

Securing Mobile Devices

Security Professionals 2011 Preconference Seminar

8:30-12:00, Monday, April 4th, 2011

Bonham D/Third Level, Grand Hyatt, San Antonio TX

Joe St Sauver, Ph.D.

Nationwide Internet2 Security Programs Manager

Internet2 and the University of Oregon

(joe@uoregon.edu or joe@internet2.edu)

Marcos Vieyra (MVIEYRA@mailbox.sc.edu)

Information Security Manager, Univ. of South Carolina

<http://pages.uoregon.edu/joe/securing-mobile-devices/>

Acknowledgement and Disclaimer

- We'd like to thank Educause and Internet2 for the opportunity to offer this preconference seminar at Security Professionals 2011 San Antonio.
- Because all of us wear a variety of different "hats" from time-to-time, let's just keep this talk straightforward by offering the following simple disclaimer: the opinions expressed in this talk are solely those of the authors, and do not necessarily reflect the opinion of any other entity.

Format of This Session

- Rather than doing this session as just a straight lecture (as we sometimes do), we wanted to try to have this be a (more fun!) interactive session.
- What we hope to do today is introduce a series of topics, offer some observations, and then encourage you, the audience, to participate in a discussion of each issue raised.
- Let's begin with introductions...

Introductions

- As we go around the room, please say:
 - your name
 - the school you're with
 - what you do there (are you a technical security guy? a CIO? a security policy person? something else?)
 - is there anything in particular that inspires your interest in mobile device security?
 - is there anything in particular you really want to make sure we talk about during today's pre-conference seminar?
 - if you've got a mobile Internet device (from your institution or personally purchased), what kind is it?

1. What Is A Mobile Device?

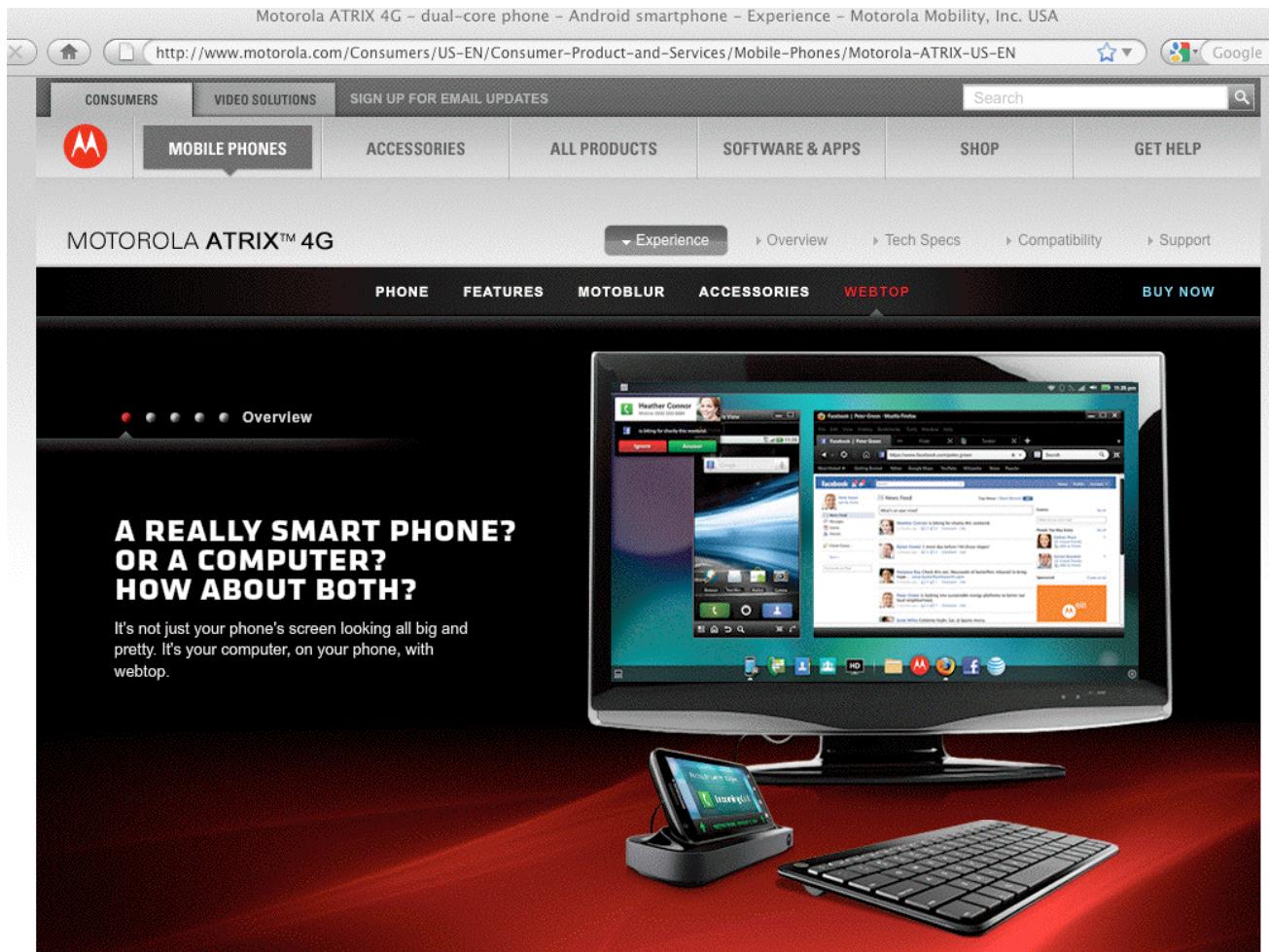
""I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it [...]"

Mr. Justice Potter Stewart,
Jacobellis v. Ohio (378 U.S. 184, 1964)

iPhones, BlackBerries, etc.

- We generally think of a “mobile Internet devices” as 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 cellular/3G/4G, WiFi, etc.
- If you like, we can stretch the definition to include tablet computers such as the iPad/iPad2 (maybe you have big pockets?), and maybe even include conventional laptops, regular cell phones, etc.
- We’ll try to draw a hard line at anything that requires fiber connectivity or a pallet jack to move. :-)
- But in all seriousness, what about devices such as the Motorola Atrix 4G?

Motorola Atrix 4G



There's also a laptop dock for the Atrix 4G now... 7

Discussion: What's Considered A "Mobile Device" At Your School?

- *What about at your school?*
- *Do you have a formal definition of what's considered a mobile Internet device, or is it just informally "understood?"*
- *Does it even matter how we define them?*
- *Note: If mobile Internet devices are "just like laptops," and we can (and do) treat them the same way, maybe we don't really need anything new/different?*

Potentially Relevant Differences

- Does it matter that most mobile devices run a specialized mobile operating system, rather than Windows or OS/X?
- Applications on mobile devices are often obtained from application stores. Does this help secure those devices?
- Many mobile devices are privately purchased. Is this a blessing (or a curse)?
- Most mobile devices are cellular/3G/4G capable, and don't "need" our networks (although they often can and will take advantage of them when they're available).
- Mobile devices are usually smaller ("pocket-sized"), with small screens and small keyboards, and limited native I/O options (such as USB ports), and integrated media (a CD or DVD drive would be bigger than the device itself!)

Similarities?

- **Same Users:** the same folks who use laptops or desktops are also using mobile Internet devices
- **Same Applications:** users want access to everything on the web, their email, etc.
- **Same Personally Identifiable Information:** mobile devices can access and store institutional PII just like a laptop or desktop
- **Same Physical Security Issues:** nothing makes mobile devices immune to damage, loss or theft
- **Same (or Similar) Short Device Life Cycle:** mobile Internet devices have a limited lifecycle (2 years?), which is similar to more traditional devices such as laptops (3-5 year lifecycles)
- And we're still expected to support "everything" :-)

Decision Point: A Potentially Strategic Choice

Should your institution treat mobile Internet devices as “just another computer?”

Note: we will not pretend to offer you the “right” answer to this (or other) questions!

We do urge you to keep these questions in mind, as we talk, however...

2. Are Our Users Embracing Mobile Devices?

After all, if “no one’s” using mobile devices, they might be something that we could just ignore (at least for now!)

Not much chance of that, unfortunately...

Students ARE Using Mobile Devices

- ECAR Study of Undergraduate Students and Information Technology 2010 (<http://www.educause.edu/ers1006>):

Do you own a handheld device that is capable of accessing the Internet (whether or not you use that capability)? Examples include iPhone, Treo, Blackberry, PocketPC, etc. [responses shown are for 4 yr schools]

Yes	62.9%
No, but I plan to purchase one in the next 12 months	11.1%
No, and I do NOT intend to purchase one in the next 12 months	24.6%
Don't know	1.3%

How About Faculty/Staff? Yep, Them Too...

- Faculty/staff ownership of mobile internet devices is more complicated: historically the IRS has treated them oddly (<http://www.irs.gov/govt/fslg/article/0,,id=167154,00.html>) although thankfully that issue has been untangled courtesy of good old Section 2043 of H.R. 5297 (the “Small Business Jobs Act of 2010”), signed into law by the President on September 27th, 2010.
- Nonetheless, many employers continue to treat mobile devices as if they are uniquely rare and particularly expensive toys, rather than a way to retain critical access to employees virtually around the clock. Mobile devices/cell phones *are* a particular favorite target for budget cutting witch hunts. For example, California just recently announced...

The screenshot shows a web browser window with the URL <http://gov.ca.gov/news.php?id=16875>. The page title is "GOVERNOR BROWN ORDERS MASSIVE CELL PHONE CUTBACK FOR STATE EMPLOYEES". Below the title, the date "1-11-2011" is listed. The main text discusses Governor Jerry Brown's executive order to collect and turn in 48,000 government-paid cell phones by June 1, 2011. It mentions that the state now pays for 96,000 cell phones, one for 40 percent of all state employees, and estimates a \$20 million annual savings by cutting usage in half. The Governor quotes as saying it's difficult to believe that 40 percent of employees must have cell phones. Brown's goal is to cut the number in half by June 1, and he explains that some phones may be under contract, so early termination penalties must be considered. He also notes that it might be possible to eliminate all phones by June 1. The final quote states that even with a 50% reduction, one-fifth of employees will still have phones, so departments and agencies should examine usage. Brown's estimate of at least \$20 million in annual savings assumes an average monthly bill of over \$36.

GOVERNOR BROWN ORDERS MASSIVE CELL PHONE CUTBACK FOR STATE EMPLOYEES

1-11-2011

SACRAMENTO – In his first executive order since taking office, Governor Jerry Brown today directed state agency and department heads to collect and turn in 48,000 government-paid cell phones—half of those now in use—by June 1, 2011.

Brown said the state now pays for 96,000 cell phones, one for 40 percent of all state employees. He estimated that the state will save at least \$20 million a year by cutting cell phone usage in half.

"It is difficult for me to believe that 40 percent of all state employees must be equipped with taxpayer-funded cell phones," the Governor said. "Some state employees, including department and agency executives who are required to be in touch 24 hours a day and seven days a week, may need cell phones, but the current number of phones out there is astounding."

Brown said his goal is to cut the number of phones in half by June 1, and said he believes the state can continue to reduce cell phone usage throughout the year. He explained that some cell phones may be under term contracts with cell carriers, and he wants to make sure that the state does not incur early termination penalties that exceed the monthly savings.

"Because of contract obligations, it is possible that we may not be able to eliminate all 48,000 cell phones by June 1, but it is also conceivable that we can do it earlier – and that is my hope," Brown said.

"Even with a 50 percent reduction, one-fifth of all state employees will still have cell phones," he said. "That still seems like too much and I want every department and agency to examine and justify all cell phone usage."

Brown's estimate of at least \$20 million in annual savings assumes that the average cell phone bill is a bit over \$36 a month, which the Department of Finance has determined is the average cost.

For context,
the Governor of
California's budget
for 2011-2012 shows
total expenditures
of \$123,371 million

$$\begin{aligned} & 20 / 123,371 * 100 \\ & = 0.0162\% \end{aligned}$$

<cough>

What About Your Site?

- Are students and faculty/staff enthusiastically adopting mobile Internet devices at your site? Are you experiencing pressures to economize by defunding institutional mobile devices?
- Anyone doing hard measurements of mobile device adoption trends at their site (formal user surveys, for example)?
- When dealing with mobile devices, one of the most influential decisions you may want to try to influence is the choice of mobile device type. Are people buying Android devices? BlackBerries? iPhones? Something else?

3. Mobile Device Operating Systems

What should people buy?
What should we support?

Starting With What We Know

- In the traditional desktop/laptop world, our choices for the question “What should we support?” are simple:
 - everyone supports some flavor of Microsoft Windows
 - most of us also support Mac OS X
 - some of us even support other operating systems such as Linux or *BSD or OpenVMS or [whatever]
- We have expertise, specialized tools and techniques, and documentation ready to support this (relatively small) number of platforms – because it’s just a few platforms.
- The world is a little more complex in the mobile internet device space. What should we support there?

One Approach: Software Quality?

- Just as Secunia tracks vulnerabilities and patches for traditional desktop and laptop computer systems, Secunia also tracks vulnerabilities for mobile Internet devices:
 - Blackberry Device Software 5.x:
secunia.com/advisories/product/32505/?task=advisories
 - iPhone OS (iOS) 4.x:
secunia.com/advisories/product/31370/?task=advisories
 - Microsoft Windows Mobile 6.x:
secunia.com/advisories/product/14717/?task=advisories
 - Palm Pre Web OS 1.x:
secunia.com/advisories/product/26219/?task=advisories
- [No Secunia page for Android currently]

Is software “quality” a decision criteria in selecting devices?

Some Stats From Secunia As of 4/1/2011

- Blackberry Device Software 5.x: 1 advisory, 1 vulnerability, 1 unpatched, most severe unpatched: less critical
- iPhone OS (iOS) 4.x: 6 advisories, 131 vulnerabilities, 2 advisories unpatched, most severe unpatched: highly critical
- Microsoft Windows Mobile 6.x: 1 advisory, 1 vulnerability, 1 unpatched, most severe unpatched: less critical
- Palm Pre Web OS 1.x: 7 advisories, 14 vulnerabilities, 1 advisory unpatched, most severe unpatched: moderately critical
- No Secunia page for Android currently

Note: Secunia specifically urges users NOT to make inter-product comparisons of this sort!

Discussion: Software Vulnerabilities

- Should software “quality” be a decision criteria in selecting which devices to support?
- If a vendor has no reported vulnerabilities, does that mean that there aren’t any vulnerabilities? Or does it actually mean that there may be many latent vulnerabilities that simply haven’t been found and patched yet?
- What if a vendor has “lots” of vulnerabilities, but quickly gets them all patched?
- What do you all think as security professionals?

One Likely Strategy: Support What's "Popular"

- If you don't have a better strategy, many sites will support what's most popular.
- So what are the most popular Internet mobile devices?
- Well, it can vary, depending on whether we're talking about just the US, or we're more concerned with global markets...

Mobile Internet Devices, U.S. Market Share

- Reportedly, U.S. market share information as of Jan 2011 (see tinyurl.com/comscore-mkt-share-3) looked like:

-- Google (Android):	31.2%
-- Research In Motion (e.g., Blackberry):	30.4%
-- Apple (iPhones):	24.7%
-- Microsoft (Windows Mobile)	8.0%
-- Palm (Palm Pixi, Palm Pre, etc.)	3.2%
-- Other	2.5%
- Nice three way “horse race” there, eh?

A Second Take On Smart Phone Market Share

- Worldwide smart phone market share, 29 Mar 11, IDC
(www.idc.com/getdoc.jsp?containerId=prUS22762811)

-- Google (Android):	39.5%
-- Symbian	20.9%
-- Apple (iPhones):	15.7%
-- Research In Motion (e.g., Blackberry):	14.9%
-- Microsoft (Windows Mobile)	5.5%
-- Other	3.5%

- Hmm. Should the take away be that we can discount or ignore Microsoft/Windows Mobile?

I Would NOT Count Microsoft Out Yet...

- “IDC predicts that by 2015, the Nokia-Microsoft partnership will produce the second largest market share at 20.9 percent, behind only Android, whose share will grow to 45.4 percent. Apple's iOS will remain third with 15.3 percent, followed by the BlackBerry OS with 13.7 percent. With Nokia all but abandoning the Symbian OS, its CAGR between 2011 and 2015 will be a 65 percent loss, resulting in a 0.2 percent market share in 2015.”
(see <http://tinyurl.com/mobile-2015>)

What About Palm?



A screenshot of a web browser window. The title bar says "HP CEO: WebOS on all our PCs in 2012 | Circuit Breaker - CNET News". Below the title bar are standard browser controls: back, forward, home, and search. The URL "http://news.cnet.com/8301-31021_3-20041158-260.html" is displayed. The main content area shows the article title and author information.

March 9, 2011 9:37 AM PST

HP CEO: WebOS on all our PCs in 2012

by Erica Ogg

[A](#) [A](#) Font size [Print](#) [E-mail](#) [Share](#) [57 comments](#)



Tweet

123



Recommend

Starting next year, Hewlett-Packard will include its mobile operating system, WebOS, on every PC it ships, according to a story quoting new CEO Leo Apotheker. WebOS will be offered in addition to Microsoft's Windows, not as a replacement.

Apotheker reportedly made the comment in [an interview with Bloomberg Businessweek](#). The motive for doing that is to augment the reach of the WebOS platform and [hopefully attract more developers](#). There are currently 6,000 apps for WebOS, compared to 350,000 in Apple's App Store, and 250,000 in Google's Android Market. And while WebOS phone sales are far behind iPhones, and Android phones, HP is the largest PC maker in the world, selling more than 60 million units last year.

HP acquired WebOS when it bought Palm last year. WebOS was designed as the operating system for Palm smartphones, though HP has reworked the software to also work with its new line-up of [tablets](#).



HP CEO Leo Apotheker.
(Credit: Dan Farber/CBS Interactive)

Symbian? (EOL? I Don't Know...)

Symbian source code released by Nokia

http://www.ubergizmo.com/2011/04/symbian-source-code-released-by-nokia/

Symbian source code released by Nokia

By George Wong 04/01/2011, 5:17 am PT

Just to confirm with people that they're finally done with the aging operating system, Nokia has released the source code to the latest version of Symbian to the public. Originally a job for the Symbian Foundation, Nokia took over when the foundation closed its doors late last year. Now the code for the Symbian platform is out in the wild, as well as the SDK and build tools. Now other developers can take Symbian and pick up where Nokia left off, and hopefully they'll be creating something new in the process – maybe a heavily modified, homebrew version of Symbian that would make even Android and iOS users want to use? (Although highly unlikely) What we do know is that Nokia is finally saying goodbye to Symbian as it prepares itself for the arrival of Windows Phone on their hardware. Bad news for the Symbian devices coming out later this year though – when people find out there's no more love for the operating system from the parent company, will they even be bothered to give those new Symbian phones a shot?



But Android's also open source... source.android.com

How Does Choice of Mobile Operating Systems Relate to Security?

- Please agree or disagree with the following statements...
 - 1) All mobile operating systems are equally secure
 - 2) We have enough resources to support “everything.”
For example, we have sample devices for all supported operating systems, so staff can get familiar with them
 - 3) We can easily keep up with new vulnerabilities on all mobile platforms
 - 4) If we needed to do forensics on any sort of mobile Internet device, we have the software tools and professional expertise to do so in a way that will survive close legal scrutiny
 - 5) [your item here...]

4. But We Need To Support Particular Operating Systems to Get the Hardware Devices That Users Demand!

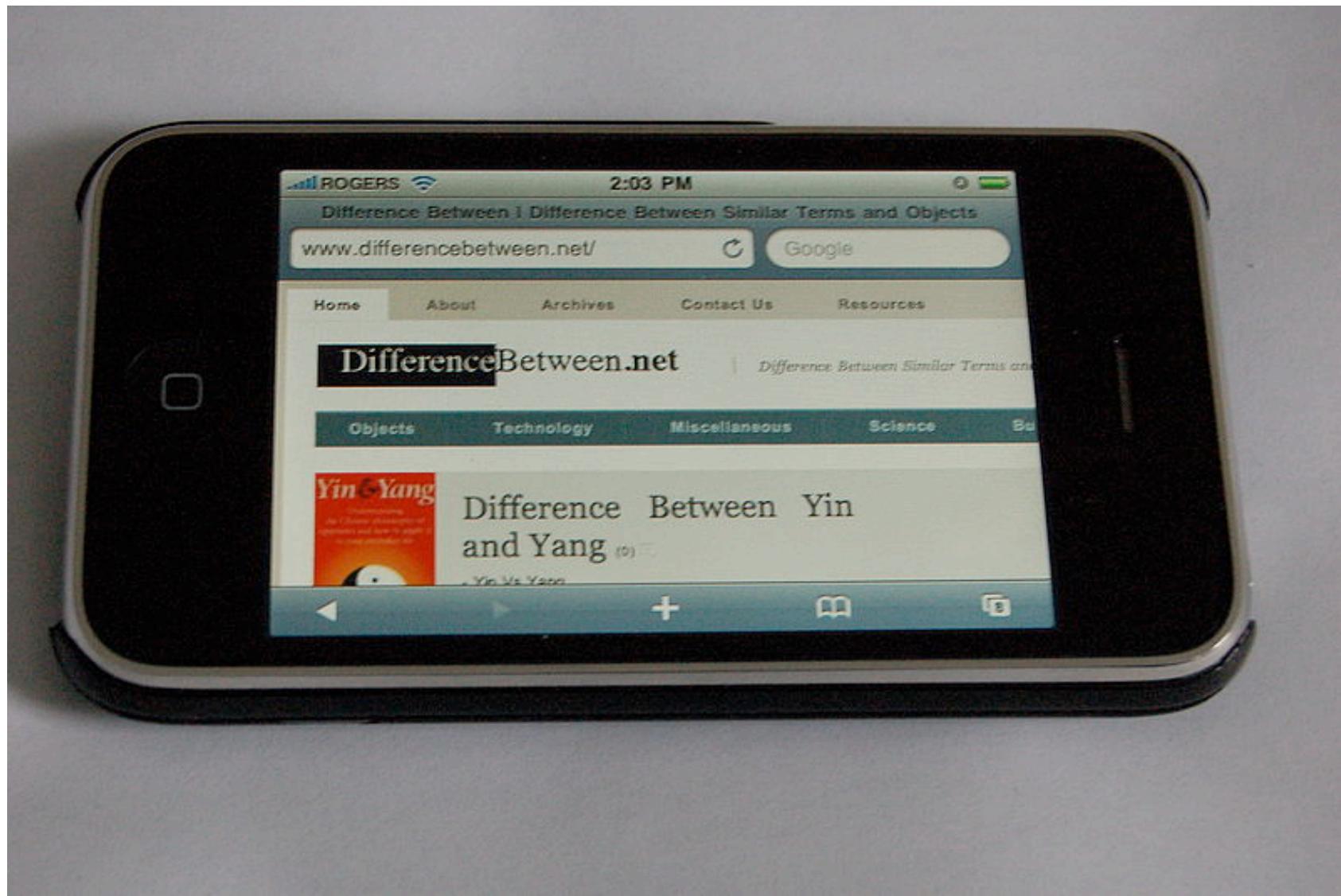
Do handset hardware features drive OS adoption? Or vice versa?

These Days Most Vendors Are Making Mobile Internet Devices in All Popular Form Factors

- Some types of device hardware are exceptionally popular
- You're going to see a lot of "touch screen devices" that (sort of) look or act like iPhones.
- You're going to see a lot of "exposed QWERTY keyboard devices" that (sort of) look or act like classic BlackBerries.
- Slide open-format devices are also quite common.
- See the following examples...

- Take away: you may not need to buy an iPhone to get a touch screen interface, or a Blackberry to get a QWERTY keyboard interface...

Sample Apple iPhone 4



Sample Blackberry Devices



[commons.wikimedia.org/wiki/
File:Blackberry_Storm.JPG](https://commons.wikimedia.org/wiki/File:Blackberry_Storm.JPG)



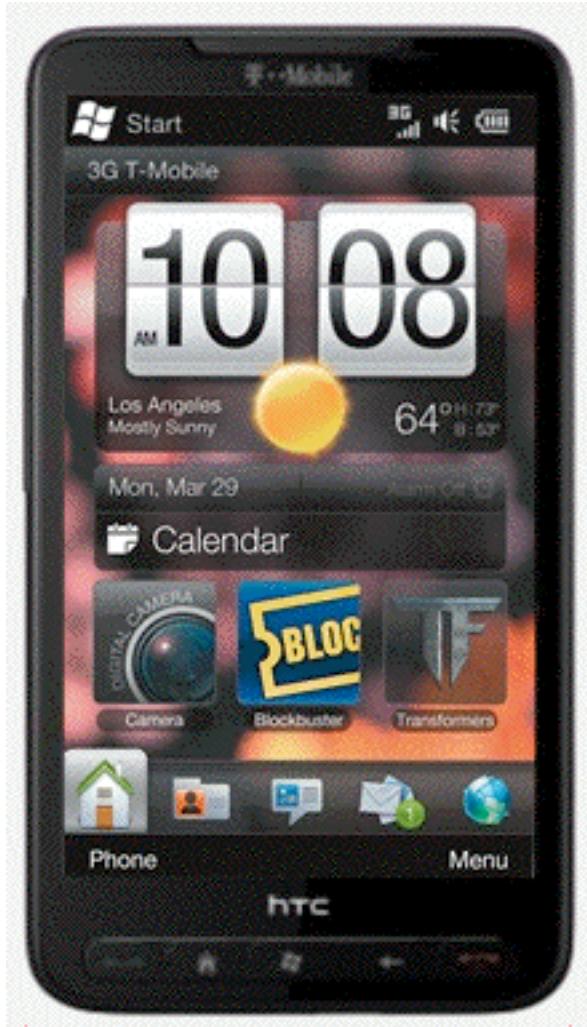
[commons.wikimedia.org/wiki/
File:BlackBerry_Curve_8330.png](https://commons.wikimedia.org/wiki/File:BlackBerry_Curve_8330.png)

Sample Android Device



[www.motorola.com/Consumers/US-EN/Consumer-Product-and-Services/
Mobile-Phones/ci.Motorola-DROID-2-US-EN.vertical](http://www.motorola.com/Consumers/US-EN/Consumer-Product-and-Services/Mobile-Phones/ci.Motorola-DROID-2-US-EN.vertical)

Sample Windows Mobile Device



htchd2.t-mobile.com/touch-screen-phones



tinyurl.com/samsung-windows-mobile

Sample Symbian Devices



europe.nokia.com/find-products/devices/nokia-c6-00

Why Not Just Support “Everything?”

- Device support costs can kill you! Sites need to buy the devices themselves, and build documentation, and *Maintain connectivity* for that stable of devices, and this gets harder (and more expensive!) as the number of mobile devices you support increases. It’s crazy to try to keep “one of everything” on hand when at least some products may rarely get purchased and used by your local users.
- In other cases, while two or three products may *seem* to be quite similar, one may in fact be decidedly better than other “similar” alternatives.
- If you’re already supporting a “best of breed” product there’s little point to supporting an “also ran” contender.
- In still other cases, at least some faculty/staff may be strongly encouraged (or required) to purchase service or devices listed on a mandatory/exclusive contract. ³⁶

5. Mobile Device Choices and Contracting Issues

Institutional cell phone contracts can be a Pandoras box



Free
Nokia 2720
850/1900
GSM/EDGE



Free
Nokia 6350
850/900/1800/1900
GSM/GPRS/EDGE



8 GB \$99
3Gs iPhone
***Requires 2yr
Contract.

30 day return policy,
10% restock fee.



16 GB \$199
 32 GB \$299
iPhone 4
***Requires 2yr
Contract.

Restrictions Apply,
not all users eligible.

RATE PLANS:

Nation 450 w/rollover min \$32.39/mo**
Nation 900 w/rollover min \$48.59/mo**
Unlimited \$69.99/mo

**Includes: Unlimited M2M, Nights & Wkds

Data Plan:

2GB DataPro Enterprise \$32.40
Add'l 1GB will automatically be added at
\$10/GB

Unlimited data \$36.45*
(*could be discontinued at any time)

TEXT Messages:

.20ea in/outgoing
.30ea pix/video
200 messages \$0*
1500 messages \$15

+taxes & \$5/mo Admin Fee

← AT&T Plan

Verizon Plan →



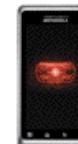
Free**
Samsung Convoy*



Free**
Samsung Gusto



\$199-299**
16 or 32G iPhone 4



\$199.99**
DROID2 by Motorola

***Subject to change without notice.*

RATE PLANS:

Local Flat Rate*:
\$8.99/mo, .10/min
.20/LD, .69/Roam (Outside OR/WA)

National Flat Rate*:
\$11.99/mo, .25/min

*NO included minutes & not compatible w/all phones.

America's Choice National:

450 min \$33.19/mo
900 min \$49.79/mo
Unlimited \$58.09/mo

+taxes & \$5/mo Admin Fee

Includes: Unlimited M2M, Nights & Wkds

Voice & Data Bundles (PDA or BB):

400 min & Unlimited Email \$49.11/mo
600 min & Unlimited Email \$62.77/mo
1000 min & Unlimited Email \$74.19/mo

Includes: Unlimited Text (not Pix/Flix)

+taxes & \$5/mo Admin Fee

Text Messaging .02 incoming .10 outgoing
Picture messaging .25/in .25/out
Packages available.

411 calls are billed \$1.25/ea
Canada & Mexico incur Int'l Roaming fees.

Why?

Do we really
need both?

Beware Potential “Contract Lock-In”

- At times it can be hard to comprehend how fast mobile Internet devices are evolving. We may have a three or even four year life cycle for desktops and laptops, but mobile devices are continually being updated, and most people update their cell devices every two years or so.
- If you have a limited list of “approved” mobile Internet devices, perhaps negotiated three or four years ago based on what was available then, what’s on the list today will often be yesterday’s technologies (and often at yesterday’s prices!)
- Be SURE to have a mechanism by which users can pass along feedback or suggestions regarding devices they’d like to have available and supported!

Some Subtle Contract-Related Issues

- If the school buys a mobile Internet device for someone:
 - What if a user runs up a substantial bill? Does your contract allow you to limit institutional liability for inappropriate or accidental device usage?
 - What if the hardware is lost, stolen or damaged? Who pays to replace the device for the remainder of the contract term?
 - What happens if the device user gets terminated or quits? Does the institution "eat" the remainder of their service contract, or can the device be transferred? Does the user have to surrender their device, or can they "buy out their contract" and keep it?
(Typical scenario: they may have purchased personal applications that may be tied to that particular phone)
What about their phone number? Can they keep it?⁴⁰

Dodging The Contract Minefield

- If you pay employees a mobile device stipend, but have them purchase their own device (as many sites do), you can avoid some of these issues, but this approach can raise issues of its own
- For example, if the device is a **personally owned** mobile device under contract, do you have a basis for obtaining non-consensual access to it or its billing records? If you don't have that sort of access, will you and your school's attorneys be okay without it?
- Another option may be **pay-as-you-go no-contract** devices (aka "prepaid" mobile devices), but that flexibility often comes (literally) at a cost: the devices themselves typically aren't free (or aren't at least heavily subsidized), and you may pay more/minute (or per month)

6. Type of Service: GSM? iDEN? CDMA?

Choice of Connectivity

- A related issue: not all devices use the same sort of connectivity. (For example, until recently, if you wanted an iPhone, you were implicitly selecting AT&T's GSM service; now you can pick AT&T/GSM, or Verizon/CDMA)
- At the same time your university is deciding on the mobile internet device operating systems it will support, and what mobile device hardware it will support, you should also be thinking about the sort of connectivity your devices-of-choice will be using.
- Call coverage and quality may be impacted by your choice, but choice of connectivity can also impact confidentiality.
- Some sites may decide to offer multiple vendors/support multiple connectivity options for very pragmatic reasons.

GSM (and UMTS)

- GSM==Global System for Mobile Communication (and the follow-on 3G Universal Mobile Telecommunication System)
- The most common worldwide (nearly 90% share).
- So-called “World Phones,” (quad-band or even penta-band phones), support multiple GSM frequency ranges:
 - GSM 850 (aka “GSM 800”) and GSM 1900; the typical GSM frequencies in the United States and Canada
 - GSM 900 and GSM 1800 (aka “Digital Cellular Service”); the most common GSM frequencies in Europe and worldwide
- GSM is used by AT&T and T-Mobile in the U.S. (note that AT&T and T-Mobile will be merging in a year or so)
- GSM uses replaceable SIM cards (but some phones may be “locked”)

Some GSM Ciphers Have Been Cracked, Too



GSM encryption crack made public

The schemes commonly used to encrypt GSM telephone calls, SMS messages, and data transmissions have been theoretically broken for years at both the protocol and cipher levels, but results presented in Berlin at the [26th Chaos Communication Congress](#) (26C3) on December 27 demonstrate that a practical attack can be easily implemented. Researchers unveiled cracking tables requiring just two terabytes of disk space that can be used to look up a GSM encryption key and decrypt a transmission. The tables were computed on 40 commodity hardware PC nodes in just a few months' time, and are shared through BitTorrent. Furthermore, the presentation explains that the more difficult practical task of intercepting and capturing GSM calls can already be done with inexpensive radio equipment and open source software.

Background

The cipher under attack is known as [A5/1](#); it was invented by the GSM Association in 1987. Due to the Cold War, A5/1 was deployed only in Western Europe and the United States, and was accompanied by a significantly weaker cipher called [A5/2](#) for export to other regions. The GSM protocol supported both A5/1 and A5/2, plus A5/0, or unencrypted connections, a choice that left the protocol itself vulnerable to attack.

A5/1 was not published, but researchers began to reverse-engineer it almost immediately, work that was completed and publicized in 1999. Theoretical attacks based on weaknesses in the cipher date back to at least 1997, but real-world attacks on the system as implemented in the global GSM network only began to appear in 2003, when the team of Elad Barkan, Eli Biham, and Nathan Keller reported that phones use the same set of keys regardless of whether A5/1 or A5/2 encryption was enabled. Thus, by momentarily tricking a phone into using A5/2 (which can be cracked in seconds), a man-in-the-middle attacker can retrieve the session key for a call and continue to decrypt it even if it subsequently switches to A5/1 at the network's request. Shortly thereafter, networks were advised to discontinue use of A5/2.

Barkan, Biham, and Keller also [published](#) a ciphertext-only attack on A5/1 itself that relied on a time-memory tradeoff: building a lookup table of partially-precomputed hash values. A5/1 uses a 64-bit key (although, interestingly enough, 10 bits are fixed at 0 in all known deployments, making the practical strength 54-bits) which would require around 128 petabytes for a complete plaintext:ciphertext table for each

January 6, 2010

This article was contributed by
Nathan Willis

Thus, by momentarily tricking a phone into using A5/2 (which can be cracked in seconds), a man-in-the-middle attacker can retrieve the session key for a call and continue to decrypt it even if it subsequently switches to A5/1 at the network's request.

A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony

Orr Dunkelman, Nathan Keller, and Adi Shamir

Faculty of Mathematics and Computer Science

Weizmann Institute of Science

P.O. Box 26, Rehovot 76100, Israel

{orr.dunkelman,nathan.keller,adi.shamir}@weizmann.ac.il

Abstract. The privacy of most GSM phone conversations is currently protected by the 20+ years old A5/1 and A5/2 stream ciphers, which were repeatedly shown to be cryptographically weak. They will soon be replaced in third generation networks by a new A5/3 block cipher called KASUMI, which is a modified version of the MISTY cryptosystem. In this paper we describe a new type of attack called a *sandwich attack*, and use it to construct a simple distinguisher for 7 of the 8 rounds of KASUMI with an amazingly high probability of 2^{-14} . By using this distinguisher and analyzing the single remaining round, we can derive the complete 128 bit key of the full KASUMI by using only 4 related keys, 2^{26} data, 2^{30} bytes of memory, and 2^{32} time. These complexities are so small that we have actually simulated the attack in less than two hours on a single PC, and experimentally verified its correctness and complexity. Interestingly, neither our technique nor any other published attack can break MISTY in less than the 2^{128} complexity of exhaustive search, which indicates that the changes made by the GSM Association in moving from MISTY to KASUMI resulted in a much weaker cryptosystem.

Still Don't "Get" The Problem with GSM?

- One more try.

See "Practical Cell Phone Snooping,"
www.tombom.co.uk/cellphonespying.odp

and

www.tombom.co.uk/blog/?p=262 (August 1st, 2010)
(odp file extension == OpenOffice)

- The GSM Security FAQ is also worth a look:
<http://www.gsm-security.net/gsm-security-faq.shtml>

iDEN

- This is the Integrated Digital Enhanced Network, a Motorola proprietary format.
- It is supported by Sprint (iDEN had formerly been a “Nextel thing”), and you can even get Boost Mobile prepaid iDEN phones (look for their “i”-prefix handsets such as the Motorola Clutch i465)
- iDEN is perhaps most famous for its nationwide “push to talk” (PTT) service, an instant-on walky-talky-like service that’s popular with federal “three letter agencies” and local/regional emergency personnel, courtesy van drivers, etc.
- Uses SIM cards (not compatible with GSM SIM cards)
- Sprint has announced that iDEN will be phased out by 2013 (see <http://tinyurl.com/iden-2013>)

CDMA (and CDMA2000)

- CDMA == Code Division Multiple Access; CDMA2000 is the 3G follow-on technology to CDMA. There are a couple of variations of CDMA2000 (e.g., 1X and EV-DO)
- CDMA is probably the most common cellular connectivity choice in the United States.
- CDMA is generally not very useful if travelling abroad (with only a few rare exceptions).
- Some leading CDMA cellular carriers in the US include: Verizon, Sprint, Cricket, MetroPCS, and Qwest
- CDMA is generally considered harder for an unauthorized party to eavesdrop upon than GSM (lawful intercept can still be performed), but from a resistance-to-eavesdropping point of view, I still like iDEN best.

So Which Cellular Technology To Pick?

- You **may** not have a choice: you may live or work somewhere where coverage is limited. If CDMA service is strong where you need coverage, and GSM is weak, buy a CDMA phone (and obviously if the opposite is true, buy a GSM phone)
- You **may** not have a choice: you may be subject to mandatory exclusive contract restrictions, although some organizations (including UO) offer both a CDMA provider and a GSM provider as an option.
- *What are YOU recommending, and why?*

7. Getting Influence Over Mobile Internet Device Choices At Your Site

If you care what folks use, you can influence those choices, but it will cost you...

Let's Admit Our Limitations

- 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.

And If You Don't Know Who Has Those Devices

- ... 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 care 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). Yes, you should care.
- You may think that that device isn’t something you need to worry about, but 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 Will 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."

- By that I mean that 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.

What About Student Mobile Devices?

- Same idea: if you have a discounted/subsidized/required mobile device purchase program for students, you *may* be able to control (or at least 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** (the upfront cost of the device itself is negligible relative to the ongoing cost of purchasing service for the device)

iPhone 4 Costs

- While the iPhone 4 starts at just \$199, the monthly recurring costs can be substantial.
- For example, on Verizon, consumer plans currently range from a bare-bones 450 minute plan with unlimited data at \$89.98/month all the way up to \$119.98/month (for unlimited voice and data). A text messaging plan, if desired, adds up to another \$20/month.
- What about AT&T? AT&T offers a consumer 450 minute voice place (with 5000 night and weekend minutes) for \$39.99, to which you can add a (comparatively tiny) 200MB data plan for another \$15, for a total of \$54.99/month. Their unlimited voice plus 4GB data with tethering plan would cost \$114.99 (plus a text messaging plan, if desired)
- Those are non-trivial ongoing costs.

Doing The Math for A Campus of 20,000

- Non-device costs for iPhones for 20,000 users for a year would run from $\$54.99/\text{month} * 12 \text{ months/year} * 20,000 = \$13,197,600/\text{yr}$ all the way up to $\$33,595,200$ (e.g., $(\$119.98 + \$20) * 12 * 20,000$).
- That's a chunk of money for pretty much any campus I can think of...

Those Cost Aren't Just an "iPhone" Thing

- Some folks may think that the prices mentioned are purely an artifact of Apple/AT&T/Verizon. They're not.
- For example, domestic consumer service plans for BlackBerry devices, e.g., from Verizon, tend to be comparable -- talk plans in Oregon run from \$39.99–\$69.99, with texting \$20 extra, with the only realistic data package you'll also need being the \$29.99 “unlimited” one.

$\$69.99 + \$20.00 + \$29.99 = \119.98

$\$119.98/\text{month} * 12 \text{ months} * 20,000 = \$28,795,200/\text{yr}$
to service 20,000 users.

Once again, that's a big chunk of dough.

One Less Expensive Option

- Boost Mobile now offers Android mobile devices such as the Motorola i1 with \$50/month unlimited nationwide talk, text, web, 411, IM and email, all with no contracts (and rates can shrink to as low as \$35/month over time); Blackberry devices are also available (however those users pay an additional \$10/month).
- For a campus of 20,000 users, that works out to “just” $20,000 * 12 * 50 = \$12,000,000/\text{yr}$, a comparative bargain :-)

International Charges

- If you have faculty or staff who travel internationally, international voice and data usage would be extra.
- In the iPhone's case, data usage ranges from \$24.99/month for just 20MB to \$199.99/month for just 200MB. Over those limits, usage runs from \$5/MB on up (ouch). These and all other rates may change over time; check with your mobile carrier for more details.
- Obviously I think many people may want to consider disabling data roaming while traveling abroad.

Your Institution May Be Able to Negotiate A Better Rate

- Never assume that the onesie-twosie consumer price is the price applicable to higher ed users; always check for existing special pricing, and don't hesitate to negotiate!
- Another possible way of making the financial picture less dire may be to offset some of those costs with related income, for example from cellular tower leases on campus real estate.
- Even if you can't chisel much off the price sometimes, you may want to at least get better contract terms as part of that arrangement.
- *Has YOUR college wrestled with the financial issues associated with mobile devices? If so, did you come up with any solutions?*

8. Secure Mobile Environment Portable Electronic Devices (SME PEDs) ("Government Style" Secure Smartphones)

Sure Mobile Internet Devices Are Popular (And Expensive!), But Are They 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?
- Since misery loves company, it may help to recognize that we're not the only ones wrestling with mobile device security. Remember when the most powerful person in the free world didn't want to part with his BlackBerry?
- Specialized, extra-secure devices (such as the GD Sectera or the L-3 Guardian) are available to users in the gov/mil/three letter agency markets, but those devices are typically expensive (\$3,500) and heavy compared to traditional mobile Internet devices, and are unavailable to those of us who do not hold federal security clearances, anyhow.

SME PED: GD Sectera

Product Details – Sectéra® Edge™ Smartphone (SME PED)

GD <http://www.gdc4s.com/content/detail.cfm?item=32640fd9-0213-4330-a742-55106fbaff32>

Sectéra® Edge™ Smartphone

Secure Mobile Environment Portable Electronic Device (SME PED)

The world's first **NSA-certified** Smartphone.

For media/press inquiries, please contact **Fran Jacques**.

Tel: +1-480-441-2885 • Cell: +1-480-586-1886

- One-touch switching between classified and unclassified PDA functions
- First ever on-the-move wireless access to the SIPRNET
- Intuitive, user-friendly interface
- NSA-certified, DISA approved
- In use and available today
- Easy, fast deployment with Configuration Tool
 - lets you update up to 16 SME PEDs at once

The Sectéra® Edge™ smartphone converges secure wireless voice and data by combining the functionality of a wireless phone and PDA — all in one easy-to-use handheld device. Developed for the National Security Agency's Secure Mobile Environment Portable Electronic Device (SME PED) program, the Sectéra Edge is certified to protect wireless voice communications classified Top Secret and below as well as access e-mail and websites classified Secret and below. **The Sectéra Edge is the only SME PED that switches between an integrated classified and unclassified PDA with a single key press.**

Secure Wireless Phone and PDA

Not only can you use the Sectéra Edge to make secure phone calls, you also have secure access to classified networks, your e-mail and web browsing via high-speed GSM or CDMA cellular networks and Wi-Fi* access points worldwide.



SME PED: L-3 Guardian

 http://www.l-3com.com/products-services/productservice.aspx?type=ps&id=601  Google 

CONTACT US SITE MAP

PRODUCTS & SERVICES

Secure Wireless Handheld Smartphone

PRODUCTS & SERVICES

[◀ Previous Product or Service](#) | [Next Product or Service ▶](#)

L-3 Guardian® SME PED – Secure Wireless Handheld Smartphone

SME PED

The L-3 Guardian® is a next-generation solution for portable secure communications being developed by L-3 under the NSA Secure Mobile Environment Portable Electronic Device (SME PED) program. The L-3 Guardian enables SCIP voice calls up to TOP SECRET level and HAIPE® e-mail/web communications up to SECRET level via commercial cell phone networks. Global cell phone connectivity to SIPRNET, NIPRNET and other classified networks is assured with GSM or CDMA capabilities, including the latest 3G technology. Multiple classified/unclassified domains can be configured into a single L-3 Guardian. The built-in secure Data at Rest (DaR) feature allows L-3 Guardian users to carry their classified data anywhere without the need for classified storage. A full featured PDA enables access to data saved in internal memory or SD flash cards. Both Type-1 and Non Type-1 encryption are provided for maximum security flexibility. For more information, contact Mark Alphonso at (856) 338-2351. HAIPE® is a registered trademark of the NSA.

Communication Systems-East
1 Federal Street
Camden, NJ 08103
Phone: (856) 338-3000
Fax: (856) 338-3345
[Go To Website](#)



The Sort of “Security” We Need

- In our case, we’re not worried about the remnants of the Cold War espionage world, or terrorists, we’re worried about issues such as:
 - Is all device traffic encrypted well enough to protect PCI-DSS or HIPAA or FERPA data that’s present?
 - Is there PII on our users’ devices? Do those devices have “whole device” data encryption to protect that data?
 - What if one gets lost or stolen? 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?
 - And how’s our mobile device security policy coming?

9. History Repeats Itself

Are We Seeing A Recapitulation of The
“Managed vs. Unmanaged PCs” Wars?

The Good Old Days for PC

- For a long time way back in “Ye Olde Days,” traditional IT management pretended that PCs didn’t exist. (Would you like some COBOL with your MVS system, ma’am?)
- While they were in “denial,” people bought the PCs they wanted and “administered” them themselves.
- Productivity increased immensely, at least for a while (it’s amazing how much work one cowboy or cowgirl, left to his or her own devices, can get done). :-)
- While that sometimes worked well, other times chaos reigned (for example, the PCs may have been Own3d).

The Modern Era

- Today's more closely managed "enterprise" model was the response to 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 (and understandable).
- Arguably, it results in less chaos, or at least more consistent and predictable chaos. :-)

Does The Following Sound Familiar?

- Users find mobile devices useful.
- Some IT folks find mobile devices threatening, or easy to dismiss, or too expensive, or simply irrelevant.
- Users buy what they want and use them in innovative ways (sometimes resulting in cheers and applause, sometimes resulting in copious weeping and extensive finger pointing)
- Prediction: Once there are “incidents,” uniform mobile devices will be centrally procured and administered, as the lesser of two evils. (But we may not be there (yet))

10. Mobile Device Policies

An Attempt at Re-asserting Control:
Mobile Device Policies

Example: Device Passwords

- If a mobile Internet device is lost or stolen, a primary protection is the device's password.
- Users hate passwords, and if left to their own devices (so to speak), if they use one at all, they might use a short and easily guessed one such as 1234
- In fairness: short all-numeric pins are familiar to users from things like their ATM card; to users, if a four digit number is good enough for something important, like a money machine, it must be good enough for a phone, eh?
- Hypothesized: 4 digit numerical PINs are not uniformly distributed. Asked to pick a four digit numerical password, if allowed to do so, people will disproportionately pick "magic" ones, e.g., 0000, 1111, 2222, ..., 9999, 1234, 4321, 2468, 2011, their birth year, last four of their SSN, etc. (Love to see a formal study of this issue)

Hypothetical PW Policy: You Must Have A Password, And It Must Be Reasonably Strong

- You and your school might prefer that users use a longer and more complex password for their mobile devices.
- If the mobile device is managed, you can usually require:
 - that it have a password,
 - that the password be strong, and
 - that the device will guard against attempts at brute force password guessing (ATM cards do this by gobbling up your card after a number of bad PIN entries; mobile devices can do something similar by erasing themselves)

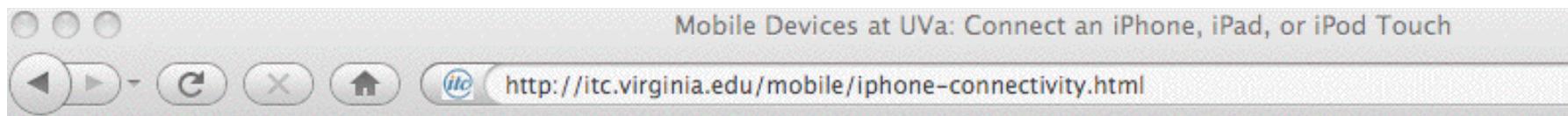
Example: What Can Be Required for iPhone Passwords?

- 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 K12/corp/gov users.

Sample Passcode Policy from U Virginia:



Option 1: Configure Your iOS Device for Encrypted Wireless, NetBadge, & VPN

Requirements & Policies Associated with the Auto-Setup Tool

Before you proceed, make sure you can comply with the following requirements.

- **Operating System:** Your iPhone, iPad, or iPod Touch must have an operating system of version 3.0 or higher. If your device has an older operating system, we recommend using iTunes to upgrade, after backing up the data on your device. (For how to do this, see Apple's articles, "[Backing up, updating, and restoring your iPhone, iPad, or iPod touch software.](#)" and/or "[Purchasing an iOS software update.](#)")
- **Passcode Policy:** To use the auto-setup tool, you will be required to set a passcode on your device for security. Anytime your iPhone/iPad/iPod Touch has been idle for a set amount of time, it will auto-lock. You will have to enter a passcode to release the auto-lock and begin using your device again. (You can set this time interval on your device, but most will not allow longer than 15 minutes.)
 - Note: **The auto-setup tool will configure your device to erase** after 10 bad consecutive passcode login attempts, so set a passcode that you can remember! After the first several incorrect entries, your device will become temporarily disabled for longer and longer intervals, until it no longer works. (If your device does get wiped, you may restore it via iTunes on the computer with which you last synched it. For more info, see Apple's articles, "[Wrong passcode results in red disabled screen](#)" and/or "[Unable to update/restore.](#)")
 - ITC recommends choosing a 4-digit numerical passcode for ease of use.

Automatic Setup Tool Instructions

iPhone Hardening Checklist from UTexas

Apple iOS Hardening Checklist – Information Security Office – UT Austin Wikis
edu https://wikis.utexas.edu/display/ISO/Apple+iOS+Hardening+Checklist

Handheld Hardening Checklists > Apple iOS Hardening Checklist

Browse Log In Search

Configuration profiles

Some of the steps in the checklist below can be configured through the use of configuration profiles. Configuration profiles can be edited and viewed with the freely available [iPhone Configuration Utility](#). The ISO has created some [sample configuration profiles](#) that may be used as a starting point (or in production if you wish.) The sample configuration profiles fully address steps 2, 3, 4, 5, 6, and 13.

Checklist

All items marked with a ! are mandatory to be considered compliant with the Minimum Standards governing the use of Category I data.

Step	?	To Do	CIS	UT Note	Cat I	Cat II/III
Security Settings						
1		Update firmware to the latest version	1.1.1	§	!	
2		Require a passcode	1.1.10	§	!	
3		Set auto-lock timeout	1.1.12	§	!	
4		Disable grace period for lock		§	!	
5		Erase data upon excessive passcode failures	1.1.14	§	!	
6		Enable Fraud Warning in Safari	1.2.2	§	!	
7		Enable Data Protection		§	!	
Additional Security Protection						
8		Turn off Ask to Join Networks	1.1.5	§		
9		Turn off Bluetooth when not needed	1.1.8	§		
10		Forget Wi-Fi networks to prevent automatic rejoin	1.1.4	§		
11		Erase all data before return, repair, or recycle	1.1.15	§	!	
12		Enable remote wipe functionality		§	!	
13		Encrypt device backups through iTunes		§	!	

UT Note: Addendum

This list provides specific tasks related to the computing environment at The University of Texas at Austin.

Discussion: Does Your School Require Strong Passwords for Mobile Internet Devices?

- If so, is the policy well known?
- What does it specifically require?
- Does your policy have “teeth” (penalties for non-compliance)?
- Who’s in charge of enforcing that policy?
- Have penalties actually been levied on anyone?
- Predictions: policies that lack technical monitoring and technical enforcement will not have very good rates of compliance; policies that are implemented via technical means may have somewhat better levels of compliance.

Enterprise Device Technical Policy Management

- 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:

[http://na.blackberry.com/eng/ataglance/security/
it_policy.jsp](http://na.blackberry.com/eng/ataglance/security/it_policy.jsp)

[http://manuals.info.apple.com/en_US/
Enterprise_Deployment_Guide.pdf](http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf)

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.

iTunes's Pivotal Role

- Apple relies on iTunes for some pretty critical purposes when it comes to managing the iPhone (including backups and updates). You **REALLY** want to encourage people to **take backups (encrypted)** of their devices!
- For better or worse, iTunes is more or less inseparably tied to QuickTime. (A complex application in its own right)
- While iTunes and QuickTime are pretty common on personal laptops or desktops, they may feel like an odd addition to an institutional laptop or desktop.
- The alternative, centralized updates done on a bring-your-device-in-basis, likely won't scale very well.
- Personally, I can live with iTunes everywhere, but how do you folks feel? (It can be a real potential issue if you're tight on bandwidth, obviously)

11. Mobile Devices In The Classroom: A Proper Subject for Policy Creation? (No, Run Away!)

Classroom Mobile Internet Device Policies

- Anyone who's ever been in a class/meeting/movie theater plagued by randomly ringing cell phones understands just how distracting they can be. Some instructors therefore insist that all mobile devices be silenced or completely turned off during class.
- Mobile Internet devices are also a potential source of unauthorized assistance during exams, and may need to be controlled to prevent rampant collusion or cheating:
 - classmates could text answers to each other during an exam
 - students could consult Internet sources for help on some subject material
 - tests used during an early section might potentially get photographed and shipped by telephone to students who will be taking the same (or a similar) test later¹⁷

Classroom Mobile Internet Device Policies (2)

- On the other hand, mobile internet devices may play a critical role in helping to keep campuses safe: a growing number of schools have programs in place to push emergency notifications to campus populations via their mobile devices, and when you're facing severe weather or an active shooter on campus, time may be of the essence.
- Mobile internet devices may also be essential for student parents to remain accessible in case a child is hurt or injured and contacting the student parent becomes necessary.
- Remaining accessible 24x7 may also be a job requirement for some emergency-related occupations (health professions, public safety work, etc.)

Academic Freedom

- Most campuses have strong traditions of academic freedom, and most administrations grant faculty (particularly tenured faculty) substantial autonomy when it comes to how they run their class rooms.
- While the administration, or more typically an expert faculty committee, might venture to make observations, or offer recommendations or advice, it would be uncommon for classroom-related policies to be centrally imposed.
- This does not mean, however, that faculty can go overboard and use technical means (such as cell phone jammers or WiFi jammers) to block cellular or WiFi signals...

Cellular Jammers: Yes, They Really Do Exist

- Under some circumstances (such as the booby-trap-rich environments of Iraq and Afghanistan), cellular jammers can be used by the good guys in life-saving roles, blocking terrorist command-detonated improvised explosive devices.
- That's a pretty unusual role, however. Nonetheless, if you Google for "cellular jammer" you'll see that yes, people really do make and sell jammers on the Internet, and yes, they are willing to attempt to ship them here to the United States (even though they're illegal to use here).
- If you rely on cellular service (or related communication services, such as GPS) for critical emergency communication, event time-stamping, or other key security-related functions, the possibility of an adversary employing a jammer should be explicitly factored into your security planning.

One Option If You Run Into a Cellular Jammer

The screenshot shows a web browser window with the title "EB - Jammer Enforcement". The URL in the address bar is <http://fcc.gov/eb/jammerenforcement/>. The page content is as follows:

EB - Jammer Enforcement

FCC > EB > Jam site map

Search the FCC: [Search Box] Go
Help | Advanced

Jammer Enforcement
Enforcing the FCC's jamming prohibition

ALERTALERT***ALERT***

Federal law prohibits the operation, marketing, or sale of any type of jamming equipment, including devices that interfere with cellular and Personal Communication Services (PCS), police radar, Global Positioning Systems (GPS), and wireless networking services (Wi-Fi).

"Jamming devices create serious safety risks. In the coming weeks and months, we'll be intensifying our efforts through partnerships with law enforcement agencies to crack down on those who continue to violate the law. Through education, outreach, and aggressive enforcement, we're tackling this problem head on."

-- P. Michele Ellison, Chief, Enforcement Bureau

Jamming Prohibition

The use of "cell jammers" or similar devices designed to intentionally block, jam, or interfere with authorized radio communications (signal blockers, GPS jammers, or text stoppers, etc.) is a violation of federal law. Also, it is unlawful to advertise, sell, distribute, or otherwise market these devices to consumers in the United States. These devices pose serious risks to critical public safety communications, and can prevent you and others from making 9-1-1 and other emergency calls. Jammers can also interfere with law enforcement communications. ***Operation of a jammer in the United States may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.***

File a Complaint

If you are aware that someone is operating, selling, leasing, advertising for sale, shipping, distributing, and/or importing jammers, you can file a complaint at: <http://www.fcc.gov/complaints>.

12. What If A Mobile Device Ends Up Lost or Stolen?

The crux of the issue...

Mobile Devices Do Routinely Get Lost or Stolen

//www.techjournalsouth.com/2011/02/more-than-a-third-of-consumers-have-had-cell-phones-lost-or-stolen/

ma sunt odiosa Whois Data Problem ... BFK edv-consulting ... PhishTank | Join the... Ur I.T. Mate Group h... R

More than a third of consumers have had cell phones lost or stolen

February 8th, 2011



city with the highest rate of cell phone loss or theft against the 20 most populated cities in the U.S.

In fact, 52 percent of respondents in Miami have experienced cell phone loss/theft. New York and Los Angeles were the #2 and #3 cities in the survey with 49 and 44 percent of respondents experiencing loss/theft respectively.

Frustration dominant

Frustration was the most dominant feeling consumers experienced when their mobile phone was lost or stolen, likely because 87 percent could neither remotely lock nor remotely wipe their phone's memory afterwards and more than half (54 percent) of all smartphone users did not password protect their phones.

MOUNTAIN VIEW, CA -Hold on to that cell phone and if you haven't already, protect your information with a password. At a time when smartphone use has become engrained in everyday life as a primary way to communicate, work and share, a new survey from Norton by Symantec (NASDAQ: SYMC) reveals that 36 percent of consumers in the U.S. have fallen victim to cell phone loss or theft.

In the new survey commissioned by Norton, Miami is revealed as the



At The Risk of Stating the Obvious

- If you suspect that you've lost your mobile device, or it's been stolen, report it to your cellular carrier at once.
- Doing this will be easier if you have (with you!):
 - your carrier's customer service phone number
 - your mobile device's phone number
 - your account security code
 - your device's IMEI (International Mobile Equipment Identity Number), ESN (Electronic Serial Number) or MEID (Mobile Equipment Identifier)
- If you support a department or school full of mobile devices, maybe central records of this information would be helpful? (carefully safeguard this key info!) 94

What May Be On A Lost Phone?

- **Contacts** (including potentially sensitive contacts, or contacts which include unpublished phone numbers)
- **Financial information** (online bank or online brokerage account information, credit card information, etc.)
- **Passwords to sensitive accounts** (hopefully you're not relying on plain passwords for root/administrative accounts, but if you are, hopefully you're not storing them in plain text on your phone, *but...*)
- **Private PGP keys, PKI certificates and cryptographic soft tokens**
- **Confidential work information** (including data covered by contractual NDAs, FERPA, HIPAA, GLB, etc.)
- **Personal content** (do you **really** want that video of you dancing the hokey-pokey at the karaoke bar after a few too many beers posted all over the Internet?)

Lost Mobile Devices: Option 1 – Encrypt It

- An example of a common security control designed to protect PII from unauthorized access is hardware encryption.
- For example, many sites require routine use of “whole disk” encryption on all institutional laptops containing PII.
- If we lose a mobile Internet device, but the device is completely encrypted, do we *really* care, other than the obvious inconvenience (and cost) associated with replacing that device and restoring from backup? (And of course, the cost of the phone can be covered by insurance, if you worry about that).
- If you’re interested, whole device encryption may be available as a software solution for at least some mobile platforms...

March 15, 2011 12:03 PM PDT

WhisperCore app encrypts all data on Android

by Elinor Mills

A

A

Font size



Print



E-mail



Share



8 comments



142



Recommend

123

Whisper Systems today began offering hard disk encryption for Android—an app called WhisperCore that is free for individuals to use.

The app includes full disk encryption for all data stored on the device and allows for SD (Secure Digital) card encryption as well, said Moxie Marlinspike, co-founder and chief technology officer of [Whisper Systems](#).

The beta release is limited to the Nexus S, but will be expanded to other devices soon, he told CNET. Meanwhile, pricing for commercial use is based on the size of the deployment.

Once the app is installed on the phone, the user sets a passphrase, which is used to generate a key that encrypts all the data on the disk.

"If the device is lost or stolen, the data is totally opaque and inaccessible," Marlinspike said, adding that his goal was to develop a system "that will transform these consumer devices into enterprise-class secure devices."

Some mobile security services offer remote wipe for lost or stolen devices, but typically the files remain on the device and can be recovered with



Moxie Marlinspike, co-founder and chief technology officer at Whisper Systems, demonstrates the new WhisperCore app on an Android phone.
(Credit: Stuart Anderson)

So What About Hardware Device Encryption?

- Some mobile Internet devices (such as earlier versions of the iPhone) did not offer hardware encryption; 3GS and 4G iPhones now do.
- However, folks have demonstrated that at least the 3Gs (and at least for some versions of iOS) was less-than-completely bullet proof; see for example Dr NerveGas (aka Jonathan Zdziarski's) demo "Removing iPhone 3G[s] Passcode and Encryption," www.youtube.com/watch?v=5wS3AMbXRLs
- This may be a consideration if you are planning to use certain types of iPhones for PII or other sensitive data and planned to rely on hardware encryption.

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 Encryption 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*

Note Those Recommended Password Lengths

- We've previously talked specifically about passwords at the 2009 NWACC Security Meeting (see www.uoregon.edu/~joe/passwords/passwords.pdf (or .ppt))
- I suspect that most folks do NOT routinely use 12 to 21 character passwords even on highly important "regular" administrative accounts, so convincing users, particularly senior administrative users, to use a 12 or 21 character password "just" for their BlackBerry may be a tough sell.

Lost Mobile Devices: Option 2 -- Find It

- If we lose a mobile Internet device, maybe the device itself can help us find it...
- For example, can the device monitor and self-report its location? Many mobile devices include integrated GPS, after all, as well as the ability to send text messages or email, or to make phone calls. (Note: Geo-location services may have problems in dense urban areas, as well as in underground parking garages, etc.)
- Unfortunately, the bad guys know that tracking applications of this sort are increasingly common, so if they steal or find a mobile device, they may immediately put it into an electrical isolation bag to prevent the device from “phoning home” until it can be sanitized.
- Also, are we okay routinely tracking the travels of legitimate users when the device isn't lost or stolen?

The screenshot shows a web browser window with the address bar displaying "http://www.gadgettrak.com/products/iphone/". The main content area features a large banner with a world map background, two devices (an iPhone and an iPad), and the "GadgetTrak" logo with the tagline "iOS Security". A red vertical sidebar on the left is labeled "Help & Support".

GadgetTrak iOS Security

With all of the photos, contacts, apps and music on your iPhone, losing it would be a massive pain. Unfortunately, that pain is felt by thousands of smartphone users every day. Ask them — they wish they'd had GadgetTrak installed.

With GadgetTrak, you greatly increase your chances of recovering your iPhone, iPad, or iPod touch by having the ability to track your device and even snap a photo of the thief!



Locate & Find



Advanced hybrid positioning

We use a combination of GPS, Wi-Fi positioning and cell tower triangulation to pinpoint location



Camera support

Snap a photo with all built-in cameras to collect crucial evidence to help catch the thief.



Push notifications

Send a discrete message to your device enticing the thief to initiate a tracking report.



Location Reports

When tracking occurs, you'll receive an email with detailed information about its current location.

Secure



Tamper proof

Once tracking is activated the software



Secure connection

When tracking data is being

System Requirements

- Requires iOS 4 or higher
- Background processing only supported on iPad, iPhone 3GS, iPhone 4, and iPod touch 3rd generation or newer

iJacking - How to Protect Yourself From Mobile Theft

GadgetTrak featured on KOMO News

Lost Mobile Devices – Option 3: Kill It

- Can the lost mobile device “defend itself?” That is, if an unauthorized person gets your device, can he get at what’s on it, or will it be resist those access attempts?
- If the device is suffering a sustained attack from a determined and patient attacker, can it electronically “kill itself” to ultimately keep its contents from being compromised?
- If we have to, can we affirmatively push an external “kill code” to the device to “brick it?” (And can we be sure a malicious bad guy *can’t* do this w/o our permission?)
- Can the device zap itself if it is simply left unused for a “long” period of time? (Will it still have enough residual power to self-zap after a month? And what if I go on a six week trip, but forget to take my mobile device?)

Risk of Access To Device Content Can Vary

- Not all threats to the security of mobile device contents are equal. The spectrum goes from:
 - non-technical curious family member or coworker
 - common thief, looking for easily exploitable financial details, equipped with just a few basic tricks
 - highly skilled mobile device forensic specialist (including technicians from the law enforcement and/or the national intelligence communities)
- Protecting a device from compromise by a curious family member or coworker is obviously far easier than protecting it from a high skilled mobile device specialist
- It can be helpful to see what's forensically possible when dealing with a cell phone – once you know what a trained guy can do, you may become a little more skeptical about the level of protection that a device offers.

Mobile Device Forensics

- 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

Mobile Device Forensic Training Options

- If you do end up needing to do mobile device forensics yourself, formal training may be very helpful. Formal training can also be useful when it comes to establishing *bona fides* if you need to testify in court about work you've done. Some training options include:
 - **BK Forensics Cell Phone Forensics 101** (3 days)
<http://www.bkforensics.com/101.html>
 - **SANS Mobile Device Forensics Course** (5 days)
<http://www.sans.org/security-training/mobile-device-forensics-1297-mid>
 - **TeelTech Adv. Smartphone Forensic Training** (5 days)
www.teeltech.com/tt3/smartphoneclass.asp?cid=18

and there are others...

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 BlackBerrys) 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 version 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>
- Complete (encrypted) device backups may exist...

Device Backup Password Recovery Tools

Recover passwords protecting iPhone/iPod and BlackBerry backups

(C) (X) (H) (D) http://www.elcomsoft.com/eppb.html Google

Elcomsoft Phone Password Breaker

Recover Password-Protected BlackBerry and Apple Backups



Elcomsoft Phone Password Breaker enables forensic access to password-protected backups for smartphones and portable devices based on RIM BlackBerry and Apple iOS platforms. The password recovery tool supports all BlackBerry smartphones as well as Apple devices running iOS including iPhone, iPad and iPod Touch devices of all generations released to date, including the latest iPhone 4 and iOS 4.1.

Unlock Apple and BlackBerry Backups

The new tool recovers the original plain-text passwords protecting encrypted backups for Apple and BlackBerry devices. The backups contain address books, call logs, SMS archives, calendars and other organizer data, camera snapshots, voice mail and email account settings, applications, Web browsing history and cache.

Fast GPU Acceleration

To unlock Apple backups even faster, the tool engages the company's patent-pending GPU acceleration technology. Elcomsoft Phone Password Breaker is the first GPU-accelerated iPhone/iPod password recovery tool on the market, and the only product to read and decrypt keychains (saved passwords to mail accounts, web sites and 3rd party applications) from password-protected backups (if password is known or recovered).

Prices:

Home Edition - \$79
Professional Edition - \$199

i [Compare editions](#)

Buy [Purchase EPPB](#)

Download [Download EPPB 1.30.761](#)

System requirements for EPPB

View the screenshot of EPPB

Read EPPB Online Documentation

Subscribe to the Password Recovery Software newsletter

? [ElcomSoft tools in eDiscovery work](#)

? [GPU Acceleration Frequently Asked Questions](#)

? [Phone Password Breaker Frequently Asked Questions](#)

? [Smartphone Forensics: Cracking BlackBerry Backup Passwords](#)

[But...]

Please note that Elcomsoft Phone Password Breaker is NOT able to remove iPhone passcode lock, unlock iPhone from the carrier, jailbreak the iPhone or remove SIM card PIN code. It is intended for recovery of backup passwords only. For more information, read the [EPPB manual](#) and [Phone Password Breaker FAQ](#).

What Are Your Plans For Departing Employees?

- Do you have a checklist you go through when an employee leaves (voluntarily or involuntarily)?
- Does the plan include mobile devices and the content thereon? (Or are you ready to crack a potentially encrypted backup you may have retained?)
- What if the employee is using a personally purchased mobile devices?

13. Mobile Device Applications

It's always been about the applications
when you get right down to it, eh?

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 ssh ("VT100-type") terminals, or solely as X Windows 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 from 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 the iPhone

- Of course, most sites don't use "VT100" and/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 or some critical applications may *strongly* prefer or require use of a particular browser)
- Traditionally, Safari was the only true web browser available for the iPhone.
- Firefox, for example, isn't and won't be available (and no, Firefox Home for iPhone does not count), see <https://wiki.mozilla.org/Mobile/Platforms>
- Opera Mini was approved for the iPhone on April 13th, 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” content for you, see www.opera.com/mobile/help/faq/#security) 113

A Review of 12 Alternative Browsers for iPhone

12 iPhone and iPod touch Web Browsers

Alternatives to the Safari Browser

By [Scott Orgera](#), About.com Guide

See More About: [iphone apps](#) [iphone browsers](#) [safari for iphone](#) [mobile browsers](#)

The majority of iPhone and iPod touch users surf the Web using their device's default browser, Safari. Although Apple's browser is a respectable offering, there are several other options available for download via the App Store. Most people are unaware of this fact, assuming that Safari is the only way to go. The following Safari alternatives each have their own unique pros and cons. They are listed in alphabetical order.

[Aquari Browser](#)



Aquari for the iPhone and iPod touch is a Web browser that provides a secure browsing experience without sacrificing other functionality. Access to the application can be protected with an optional 4-digit passcode, giving you the ability to prevent others from accessing your bookmarks, history, and other configuration items.

[More Info](#)

[Hot Browser](#)



Hot Browser for the iPhone and iPod touch is a Web browser that loads a random news website each time you shake your device. This random site is supposedly determined by current popularity across the Web. Some common results that are served up include Slashdot and the New

See: <http://browsers.about.com/od/iphonewebbrowsers/tp/iphone-web-browsers.htm>

Web Based Applications on the BlackBerry

- What about BlackBerry users?

Just like iPhone users, BlackBerry users can run Opera Mini (see www.opera.com/mobile/download/blackberry/) but not Firefox (see https://wiki.mozilla.org/Mobile/Platforms#Supported_Platforms)

There's a nice review of some other mobile web browsers at www.pcmag.com/article2/0,2817,2358239,00.asp

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, othertimes 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; some 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.htmlSee <http://www.dataoutagenews.com/> for more outages.
- Availability is, or can be, another critical information security consideration (remember "confidentiality, integrity and availability"!)

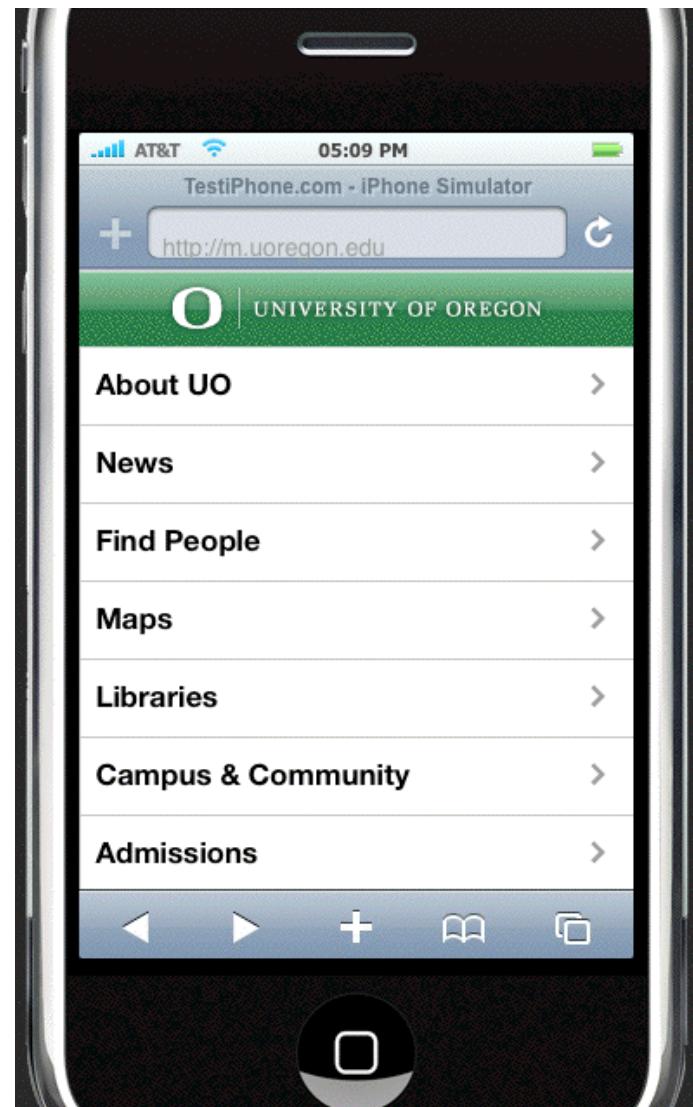
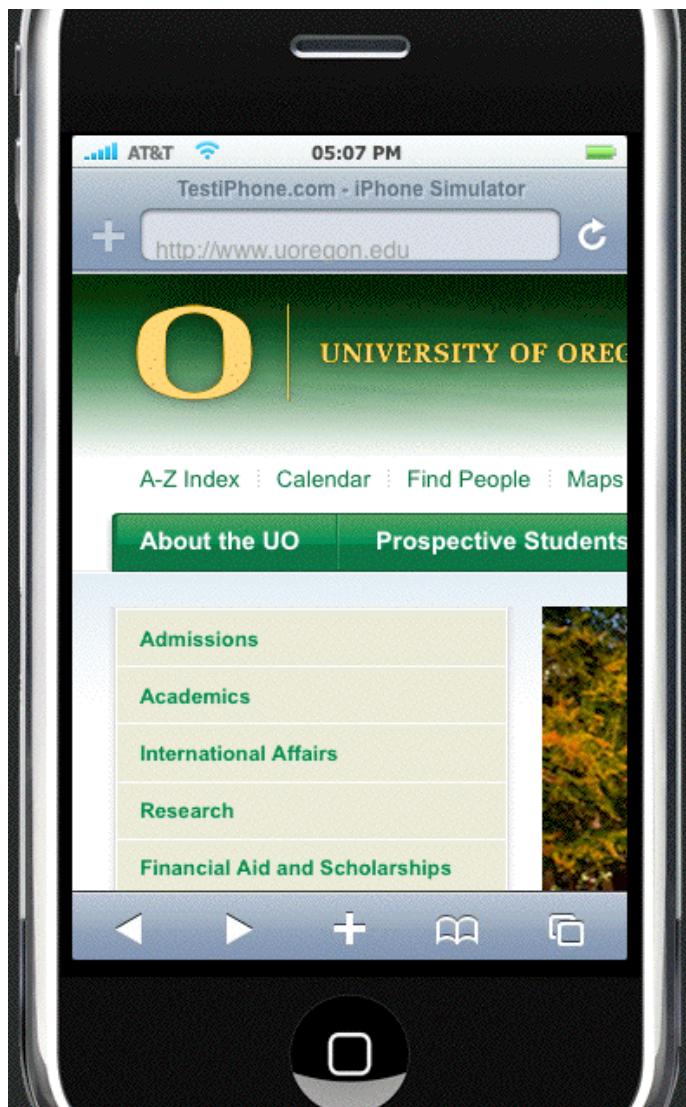
Web Browsers and Android

The screenshot shows the Android Market interface for the Mozilla Firefox Web Browser. The top navigation bar includes links for Gmail, Calendar, Documents, Photos, Reader, Web, more, Sign in, and Google search. The main header reads "Android Market" with a lock icon. Below it, the category "ANDROID MARKET > PRODUCTIVITY > MOZILLA FIREFOX WEB BROWSER" is displayed. The central content area features a large image of the Firefox logo and the text "Mozilla Firefox Web Browser" by Mozilla. It shows a rating of 4.5 stars from 16,146 reviews and an "INSTALL" button. To the right, there are tabs for OVERVIEW, USER REVIEWS (279), WHAT'S NEW, and PERMISSIONS. The DESCRIPTION section contains a brief overview of the app's features, mentioning synchronization, add-ons, and the Awesome Screen. Below the description, there is a "Visit Developer's Website" link. The RELATED section lists four other browser apps: Dolphin Browser HD, xScope Browser Pro, Miren Browser, and Opera Mini Web Browser, each with its own thumbnail, name, developer, rating, number of reviews, price, and a "View Details" button. To the right of the main content, there is a sidebar titled "ABOUT THIS APP" with details like Rating (4.5 stars), Updated (March 21, 2011), Current Version (4.0), Requires Android (2.0 and up), Category (Productivity), Installs (1,000,000 - 5,000,000), Size (14M), and Price (Free). Below the sidebar, two screenshots of the Firefox interface on Android are shown, demonstrating its look and feel.

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 may be 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? Has someone else *already* created such a site?

Sample Web Page



Quick Response Codes

- Speaking of mobile devices and the web, a relatively new development is the “Quick Response” or “QR” code, the little square dot-like bar codes that are meant to be photographed by mobile devices as a convenient way of taking your mobile device to a particular location online (or giving folks a phone number, text, etc.)



- Quick, what *do* those barcodes say, eh?

Do We All Think Like Security People?

- What was the first thing you thought when you saw those things?
- I know what *my* first thought was... Just looking at one of those things with the naked eye, you sure can't tell WHAT you're going to get/where you're going to go.
- Yes, we are a relatively cynical/paranoid lot, aren't we?
- There may be offsetting/compensating controls (but those controls may also potential impact user/site privacy)

Email On Your Mobile Device May Be Routinely Monitored, At Least In Some Jurisdictions

- India is the canonical example of this, heavily pressuring Research In Motion to provide email intercept solutions for traffic involving BlackBerries in India.
- If we assume that other governments have also demanded these technical capabilities, prudent individuals (at least those who may travel to areas where monitoring may be taking place), should consider employing strong local email encryption (such as PGP/GPG) to protect the privacy and security of email sent from their mobile device.

Securing Email On Your Mobile Device

- If you do worry about the security of email, you may want to routinely use PGP/GPG, or perhaps S/MIME, to secure your message traffic.
- You can now get a PGP implementation for the iPhone, see SecuMail, <http://itunes.apple.com/us/app/secumail/id414328661?mt=8> and for the Blackberry see us.blackberry.com/ataglance/security/products/pgp.jsp
- There's an S/MIME *reading* client available for the iPhone, see <http://itunes.apple.com/us/app/smime-reader/id404388231?mt=8> ; for the Blackberry see us.blackberry.com/ataglance/security/products/smime.jsp
- I'm interested in hearing any feedback that folks might want to share about these or similar email encryption applications.

14. Spam, Malware, and Broken Jails

Malware can be the other big worry,
particularly since antivirus options are “limited”

Spam Sent Directly to Mobile Devices

- Some users may read their “regular” email via their mobile devices; in those cases, their “regular” host-based spam filtering will continue to be applicable, regardless of the device used to read that email.
- Managing spam sent *directly* to mobile devices is a different problem: users need to rely more on the provider’s filtering (good or bad as it may be), having few if any options for doing their own bespoke filtering.
- A cool new initiative: while many mobile operators have intra-company spam reporting, GSM mobile users should be aware of a new effort which will allow them to easily *centrally* report any spam that may have slipped through.
See: “Phone Networks Try New Spam Abuse System,”
25 March 2010, <http://tinyurl.com/gsm-7726>
Use the SMS code 7726 (or 33700 in some locations)

Malware and A/V on the Non-Jailbroken iPhone

- Because earlier versions of the iPhone disallowed applications running in the background, it was difficult for traditional antivirus products to be successfully ported to the iPhone.
- To the best of my knowledge, your options for antivirus software on the iPhone are still “quite limited,” with no iPhone A/V offering from traditional market leaders such as Symantec* and McAfee at this time.
- On the other hand, since the iPhone used/uses a sandbox-and-cryptographically “signed app” model, it’s hard(er) for the iPhone to get infected.

* <http://www.symantec.com/business/support/index?page=content&id=TECH133834>
126

Malware and A/V on the BlackBerry

- Regarding the BlackBerry, see RIM's FAQ item

"Does my BlackBerry smartphone need anti-virus software?" at

[http://na.blackberry.com/eng/ataglance/security/
knowledgebase.jsp#faq8](http://na.blackberry.com/eng/ataglance/security/knowledgebase.jsp#faq8)

And If There's NOT A/V For Mobile Devices...

- Some sites may “accidentally” adopt an “overly broad” policy when it comes to deploying antivirus, perhaps decreeing that “If it can’t run antivirus, it can’t run.”

As you might expect, I believe this is a mistake when there are compensating controls (such as use of a signed-app model in the case of the iPhone), or cases where the demand for A/V on a platform is so minimal there’s not even a commercial A/V product available.

There are ways to avoid malware besides just running antivirus software!

- Remember “compensating controls!”

What About Jailbroken iPhones?

- Normally only Apple-approved applications run on the iPhone. However, some users have developed hacks (NOT blessed by Apple!) that will allow users to “break out of that jail” and run whatever applications they want.
- Jailbreaking your iPhone violates the license agreement and voids its warranty, but it is estimated that 5-10% of all iPhone users have done so.
- Q: “Is jailbreaking my iPhone legal?”
A: I am not a lawyer and this is not legal advice, but see:

“EFF Wins New Legal Protections for Video Artists, Cell Phone Jailbreakers, and Unlockers,” July 26, 2010,
<http://www.eff.org/press/archives/2010/07/26>

Jailbroken iPhones and Upgrades

- When a jail broken iPhones gets an OS upgrade, the jailbreak gets reversed and would typically need to be redone.
- This may cause some users of jail broken iPhones to be reluctant to apply upgrades (even upgrades with critical security patches!), until the newly released version of iOS also gets jailbroken.
- That's obviously a security issue and cause for concern.

Jail Breaking Apps Are OS Release-Specific

- Because jail breaking the iPhone is (cough!) not a supported and endorsed activity, every time Apple upgrades its iOS, it inevitably “fixes” (e.g., breaks) the exploits that were formerly being used to escape the iPhone jail.
- As a result, whenever there’s an upgrade, there are a whole bunch of jailbroken iPhone users who anxiously await some new jailbreak for the new version of the iPhone operating system.
- There are real applications which will accomplish this...

GreenPois0n

The screenshot shows a web browser window with the URL <http://www.iphonedownloadblog.com/jailbreak/>. The page content is organized into sections for different iPhone models and their respective iOS versions.

Jailbreak iPhone iOS 4.2.1

- [Jailbreak iPhone 4 iOS 4.2.1 with GreenPois0n](#) (recommended)
- [Jailbreak iPhone 4 with PwnageTool](#)
- [Jailbreak iPhone 4 iOS 4.2.1 with RedSn0w](#)
- [Jailbreak iPhone 3GS iOS 4.2.1 with GreenPois0n](#) (recommended)
- [Jailbreak iPhone 3GS with PwnageTool](#)
- [Jailbreak iPhone 3GS iOS 4.2.1 with RedSn0w](#)
- [Jailbreak iPhone 3G iOS 4.2.1 with GreenPois0n](#) (recommended)
- [Jailbreak iPhone 3G with PwnageTool](#)
- [Jailbreak iPhone 3G iOS 4.2.1 with RedSn0w](#)

Jailbreak iPhone iOS 4.1

- [Jailbreak iPhone 4 iOS 4.1 with PwnageTool](#)
- [Jailbreak iPhone 4 iOS 4.1 with GreenPois0n](#) (recommended)
- [Jailbreak iPhone 4 iOS 4.1 with LimeRa1n](#)
- [Jailbreak iPhone 3GS iOS 4.1 with PwnageTool](#)

Note: our mentioning this site should NOT be taken as a recommendation that you should jailbreak your iPhone! 132

Beware Fake Jailbreaking Apps

Fake iPhone jail-breaking tool packed with malware |
<http://www.zdnet.com/blog/security/fake-iphone-jail-breaking-tool-packed-with-malware/7381>

Fake iPhone jail-breaking tool packed with malware

By Ryan Naraine | September 20, 2010, 10:51pm PDT

Summary

Malicious hackers are preying on iPhone users who want to jail-break their devices, exploiting the increased interest around jail-breaking tools to launch malware attacks.

Topics

[Apple iPhone](#), [Malware](#),
[Ryan Naraine](#), [Tool](#),
[Spyware](#), [Adware & Malware](#), [Smart Phones](#),
[Cyberthreats](#), [Hacking](#),
[Productivity](#), [more +](#)

Blogger Info

Ryan Naraine
[Bio](#) [Contact](#)
Dancho Danchev
[Bio](#) [Contact](#)

Vendor HotSpot

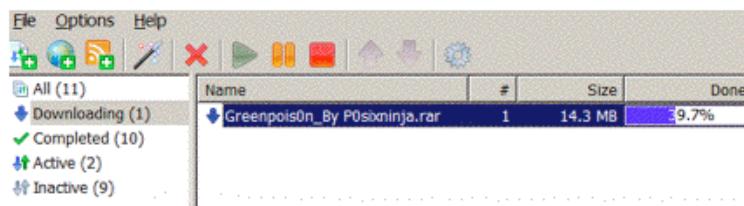
[Here to help you with your...](#)

Malicious hackers are preying on iPhone users who want to jail-break their devices, exploiting the increased interest around jail-breaking tools to launch malware attacks.

According to Kaspersky Lab's Costin Raiu (see disclosure), a rumored jail-breaking utility for iPhone 4 comes with a nasty surprise:

Cybercriminals have definitely been riding the buzz around the supposed jailbreaking tool. It's presumed to be called "Greenpois0n" and it's expected to be released any day now. Not surprisingly, we've seen a number of fake "Greenpois0n" Trojans.

If you search for the Greenpoison on torrent sites you might be in for a surprise:



Raiu said all the existing "greenpois0n" archives at the moment contain Trojans designed to steal passwords and other private data from infected systems.

In addition to the Trojans, Raiu also found fake (rogue) jail-breaking websites hawking tools that pretend to can jailbreak any version of iPhone with any version of iOS. The average cost for these is \$25-\$40.

And When You *Do* Get Successfully Jailbroken

- If you do successfully jailbreak your iPhone (with an app that's not malicious in and of itself!), your exposure to OTHER malware *will* increase.
- Some of the malware which has targeted jailbroken iPhones has targeted unchanged OpenSSh passwords for the root and/or mobile accounts (which defaulted 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)

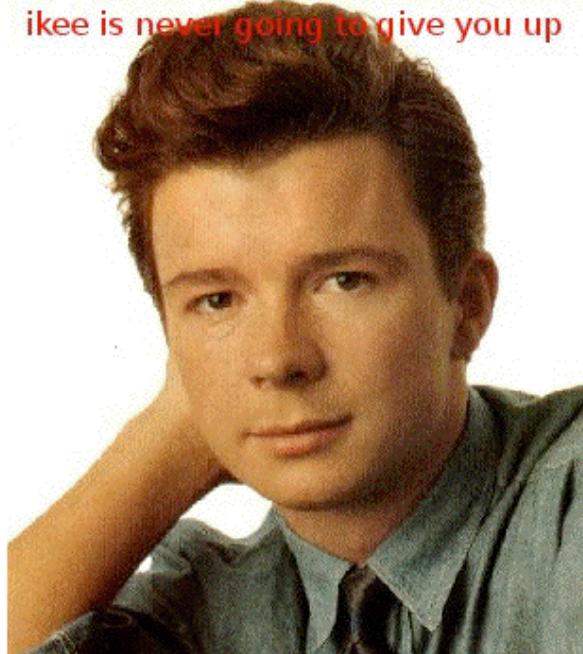
The “ikee” Worm

Ikee Worm Rickrolls Jailbroken iPhones | Symantec Connect

<http://www.symantec.com/connect/blogs/ikee-worm-rickrolls-jailbroken-iphones>

Many users who have jailbroken their iPhones in order to customize them have not changed their SSH password, allowing others to log in to their phone. In the case of Ikee, the worm scans random IP ranges and also specifically targets Optus, Vodafone, and Telstra's IP ranges, which are the common telephony providers in Australia. Once a vulnerable iPhone is found, the worm changes the wallpaper to a picture of Rick Astley (a prank known as Rickrolling), deletes the SSH daemon, and begins scanning the network for other vulnerable phones. Note that some of these telephony networks use NAT (network address translation)—such that iPhones may not actually be reachable by Ikee's scans.

ikee is never going to give you up



Unfortunately, the first variant worm also had a slight bug. This bug can cause the background of an infected user's iPhone to be picked up and sent to new infections, instead of the picture of Rick Astley. Later variants of the worm corrected this problem.

The “Duh” Worm

New virus for jailbroken iPhones the most serious so far

S http://www.sophos.com/pressoffice/news/articles/2009/11/iphone-worm-duh.html

"This latest iPhone malware is doubly criminal. Not only does it break into your iPhone without permission, but it also cedes control of your phone to a botnet command server in Lithuania," said [Graham Cluley](#), senior technology consultant at Sophos "That means your iPhone has just been turned into a zombie, ready to download and to perform any commands the cybercriminals might want in the future. If infected, you have to consider all of the data that passes through your iPhone compromised."

In addition, Sophos reports that "Duh" changes the password on your iPhone - meaning that cybercriminals know what it is but infected users don't, allowing criminals to log back into your iPhone later. However, Sophos expert Paul Ducklin [managed to recover the password](#) - revealing that infected users can login as root with the password 'ohshit'.

"Apple's default root password - 'alpine' - on the iPhone breaks two fundamental rules - it's both a dictionary word and well known. This doesn't matter for most iPhone users, as they

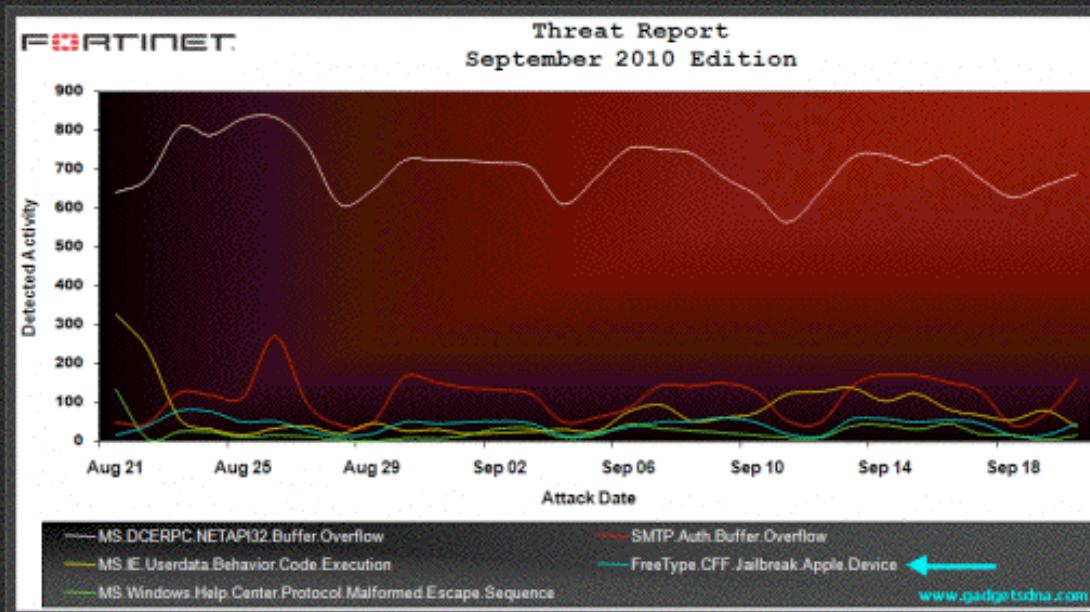
Mobile Malware May Exploit Vulnerable Apps

- For example, just as Adobe Reader has been a popular target for malware on traditional desktop and laptop computers, Adobe Reader is also a popular attack vector on handheld mobile devices.
- Likewise, Adobe Flash Player on Android has also surfaced as having vulnerabilities.

PDF Vulnerabilities on the iPhone

PDF Vulnerability Being Used For Malicious Purposes On iPhone iOS

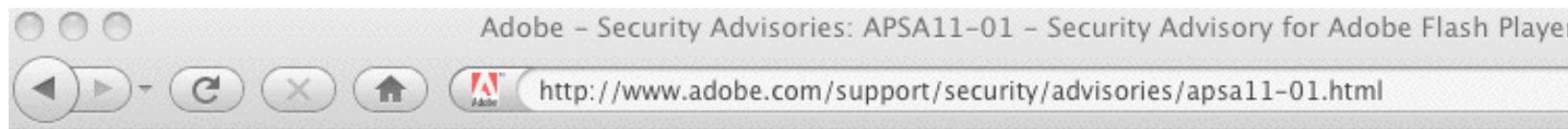
By _GadgetNews - October 3, 2010



The security firm Fortinet has shown a new vulnerability (CVE-2010-2972) that is being used to exploit jailbroken Apple iPhones leveraging the PDF file format. A few weeks back, Apple fixed the security vulnerability (CVE-2010-1797) associated with viewing malicious PDF files in iOS 4.0.2 and iPad 3.2.2 firmwares.

The problem lies in the Compact Font Format, which is supported in popular document formats such as PDF. The interesting aspect here though is that this it is often used intentionally to jailbreak devices. However, as with any vulnerability, a scenario could exist where an attacker could jailbreak a phone for malicious purposes. The exploit **FreeType.CFF.Jailbreak.Apple.Device.Buffer.Overflow** jumped into fourth position in last month report.

Flash Vulnerabilities on Android



Adobe recommends users of Adobe Flash Player 10.2.152.33 and earlier versions (Adobe Flash Player 10.2.154.18 and earlier versions for Chrome users) for Windows, Macintosh, Linux, and Solaris operating systems update to Adobe Flash Player 10.2.153.1 (Adobe Flash Player 10.2.154.25 for Chrome users). Adobe recommends users of Adobe Flash Player 10.1.106.16 and earlier versions for Android update to Adobe Flash Player 10.2.153.1. Adobe recommends users of Adobe AIR 2.5.1 and earlier versions for Windows, Macintosh and Linux update to Adobe AIR 2.6. For more information, please refer to [Security Bulletin APSB11-05](#).

Adobe recommends users of Adobe Reader X (10.0.1) for Macintosh update to Adobe Reader X (10.0.2). For users of Adobe Reader 9.4.2 for Windows and Macintosh, Adobe has made available the update, Adobe Reader 9.4.3. Adobe recommends users of Adobe Acrobat X (10.0.1) for Windows and Macintosh update to Adobe Acrobat X (10.0.2). Adobe recommends users of Adobe Acrobat 9.4.2 for Windows and Macintosh update to Adobe Acrobat 9.4.3. Because Adobe Reader X Protected Mode would prevent an exploit of this kind from executing, we are planning to address this issue in Adobe Reader X for Windows with the next quarterly security update for Adobe Reader, currently scheduled for June 14, 2011. For more information, please refer to [Security Bulletin APSB11-06](#).

AFFECTED SOFTWARE VERSIONS

- Adobe Flash Player 10.2.152.33 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems
- Adobe Flash Player 10.2.154.18 and earlier for Chrome users
- Adobe Flash Player 10.1.106.16 and earlier for Android
- The Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems.

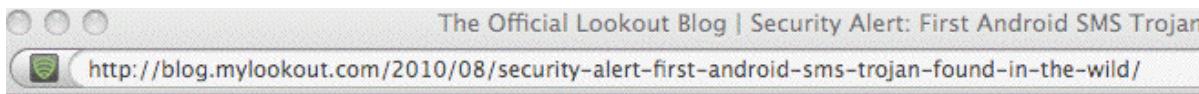
App Vetting and Third Party App Sources

- 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.

- The problem of rogue applications is not unique to just the iPhone...

A Sample Malicious Android Application



Security Alert: First Android SMS Trojan Found in the Wild

tim August 10

11 Comments

UPDATE: Lookout has pushed an over-the-air (OTA) update to automatically protect all Lookout Android users from this newly reported Trojan. If you already have Lookout installed, the update will be automatically pushed down to your device. If you don't have Lookout, go to www.mylookout.com from your phone to download it now or find Lookout in the Android Market.

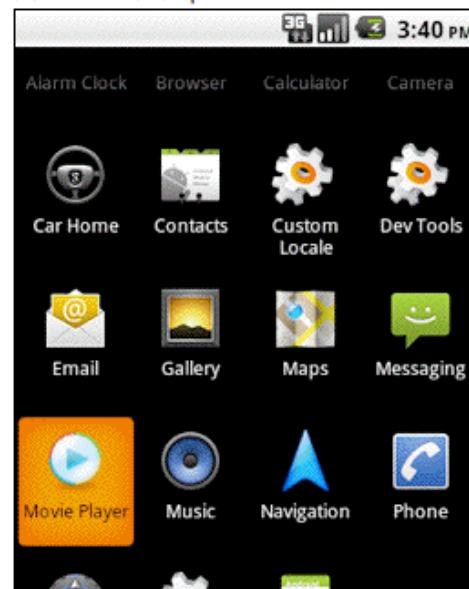
=====

Today, Kaspersky Labs reported the first SMS Trojan that infects Android smartphones.

The Threat: The Trojan is hidden inside an application called "Movie Player." Users are prompted to install an application that looks like a media player of just over 13KB to their phone from a website. Take note that the app does list "Services that cost you money (send SMS messages)" as one of the required permissions prior to installation.

How it Works: Once installed, the Trojan proceeds to send SMS messages to premium-rate numbers charging several dollars per message without the owner's knowledge or consent.

Phones it Affects: So far this has only affected Android smartphone users in Russia and only works on Russian networks. As far as we know, there is no indication that this app is in the Android Market.



15. Wireless Issues

Mobile Devices Want To Connect

- Just like many laptops, many mobile devices want to connect to any open WiFi network they can find.
- In some cases, those networks may be intentionally open, and provided by community-spirited people who want to share their good fortune with neighbors or passersby who may temporarily need network connectivity. (A noble, if rather foolhardy, decision)
- In other cases, networks may be unintentionally open, and use of those networks by random people may be unwelcome (just because my door may be unlocked, doesn't mean I want you to wander in and watch my TV).
- A third class of available WiFi networks may be malicious, and may intercept or modify any traffic passing through.
- Should your mobile devices “know to avoid random WiFi hotspots?

What About Bluetooth?

- If you don't need it, as always, turn it off.
- If you're not keeping up on wireless hacking/cracking tools in circulation, you may want to review some of the Bluetooth security tools at

[http://www.wi-foo.com/ViewPagea038.html?
siteNodeId=56&languageId=1&contentId=-1](http://www.wi-foo.com/ViewPagea038.html?siteNodeId=56&languageId=1&contentId=-1)

A Less Common BlueTooth Vulnerability



HTC Issues Hotfix for Bluetooth Vulnerability in Smartphones

By [Sumner Lemon, IDG News](#) Jul 16, 2009 7:40 pm

HTC released a software update on Thursday that fixes a Bluetooth vulnerability disclosed earlier this week by a Spanish security researcher.

The vulnerability, found in an HTC Bluetooth driver, obexfile.dll, could allow an attacker to gain access to all files on a phone by connecting to it via Bluetooth, according to Alberto Moreno Tablado, the researcher who discovered the bug in the OBEX FTP service and first reported it earlier this year.

The OBEX FTP directory traversal attack requires that a victim's phone has Bluetooth switched on and Bluetooth file sharing is activated. The vulnerability allows an attacker to move from the phone's Bluetooth shared folder into other folders. This gives the attacker access to contact details, e-mails, pictures or other data stored on the phone. They can also upload software to the phone, including malicious code.

The vulnerability affects nearly all HTC handsets running Windows Mobile 6 or Windows Mobile 6.1. HTC handsets running Windows Mobile 5 are not affected. Because the flaw is found in an HTC driver, handsets from other companies are not affected by the problem.

Moreno Tablado notified HTC of the flaw in February but the company didn't fix it, and he ultimately decided to disclose details of the vulnerability on his blog to give users a chance to protect themselves. The following day, HTC made available a [hotfix](#) for its Touch Pro, Touch Diamond, and Touch HD handsets that increases Bluetooth security.

The hotfix fixes the vulnerability that causes allows the directory traversal attack, Moreno Tablado said.

16. Some Hardware Issues

1) Non-Vendor 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.

“Apple Peel:” iPod into iPhone?



‘Apple Peel’ Inventors Defend Device Turning iPod Into iPhone

By Tim Culpan and Margaret Conley - Sep 23, 2010

Pan Lei and Pan Yong, the Chinese brothers who invented a device to convert [Apple Inc.](#)’s iPod Touch into an iPhone, say they are innovators, not copycats.

Their Apple Peel 520 is a case including a circuit board and battery that wraps around the iPod Touch media player, allowing calls to be made after software is installed. The device, which requires breaking into Apple’s operating system, isn’t a counterfeit iPhone, Pan Lei, 25, told Bloomberg Television.

“We’re capable of coming up with something original,” Pan Lei, who quit his job as an interior designer to found Shenzhen, China-based [Yosion Technology Co.](#) with his 23-year-old software- engineer brother, said in an interview broadcast today.

The iPod music player has [sold](#) more than 220 million units since it was first released in 2001, according to the company. Apple first released its iPhone in 2007, climbing to 2.7 percent of the global market by June this year and sparking copycat models from Chinese grey market, or Shanzhai, vendors.

“The brothers who invented this Apple Peel probably ran down a list of how many ways could they annoy [Steve Jobs](#),” said Jonathan Hudis, chairman of the American Bar Association’s [Trademarks and Unfair Competition](#) Division. “I could not see Apple standing by to let this continue, especially if it results in product shipping into the United States.”

U.S. users can save at least \$770 by using the device to be priced at \$60. [Jill Tan](#), a Hong Kong-based spokeswoman for Apple, said any product that’s been tampered with won’t receive warranty support. Apple is aware of Apple Peel, she said, declining to comment further.

“Very Creative”

Apple Peel sells for 520 yuan (\$78) on Taobao.com, China’s largest online shopping site. Yosion agreed to offer the device in the U.S. with New Orleans-based [Go Solar USA Inc.](#), whose website teaches users to “jailbreak” the iPod Touch in preparation for installing Apple Peel software.

Some Implications of Non-Vendor Hardware

- Manufacturers are obviously unhappy at losing profit from what they view as a key market segment to unauthorized clone makers
- Customers may get a lower quality product, or may not be able to get warranty service, or may find that in the future they can't install updated versions of the mobile device OS.
- There is also the possibility that the counterfeit device is intentionally “hardware backdoored” – you just don’t know.
- Of course, the “real thing” is also sourced offshore...

2) Are Mobile Internet Devices Tough Enough?

- Mobile devices (even devices from the real vendors!) 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?
- The best solution may be relatively inexpensive water tight cases from vendors such as drycase.com or otterbox.com

DryCase

WATE



17. Privacy Issues

Shoulder Surfing Is Still A Potential Issue

- Should you consider using something like 3M's Mobile Privacy Film to protect your mobile device display from gratuitous viewing?

See, for example:

<http://www.shop3m.com/3m-mobile-privacy-film.html>

Throw Away Prepaid Cell Phones

- One aggressive approach to mobile privacy is to use cheap throw away prepaid cell phones, and change them often.
- While this approach may not provide technical security, it may do surprisingly well when it comes to making your traffic difficult to find and intercept (assuming you don't always call the same predictable set of friends!)
- It may not work so well for incoming calls (assuming you get a new number each time you change phones). Of course, if you kept the same phone number, there wouldn't be much point to changing phones, now would there be?)

Geolocation

- Your phone knows where it is:
 - Lat, Long, Elevation (think office towers!)
 - Tower triangulation
 - GPS
- This may be unquestionably a good thing:
 - it enables voluntary location based services ("Where is the nearest Krispy Kreme donut store?")
 - I'm having a coronary but manage to dial 911
- But what if I'm a dissident in a foreign country?
- Should a court order or other paperwork be required to monitor someone's geolocation, or is geolocation data inherently public, like watching someone walk down the street?
- How much precision is "enough?"
- How long should location data be retained?

iPhone UDIDs

macnn news >

Most iPhone apps harvesting unique IDs, group claims

Only 14 percent of apps described as 'clean' Text Size ▲ ▼

updated 10:00 am EDT, Mon October 4, 2010

Most iPhone apps represent a potential privacy threat, a group of IT specialists claims. pskl.us notes that out of a collection 57 apps, taken from the App Store's Top Free and Most Popular categories, 68 percent were found to be sending UDIDs -- Unique Device Identifiers -- to servers under the developer's control each time they launch. 18 percent of the apps encrypted their data, making it unclear what they were sending. Only 14 percent of apps appeared to be completely innocuous.

The difficulty is that because UDIDs are specific to individual devices, they can potentially be used to track a person. At least some of the tested apps are said to be capable of pairing UDIDs with real-world personal data. pskl compares the situation to that of the Pentium III, which generated a serial number that could be used to track a person's online activity. Intel ultimately removed the technology from its processors due to protest, but people don't seem to be as concerned about iPhone apps, pskl [observes](#).

No active threats have been identified, and Apple's official guidelines for developers generally prohibit harvesting personal information. "For user security and privacy, you must not publicly associate a device's unique identifier with a user account," one section reads. A lack of shared data has actually been a concern of magazine and newspaper publishers, who may be having a [harder time marketing ads in iOS apps](#) as a result.

And Now With Mobile Devices Getting Used for 2nd Channel Auth Purposes: Zitmo

The screenshot shows a web browser window with the following details:

- Address bar: http://blog.fortinet.com/tag/zitmo/
- Title bar: Zitmo | Fortinet Security Blog
- Content area:
 - Section title: What's new in Zitmo.B?
 - Author: Axelle Apvrille
 - Date: February 23, 2011 at 7:43 am
 - Share icons: Facebook, Twitter, Email, and a share button.
 - Text: "Zitmo is a mobile malware Fortinet has particularly been focusing on since the beginning (see our [first blog post](#) and my [presentation](#) at ShmooCon 2011) as it is one of the first palpable signs organized criminals show interest in infecting mobile phones. As you may know (see [F-Secure](#) and [Kaspersky's](#) blog posts), it is unfortunately back, with a new version."
 - Text: "So, technically speaking, what's new?"
 - List:
 - » it now supports [Windows Mobile](#) phones too. Not only Symbian (there were rumors concerning a BlackBerry version – never confirmed).
 - » the default phone number it sends intercepted SMS to has changed, though it is still a mobile phone number, in the UK and probably from the same operator.
 - » it intercepts both incoming and outgoing SMS. The previous version only intercepted incoming SMS and did not care about outgoing ones. It is possible this feature isn't actually used by the gang, but has just been put back in the executable from "SMS Monitor", the trojan spyware Zitmo is highly inspired from.
 - » it sends an SMS (to the UK number by default) with the text "app installed ok" each time a SET ADMIN command is processed. In the previous version, this SMS was only sent at the first install of the trojan.
 - » it features a new command "UNINSTALL"... which actually installs a new package (see Figure below). Zitmo searches on the mobile phone for a file named c:\system\apps\u.dat (note the file is not downloaded from the web – Zitmo does not connect to Internet). The extension of this file is intentionally misleading, it is actually a Symbian package. Zitmo renames it u.sisx and silently installs it on the phone (no prompt no confirmation).

Mobile Money (Mobile Phishing, Too?)

[America.gov](#) (Washington, DC)

Africa: Cell Phone Technology Can Empower the World's Poorest

Stephen Kaufman

4 August 2010

Global cellular phone coverage has far outpaced the expansion of essential services such as water and electricity, as well as access to financial services. For this reason, "mobile money" is seen as a means to transform the notion of banking around the world, and broaden access to credit, insurance and secure savings that are desperately needed in the developing world as individuals seek to enhance their well-being and emerge from poverty.

[Email](#) | [Print](#) | [Comment](#)

Share:



The rapid proliferation of cellular phones around the world "has changed the course of human development," Under Secretary of State for Democracy and Global Affairs Maria Otero said August 2 at the State Department conference "Tech@State: Mobile Money and Financial Inclusion."

Yet, at the same time, 1.7 billion low-income cell phone users do not have a bank account. In effect, they "remain outside of the realm of economic opportunities that is represented by financial access," she said.

Through their phone connections, small business owners, farmers and others either living in rural areas or at the bottom end of the socio-economic pyramid are obtaining the ability to communicate instantly and transfer funds to individuals and institutions. The service provides a quick, secure and transparent means of performing transactions. The widespread dissemination of cellular phones also means that the relative few without a phone likely will have a close friend or relative they could turn to for the same purposes.

18. Health and Safety Issues

Cellular Radiation Risks

- Each phone has a Specific Absorbtion Rate, or SAR, and cannot exceed 1.6 watts per kilogram by law in the U.S.
- SARs vary dramatically from phone to phone, see
[http://www.ewg.org/cellphoneradiation/
Get-a-Safer-Phone?allavailable=1](http://www.ewg.org/cellphoneradiation/Get-a-Safer-Phone?allavailable=1)
- Are you and your users even thinking about this issue?
- Use of blue tooth hands-free devices may at least move the primary radiation source somewhat away from your brain, or minimize your usage (yeah, right!)

DWD (Driving While Distracted)

- Use of cell phones while driving is widely prohibited, although in some cases it is allowed if you use a “hands free” kit (as suggested on the preceding page)
- Bottom line, it still distracts you from what you’re (supposed to be) doing: driving
- Is DWD the biggest potential “health risk” of them all?
- Does your institution have policy guidance on this sort of thing for employees who are operating institutional motor vehicles, or who routinely log a lot of miles?

Thanks For the Chance to Talk!

Are there any questions?

What did we forget to cover that we should have mentioned?