The Security of Mobile Internet Devices

Northwest Academic Computing Consortium (NWACC)
2010 Network Security Workshop

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

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

This talk has been prepared in a detailed format for ease of indexing and to insure accessibility for the disabled.

Acknowledgement and Disclaimer

- I'd like to begin by thanking Adrian Irish for the opportunity to share some thoughts with you today.

- I'd also like to thank NWACC for continuing to host these security workshops. I know there are a lot of topics competing for NWACC attention and support, so it's gratifying to see network and system security continuing to be identified as a topic of ongoing interest.

- Because I wear a variety of different "hats" from time-to-time, let me keep this talk straightforward by offering the following simple disclaimer: the opinions expressed in this talk are solely those of the author, 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 I sometimes do), I decided that I wanted to try to have this be at least a little more of an interactive session.

  I know some of you are likely tired from all the earlier sessions held as part of this workshop, and some of you may even feel ready to be heading home, so let me say thank you for sticking it out for the very last session!

- Anyhow, what I'm hoping 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. This is a bit of an experiment…

1. What *Is* A Mobile Device? Are Your Users Using Them?

iPhones, BlackBerries, etc.

- I 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 (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. :-)
- *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?"*

Are Students Using Them? Yes

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

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

- Another study, by the Ball State Institute for Mobile Media Research, states that 99.8% of all students have a cell phone and "smart phones now account for 49% of mobile communication devices on campus," see http://www.bsu.edu/news/article/0,1370,7273-850-64351,00.html

Mobile Internet Devices at UO

- A local Eugene example: "High Tech Ubiquitous on Campus," Eugene Register Guard, Thursday, Sept 20, 2010, www.registerguard.com/csp/cms/sites/web/news/cityregion/25348487-41/corner-welch-bookstore-hall-cell.csp

  Reporter Bob Welch surveyed the campus scene near the UO Bookstore last month, and found that these days…

  > […] what you mainly see is gobs of students talking on phones, texting on phones and grooving to who knows what inside their white-budded ears. Of a random sample of 100 young people, 44 were either talking, Tweeting or texting on phones — or plugged into headphones. Sometimes both. [article continues]

What About Faculty/Staff?

- Faculty/staff ownership of mobile internet devices is more complicated:
  -- costs of service plans can be high ("It costs HOW much per month for your data plan???"), and
  -- historically the IRS has treated them oddly (see www.irs.gov/govt/fslg/article/0,,id=167154,00.html) although thankfully that issue is beginning to get 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. (Revised tax guidance from the IRS is expected)
  -- **there are a variety of devices available, so which one(s) should the institution buy and support? What are you doing at your school?**

2. *Which* Mobile Devices *Should* You 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 <u>should</u> 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 4.x:
  secunia.com/advisories/product/14662/?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?

More Likely Strategy: Pick What's "Popular"

- If you don't have a better strategy, another option is to pick what's most popular, and just support those sort of devices.

- So what are the most popular Internet mobile devices?

- Well, it can vary…

Mobile Internet Devices, *U.S.* Market Share

- Reportedly, U.S. market share information as of July 2010 (see tinyurl.com/comscore-mkt-share-2) looks like:

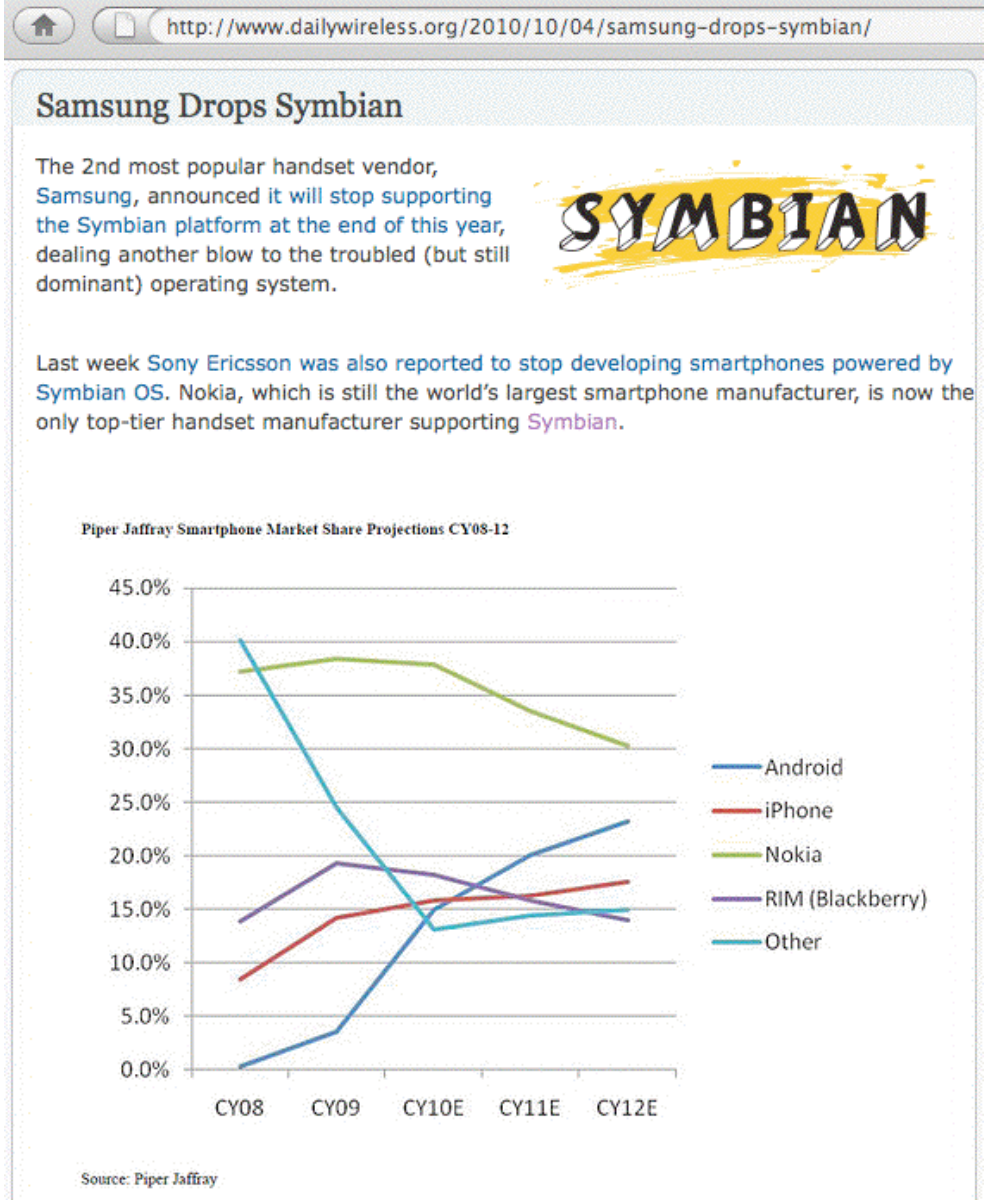
-- Research In Motion (e.g., Blackberry):	39.3%
-- Apple (iPhones):	23.8%
-- Google (Android):	17.0%
-- Microsoft (Windows Mobile)	11.8%
-- Palm (Palm Pixi, Palm Pre, etc.)	4.9%
-- Other	3.2%

A Second Take On Smart Phone Market Share

- Worldwide smart phone market share, 2Q10, Gartner:

-- Symbian	***41.2%***
-- Research In Motion (e.g., Blackberry):	18.2%
-- Google (Android):	17.2%
-- Apple (iPhones):	14.2%
-- Microsoft (Windows Mobile)	5.0%
-- Other	4.2%

But Note, When It Comes to Symbian…



http://www.dailywireless.org/2010/10/04/samsung-drops-symbian/

Samsung Drops Symbian

The 2nd most popular handset vendor, Samsung, announced it will stop supporting the Symbian platform at the end of this year, dealing another blow to the troubled (but still dominant) operating system.

Last week Sony Ericsson was also reported to stop developing smartphones powered by Symbian OS. Nokia, which is still the world's largest smartphone manufacturer, is now the only top-tier handset manufacturer supporting Symbian.

Piper Jaffray Smartphone Market Share Projections CY08-12

Source: Piper Jaffray

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

- Some device types are exceptionally popular (in general)

- **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…

Sample Apple iPhone 4

ROGERS
2:03 PM
Difference Between | Difference Between Similar Terms and Objects
www.differencebetween.net/
Google
Home
About
Archives
Contact Us
Resources
DifferenceBetween.net
Difference Between Similar Terms and
Objects
Technology
Miscellaneous
Science
Yin&Yang
Difference Between Yin and Yang

commons.wikimedia.org/wiki/File:Safari_iphone.JPG

Sample Blackberry Devices

commons.wikimedia.org/wiki/
File:Blackberry_Storm.JPG

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

Sample Windows Mobile Device

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

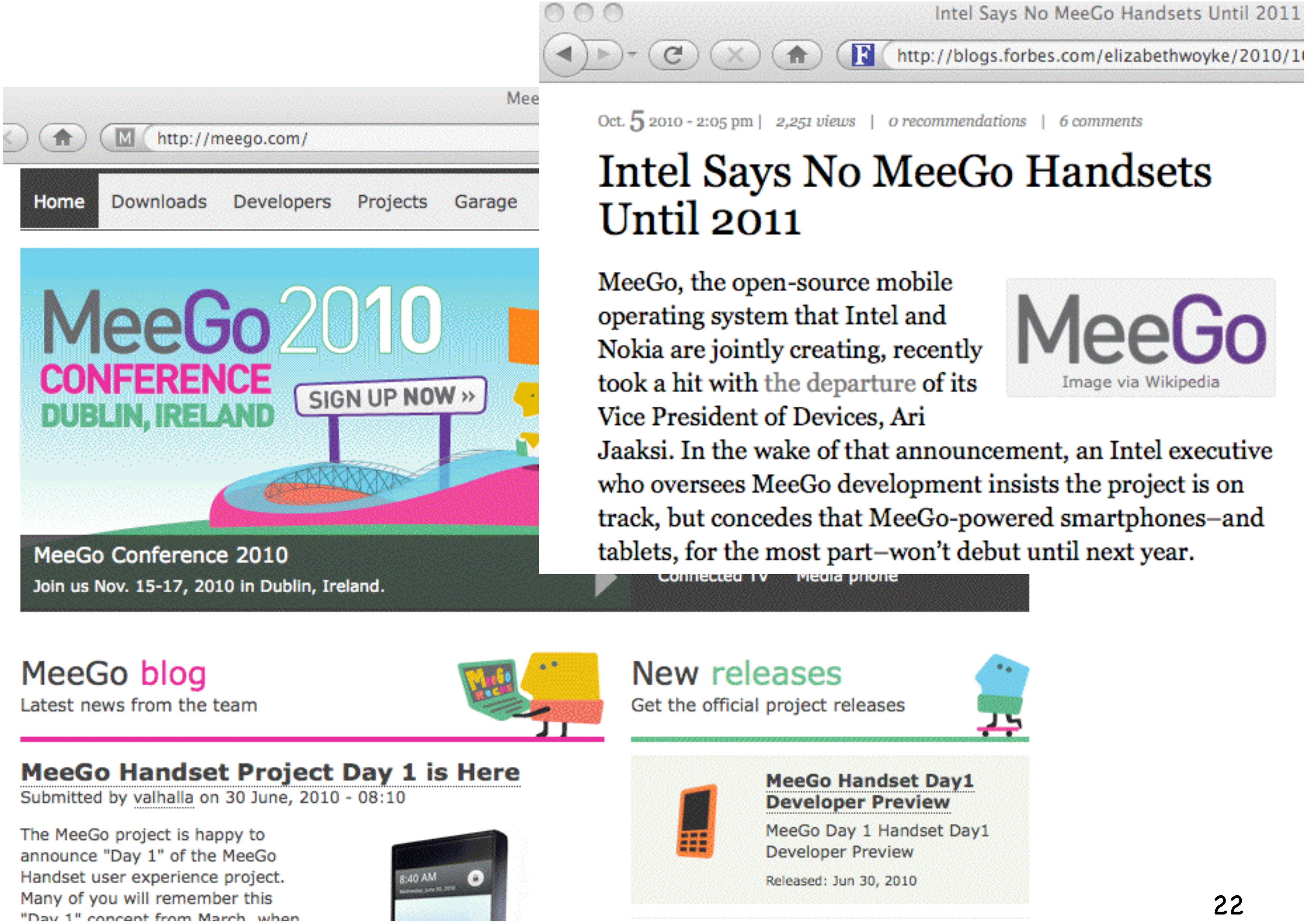
tinyurl.com/samsung-windows-mobile

Sample Symbian Devices

tinyurl.com/symbian-nuron

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

What About "Open Source" Mobile Devices?



Oct. 5 2010 - 2:05 pm | 2,251 views | 0 recommendations | 6 comments

Intel Says No MeeGo Handsets Until 2011

MeeGo, the open-source mobile operating system that Intel and Nokia are jointly creating, recently took a hit with the departure of its Vice President of Devices, Ari Jaaksi. In the wake of that announcement, an Intel executive who oversees MeeGo development insists the project is on track, but concedes that MeeGo-powered smartphones–and tablets, for the most part–won't debut until next year.

MeeGo

Image via Wikipedia

MeeGo Conference 2010

Join us Nov. 15-17, 2010 in Dublin, Ireland.

MeeGo blog

Latest news from the team

MeeGo Handset Project Day 1 is Here

Submitted by valhalla on 30 June, 2010 - 08:10

The MeeGo project is happy to announce "Day 1" of the MeeGo Handset user experience project. Many of you will remember this "Day 1" concept from March, when

New releases

Get the official project releases

MeeGo Handset Day1 Developer Preview

MeeGo Day 1 Handset Day1 Developer Preview

Released: Jun 30, 2010

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/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 only be allowed to purchase devices listed on a mandatory/exclusive contract.**

Beware "Contract Lock-In" On Old, Crumby Devices

- 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.
- If you have a limited list of "approved" mobile Internet devices, negotiated three or four years ago based on what was available then, what's on the list today will definitely 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!

3. GSM? iDEN? CDMA?

Choice of Connectivity

- Not all phones use the same sort of connectivity.

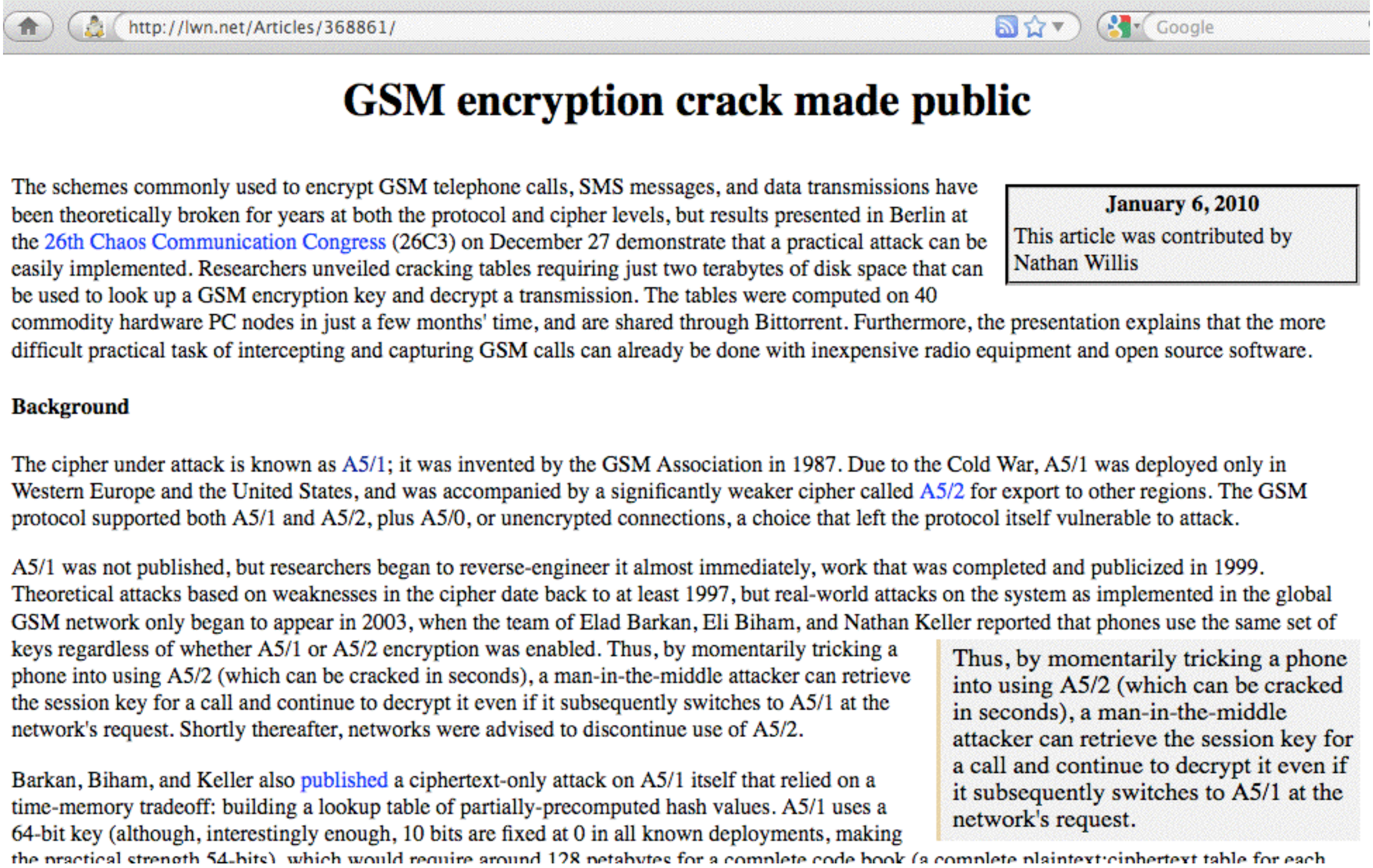
- At the same time your university is deciding on which mobile internet device operating systems it will support, you should also be thinking about the sort of connectivity your phones-of-choice will be using.

- 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 (82% 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.
- Uses SIM cards (but some phones may be “locked”)
- Unfortunately both GSM’s A5/1 and A5/3 encryption *have* been cracked



GSM encryption crack made public

January 6, 2010

This article was contributed by Nathan Willis

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.

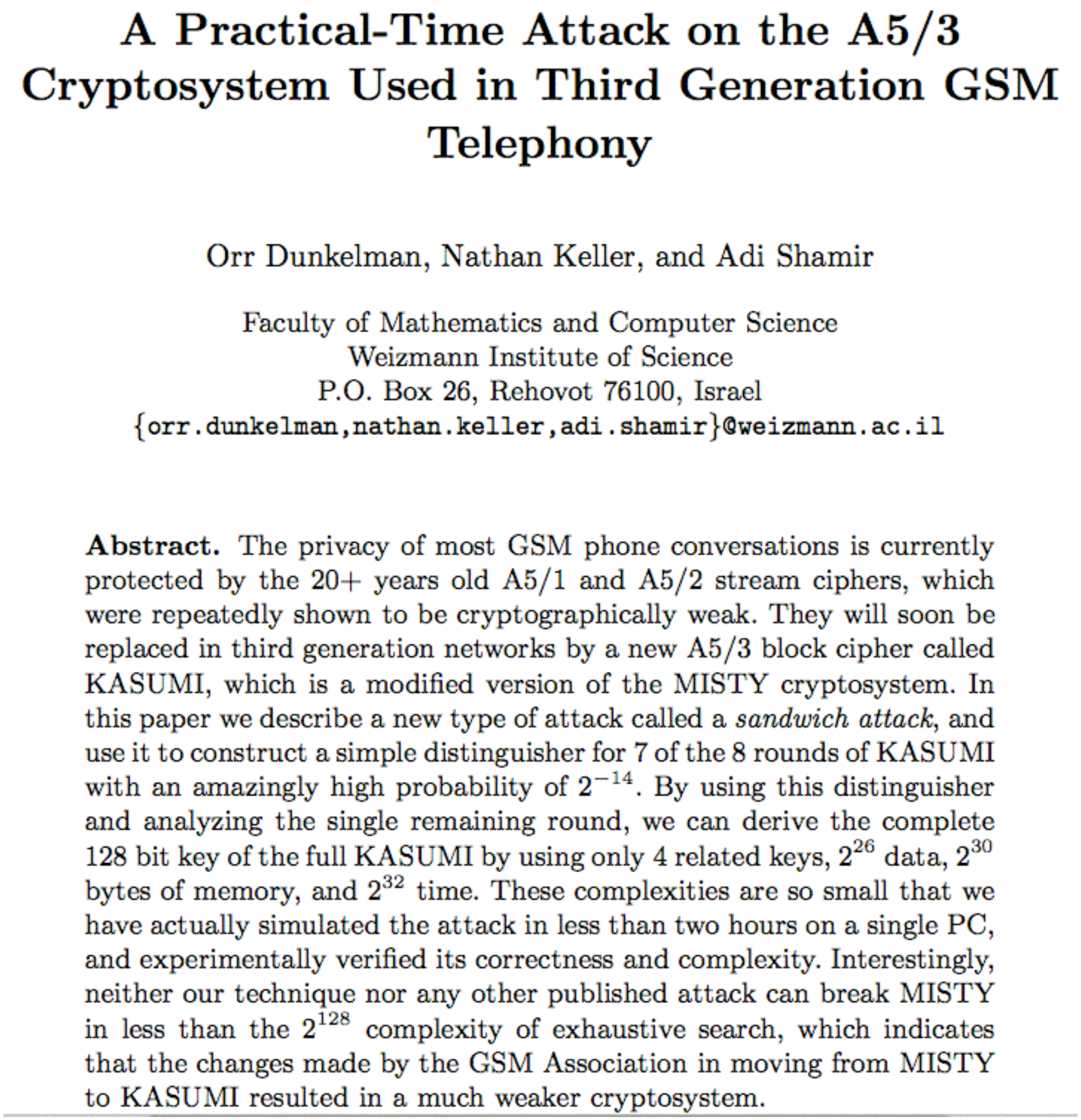
Background

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.

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.

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 code book (a complete plaintext:ciphertext table for each



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

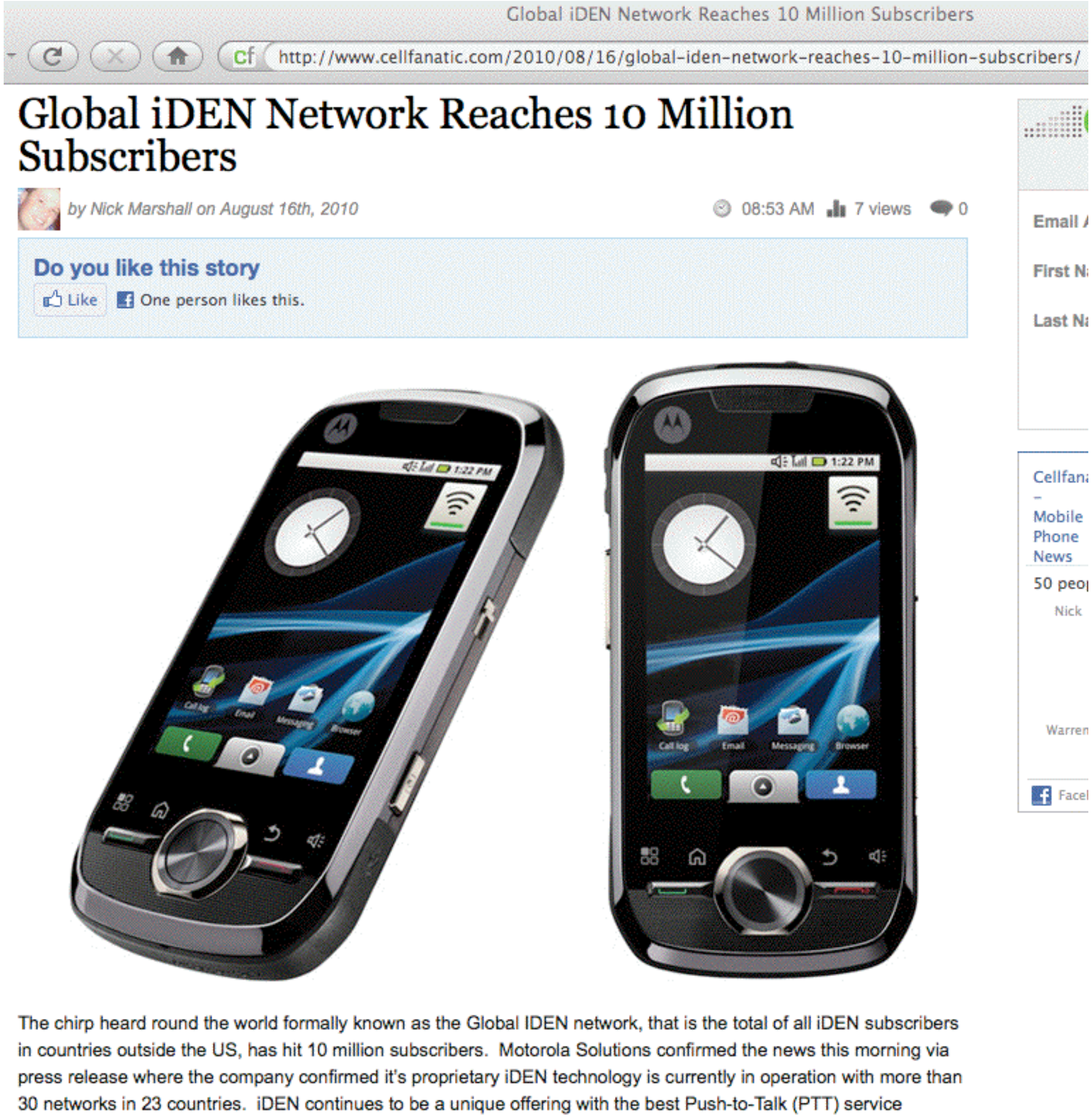
  www.tombom.co.uk/blog/?p=262 (August 1st, 2010)

  (odp file extension == OpenOffice)

iDEN

- Integrated Digital Enhanced Network.
- Motorola proprietary format.
- 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
- Popular with federal "three letter agencies" and local/ regional emergency personnel, courtesy van drivers, etc.
- There have been persistent rumors that iDEN will be phased out, reserved for **exclusive** use by the Feds, etc.
- Uses SIM cards (not compatible with GSM SIM cards)

Rumors of iDEN's Demise Are Premature



Global iDEN Network Reaches 10 Million Subscribers

by Nick Marshall on August 16th, 2010

The chirp heard round the world formally known as the Global IDEN network, that is the total of all iDEN subscribers in countries outside the US, has hit 10 million subscribers. Motorola Solutions confirmed the news this morning via press release where the company confirmed it's proprietary iDEN technology is currently in operation with more than 30 networks in 23 countries. iDEN continues to be a unique offering with the best Push-to-Talk (PTT) service

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: if you want an iPhone, that's a "GSM only" proposition (at least for now; rumors about release of a CDMA iPhone continue to circulate – we'll see what comes out next year)
- 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.
- 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?*
- CAN you influence what phones people buy and use?

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

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

- ***Who at your site has a mobile Internet device?***

- You simply may not know -- users will often independently purchase mobile devices (particularly if it's hard/uncommon for a site to do so for its staff)

- Those devices may connect via a third party/commercial network, and *may* not even directly access your servers.

- If those devices *do* access your servers, unless they have to authenticate to do so, you may not know that it is a device belonging to one of your users.

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 <u>care</u> that it exists?"*** (Not quite as pithy as, "If a tree falls in the forest when no one's around, does it still make any sound?" but you get the idea). <u>**Yes, you *should* care.**</u>

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

Want Influence? It'll Probably Cost You…

- This is the slide that I hate having to include, but truly,

  If you want the ability to influence/control what happens on mobile Internet devices on your campus, you're probably going to need to "buy your way in."

- 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) <u>what</u> gets purchased,
  (b) <u>how</u> those devices get configured, and
  (c) (maybe) you'll then even know <u>who</u> 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)
- For example, while the iPhone 3GS itself starts at just $99, and the iPhone 4 starts at just $199, the monthly recurring costs currently range from a bare-bones plan at $54.95/month all the way up to $114.99/month from AT&T in the U.S.; a text messaging plan, if desired, adds up to another $20/month.
- Thus, non-device costs for iPhones for 20,000 users for a year would cost from $54.99/month*12 months/year *20,000 = **$13,197,600/yr** all the way up to **$32,397,600** (e.g., ($114.99+$20)*12*20,000). That's a *chunk* of money.

Those Cost Aren't Just an "iPhone" Thing

- Some folks may think that the prices mentioned are purely an artifact of Apple/AT&T. They're not.

- For example, domestic 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/month*12 months*20,000 = $28,795,200/yr to service 20,000 users.

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

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 retail price is the price applicable to higher ed users; always check for existing special pricing, and don't hesitate to negotiate!

- Even if you can't chisel much off the price sometimes, you may at least get better contract terms as part of that arrangement.

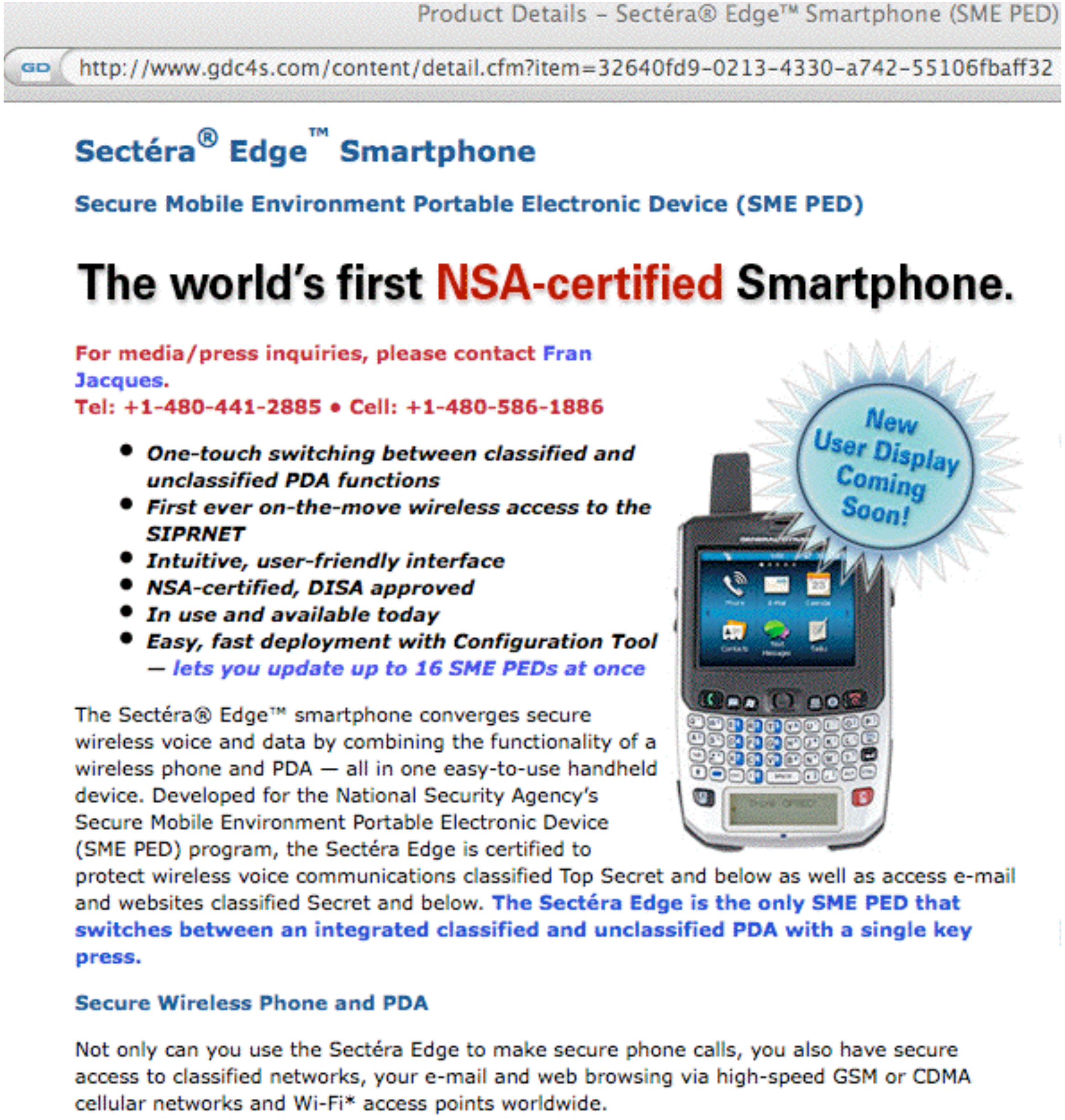
- *Has YOUR college wrestled with the financial issues associated with mobile devices? If so, did you come up with any solutions?*

5. Mobile Device Policies

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)

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

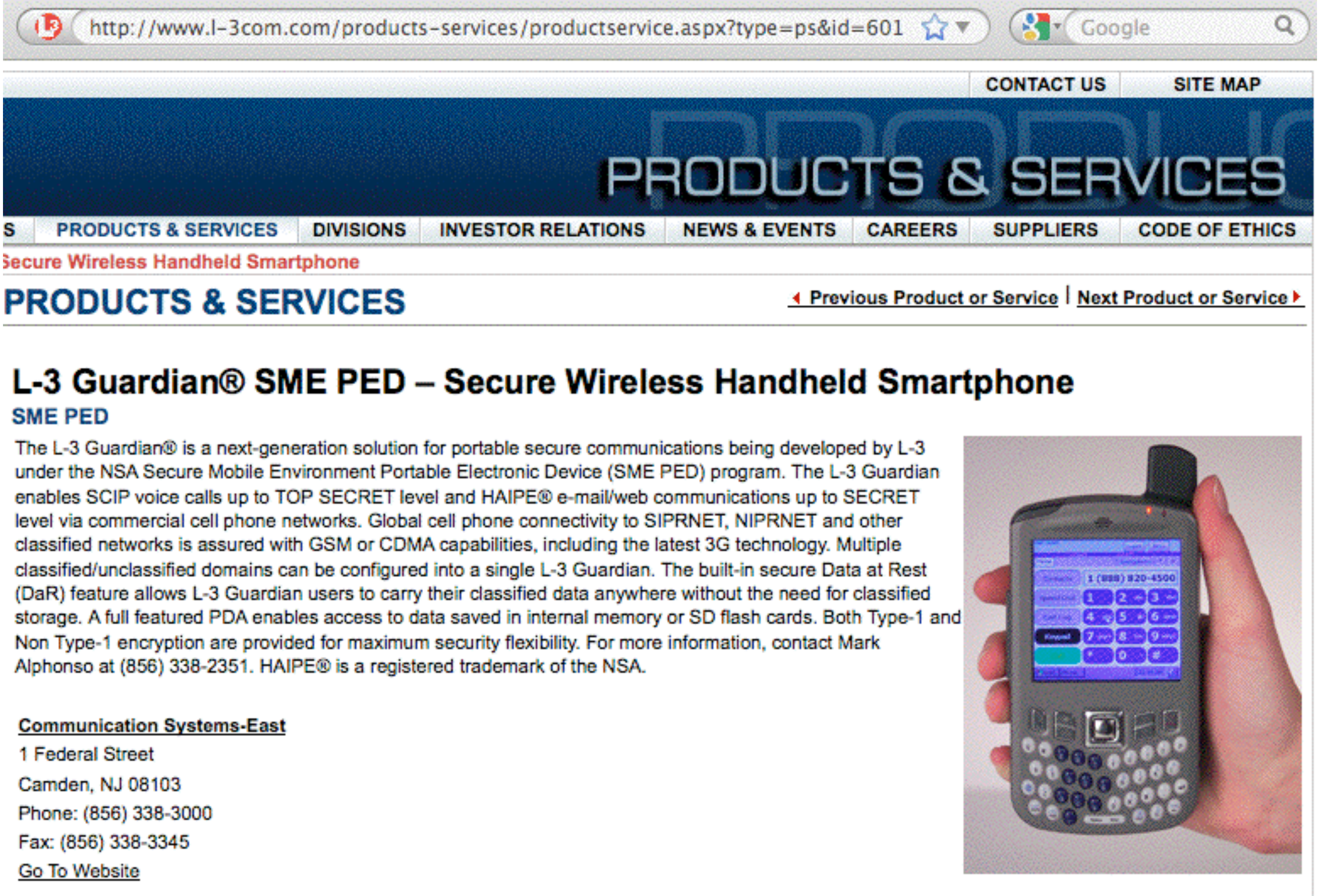
- ***One-touch switching between classified and unclassified PDA functions***
- ***First ever on-the-move wireless access to the SIPRNET***
- ***Intuitive, user-friendly interface***
- ***NSA-certified, DISA approved***
- ***In use and available today***
- ***Easy, fast deployment with Configuration 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



PRODUCTS & SERVICES

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" <u>We</u> 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 get 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?

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

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

An Example Device Policy: Device Passwords

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

Managing Mobile Internet Device Policies

- 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://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Example:
What Can Be Required for iPhone Passwords?

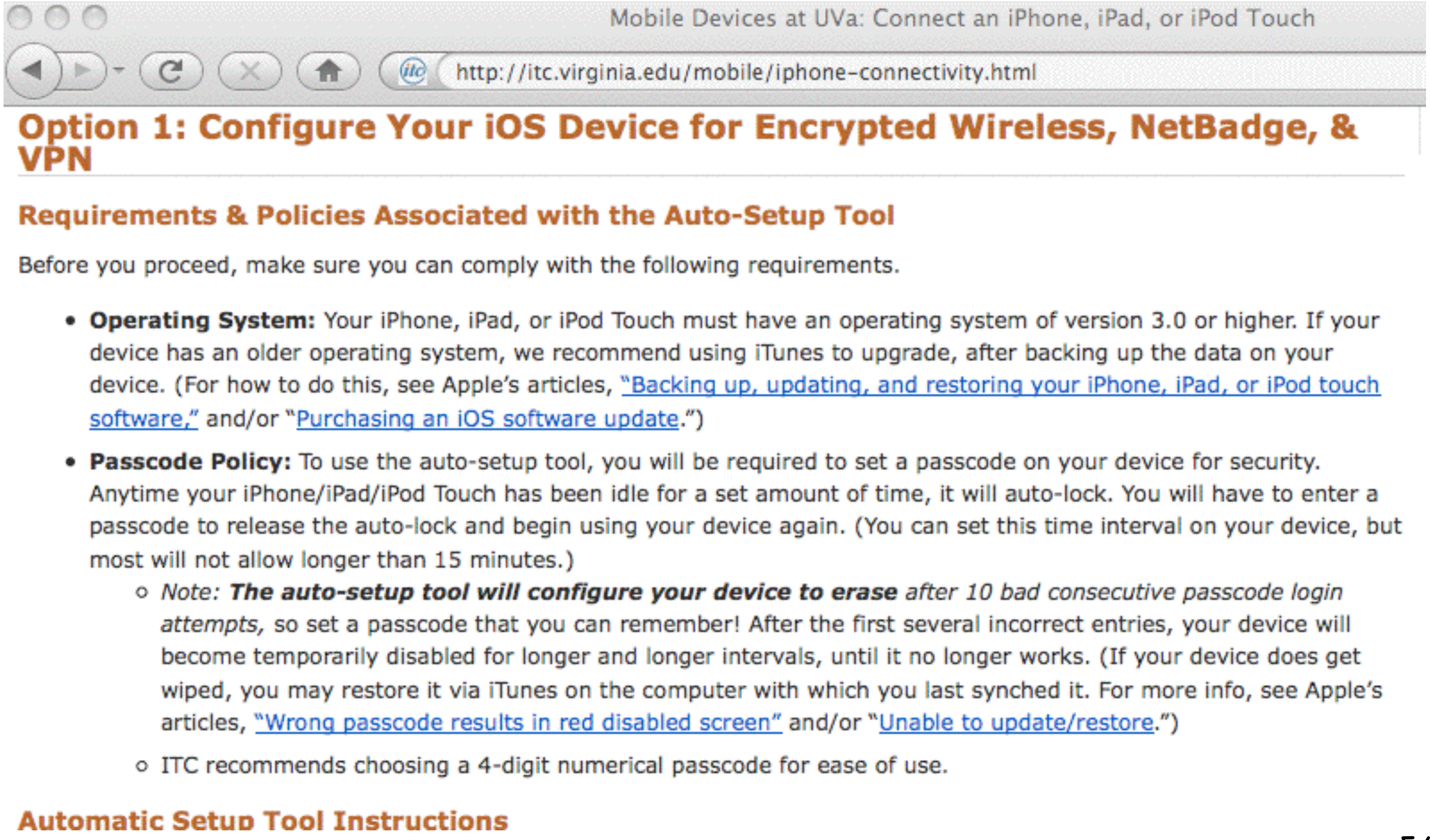
- Looking at the iPhone Enterprise Deployment Guide:

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

- RIM offer similar controls for BlackBerry devices.

What Policies Has Your Site Adopted?

- Do you have mobile Internet device-specific policies at your site? An example from UVa:



Mobile Devices at UVa: Connect an iPhone, iPad, or iPod Touch
http://itc.virginia.edu/mobile/iphone-connectivity.html

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

Other Potential Local iPhone “Policies” Include

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

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

Scalably Pushing Policies to the iPhone

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

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

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

  -- change their name servers (and if I can change their name servers, I can <u>totally</u> 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.

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 cell phones be silenced or turned off completely 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 later.

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.

Phones in Another "Controlled Environment"

- If you think higher ed struggles with its mobile internet devices, things are far worse in some other environments.
- For example, cell phones are routinely banned outright in most prisons, but reportedly contraband cell phones may sell "inside" for as much as $5,000.* (Inmates cherish cell phones because they allow them to remain surreptitiously in control of criminal enterprises even while incarcerated)
- Some prison authorities have begun to lobby for authority to use cell phone jammers to control inmate cell phone use, however the FCC has historically been unwilling or unable to permit their use, even in penitentiaries. (Sniffers or passive detection may be an option, however)

----

* "Cell phones behind bars: Can you hear me now?" http://www.corrections.com/articles/13233-cell-phones-behind-bars-can-you-hear-me-now-

Mobile Device Forensic Tools

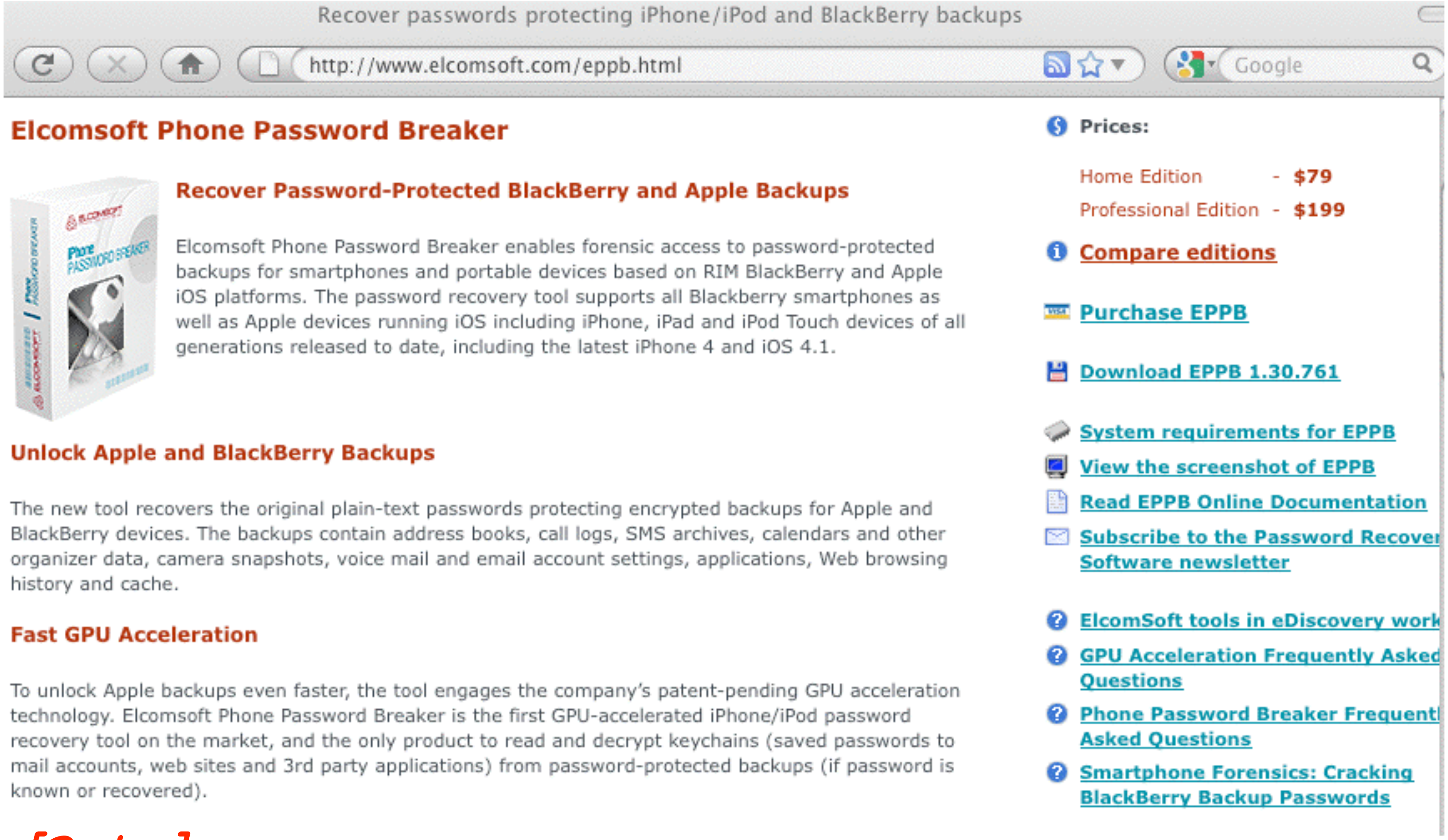
- What if an iPhone **IS** lost/stolen/seized/confiscated, what sort of information might be able to be recovered?
- See the book “iPhone Forensics” by Jonathan Zdziarski, http://oreilly.com/catalog/9780596153595
- Some (of many) potential tools (in alphabetical order):
  -- Device Seizure, http://www.paraben.com/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

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

What About Hardware Encryption?

- An example of a common security control designed to protect PII from unauthorized access is hardware encryption. For example, many sites require "whole disk" encryption on all institutional laptops containing PII.
- Some mobile Internet devices (such as earlier versions of the iPhone) did not offer hardware encryption; 3GS 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.

Professional Phone Password Recovery Tools



Recover passwords protecting iPhone/iPod and BlackBerry backups
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**

Compare editions

Purchase EPPB

Download EPPB 1.30.761

System requirements for EPPB

View the screenshot of EPPB

Read EPPB Online Documentation

Subscribe to the Password Recover Software newsletter

ElcomSoft tools in eDiscovery work

GPU Acceleration Frequently Asked Questions

Phone Password Breaker Frequentl 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.

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 <u>manually</u>, be sure to set
  -- Content Protection, AND
  -- Enable Media Card Support, AND Encrypt Media Files
- If setting encryption <u>centrally</u>, be sure to set all of…
  -- Content Protection Strength policy rule
  -- External File System Encruption Level policy rule
  -- Force Content Protection for Master Keys policy rule
- ***For "stronger" or "strongest" Content Protection levels, set min pwd length to 12 or 21 characters, respectively***

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.

Remotely Zapping Compromised Mobile Devices

- Strong device passwords and hardware encryption are primary protections against PII getting compromised, but another potentially important option is being able to remotely wipe the hardware with a magic "kill code." Both iPhones and BlackBerry devices support this option.
- Important notes:

  -- If a device is taken off the air (e.g., the SIM card has been removed, or the device has been put into a electromagnetic isolation bag), a device kill code may not be able to be received and processed.

  -- Some devices (including BlackBerries) acknowledge receipt and execution of the kill code, others may not.

  -- Pre-3GS versions of the iPhone may take an hour per 8GB of storage to wipe; 3GS's wipe instantaneously.

Terminating Mobile Device-Equipped Workers

- A reviewer who looked at a draft of these slides pointed out an interesting corner case for remote zapping:

  -- Zap codes are usually transmitted via Exchange Active Sync when the mobile device connects to the site's Exchange Server, and the user's device authenticates

  -- HR departments in many high tech companies will routinely kill network access and email accounts when an employee is being discharged to prevent "incidents"

  -- If HR gets network access and email access killed <u>before</u> the zap code gets collected, the device may not be able to login (and get zapped), leaving the now ex-employee with the complete contents of the device

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

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?
- What if the employee is using a personally purchased mobile devices?

6. Mobile Device Applications

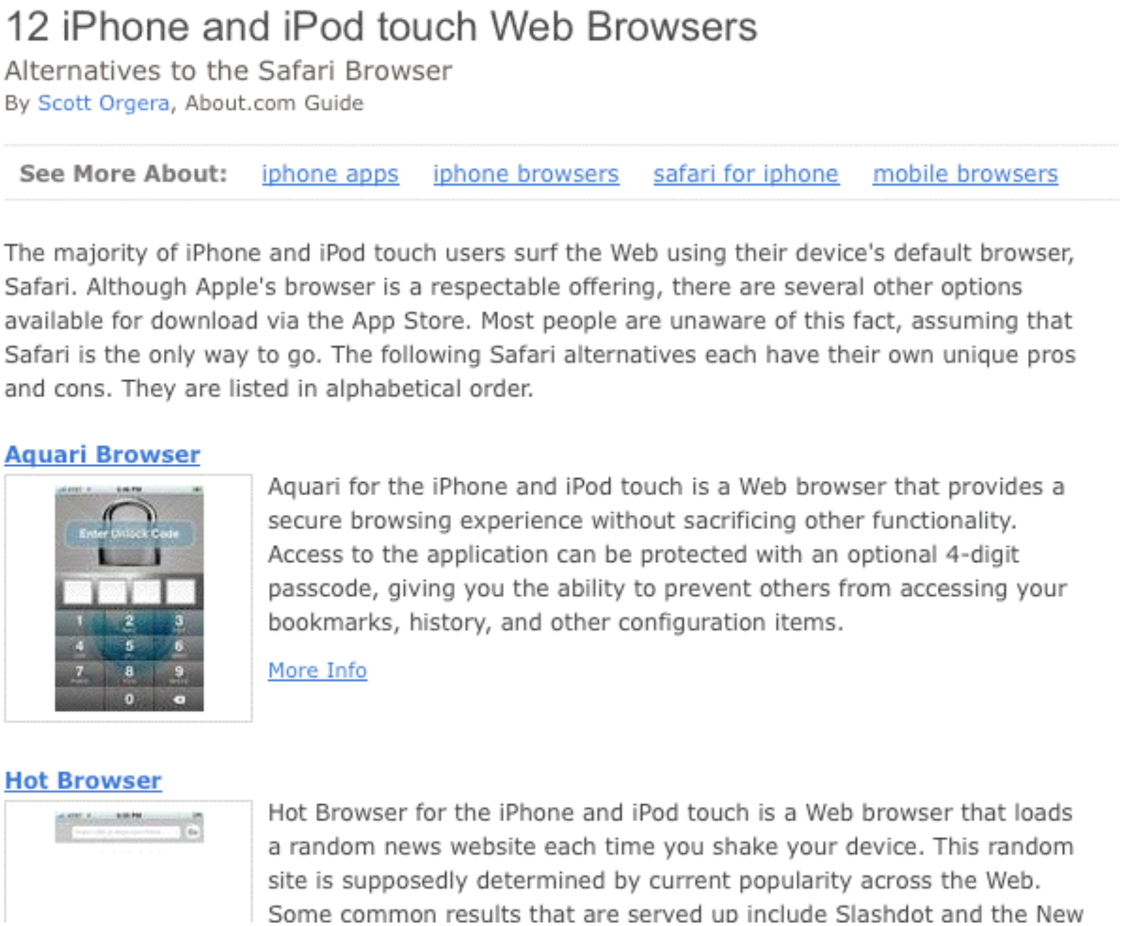
Mobile Devices as Terminals/X Terminals

- 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)

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

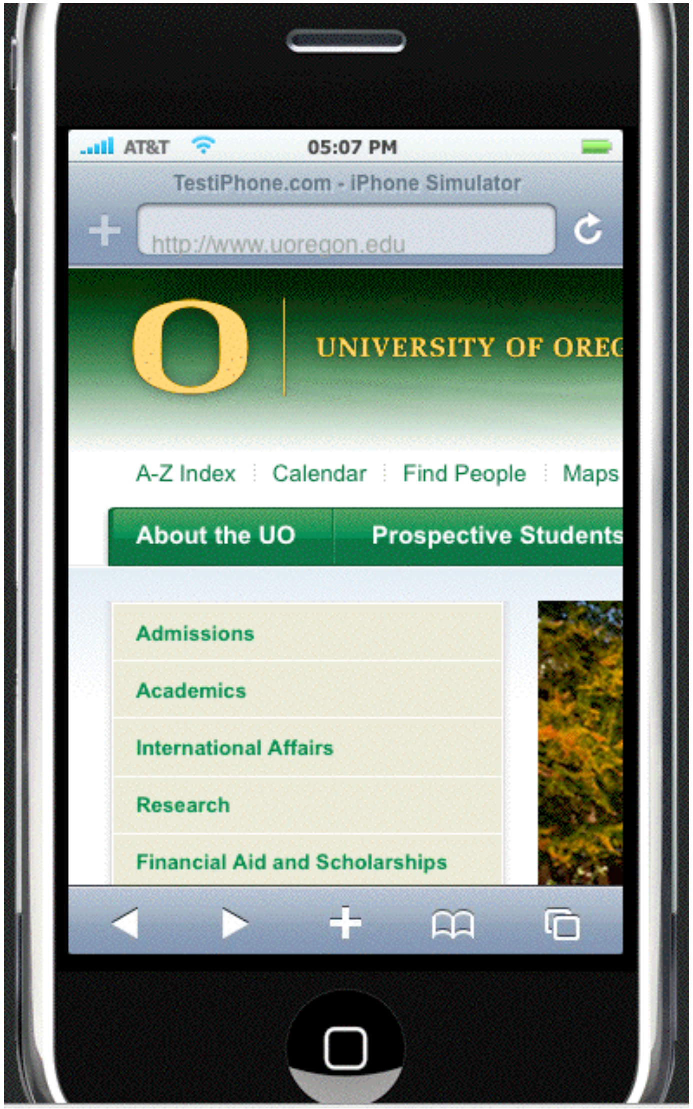
Back End Servers Supporting Mobile Devices

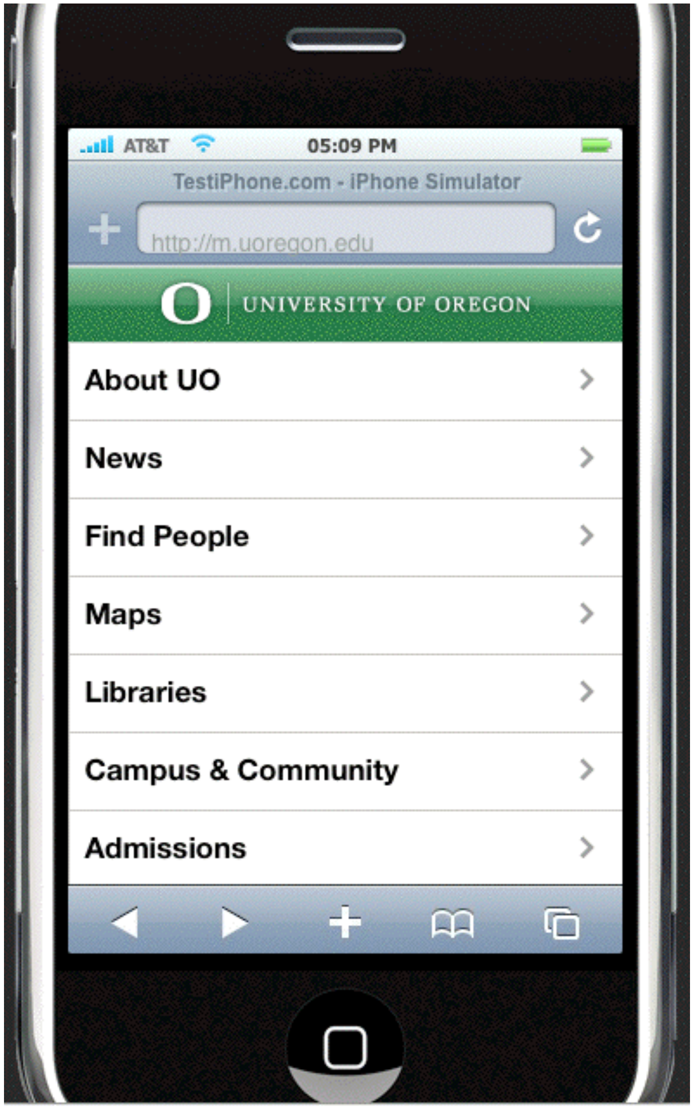
- Many mobile Internet apps, not just Opera Mini, rely on services provided by back end servers -- sometimes servers which run locally, othertimes servers which run "in the cloud."
- If those servers go down, your service may be interrupted. This is a real risk and has happened multiple times to BlackBerry 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.html
  See http://www.dataoutagenews.com/ for more outages.
- Availability is, or can be, another critical information security consideration (remember "confidentiality, integrity and ***availability***"!)

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)

7. Spam, Malware, and Broken Jails

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 offering from traditional market leaders such as Symantec and McAfee at that time.

- On the other hand, since the iPhone used/uses a sandbox-and-cryptographically "signed app" model, it was hard for the iPhone to get infected.

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

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.

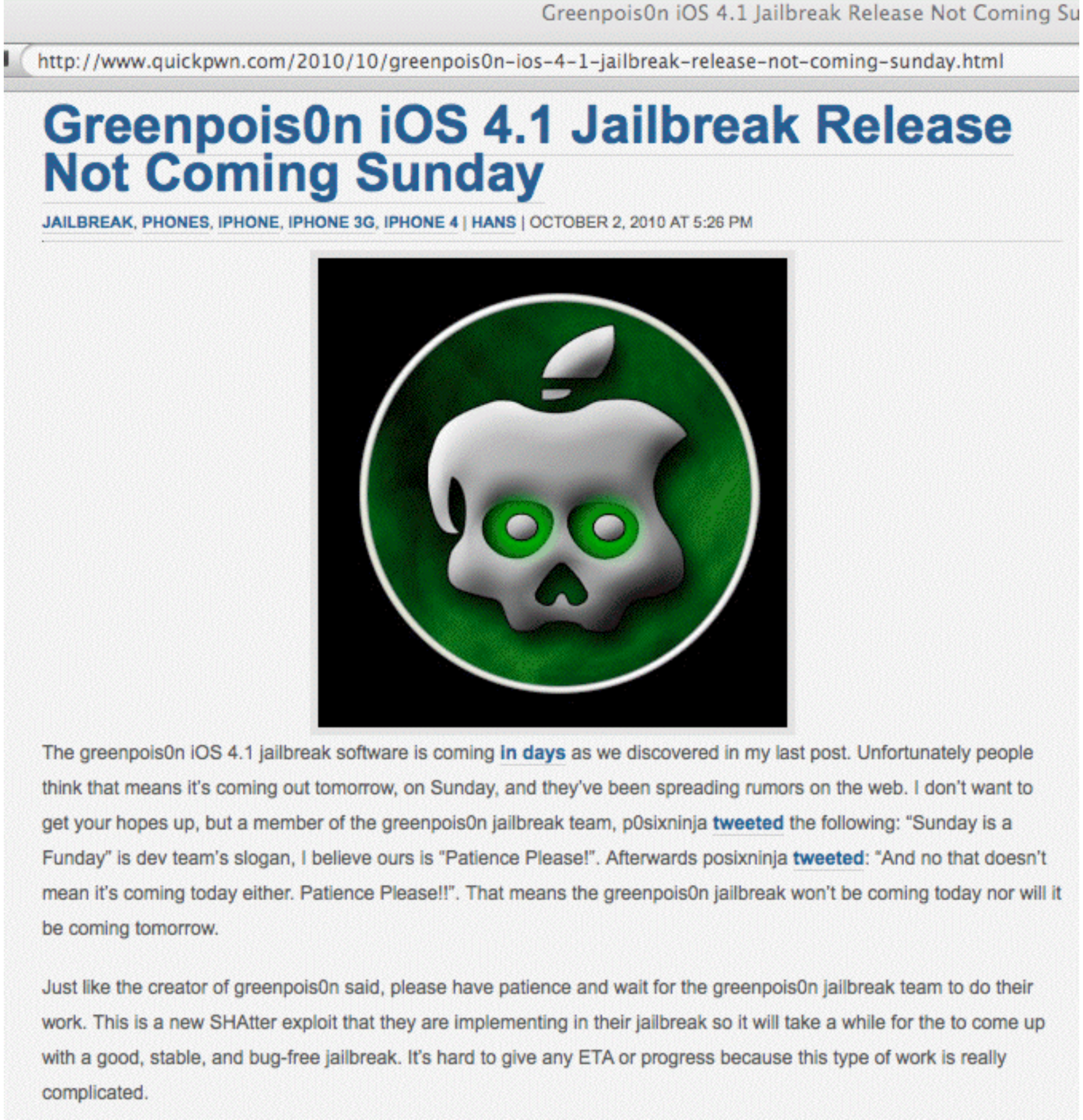
Jail Breaking Apps Are OS Release-Specific

- 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 (eventually) accomplish this, such as…

GreenpoisOn for iOS 4.1



GreenpoisOn iOS 4.1 Jailbreak Release Not Coming Su
http://www.quickpwn.com/2010/10/greenpois0n-ios-4-1-jailbreak-release-not-coming-sunday.html

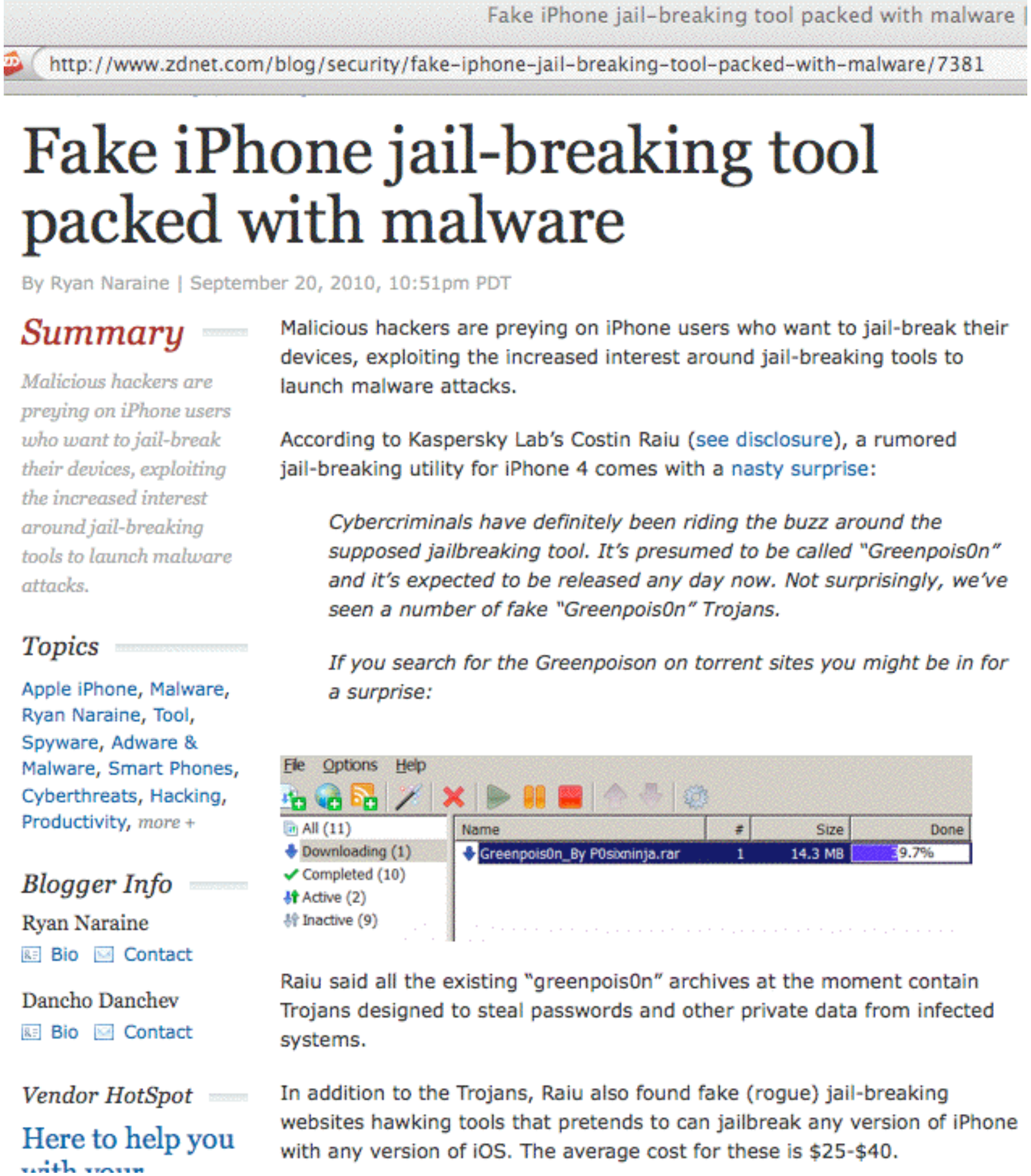
Greenpois0n iOS 4.1 Jailbreak Release Not Coming Sunday

JAILBREAK, PHONES, IPHONE, IPHONE 3G, IPHONE 4 | HANS | OCTOBER 2, 2010 AT 5:26 PM

The greenpois0n iOS 4.1 jailbreak software is coming in days as we discovered in my last post. Unfortunately people think that means it's coming out tomorrow, on Sunday, and they've been spreading rumors on the web. I don't want to get your hopes up, but a member of the greenpois0n jailbreak team, p0sixninja tweeted the following: "Sunday is a Funday" is dev team's slogan, I believe ours is "Patience Please!". Afterwards posixninja tweeted: "And no that doesn't mean it's coming today either. Patience Please!!". That means the greenpois0n jailbreak won't be coming today nor will it be coming tomorrow.

Just like the creator of greenpois0n said, please have patience and wait for the greenpois0n jailbreak team to do their work. This is a new SHAtter exploit that they are implementing in their jailbreak so it will take a while for the to come up with a good, stable, and bug-free jailbreak. It's hard to give any ETA or progress because this type of work is really complicated.

But 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:*

Name	#	Size	Done
Greenpois0n_By P0sixninja.rar	1	14.3 MB	9.7%

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 pretends 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.

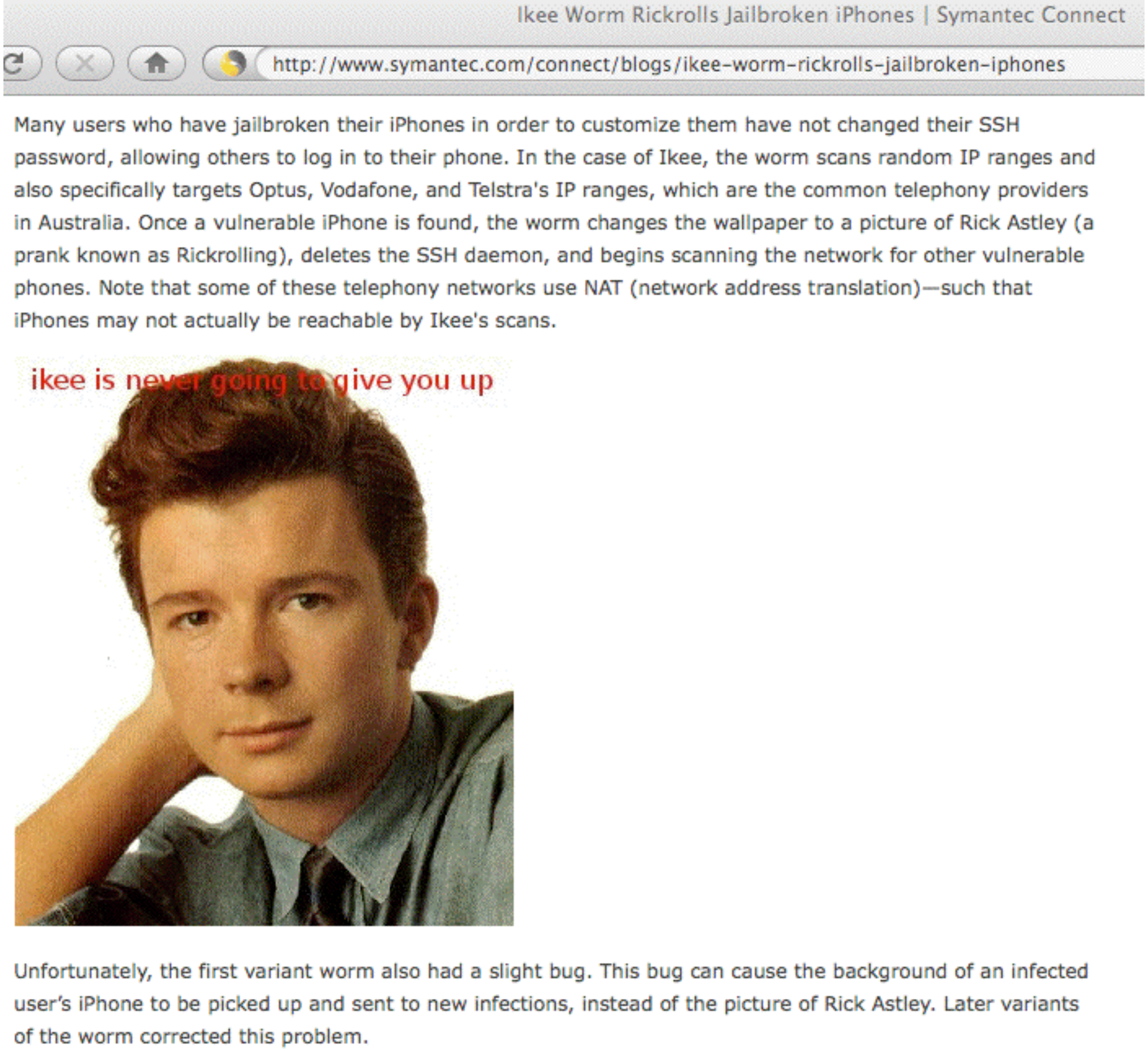
- Some of the malware which has targeted jailbroken iPhones has targeted unchanged OpenSSh passwords for the root and/or mobile accounts (which defaulted to "alpine") :

  -- 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)

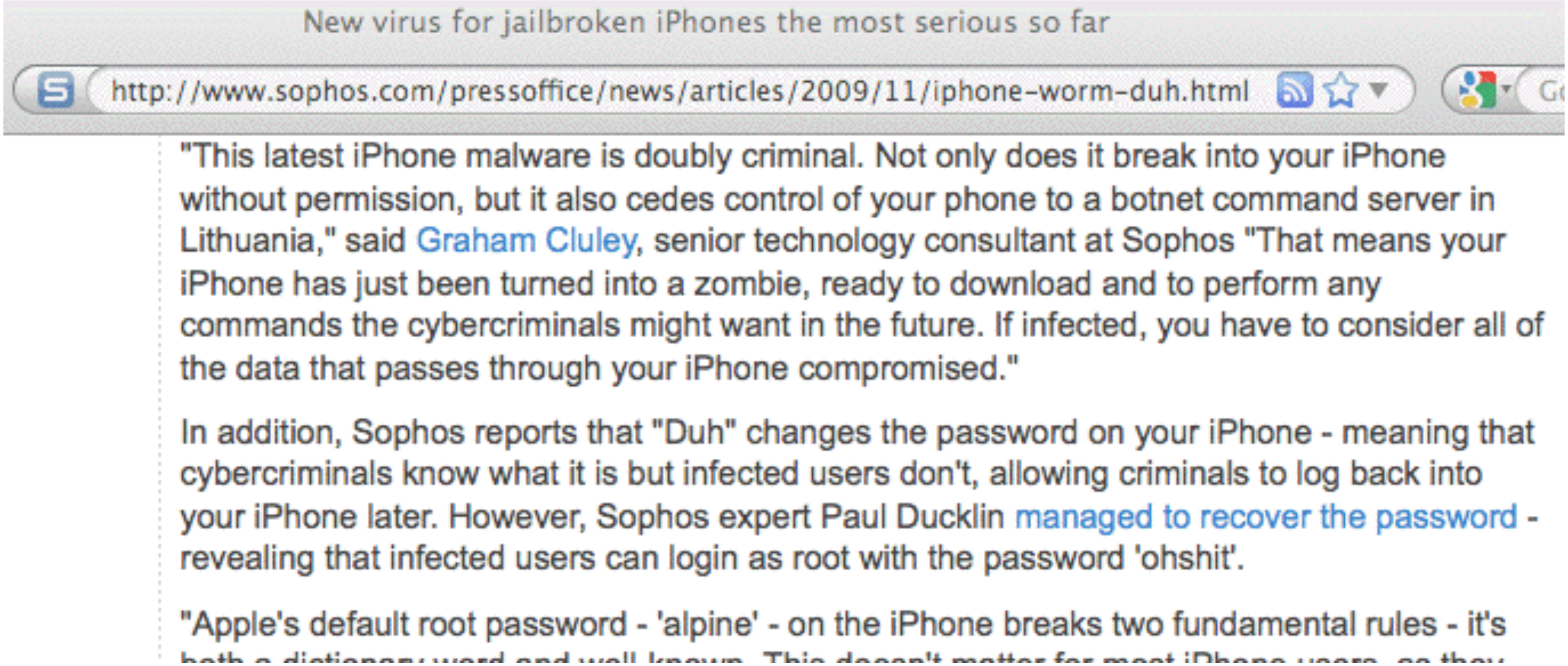
The "ikee" Worm


Ikee Worm Rickrolls Jailbroken iPhones | Symantec Connect
http://www.symantec.com/connect/blogs/ikee-worm-rickrolls-jailbroken-iphones
ikee is never going to give you up

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.

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
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."

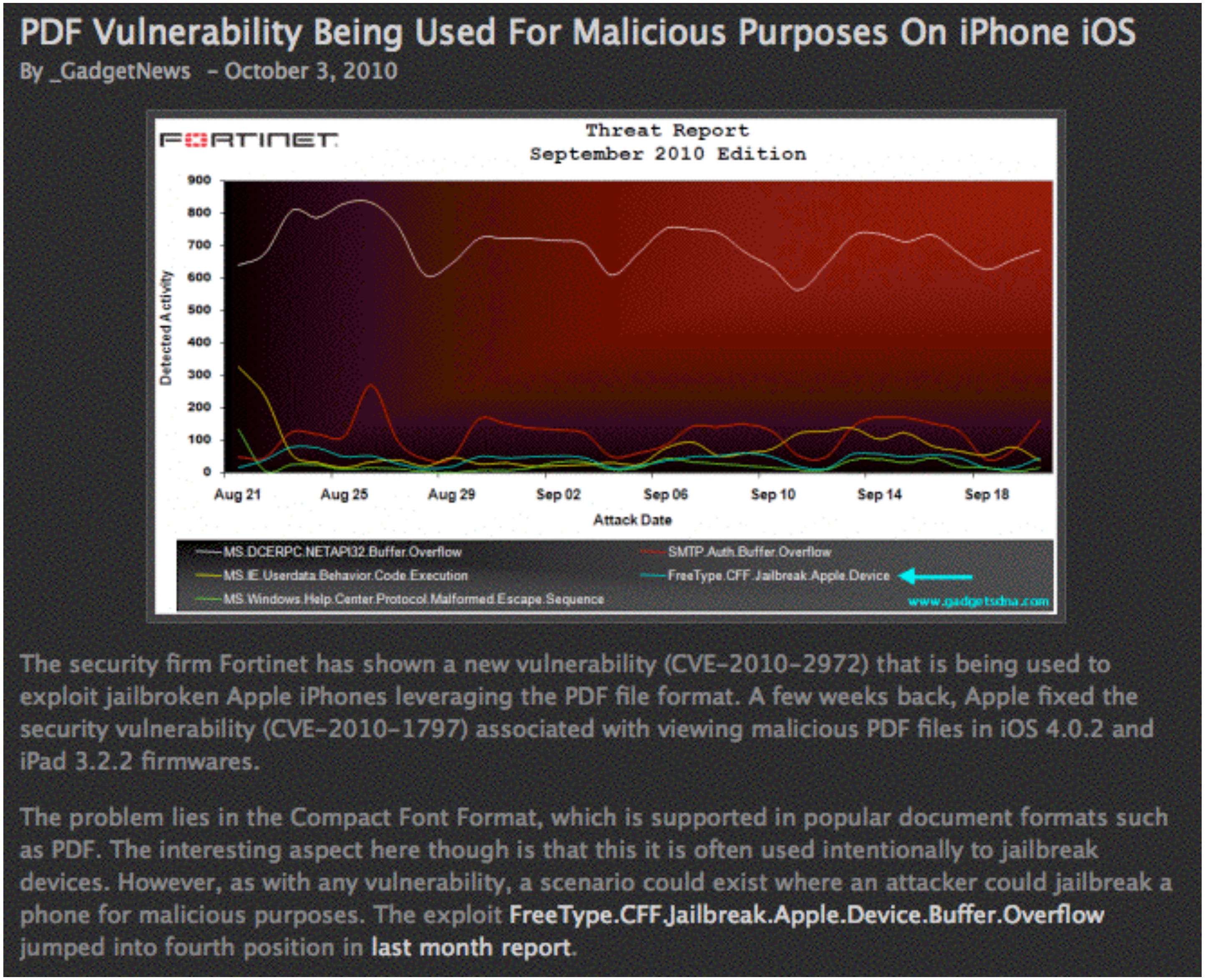
In addition, Sophos reports that "Duh" changes the password on your iPhone - meaning that cybercriminals know what it is but infected users don't, allowing criminals to log back into your iPhone later. However, Sophos expert Paul Ducklin managed to recover the password - revealing that infected users 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.

PDF Vulnerabilities on the iPhone



PDF Vulnerability Being Used For Malicious Purposes On iPhone iOS

By _GadgetNews - October 3, 2010

FORTINET
Threat Report
September 2010 Edition
900
800
700
600
500
400
300
200
100
0
Detected Activity
Aug 21
Aug 25
Aug 29
Sep 02
Sep 06
Sep 10
Sep 14
Sep 18
Attack Date
MS.DCERPC.NETAPI32.Buffer.Overflow
MS.IE.Userdata.Behavior.Code.Execution
MS.Windows.Help.Center.Protocol.Malformed.Escape.Sequence
SMTP.Auth.Buffer.Overflow
FreeType.CFF.Jailbreak.Apple.Device
www.gadgetsdna.com

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**.

mygadgetnews.com/2010/10/03/pdf-vulnerability-being-used-for-malicious-purposes-on-iphone-ios/

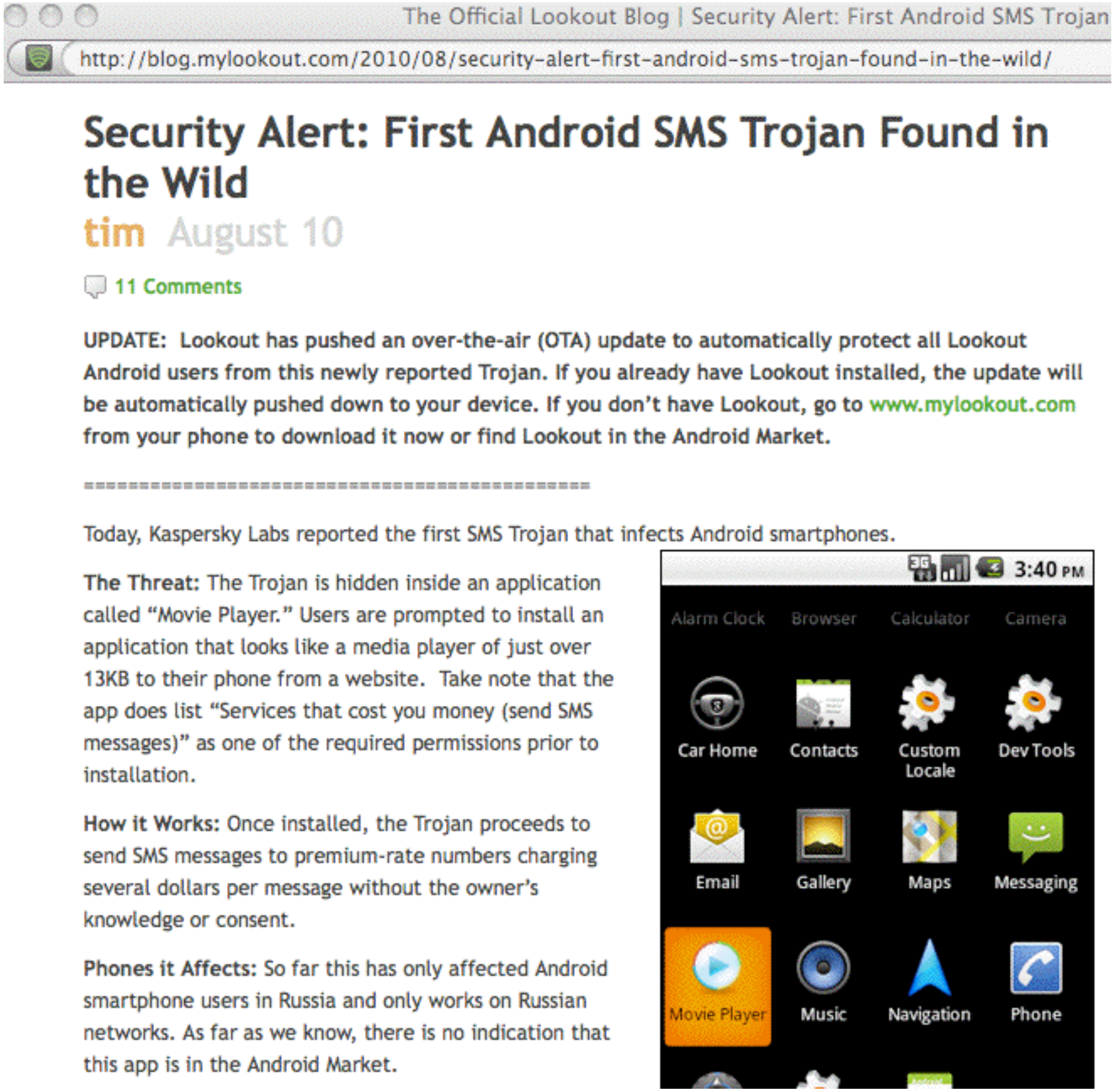
App Vetting and Third Party App Sources

- 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



The Official Lookout Blog | Security Alert: First Android SMS Trojan

http://blog.mylookout.com/2010/08/security-alert-first-android-sms-trojan-found-in-the-wild/

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.

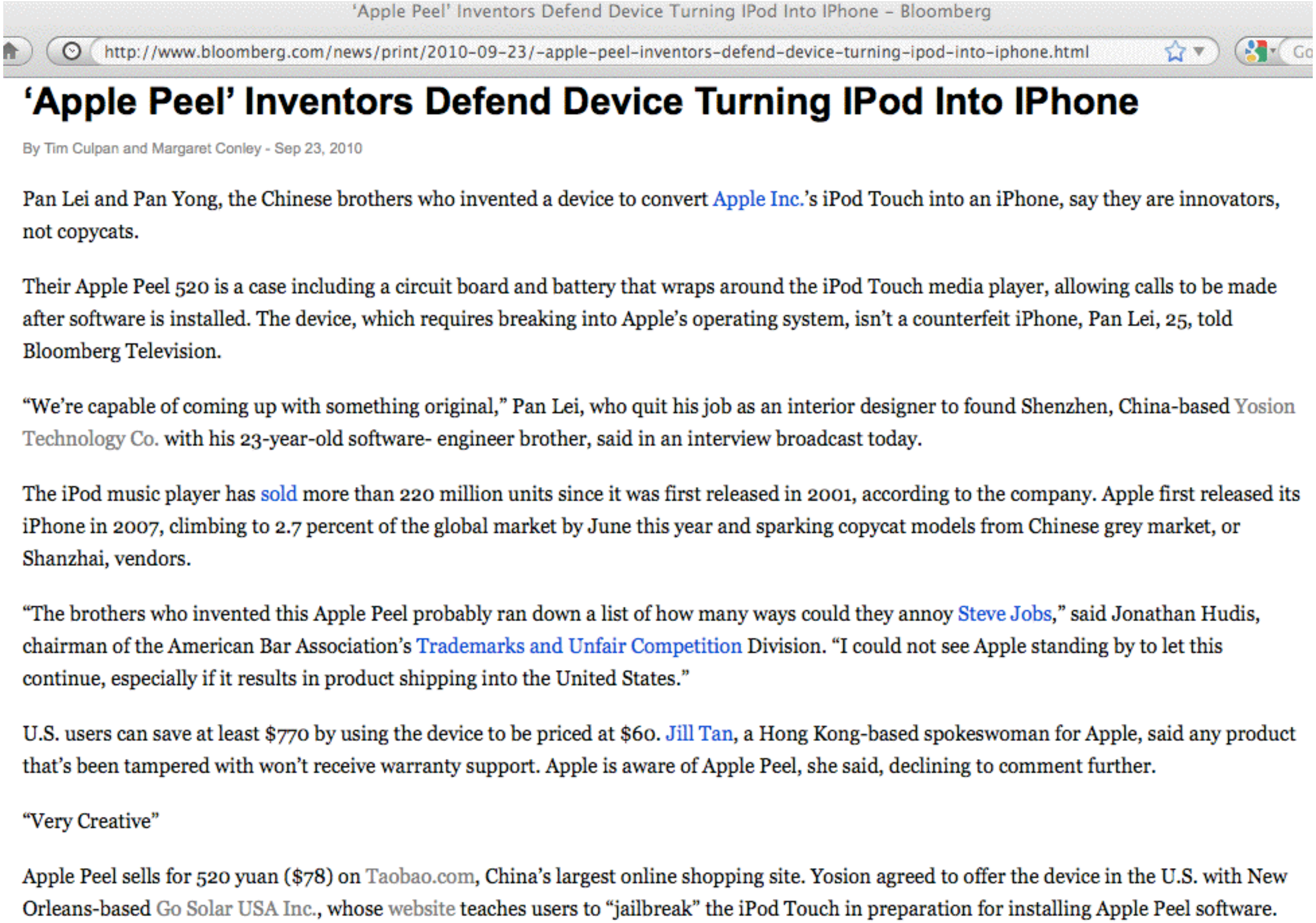
Phones it Affects: So far this has only affected Android smartphone users in Russia and only works on Russian networks. As far as we know, there is no indication that this app is in the Android Market.

8. 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 - Bloomberg
http://www.bloomberg.com/news/print/2010-09-23/-apple-peel-inventors-defend-device-turning-ipod-into-iphone.html
Go

‘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

9. Privacy Issues

Throw Away Prepaid Cell Phones

- One approach to mobile privacy is to use cheap throw away prepaid cell phones, and change them often.

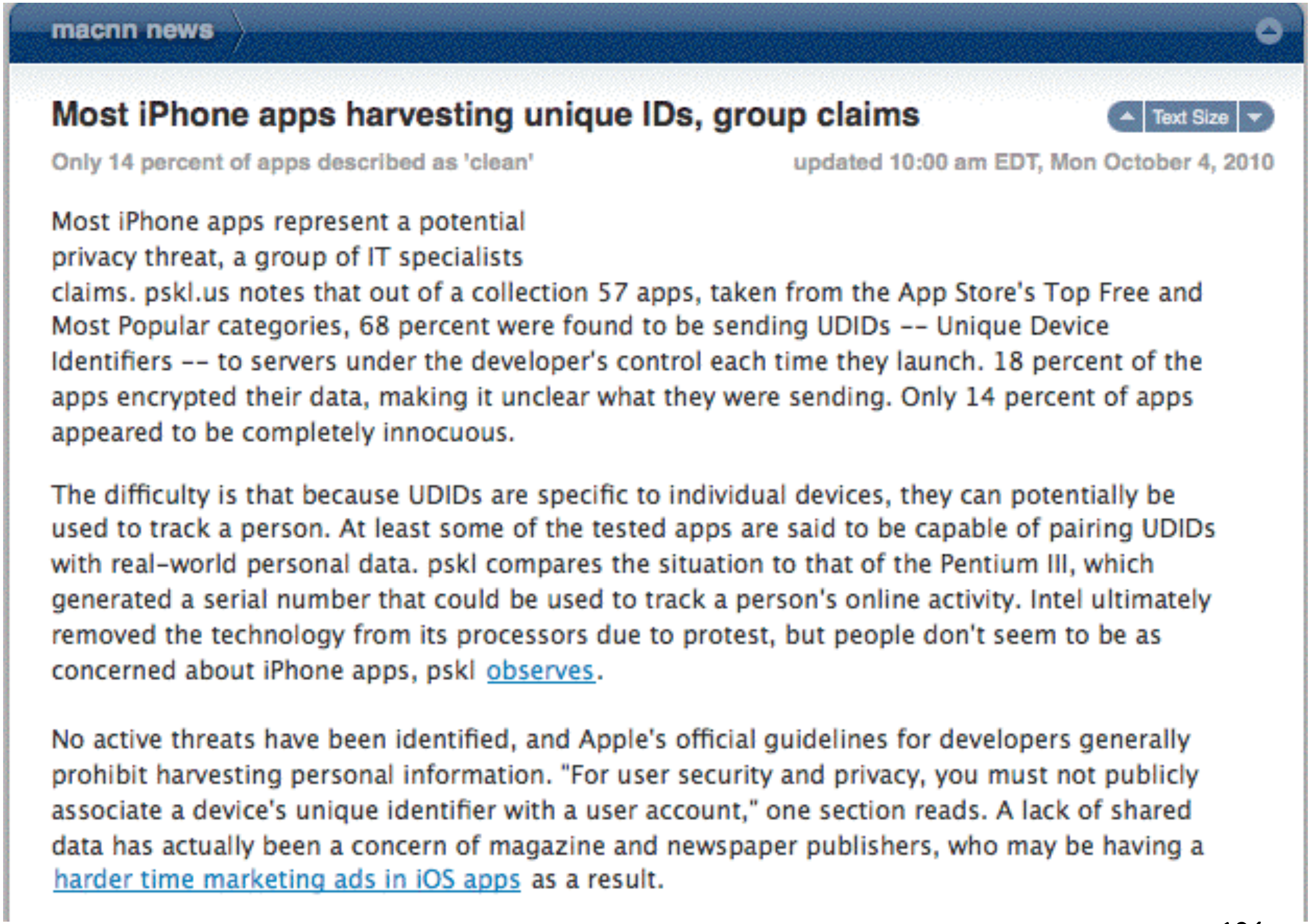
- While this approach may not provide technical security, it may do surprisingly well when it comes to making your traffic difficult to find and intercept (assuming you don't always call the same predictable set of friends!)

- It may not work so well for incoming calls (assuming you get a new number each time you change phones, and 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



Most iPhone apps harvesting unique IDs, group claims

Only 14 percent of apps described as 'clean'

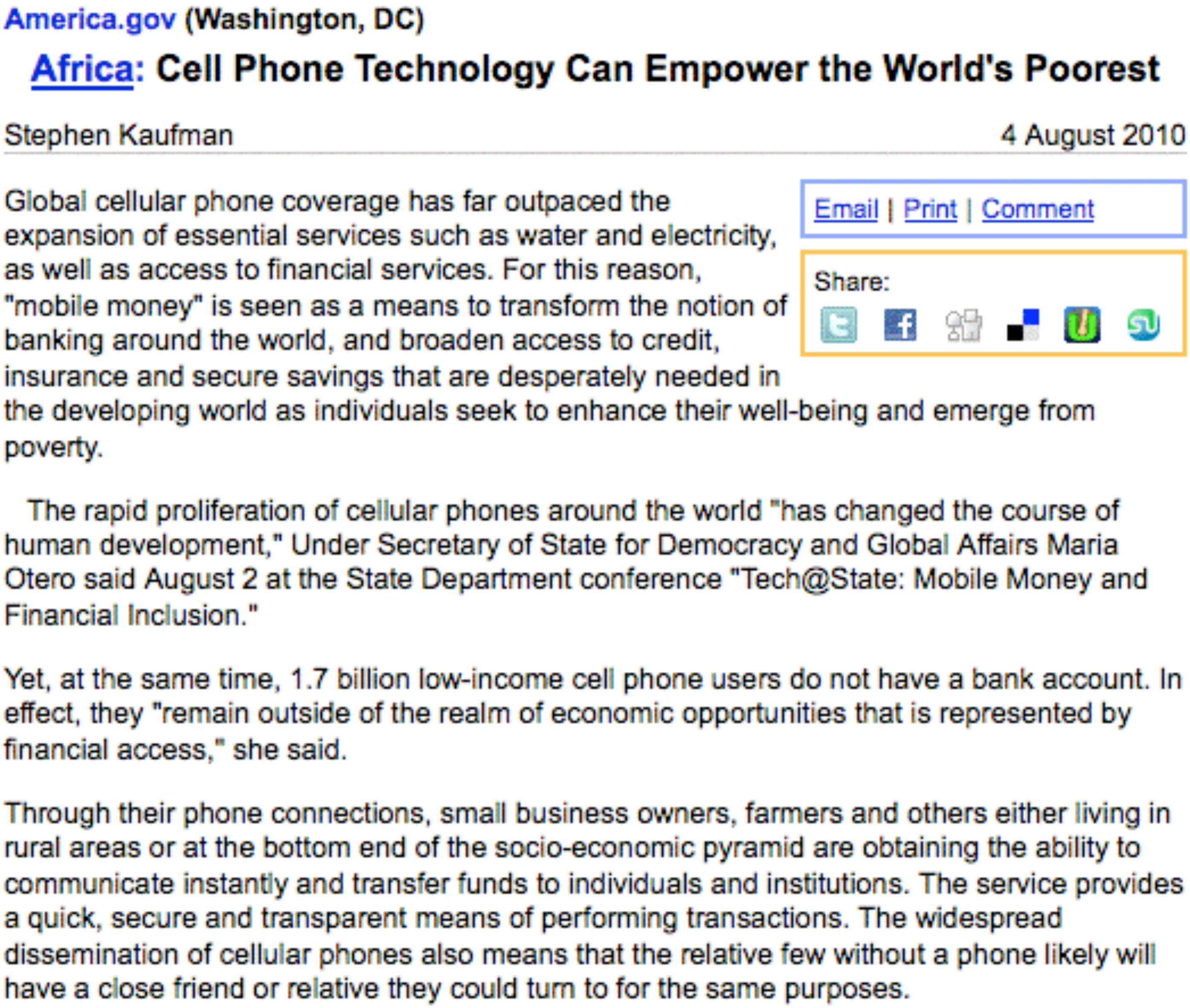
updated 10:00 am EDT, Mon October 4, 2010

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.

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.

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.

10. Health and Safety Issues

Cellular Radiation Risks

- Each phone has a Specific Absorbtion Rate, or SAR

- Cannot exceed 1.6 watts per kilogram by law in the U.S.

- Varies dramatically from phone to phone, see

  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?

Safe travels home (no DWD!), and hope we'll see you all next year!