Updates on Two Topics: The Security of Cloud Computing, and The Security of Mobile Internet Devices

Joe St Sauver, Ph.D.
Security Programs Manager, Internet2
joe@uoregon.edu or joe@internet2.edu

Internet2 Fall Member Meeting, Arlington VA
Salon B, 1:15-2:30, Tuesday, April 27th, 2010

http://www.uoregon.edu/~joe/sec-update-spring10/

Disclaimer: all opinions strictly my own.

Introduction

Today's Talk: The Security of Cloud Computing, and The Security of Mobile Internet Devices

- In the past we've tried covering a lot of ground during some security updates, and in fact, some of the feedback we've received has been that we've tried to cover **too much** material. We're working on being better about listening to that sort of feedback. :-)
- So, today, in part because we've got two other speakers during this session, we're focusing on just two timely topics:
  -- the security of cloud computing, and
  -- the security of mobile devices.
- Our coverage of these topics today is based on talks we did earlier at Internet2 Joint Techs in Salt Lake City, and at Educause Security Professionals in Atlanta, but we don't think there's likely to be much overlap between the attendees at those earlier sessions and today's audience.

Part I: The Security of Cloud Computing

Some Cautions About Our First Topic Today

- As you likely already know, there's a LOT of hype associated with cloud computing. I'm sorry about that (but I can't fix that)
- Cloud computing is a huge topic. It encompasses diverse models and technologies, even though users and the trade press tend to lump them under a common name. Covering all potential security issues in part of one session is impossible.
- For that matter, please note that we're still discovering many of the security issues which will challenge cloud computing!
- Why? In part, that's because cloud computing is still a work-in-progress. Because it is rapidly evolving, what I tell today you may quickly become irrelevant or obsolete.
- Nonetheless, there's so much thrust behind cloud computing that we simply don't have the option of sitting back and waiting to understand address cloud computing security issues.

What's Driving Cloud Computing? Drivers Include…

- Thought leaders: Amazon, Google, Microsoft and many other Internet thought leaders have all aligned behind the cloud
- The economy: Because cloud computing should theoretically help sites avoid major new capital expenditures (capex) while also controlling some ongoing operational expenses (opex), cloud computing is potentially a "lifesaver" for financially strapped businesses, including many major universities.
- The Feds: Cloud computing has *substantial* momentum in Washington DC: it was featured in the just-released federal IT budget; Vivek Kundra, the federal CIO, has championed creation of http://apps.gov/ , a “one-stop shop” for cloud computing services for federal agencies; DISA has created a very successful cloud computing project called "RACE;" and Howard Schmidt, the new federal cyber security coordinator, has said that securing cloud computing will be a top priority.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Federal IT Budget Grows To $79.4 Billion

Tech spending in the U.S. government's just-released fiscal 2011 budget will go toward open government, cloud computing, cybersecurity, procurement, and performance management.

By J. Nicholas Hoover, InformationWeek
Feb. 1, 2010
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=222600650

President Obama's fiscal 2011 budget includes $79.4 billion for federal IT spending, a 1.2% bump from the $78.4 billion 2010 budget level.

That number includes bullet point like $364 million for the operations of the Department of Homeland Security' National Cyber Security Division, a 30% increase in the budget for the Federal Adviation Administration's next-generation air traffic control system, new spending on health IT and increased spending to upgrade IT at the Small Business Administration.

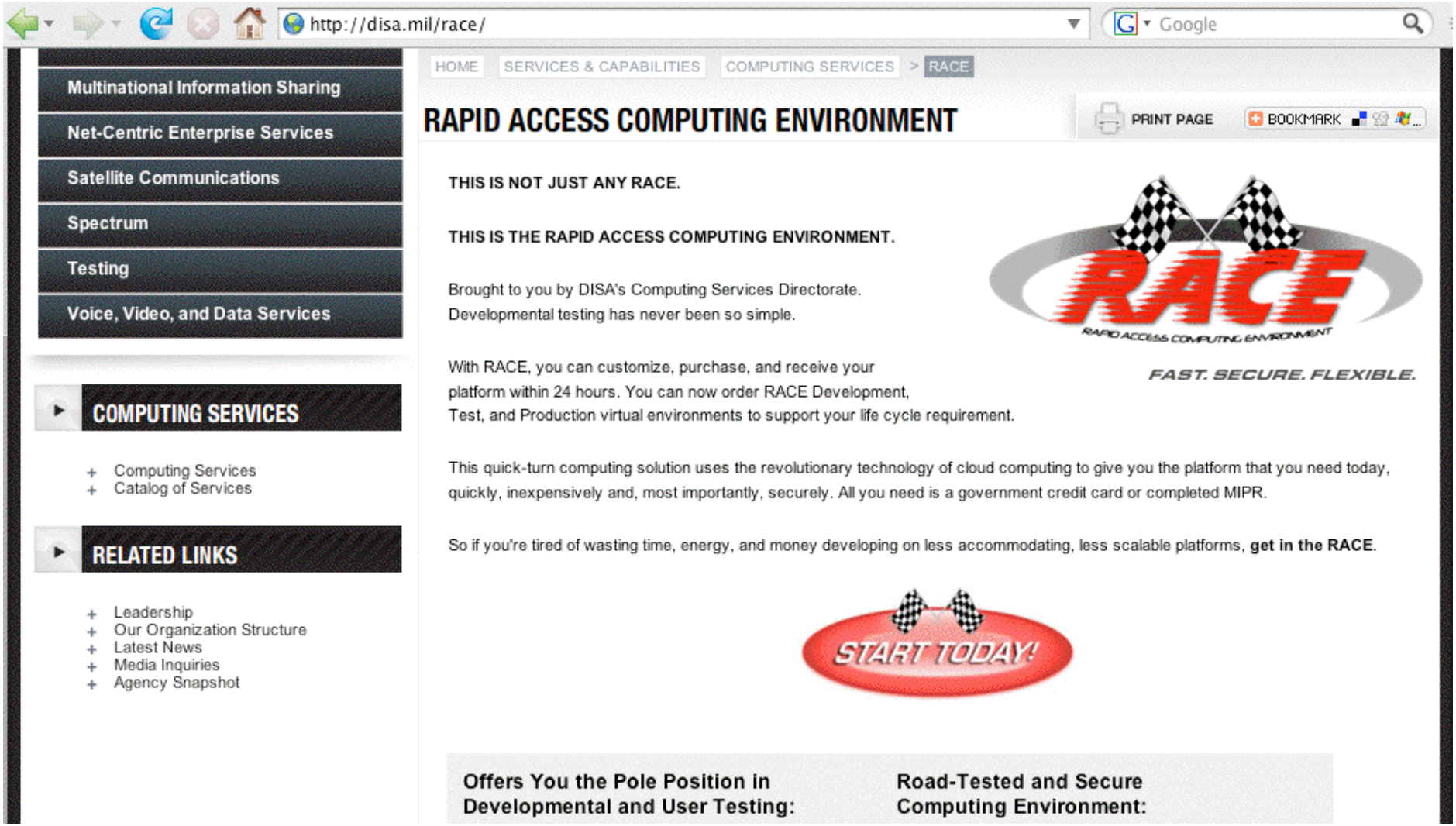
The budget also lays out a number of key administration strategies for IT over the next year. For example, data center glut has become a major problem for the federal government, with the number of federal data centers jumping from 432 in 1998 to more than 1,100 last year, and the administration hopes to reverse this trend, it notes in the budget. Though the timing is unclear, the Office of Management and Budget plans to release a strategy to reduce both the number and cost of federal data centers.

The budget paints government cloud computing efforts -- which federal CIO Vivek Kundra has looked toward as a partial solution to some of the government's data center problems -- with a broad brush, saying only that, "after evaluation in 2010, agencies will deploy cloud computing solutions across the government" and pointing to both Apps.gov and the importance of security in cloud computing.

Apps.Gov


https://apps.gov/cloud/advantage/main/start_page.do
Google
What type of solution do you need?
Business Apps
Your agency or service is complex and requires state-of-the-art software to get business done.
GSA Cloud Business Apps has a solution!
Cloud IT Services
Need a better solution to reduce cost and implement projects faster?
GSA Cloud IT Services has the answer!
Productivity Apps
You need to get things done and GSA is there to help you do just that.
GSA Cloud Productivity Apps has the tools!
Social Media Apps
Social media tools make it easier to discuss the things we care about and help us get the job done.
GSA Social Media Apps can help you get the word out!
Before using/purchasing the products and services on apps.gov, please do so in accordance with your agency's policies and procedures pertaining to Procurement, Information Technology, Cyber Security, Privacy, Accessibility, Social Media, and any other applicable Federal mandates. If you have any questions about your agency's policies and procedures, please contact your agency's Office of the Chief Information Officer or Terms of Service point of contact.
Home | Register | Order History/Status | Cloud FAQs | Vendor FAQs | Contact Us
••• WARNING •••
This is a U.S. General Services Administration computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.
Privacy and Security

DISA's RACE


http://disa.mil/race/
Google
Multinational Information Sharing
Net-Centric Enterprise Services
Satellite Communications
Spectrum
Testing
Voice, Video, and Data Services
COMPUTING SERVICES
Computing Services
Catalog of Services
RELATED LINKS
Leadership
Our Organization Structure
Latest News
Media Inquiries
Agency Snapshot
HOME
SERVICES & CAPABILITIES
COMPUTING SERVICES
RACE
RAPID ACCESS COMPUTING ENVIRONMENT
PRINT PAGE
BOOKMARK
THIS IS NOT JUST ANY RACE.
THIS IS THE RAPID ACCESS COMPUTING ENVIRONMENT.
Brought to you by DISA's Computing Services Directorate.
Developmental testing has never been so simple.
RACE
RAPID ACCESS COMPUTING ENVIRONMENT
FAST. SECURE. FLEXIBLE.
With RACE, you can customize, purchase, and receive your platform within 24 hours. You can now order RACE Development, Test, and Production virtual environments to support your life cycle requirement.
This quick-turn computing solution uses the revolutionary technology of cloud computing to give you the platform that you need today, quickly, inexpensively and, most importantly, securely. All you need is a government credit card or completed MIPR.
So if you're tired of wasting time, energy, and money developing on less accommodating, less scalable platforms, get in the RACE.
START TODAY!
Offers You the Pole Position in Developmental and User Testing:
Road-Tested and Secure Computing Environment:

Our Community Is Also Pressing Ahead

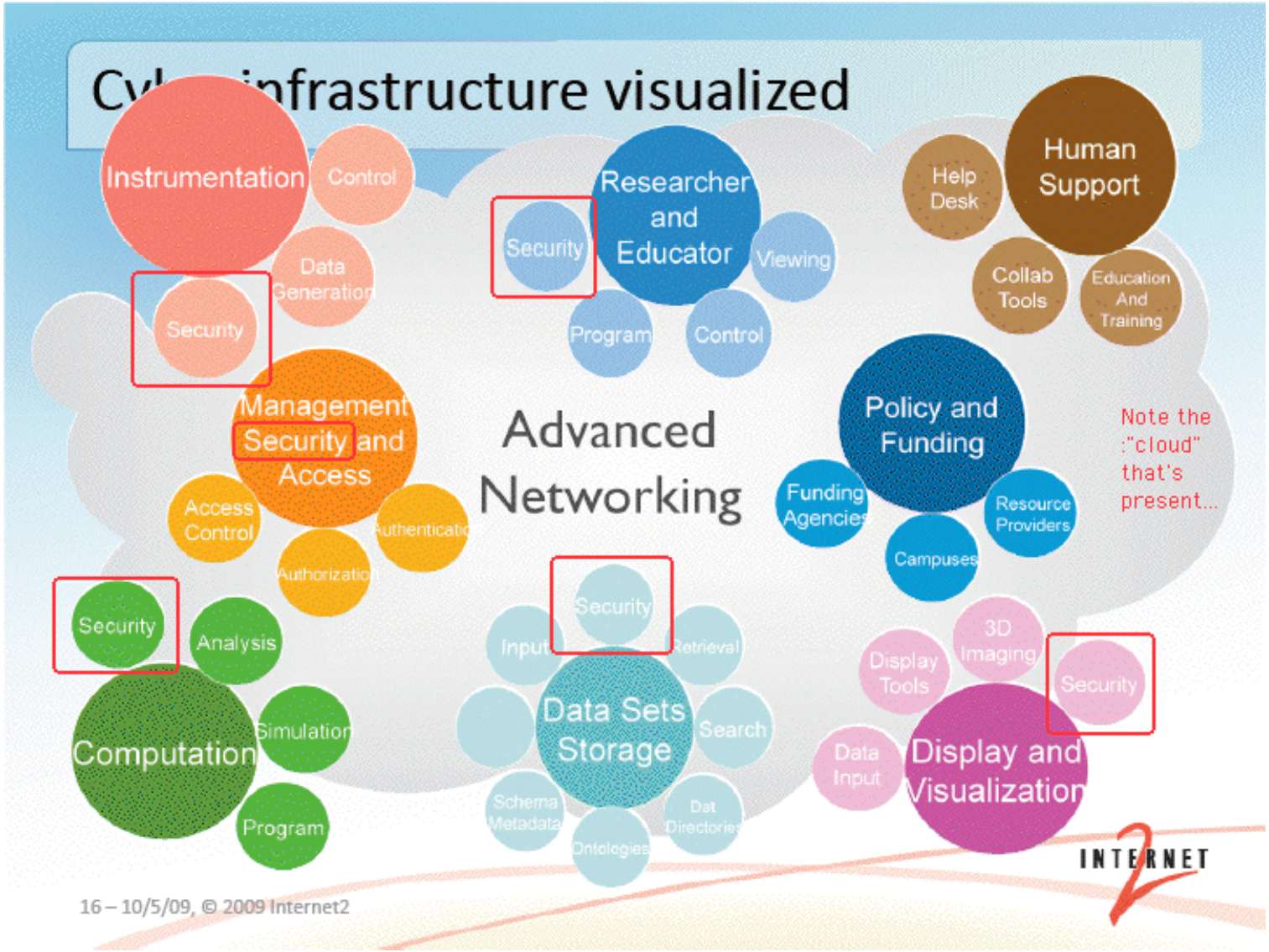
- Cloud computing seem to be turning up on pretty much every networking and security mailing list I'm on

- You've heard/will be hearing a number of cloud computing talks during this week's meeting, which is probably not surprising since cloud computing was a Member Meeting explicit focus area.

- But I'm seeing clouds everywhere, not just here at the Member Meeting.

- Heck, I'm even seeing "clouds" (with frequent references to security!) appear in things like the last Internet2 Member Meeting "Introduction to Internet2" talk

"Cyberinfrastructure Visualized:"
A Cloud, With Lots of "Security" References



Why Is "Security" Everywhere on That Slide?

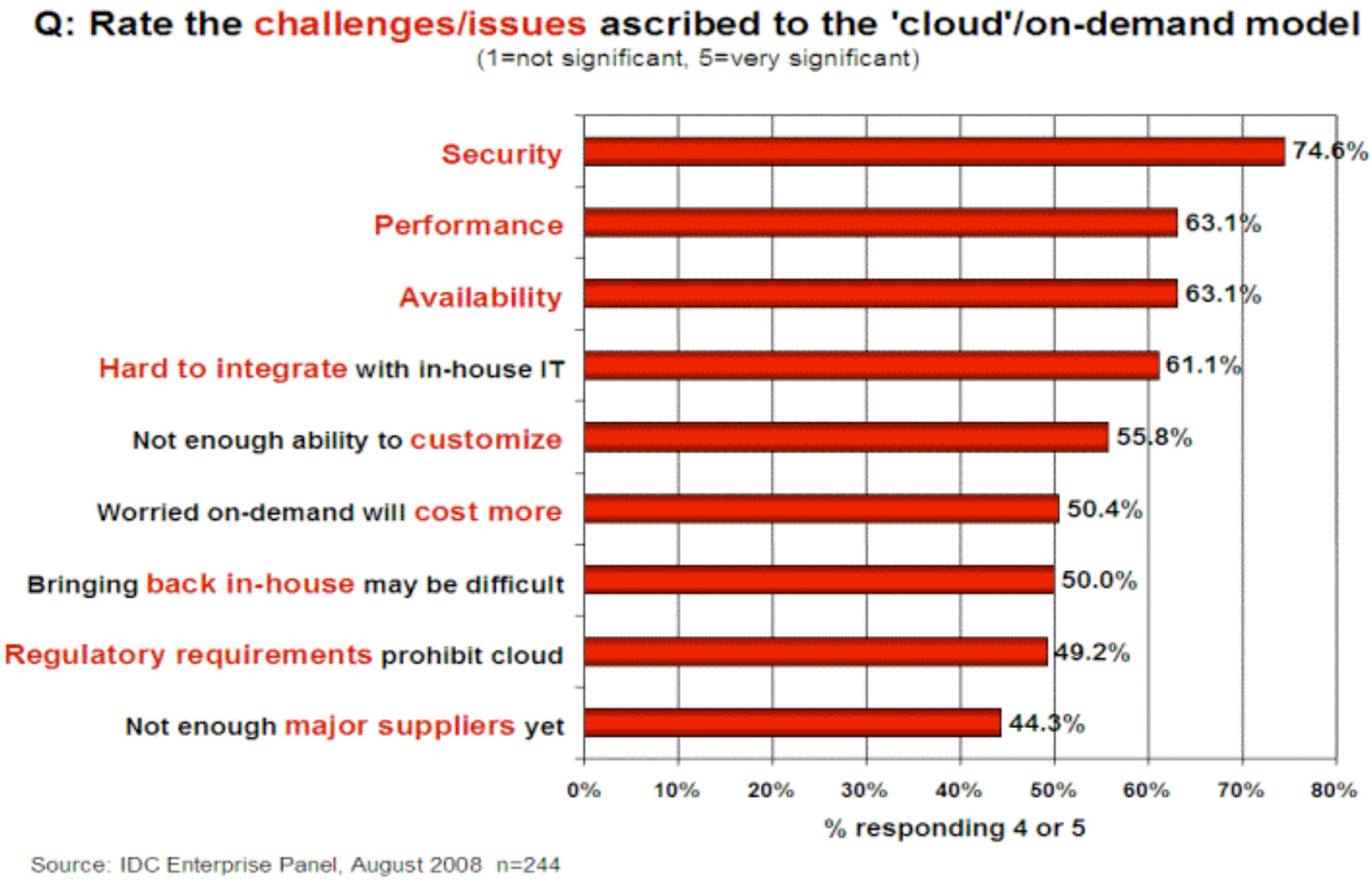
- Security is generally perceived as a huge issue for the cloud:

During a keynote speech to the Brookings Institution policy forum, "Cloud Computing for Business and Society," [Microsoft General Counsel Brad] Smith also highlighted data from a survey commissioned by Microsoft measuring attitudes on cloud computing among business leaders and the general population.

The survey found that while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, ***more than 90 percent of these same people are concerned about the security, access and privacy of their own data in the cloud.***

http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx

Another Data Point for Clouds and Security



Source: http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt at slide 17

Cloud Computing Is Many Different Things to Many Different People

- All of the following have been mentioned from time to time as examples of “cloud computing:”
  -- Amazon Web Services including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc.)
  -- Rackspace Cloud (formerly Mosso)
  -- Google’s App Engine
  -- Windows Azure Platform (now a production/for-fee service)
  -- the OGF (including its Open Cloud Computing Interface)
  -- SETI@Home, Folding@Home, distributed.net, etc.
  -- outsourced campus email service (to Gmail or Live.com), or outsourced spam filtering (e.g., to Postini or Ironport)
  -- use of virtualization (e.g., VMware) to host departmental systems either on local servers, or on outsourced VPS
- In reality, some of those activities are not (strictly speaking) what's usually defined as "cloud computing."

Some Generally Accepted Characteristics

- Most people would agree that true cloud computing…
  -- usually has low or zero up front capital costs
  -- largely eliminates operational responsibilities (e.g., if a disk fails or a switch loses connectivity, you don't need to fix it)
  -- for the most part, cloud computing eliminates knowledge of WHERE one's computational work is being done; your job is being run "somewhere" out there in the "cloud"
  -- offers substantial elasticity and scalability: if you initially need one CPU, that's fine, but if you suddenly need 999 more, you can get them, too (and with very little delay!) If/when demand drops, you can scale your usage back, too
  -- cloud computing leverages economies of scale (running mega data centers with tens of thousands of computers is far less expensive (per computer) than running a small machine room with just a modest cluster of systems)

Some "Clouds" Won't Necessarily Have All of Those Characteristics

- For instance, if your site is running a **local** private cloud:

  -- there WILL be capital expenditures up front,
  -- you (or someone at your site) WILL still care about things like hardware failures, and
  -- you likely WON'T have the illusion of a seemingly infinite inventory of processors (or memory or disk)

  Nonetheless, a local private cloud service may functionally work the same way as a public cloud service, and hybrid cloud models may even combine private and public cloud services in a fairly seamless way.

- Ubuntu's enterprise cloud offering is a nice example of this.


Cloud computing on Ubuntu | Ubuntu
http://www.ubuntu.com/cloud
Google
Cloud computing on Ubuntu | Ubu...
ubuntu
Ubuntu
Server
Cloud
Support
Community
Partners
News
Search
Why Ubuntu?
Private cloud
Public cloud
Consulting
Training
Support
Management
Ubuntu private cloud is compatible with the Amazon EC2 public cloud
Immediacy and elasticity behind the firewall
Migrate between public and private clouds easily
Burst to public clouds when needed
Why Ubuntu?
Private Cloud »
Ubuntu Enterprise Cloud
Private clouds offer immediacy and elasticity in your own IT infrastructure. Using Ubuntu
Public Cloud »
Ubuntu on Amazon EC2
Amazon's Elastic Computing (EC2) cloud allows you to build on-demand virtual systems with

Will *Your* Campus Offer Private Cloud Services?

- If you haven't been thinking about offering private cloud services, I would suggest that you might want to, including thinking hard about any potential security issues associated with doing so.

So What About *Security* in the Cloud*?*

For the remainder of this half of our talk, we'll outline some of the security issues you might run into when using cloud computing

In Some Ways, "Cloud Computing Security" Is No Different Than "Regular Security"

- For example, many applications interface with end users via the web. All the normal OWASP web security vulnerabilities -- things like SQL injection, cross site scripting, cross site request forgeries, etc., -- all of those vulnerabilities are just as relevant to applications running on the cloud as they are to applications running on conventional hosting.
- Similarly, consider physical security. A data center full of servers supporting cloud computing is internally and externally indistinguishable from a data center full of "regular" servers. In each case, it will be important for the data center to be physically secure against unauthorized access or potential natural disasters, but there are no special new physical security requirements which suddenly appear simply because one of those facilities is supporting cloud computing

There *Are* Some Unique Cloud-Related Areas Which We're NOT Going To Worry About Today

- Contracting for Cloud Services: Even though contractual terms (including things like SLAs) can be used to mitigate some risks, I'm not a lawyer, and I'm not going to pretend to be one, so we're not going to cover issues related to contracting for cloud services. Fortunately, NACUA did a great job discussing this topic in a recent seminar, see www.nacua.org/meetings/VirtualSEminars/december2009/home.html
- Compliance, Auditing and eDiscovery: Because this meeting is primarily about research and education, not business processes and university administration, we will not consider the potential need for cloud computing to be compliant with Payment Card Industry security standards, FERPA, HIPAA, GLBA, or other related compliance mandates.
- So what are some cloud-related security issues?

The "A" in The Security "C-I-A" Objectives

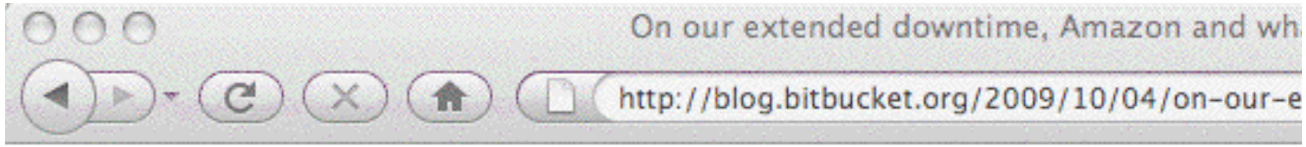
- Computer and network security is fundamentally about three goals/objectives:

  -- confidentiality (C)
  -- integrity (I), and
  -- availability (A).

- **Availability is the area where cloud based infrastructure appears to have had its largest (or at least most highly publicized) challenges to date.**

- For example, consider some of the cloud-related outages which have been widely reported…

Bitbucket, DDoS'd Off The Air



On our extended downtime, Amazon and what's coming

As many of you are well aware, we've been experiencing some serious downtime the past couple of days. Starting Friday evening, our network storage became virtually unavailable to us, and the site crawled to a halt.

We're hosting everything on Amazon EC2, aka. "the cloud", and we're also using their EBS service for storage of everything from our database, logfiles, and user data (repositories.)

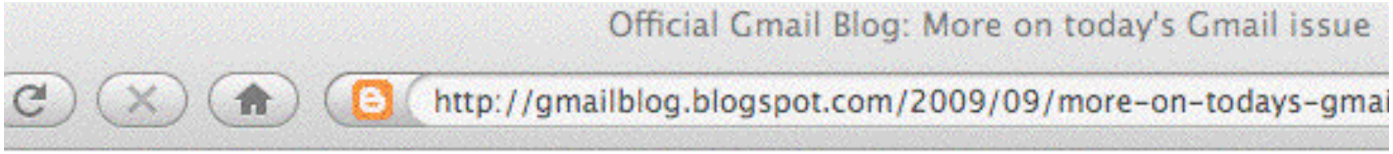
Amazon EBS is a persistent storage solution for EC2, where you get high-speed (and free) connectivity from your instances, while it's also replicated. That gives you a lot for free, since you don't have to worry about hardware failure, and you can create periodic "snapshots" of your volumes easily.

While we were down, it was unknown to us what exactly the problem was, but it was almost certainly a problem with the EBS store. We've been working closely with Amazon the past 24 hours resolving the issue, and this post will outline what exactly went wrong, and what was done to remedy the problem.

Symptoms

What we were seeing on the server was high load, even after turning off anything that took up CPU. Load is a result of stuff "waiting to happen", and after reviewing iostat, it became apparent that the "iowait" was very high, while the "tps" (transactions per second) was very low for our

Maintenance Induced Cascading Failures



More on today's Gmail issue

Tuesday, September 01, 2009 6:59 PM
Posted by Ben Treynor, VP Engineering and Site Reliability Czar

Gmail's web interface had a widespread outage earlier today, lasting about 100 minutes. We know how many people rely on Gmail for personal and professional communications, and we take it very seriously when there's a problem with the service. Thus, right up front, I'd like to apologize to all of you — today's outage was a Big Deal, and we're treating it as such. We've already thoroughly investigated what happened, and we're currently compiling a list of things we intend to fix or improve as a result of the investigation.

Here's what happened: This morning (Pacific Time) we took a small fraction of Gmail's servers offline to perform routine upgrades. This isn't in itself a problem — we do this all the time, and Gmail's web interface runs in many locations and just sends traffic to other locations when one is offline.

However, as we now know, we had slightly underestimated the load which some recent changes (ironically, some designed to improve service availability) placed on the request routers — servers which direct web queries to the appropriate Gmail server for response. At about 12:30 pm Pacific a few of the request routers became overloaded and in effect told the rest of the system "stop sending us traffic, we're too slow!". This transferred the load onto the remaining request routers, causing a few more of them to also become overloaded, and within minutes nearly all of the request routers were overloaded. As a result, people couldn't access Gmail via the web interface because their requests couldn't be routed to a Gmail server. IMAP/POP access and mail processing continued to work normally because these requests don't use the same routers.

It's Not Just The Network: Storage Is Key, Too

T-Mobile: we probably lost all your Sidekick data

By Chris Ziegler posted Oct 10th 2009 3:45PM

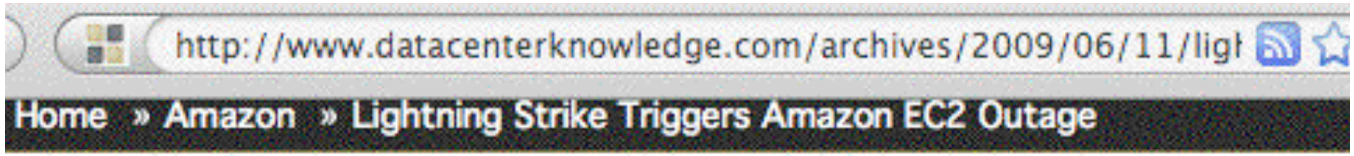
BREAKING

Well, this is shaping up to be one of the biggest disasters in the history of cloud computing, and certainly the largest blow to Danger and the Sidekick platform: T-Mobile's now reporting that personal data stored on Sidekicks has "almost certainly has been lost as a result of a server failure at Microsoft/Danger." They're still looking for a way to recover it, but they're not giving users a lot of hope -- meanwhile, servers

See http://www.engadget.com/2009/10/10/t-mobile-we-probably-lost-all-your-sidekick-data/

However, see also: Microsoft Confirms Data Recovery for Sidekick Users
http://www.microsoft.com/Presspass/press/2009/oct09/10-15sidekick.mspx

And Let's Not Forget About Power Issues



Lightning Strike Triggers Amazon EC2 Outage

June 11th, 2009 : Rich Miller

Some customers of Amazon's EC2 cloud computing service were offline for more than four hours Wednesday night after an electrical storm damaged power equipment at one of the company's data centers. The problems began at about 6:30 pm Pacific time, and most affected customers were back online by 11 p.m., according to Amazon's status dashboard. The company said the outage was limited to customers in one of Amazon's four availability zones in the U.S.

"A lightning storm
caused damage to a single Power Distribution Unit (PDU) in a single Availability Zone, the company reported. "While most instances were unaffected, a set of racks does not currently have power, so the instances on those racks are down. We have technicians on site, and we are working to replace the affected PDU."

EC2 previously experienced extended outages in February 2008 and October 2007.

Mitigating Cloud Computing Availability Issues

- Risk analysts will tell you that when you confront a risk, you can try to eliminate the risk, you can mitigate/minimize the impact of the risk, or you can simply accept the risk.
- If you truly require non-stop availability, you can try using multiple cloud providers, or you could use public and private cloud nodes to improve redundancy.
- Some cloud computing services also offer service divided into multiple "regions." By deploying infrastructure in multiple regions, isolation from "single-region-only" events (such as the power outage mentioned previously) can be obtained.
- Availability issues may also be able to be at least partially mitigated at the application level by things like local caching.
- Sometimes, though, it may simply make financial sense for you to just accept the risk of a rare and brief outage. (Remember, 99.99 availability==> 52+ minutes downtime/yr)

Mitigating Data Loss Risks

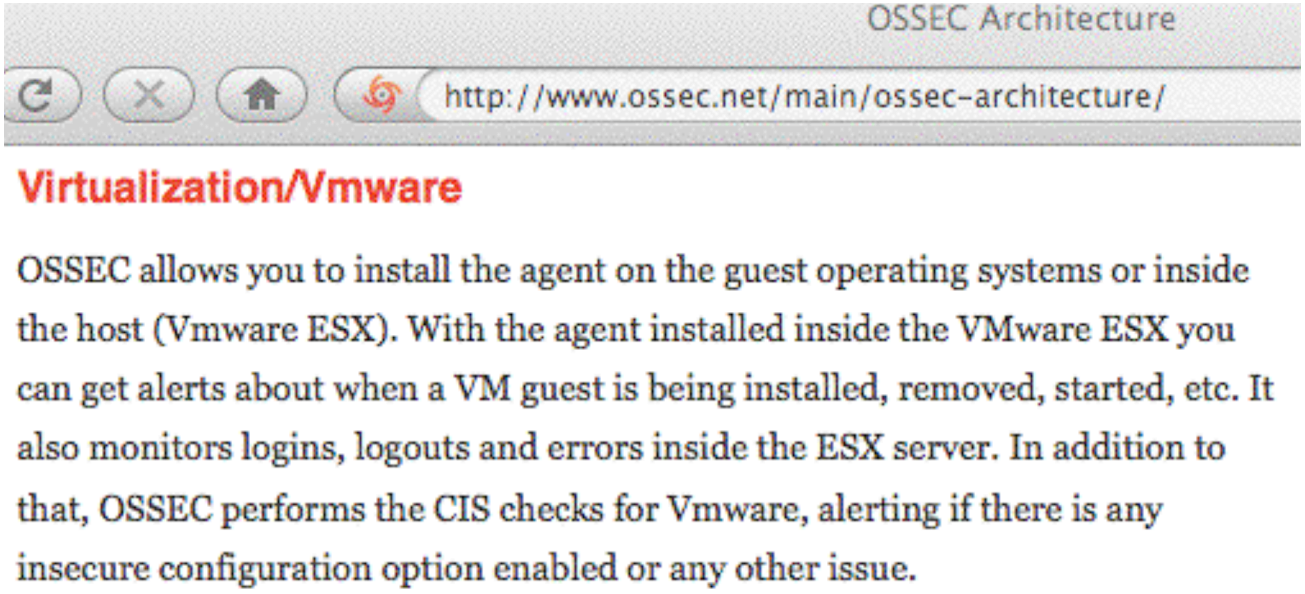
- The risk of data loss (as in the T-Mobile Sidekick case) is an exception to the availability discussion on the preceding slide. Users may be able to tolerate an occasional service interruption, but non-recoverable data losses can kill a business.
- Most cloud computing services use distributed and replicated global file systems which are designed to insure that hardware failures (or even loss of an entire data center) will not result in any permanent data loss, but I believe there is still value in doing a traditional off site backup of one's data, whether that data is in use by traditional servers or cloud computing servers.
- When looking for solutions, make sure you find ones that backs up data FROM the cloud (many backup solutions are meant to backup local data TO the cloud!)

Cloud Computing And Perimeter Security

- While I'm **not** a huge fan of firewalls (as I've previously discussed at the Spring 2008 I2MM in "Cyberinfrastructure Architectures, Security and Advanced Applications," see http://www.uoregon.edu/~joe/architectures/architecture.pdf), at least some sites do find value in sheltering at least some parts of their infrastructure behind a firewall.
- There may be a misconception that cloud computing resources can't be sheltered behind a firewall (see for example "HP's Hurd: Cloud computing has its limits (especially when you face 1,000 attacks a day)," Oct 20th, 2009, http://blogs.zdnet.com/BTL/?p=26247)
- Contrast that with "Amazon Web Services: Overview of Security Processes" (see the refs at the back). AWS has a mandatory inbound firewall configured in a default deny mode, and customers must explicitly open ports inbound

Cloud Computing & Host-Based Intrusion Detection

- While I'm not very enthusiastic about firewalls, I **am** a big fan of well-instrumented/well-monitored systems and networks.
- Choosing cloud computing does not necessarily mean forgoing your ability to monitor systems for hostile activity. One example of a tool that can help with this task is OSSEC (the Open Source Host-Based Intrusion Detection System), an IDS which supports virtualized environments:



Cloud Computing Also Relies on the Security of Virtualization

- Because cloud computing is built on top of virtualization, if there are security issues with virtualization, then there will also security issues with cloud computing.
- For example, could someone escape from a guest virtual machine instance to the host OS? While the community has traditionally been somewhat skeptical of this possibility, that changed with Blackhat USA 2009, where Kostya Kortchinsky of Immunity Inc. presented "Cloudburst: A VMware Guest to Host Escape Story", see
  http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf
- Kostya opined: "VMware isn't an additional security layer, it's just another layer to find bugs in" [put another way, running a virtualization product increases the attack surface]

Choice of Cloud Provider

- Cloud computing is a form of outsourcing, and you need a high level of trust in the entities you'll be partnering with.

- It may seem daunting at first to realize that your application depends (critically!) on the trustworthiness of your cloud providers, but this is not really anything new -- today, even if you're not using the cloud, you already rely on and trust:

  -- network service providers,
  -- hardware vendors,
  -- software vendors,
  -- service providers,
  -- data sources, etc.

  Your cloud provider will be just one more entity on that list.

Cloud Provider Location

- You may want to know (roughly) where your cloud lives.
- For example, one of the ways that cloud computing companies keep their costs low is by locating their mega data centers in locations where labor, electricity and real estate costs are low, and network connectivity is good.
- Thus, your cloud provider could be working someplace you may never have heard of, such as The Dalles, Oregon, where power is cheap and fiber is plentiful, or just as easily some place overseas.
- If your application and data do end up at an international site, those systems will be subject to the laws and policies of that jurisdiction. Are you comfortable with that framework?
- Are you also confident that international connectivity will remain up and uncongested? Can you live with the latencies involved?

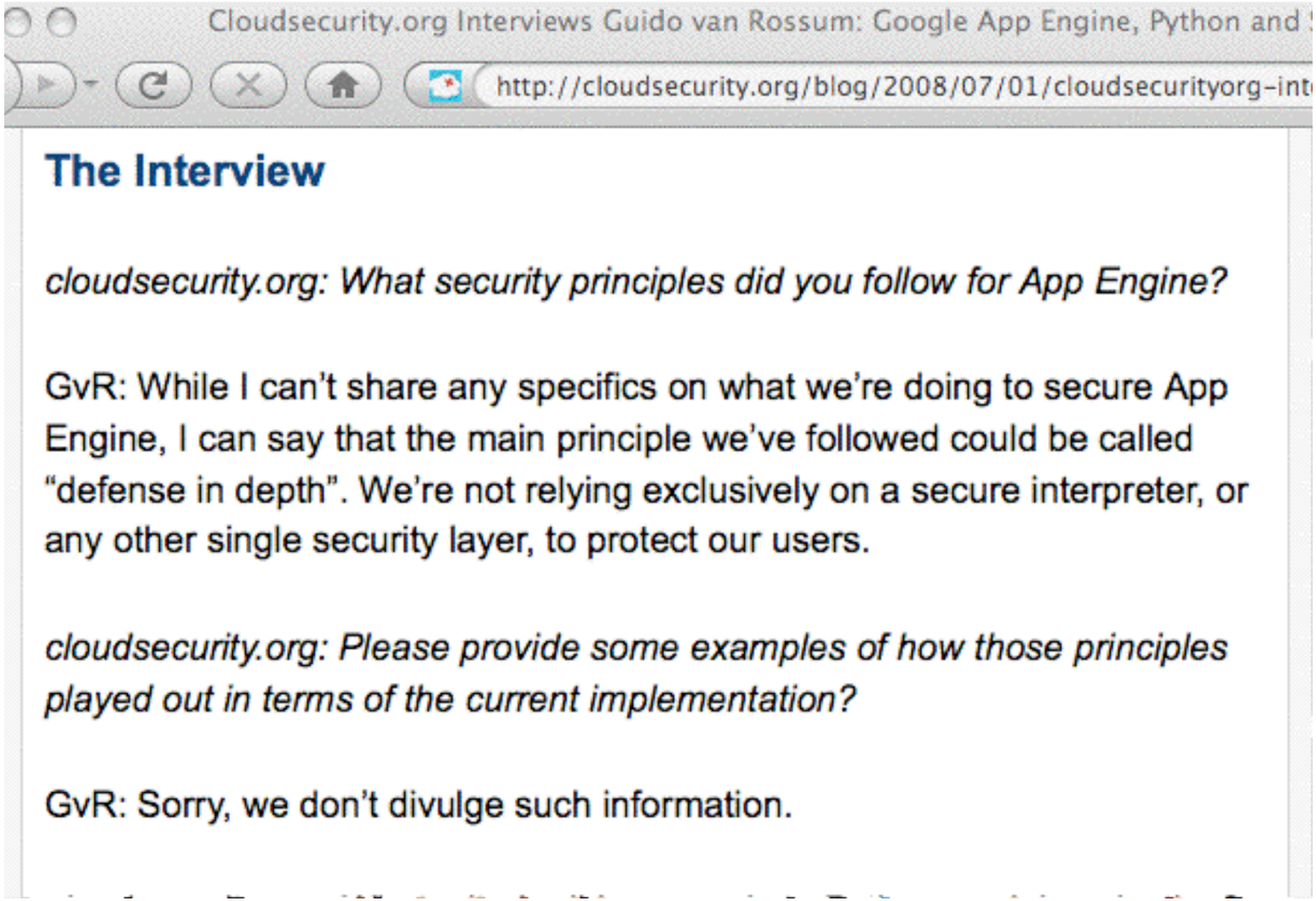
Cloud Provider Employees

- If you're like most sites, you're probably pretty careful about the employees you hire for critical roles (such as sysadmins and network enginers). But what about your cloud provider? If your cloud provider has careless or untrustworthy system administrators, the integrity/privacy of your data's at risk.
- How can you tell if your cloud provider has careful and trustworthy employees? You need to ask them!
  -- Do backgrounds get checked before people get hired?
  -- Do employees receive extensive in-house training?
  -- Do employees hold relevant certifications?
  -- Do checklists get used for critical operations?
  -- Are system administrator actions tracked and auditable on a *post hoc* basis if there's an anomalous event?
  -- Do administrative privileges get promptly removed when employees leave or change their responsibilities?

Cloud Provider Transparency

- You will only be able to assess the sufficiency of cloud provider security practices if the cloud provider is willing to disclose its security practices to you.
- If your provider treats security practices as a confidential or business proprietary thing, and won't disclose their security practices to you, you'll have a hard time assessing the sufficiency of their security practices. Unfortunately, you may need to consider using a different provider.
- Remember: "Trust, but verify." [A proverb frequently quoted by President Reagan during arms control negotiations]
- I'm not known for being a big Microsoft cheerleader, but Microsoft deserves recognition for promoting both their Cloud Computing Advancement Act and pressing cloud vendors to police themselves when it comes to transparency. See www.microsoft.com/presspass/presskits/cloudpolicy/

An Example of The *Wrong* Approach



Source: http://cloudsecurity.org/blog/2008/07/01/cloudsecurityorg-interviews-guido-van-rossum-google-app-engine-python-and-security.html

Provider Failures Are Also A Real Possibility

- Even for a red-hot technology like cloud computing, there is no guarantee that your providers will financially survive. What will you do if your provider liquidates?

Pen Testing; Working Incidents In The Cloud

- Standard pen testing processes which you may use on your own infrastructure may not be an option in an outsourced environment (the cloud provider may not be able to distinguish your tests from an actual attack, or your tests may potentially impact other users in unacceptable ways)

- If you do have a security incident involving cloud-based operations, how will you handle investigating and working that incident? Will you have the access logs and network traffic logs you may need? Will you be able to tell what data may have been exfiltrated from your application?

- What if your system ends up being the origin of an attack? Are you comfortable with your provider's processes for disclosing information about you and your processes/data?

OECD, The Cloud, and Privacy

Security, Privacy, and Accountability

41. ***Privacy and security.*** Many of the most successful and most visible applications of Cloud computing today are consumer services such as e-mail services, social networks, and virtual worlds. The companies providing these services collect terabytes of data, much of it sensitive, personal information, which then is stored in data centres in countries around the world. How these companies, and the countries in which they operate, address privacy issues will be a critical factor affecting the development and acceptance of Cloud computing.

42. Who will have access to billing records? Will government regulation be needed to allow anonymous use of the Cloud and to put strict controls on access to usage records of Cloud service providers? Will government regulators be able to adapt rules on the use of private, personal information when companies are moving terabytes of sensitive information from employees and customers across national borders? Companies that wish to provide Cloud services globally must adopt leading-edge security and auditing technologies and best-in-class practices. If they fail to earn the trust of their customers by adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments will come under increasing pressure to regulate privacy in the Cloud. And if government policy is poorly designed, it could stymie the growth of the Cloud and commercial Cloud services.

Cloud Computing and Public Policy, 14 October 2009
http://www.olis.oecd.org/olis/2009doc.nsf/ENGDATCORPLOOK/NT00004FC6/$FILE/JT03270509.PDF

World Privacy Forum Privacy In The Clouds Report

From: "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," Released February 23, 2009, http://www.worldprivacyforum.org/cloudprivacy.html

Part II: The Security of Mobile Internet Device

What's A Mobile Internet Device?

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

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

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

Mobile Devices Are Common in Higher Ed

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

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

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

But Are Mobile Internet Devices Secure?

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

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

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

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

A Semi-Zen-like Koan

- ***"If I didn't buy the mobile device, and the mobile device isn't using my institutional network, and the mobile device isn't directly touching my servers, do I even 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'll Probably Cost You…

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

Mobile Data Plans Are Expensive

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

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

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

An Example Device Policy: Device Passwords

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

Managing Mobile Internet Device Policies

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

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

Example: What Can Be Required for iPhone Passwords?

- Looking at the iPhone Enterprise Deployment Guide:

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

- RIM offer similar controls for BlackBerry devices.

Other Potential Local iPhone "Policies" Include

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

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

Scalably Pushing Policies to the iPhone

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

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

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

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

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

We Need to Encourage "Healthy Paranoia"

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

Mobile Device Forensic Tools

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

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

What About Hardware Encryption?

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

Hardware Encryption on the BlackBerry

- Hardware encryption on the BlackBerry is described in some detail in "Enforcing encryption of internal and external file systems on BlackBerry devices," see http://docs.blackberry.com/en/admin/deliverables/3940/file_encryption_STO.pdf
- If setting encryption manually, be sure to set
  -- Content Protection, AND
  -- Enable Media Card Support, AND Encrypt Media Files
- If setting encryption centrally, be sure to set all of…
  -- Content Protection Strength policy rule
  -- External File System Encruption Level policy rule
  -- Force Content Protection for Master Keys policy rule
- For "stronger" or "strongest" Content Protection levels, set min pwd length to 12 or 21 characters, respectively (yes, dang, those are long passwords, aren't they?)

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 an early draft of this talk 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 regretable "incidents"
  -- If HR gets network access and email access killed before the zap code gets collected, the device may not be able to login (and get zapped), leaving the now ex-employee with the complete contents of the device

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

Mobile Devices as Terminals/X Terminals

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

Web Based Applications on Mobile Devices

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

Back End Servers Supporting Mobile Devices

- Many mobile Internet apps, not just Opera Mini, rely on services provided by back end servers, sometimes servers which run locally, sometimes servers running "in the cloud."

- If those servers go down, your service may be interrupted. This is a real risk and has happened multiple times to BlackBerry users; recent examples include:

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

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

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

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

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

Malware and A/V on Mobile Devices

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

Speaking of Jail Breaking the iPhone…

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

Counterfeit Hardware

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

Are Mobile Internet Devices Tough Enough?

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

Are There Any Questions?

- Thanks for the chance to talk today!

Additional Cloud Computing Security Resources

- "AWS Security Whitepaper," http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf
- "Cloud Computing Security: Raining On The Trendy New Parade," BlackHat USA 2009, www.isecpartners.com/files/Cloud.BlackHat2009-iSEC.pdf
- “ENISA Cloud Computing Risk Assessment,” November 20th, 2009, www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
- “Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26,” 10/7/2009, NIST, http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt
- “Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1,” December 2009, Cloud Security Alliance, http://www.cloudsecurityalliance.org/csaguide.pdf