Mobile Internet Device Security: Some Introductory Slides

Educause Security Professionals

Atlanta GA, April 12th-14th, 2010

Joe St Sauver, Ph.D.
Internet2 Security Programs Manager
Internet2 and the University of Oregon
(joe@uoregon.edu or joe@internet2.edu)

http://www.uoregon.edu/~joe/mobile-device-security/

Disclaimer: all opinions expressed are those of the author and do not necessarily represent the opinion of any other entity or organization.

The Format Of This Session

- The format of this session is a little different than traditional Educause Security Professionals Sessions:

  -- it is an experimental "Hot Topics" session that combines two presentations by two different speakers on topics of substantial emerging community interest

  -- each lead presenter will do a brief 15-20 minute "introductory" or "framing" presentation, with the remainder of the session reserved for discussion

  -- this session is also being netcast, to allow interested folks who couldn't come to Atlanta to still participate

This Part of Today's Hot Topic Session: Security of Mobile Internet Devices

- For the purposes of this session, we'll define "mobile Internet devices" to be the sorts of things you might expect: iPhones, BlackBerry devices, Android phones, Windows Mobile devices, etc. -- pocket size devices that can access the Internet via WiFi, cellular/3G, etc.

- If you like, we can stretch the definition to include traditional laptops and tablet computers such as the iPad (maybe you have big pockets?), and maybe even conventional cell phones, thumb drives, etc.

- We'll try to draw a hard line at anything that requires fiber connectivity or a pallet jack to move. :-)

Mobile Devices Are Common in Higher Ed

- ECAR Study of Undergraduate Students and Information Technology 2009 (http://www.educause.edu/ers0906):

  > About half of the respondents (51.2%) indicated that they own an Internet capable handheld device, and another 11.8% indicated that they plan to purchase one in the next 12 months [...]

- Faculty/staff ownership of mobile internet devices is more complicated: there are a variety of devices available ("Which one(s) should we support?"), costs of service plans can be high ("It costs how much per month for your data plan???"), and the IRS' treats them oddly (see www.irs.gov/govt/fslg/article/0,,id=167154,00.html)

But Are Mobile Internet Devices Secure?

- Many sites, faced with the *ad hoc* proliferation of mobile devices among their users, have become concerned: ***Are all these new mobile Internet devices secure?***

- Sometimes, that concern manifests itself as questions:
  -- Who has one?
  -- Is there PII on them? What if one get lost or stolen? Does it have "whole device" data encryption? Can we send the device a remote "wipe" or "kill" code?
  -- How are we sync'ing/backing those devices up?
  -- Do we need antivirus protection for mobile devices?
  -- Is all the WiFi/cellular/3G traffic encrypted? Will they work with our VPN (even with VPN hw tokens)?
  -- And how's our mobile device security policy coming?

Let's Start With a Very, Very, Basic Question

- ***Who at your site has a mobile Internet device?***
- You simply may not know -- users will often independently purchase mobile devices (particularly if it's hard/uncommon for a site to do so for its staff)
- Those devices may connect via a third party/commercial network, and *may* not even directly access your servers.
- If those devices *do* access your servers, unless they have to authenticate to do so, you may not know that it is a device belonging to one of your users.
- *Postulated:* If you don't even know who has a mobile Internet device, you probably **also** don't know how they're being configured and maintained, or what data may be stored on them.

A Semi-Zen-like Koan

- ***"If I didn't buy the mobile device, and the mobile device isn't using my institutional network, and the mobile device isn't directly touching my servers, do I even <u>care</u> that it exists?"*** (Not quite as pithy as, "If a tree falls in the forest when no one's around, does it still make any sound?" but you get the idea). **<u>Yes, you *should* care.</u>**

- You may <u>think</u> that that device isn't something you need to worry about, <u>but</u> at some point in the future that WILL change. Suddenly, for whatever reason (or seemingly for no reason) at least some of those devices WILL begin to use your network and/or servers, or some of those devices WILL end up receiving or storing personally identifiable information (PII).

Want Influence? It'll Probably Cost You…

- This is the slide that I hate having to include, but truly, if you want the ability to influence/control what happens on mobile Internet devices on your campus, you're probably going to need to "buy your way in."
- If you purchase mobile Internet devices for your faculty or staff, you'll then have an acknowledged basis for controlling/strongly influencing (a) what gets purchased, (b) how those devices get configured, and (c) (maybe) you'll then even know who may be using these devices.
- Similarly, if you have a discounted/subsidized/required mobile device purchase program for students, you may be able to control/strongly influence what they purchase, how those devices gets configured, etc.
- But buying in may not be cheap…

Mobile Data Plans Are Expensive

- One factor that I believe is an impediment to mobile device deployment at some institutions is the cost of the service plans required to connect the devices. For example, while the iPhone 3GS itself starts at just $199 for qualified customers, the monthly recurring costs currently range from $69.99 to $99.99 from AT&T in the U.S. plus a text messaging plan of up to $20/month. (Domestic service plans for BlackBerry devices, e.g., from Verizon, tend to be comparable). Thus, iPhones for 20,000 users would cost from $1.6 to $2.4+ million/yr!
- If you travel internationally, intl voice and data usage is extra, ranging from $24.99/month for 20MB to $199.99/month for 200MB. Over those limits, usage runs from $5/MB to $20/MB (ouch). (You may want to consider disabling data roaming while traveling abroad.)

Are We Seeing A Recapitulation of The Good Old "Managed vs. Unmanaged PCs" Paradigm?

- For a long time way back in the "old days," traditional IT management pretended that PCs didn't exist. While they were in "denial," people bought whatever PCs they wanted and "administered" them themselves. While that sometimes worked well, other times chaos reigned.
- Today's more closely managed "enterprise" model was the result of that anarchy. At some sites, standardized PC configurations are purchased and tightly locked down and are then centrally administered. While I'm not a fan of this paradigm, I recognize that it is increasingly common.
- Are we re-experiencing that same evolution for mobile Internet devices? Or are we still denying that mobile Internet devices even exist? What policies might we see?

An Example Device Policy: Device Passwords

- If a mobile Internet device is lost or stolen, a primary technical control preventing access to/use of the device is the device's password.
- Users hate passwords, but left to their own devices (so to speak), they might use a short (and easily overcome) one such as 1234
- You/your school might prefer that users use a longer and more complex password, particularly if that mobile Internet device is configured to automatically login to your VPN or the device has sensitive PII on it. You might even require use of two factor auth for your VPN, or require the device to wipe itself if it detects that it is the target of an password brute force attack.
- <u>If</u> the device is managed, you **<u>can</u>** require these things.

Managing Mobile Internet Device Policies

- Because Blackberries (42.1% U.S. market share as of April 2010 reports, see tinyurl.com/comscore-mkt-share) and iPhones (25.4% U.S. market share) are the most popular mobile Internet devices, we'll focus on them for the following discussion. (Usage patterns will likely vary in higher ed, but if anything, I'd expect a greater iPhone market share in higher ed than anything else)
- Both RIM and Apple offer guidance for configuring and centrally managing their mobile Internet devices in an enterprise context. If you're interested in what it would take to centrally manage these devices and you haven't already seen these documents, I'd urge you to see:

  -- na.blackberry.com/eng/ataglance/security/it_policy.jsp
  -- manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Example:
What Can Be Required for iPhone Passwords?

- Looking at the iPhone Enterprise Deployment Guide:

  -- you can require the user *have* a password
  -- you can require a *long*/*complex* password
  -- you can set max number of failures (or the max days of non-use) before the device is wiped out (the device can then be restored from backup via iTunes)
  -- you can specify a maximum password change interval
  -- you can prevent password reuse via password history
  -- you can specify an interval after which a screen-lock-like password will automatically need to be re-entered

- RIM offer similar controls for BlackBerry devices.

Other Potential Local iPhone "Policies" Include

- Adding or removing root certs
- Configuring WiFi including trusted SSIDs, passwords, etc.
- Configuring VPN settings and usage
- Blocking installation of additional apps from the AppStore
- Blocking Safari (e.g., blocking general web browsing)
- Blocking use of the iPhone's camera
- Blocking screen captures
- Blocking use of the iTunes Music Store
- Blocking use of YouTube
- Blocking explicit content

- Some of these settings may be less applicable or less important to higher ed folks than to corp/gov users.

Scalably Pushing Policies to the iPhone

- To configure policies such as those just mentioned on the iPhone, you can use configuration profiles created via the iPhone Configuration Utility (downloadable from http://www.apple.com/support/iphone/enterprise/)
- Those configuration files can be downloaded directly to an iPhone which is physically connected to a PC or Mac running iTunes -- but that's not a particularly scalable approach. The configuration files can also be emailed to your user's iPhones, or downloaded from the web per chapter two of the Apple Enterprise Deployment Guide.
- **While those configuration files need to be signed (and can be encrypted), there have been reports of flaws with the security of this process; see "iPhone PKI handling flaws" at cryptopath.wordpress.com/2010/01/**

What's The 'Big Deal' About Bad Config Files?

- If I can feed an iPhone user a bad config file and convince that user to actually install it, I can:

  -- change their name servers (and if I can change their name servers, I can totally control where they go)
  -- add my own root certs (allowing me to MITM their supposedly "secure" connections)
  -- change email, WiFi or VPN settings, thereby allowing me to sniff their connections and credentials
  -- conduct denial of service attacks against the user, including blocking their access to email or the web

- **These config files also can be made non-removable (except through wiping and restoring the device).**

We Need to Encourage "Healthy Paranoia"

- Because of the risks associated with bad config files, and because the config files be set up with attributes which increase the likelihood that users may accept and load a malicious configuration file, **iPhone users should be told to NEVER, EVER under any circumstances install a config file received by email or from a web site.**
- Of course, this sort of absolute prohibition potentially reduces your ability to scalably and securely push mobile Internet device security configurations to iPhones, but…
- This issue also underscores the importance of users routinely sync'ing/backing up their mobile devices so that if they have to wipe their device and restore it from scratch, they can do so without losing critical content.

Mobile Device Forensic Tools

- What if an iPhone **IS** lost/stolen/seized/confiscated, what sort of information might be able to be recovered?
- See the book "iPhone Forensics" by Jonathan Zdziarski, http://oreilly.com/catalog/9780596153595
- Some (of many) potential tools (in alphabetical order):
  -- Device Seizure, http://www.paraben.com/
  -- iPhone Insecurity, http://www.iphoneinsecurity.com/
  -- Lantern, http://katanaforensics.com/
  -- Oxygen, http://www.iphone-forensics.com/

  Notes: Some tools may only be available to gov/mil/LE. Also, if you must jailbreak an iPhone to use a tool, this may complicate use of resulting evidence for prosecution
- Interesting review from 2009: viaforensics.com/wpinstall/wp-content/uploads/2009/03/iPhone-Forensics-2009.pdf

What About Hardware Encryption?

- An example of a common security control designed to protect PII from unauthorized access is hardware encryption. For example, many sites require "whole disk" encryption on all institutional laptops containing PII.
- Some mobile Internet devices (such as earlier versions of the iPhone) did not offer hardware encryption; 3GS iPhones now do. **However, folks have demonstrated that this is less-than-completely bullet proof [cough]; see for example Dr NerveGas (aka Jonathan Zdziarski's) demo "Removing iPhone 3G[s] Passcode and Encryption," http://www.youtube.com/watch?v=5wS3AMbXRLs**
- This lack of hardware encryption may make it difficult to securely use even a 3GS iPhone for PII or other sensitive data.

Hardware Encryption on the BlackBerry

- Hardware encryption on the BlackBerry is described in some detail in "Enforcing encryption of internal and external file systems on BlackBerry devices," see http://docs.blackberry.com/en/admin/deliverables/3940/file_encryption_STO.pdf
- If setting encryption manually, be sure to set
  -- Content Protection, AND
  -- Enable Media Card Support, AND Encrypt Media Files
- If setting encryption centrally, be sure to set all of...
  -- Content Protection Strength policy rule
  -- External File System Encruption Level policy rule
  -- Force Content Protection for Master Keys policy rule
- For "stronger" or "strongest" Content Protection levels, set min pwd length to 12 or 21 characters, respectively

Remotely Zapping Compromised Mobile Devices

- Strong device passwords and hardware encryption are primary protections against PII getting compromised, but another potentially important option is being able to remotely wipe the hardware with a magic "kill code." Both iPhones and BlackBerry devices support this option.
- Important notes:
  -- If a device is taken off the air (e.g., the SIM card has been removed, or the device has been put into a electromagnetic isolation bag), a device kill code may not be able to be received and processed.
  -- Some devices (including BlackBerries) acknowledge receipt and execution of the kill code, others may not.
  -- Pre-3GS versions of the iPhone may take an hour per 8GB of storage to wipe; 3GS's wipe instantaneously.

Terminating Mobile Device-Equipped Workers

- A reviewer who looked at a draft of these slides pointed out an interesting corner case for remote zapping:
  -- Zap codes are usually transmitted via Exchange Active Sync when the mobile device connects to the site's Exchange Server, and the user's device authenticates
  -- HR departments in many high tech companies will routinely kill network access and email accounts when an employee is being discharged to prevent "incidents"
  -- If HR gets network access and email access killed before the zap code gets collected, the device may not be able to login (and get zapped), leaving the now ex-employee with the complete contents of the device

  See: http://tinyurl.com/zap-then-fire
- Of course, complete device backups may *also* exist…

Mobile Devices as Terminals/X Terminals

- One solution to the problem of sensitive information being stored on mobile Internet devices is to transform how they're used.
- For example, if mobile Internet devices are used solely as terminals (or X terminals), the amount of sensitive information stored on the device could presumably be minimized (modulo caching and other incidental PII storage).
- iPhone users can obtain both ssh and X terminal server applications for their devices from www.zinger-soft.com and other vendors
- It is critical that communications between the mobile device and the remote system be encrypted (including having X terminal session traffic securely tunneled)

Web Based Applications on Mobile Devices

- Of course, most sites don't rely on terminal or X term apps any more -- everything is done via a web browser.
- So what web browsers can we use on our mobile devices? (some sites strongly prefer use of particular browsers)
- On the iPhone, **Safari is the only true web browser normally available** (Firefox, for example, isn't and won't be available: https://wiki.mozilla.org/Mobile/Platforms)
- Opera Mini was submitted to the Apple App Store on March 23rd, 2010, but note that Opera Mini differs from "regular" Opera in that remote servers are used to render what Opera Mini displays (and they auto-"MITM" secure sites for you, see www.opera.com/mobile/help/faq/#security)
- What about BlackBerry users? Just like iPhone users, BlackBerry users can run Opera Mini but not Firefox.

Back End Servers Supporting Mobile Devices

- Many mobile Internet apps, not just Opera Mini, rely on services provided by back end servers, sometimes servers which run locally, sometimes servers which run "in the cloud."
- If those servers go down, your service may be interrupted. This is a real risk and has happened multiple times to BlackBerry users; recent examples include:

  -- "International Blackberry Outage Goes Into Day 2," March 9th, 2010, http://tinyurl.com/intl-outage-2nd-day

  -- "BlackBerry users hit by eight-hour outage," December 23rd, 2009, www.cnn.com/2009/TECH/12/23/blackberry.outage/index.html

- Availability is, or can be, another critical consideration.

What Do Your Key Websites Look Like On Your Mobile Internet Device?

- Web sites optimized for fast, well-connected computers with large screens may not look good or work well on mobile devices. If those sites are running key applications, a lack of mobile device app usability may even be a security issue (for example, normal anti-phishing visual cues may be hard to see, or easily overlooked on a knock-off "secure" site).
- Have you looked at your home page and your key applications on a mobile Internet device? How do they look? One web site which may help open your eyes to the need for a redesign (or at least a separate website for mobile devices) is http://www.testiphone.com/
- Should you create an http://m.<yoursite>.edu/ page?

Malware and A/V on Mobile Devices

- Because Apple disallows applications running in the background, it is difficult for traditional antivirus products to be successfully ported to the iPhone. On the other hand, since the iPhone uses a sandbox and a cryptographically "signed app" model, it is also difficult for the iPhone to get infected.
- All bets are off, however, if you jailbreak your iPhone so that it can run non-Apple-approved applications. Malware which has targeted jailbroken iPhones has (so far) been targeting unchanged OpenSSh passwords for the root and/or mobile accounts (which defaults to "alpine") :
  -- the "ikee" worm (aka "RickRolling" worm)
  -- the "Duh" worm (which changed "alpine" to "ohshit", scanned for other vulnerable iPhones, and stole data)
  -- the "iPhone/Privacy.A" (stole data/opened a backdoor)

Speaking of Jail Breaking the iPhone…

- Blackra1n is one of the most well known tools for jail breaking the iPhone (so it can run non-Apple-approved apps. Jailbreaking your iPhone violates the license agreement and voids the warranty, but it is estimated that 5-10% of all iPhone users have done so.
- When a jail broken iPhones gets an OS upgrade, the jailbreak gets reversed/must typically be redone. This may cause some users of jail broken iPhones to be reluctant to apply upgrades (even upgrades with critical security patches!). That is obviously a potential security issue and cause for concern.
- While regular iPhones usually get apps from the iTune Apps Store, jail broken phones can get apps from 3rd party repositories such as Cydia. It is unclear how much vetting new apps get before being listed at Cydia.

Counterfeit Hardware

- Counterfeit computer and network hardware is a major concern for some manufacturers and the U.S. government
- Knock-off iPhones are currently being seen in the U.S. One good description of a knock off iPhone is available at http://www.macmedics.com/blog/2009/06/27/counterfeit-iphone-3g-stops-by-macmedics-by-way-of-disputed-ebay-auction/
- Apple and legal authorities are putting pressure on the sources of some of these knock-offs (e.g., see "Chinese Counterfeit iPhone Workshop Raided," Jan 20, 2010, http://www.tuaw.com/2010/01/20/chinese-counterfeit-iphone-workshop-raided/), but until this problem is resolved (if ever!) you should be on guard against counterfeit hardware from 3rd party sources.

Are Mobile Internet Devices Tough Enough?

- Mobile devices, even more so than laptops, can be exposed to pretty tough conditions -- pockets and belt holsters can be pretty unforgiving places. Mobile devices end up getting dropped, exposed to moisture (especially here in the Northwest!), extremes of temperature, etc. Are mobile Internet devices tough enough to hold up?
- Specialized extra-rugged devices (such as the GD Sectera) are available to users in the gov/mil/three letter agency markets, but those devices are typically expensive and heavy compared to traditional mobile Internet devices, and are unavailable to those of us who do not hold federal security clearances.
- The rest of us may best off just improvising at least partial protection with inexpensive water tight cases from vendors such as drycase.com or otterbox.com

Discussion Time!

- Now that we've finished outlining some of the security issues that we think may be associated with mobile Internet devices, we'd like to hear what you think!
- Are you and your users embracing mobile Internet devices? What kind? iPhones? BlackBerries? Other?
- What's been your experience? Successes? Challenges?
- Who's the biggest advocate of mobile devices at your site? Students? Faculty members? Administrators?
- Do you have a campus mobile device policy?
- Do you have a designated group on campus that serves as the point of contact for mobile device support?
- How are you control PII exposure on those devices?
- Are you satisified with your devices backups?
- What would YOU like to talk about around this topic?