installed onto the mobile devices.
Apple has 1.3 million apps in the store.
 - I did not find a current android quote of numbers, but they went over a million in 2013.
 - Occasionally, these clouds get compromised and the information stored there is at risk.

Securing Mobile Devices

- * Incidental cloud usage—Data leakage
 - Educate users and also determine to what extent your MDM can assist in controlling the applications:
 - Can it scan for applications installed?
 - Can it remove applications that do not comply with policy?

Securing Mobile Devices

- * Virtual guest or Sandboxing on the mobile device.
 - This is similar to desktop virtualization.
 - Most promising security solution, as all data is in an isolated “sandbox,” malware and viruses cannot get to it.
 - Solutions are getting much better and most MDM solutions support it.

Securing Mobile Devices

* User Training

- It is a never ending process, but users should also be trained since they are often the “frontline” when it comes to mobile device security.
- They need to use a PIN, this can also be enforced through the MDM.
- They need to be aware of where the device is at all times—hopefully they won’t lose it!!
- They need to be careful when using free WI-FI; much of it is rogue these days.

Securing Mobile Devices

- * Encryption of the device
 - Apples iOS has an encrypted file system by default.
 - Windows Mobile has Bitlocker built in but feedback is that it is not easy to implement.
 - Android has it built in, but has to be enabled.

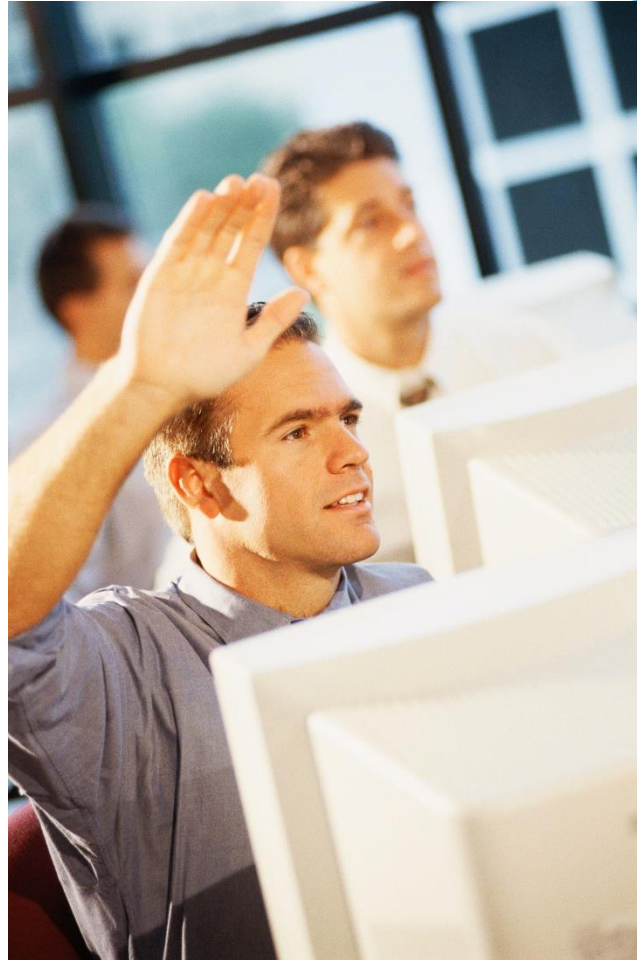
Securing Mobile Devices

- * Virus and malware protection
 - The operating system that powers the mobile devices needs to be protected just like a desktop.
 - Most of the same vendors provide virus and malware protection for the devices.
 - Apple is not as widely available, but McAfee and others offer it.

References

- * Center for Information Security Benchmarks (CIS)
 - They maintain a list of security setting benchmarks for almost ALL mobile devices.
- * NIST Special Publication 800-124
 - A good baseline document describing in good detail what a secure mobile device environment looks like.

Questions?



Thank you

Loras Even

Principal

Regional Leader Security and Privacy Services

McGladrey LLP

319.274.8541

loras.even@mcgladrey.com