A Conversation About Cloud Computing and Security

Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu)

NWACC Security Meeting, October 10th, 2013

http://pages.uoregon.edu/joe/nwacc-security-2013/

Disclaimer: all opinions expressed are solely those of the author and do not necessarily represent the opinion of any other party

I. Introduction

Thanks and A Disclaimer

- I'd like to begin by thanking Adrian Irish of UMT and NWACC for the chance to talk about cloud computing security today.

- Adrian and Molly and the whole NWACC team put a lot of work into this event, and I really appreciate the opportunity to be part of it.

- I also wanted to remind folks that all opinions expressed this morning represent solely my own perspective, and do NOT necessarily represent the opinion of Adrian, UMT, NWACC, Internet2, InCommon, nor the University of Oregon.

BTW, Speaking Of Organizations...

- Before we dig into cloud security, let me make a brief plug for some security-related job opportunities, if anyone in the audience knows of someone who might be interested:

  -- The University of Oregon is seeking to hire a Chief Information Security Officer, see http://jobs.uoregon.edu/unclassified.php?id=4158

  -- Internet2 would like to hire a Chief Cyberinfrastructure Security Officer, see http://www.internet2.edu/about/staff/careers#ccso

  -- ISOC would like to hire a Trust and Identity Lead, see http://www.internetsociety.org/jobs/trust-identity-program-lead

Format of This Talk

- Yes, this is another oddly-formatted "Joe talk."

- For those who haven't seen one of my talks before, I make them verbose so they'll be readable after the fact for those who couldn't be here today, as well as for search engines, readers for whom English is a second language, the hearing impaired, etc. Please don't let my odd slide format shake you up. :-) I promise ***I*** won't read my slides to you, nor do ***you*** need to try to read them as I talk.

- I also want to explicitly encourage you to **ask questions** as we go along, or to **question/challenge** things I may say. As the title of this talk hints, I truly want this to be a **conversation**, not just me yammering for 90 minutes.

What Cloud Security Topics Are YOU Interested In/Thinking About?

- To help get people comfortable speaking up, let's take a few minutes and go around the room...

- **What's your name and school?**

- **Is your school currently doing anything in the cloud?**

- **Do you have any specific cloud security concerns or questions?**

Some Context: Past NWACC Talks

- I've been pleased to have had the opportunity to talk at a number of prior NWACC events, including doing talks on:
  -- ***The Security of Mobile Devices*** in 2010, http://pages.uoregon.edu/joe/nwacc-mobile-security/
  -- ***Passwords***, at an NWACC Security event in 2009, http://pages.uoregon.edu/joe/passwords/
  -- ***The Inescapability of Convergence (Unless You 'Help')***, 2006, http://pages.uoregon.edu/joe/convergence/
  -- ***Winning the War On Spam***, June 2003, http://pages.uoregon.edu/joe/spamwar/winning-the-war-on-spam.pdf and even, way back when:
  -- ***Thinking About Your Wide Area Connectivity,*** in 2001, http://pages.uoregon.edu/joe/nwacc-bandwidth-presentation.pdf
- Today, though, we're going to talk about ***cloud security.***

This Is My First Talk on *Cloud Security* for NWACC, But It Is Not My First Cloud Security Talk...

- ***Internet2 NET+ Technical Architecture: An Introduction to Security Considerations,*** Internet2 Member Meeting, April 2012, http://pages.uoregon.edu/joe/netplus-sec/
- ***Updates on Two Topics: The Security of Cloud Computing and The Security of Mobile Devices,*** Internet2 Member Meeting, April 2010, http://pages.uoregon.edu/joe/sec-update-spring10/
- ***Cloud Computing and Security Considerations,*** Internet2 Joint Techs, February 2010, http://pages.uoregon.edu/joe/cloud-computing-security/

- Hopefully the thoughts in those will be consistent with what I tell you today :-)

II. Why Talk About Cloud Computing Security?

And Why Talk About Cloud Computing NOW?

Answer: The Cloud's Here/Coming, and Security Is In The "Critical Path" When It Comes to Cloud Adoption

Seems Like EVERYONE's Now At Least Considering the Cloud

- **"94% of Enterprises are at least discussing cloud or cloud services"**

  "Avoiding the Hidden Costs of the Cloud," PDF page 4, http://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf

Trendy Pundit Jargon: "Third Platform"

- **Platform One:** mainframe and terminals (pre-1985)
- **Platform Two:** LAN/Internet, Client/Server, PC ('85-'05)
- **Platform Three:** Mobile Broadband, Big Data/Analytics, Social Business, **Cloud Services,** Mobile Devices and Apps ('05-20+)

- 3rd Platform technologies currently "represent just 22% of ICT spending," but are believed to account for 98% of growth by 2020... Hmm.

- See for example figure 1
  "Top 10 Predictions 2013: Competing on the 3rd Platform,"
  http://www.idc.com/research/Predictions13/downloadable/238044.pdf

Cloud-Based Services Are Also A Major Focus for Internet2

- I work with Internet2 and InCommon under contract through UO.
- If you're paying attention to what Internet2's been working on, it's been hard to miss that NET+ is a major area of emphasis now (and for the last year or so), see http://www.internet2.edu/netplus/
- Given that, if you are at an Internet2 school, your institution might end up (a) sponsoring a cloud-based NET+ service, or (b) participating as a service validation or early adopter school, or (c) simply using a NET+ service. Thus, the security of cloud-based services might be an area that touches you personally/professionally.
- But let's take a second to talk a little about cloud adoption

Some Sites Decide to Use The Cloud. Others DON'T. Why?

- Is it a substantive matter of the features/functionality available from cloud provider's products or services?

- Is it a business matter, perhaps how much the product or service cost, or the terms of the agreement available?

- Or is the problem with infrastructure issues, maybe? For example, perhaps the service doesn't integrate well with your current identity management system, or requires network bandwidth you don't currently have?

- **Or is security (or privacy, or compliance) the problem? What do we empirically know?**

Security As Potential Block to Adoption

- "PC Connection, in partnership with Cisco, recently released the results of its **2013** Outlook on Technology: Cloud Computing Survey. The survey, the results of which are available at InfoWorld, queried over 500 organizations of all sizes to ascertain what they are seeking in a cloud solution, what concerns they have about the technology and what obstacles they see between their organization and further cloud adoption. [...] **Perhaps the most surprising information gleaned from the cloud computing usage survey is that security is the top obstacle to cloud adoption, according to 65 percent of the survey responses.** Integration was the next biggest obstacle, but it was listed in just 34 percent of responses." "Cloud Computing Usage: Security Still Considered a Barrier," http://midsizeinsider.com/en-us/article/cloud-computing-usage-security-still-co

Or Does Using The Cloud Actually IMPROVE Data Security?

- "**Fifty-one percent of IT executives surveyed believe that the cloud increases data security overall.** However, almost 70 percent of respondents indicated that consumer cloud services pose a risk to sensitive data in their organizations and **45 percent are not fully confident that their cloud provider's security processes and programs meet their data security requirements.**"

- "Data security, compliance top concerns of cloud adopters" http://www.techjournal.org/2013/05/data-security-compliance-top-concerns-of-cloud-adopters/

Some Proceed To Move To The Cloud, Even If There *May Be* "Security Issues"...

- 'A new report by the agency's Office of the Inspector General says that NASA needs to work on strengthening its information technology security practices. [...] **According to the report, NASA had five contracts for cloud hosting and none of these "came close" to meeting data security requirements.** [...] Over the past year, NASA spent less than 1 percent of its $1.5 billion annual IT budget on cloud computing. However, moving forward, the agency plans to dedicate much more to cloud security and initiatives. **Within the next five years, NASA is planning to have up to 75 percent of its new IT programs begin in the cloud and 100 percent of the agency's public data stored in cloud.'**
- "NASA Falls Short on Its Cloud Computing Security," http://news.cnet.com/8301-1009_3-57596053-83/nasa-falls-short-on-its-cloud-computing-security/

What Gets Moved Into The Cloud May Not *Stay* There. Why? "Security Concerns"...

- "IDG Enterprise recently published Cloud Computing: Key Trends and Future Effects Report, showing how enterprises continue to struggle with security, integration and governance [...] IDG's methodology is based on interviews with 1,358 respondents [...] **42% of cloud-based projects are eventually brought back in-house, with security concerns (65%),** technical/oversight problems (64%), and the need for standardization (on one platform) (48%) being the top three reasons why. **[...] For IT, concerns regarding security (66%),** integration stability and reliability (47%) and ability of cloud computing solutions to meet enterprise/industry standards (35%) challenge adoption.
- http://www.forbes.com/sites/louiscolumbus/**2013**/08/13/idg-cloud-computing-survey-security-integration-challenge-growth/

Security May Not Be The Only Issue

- Sometimes folks talk about "security" when they're really worried about something else, like privacy:

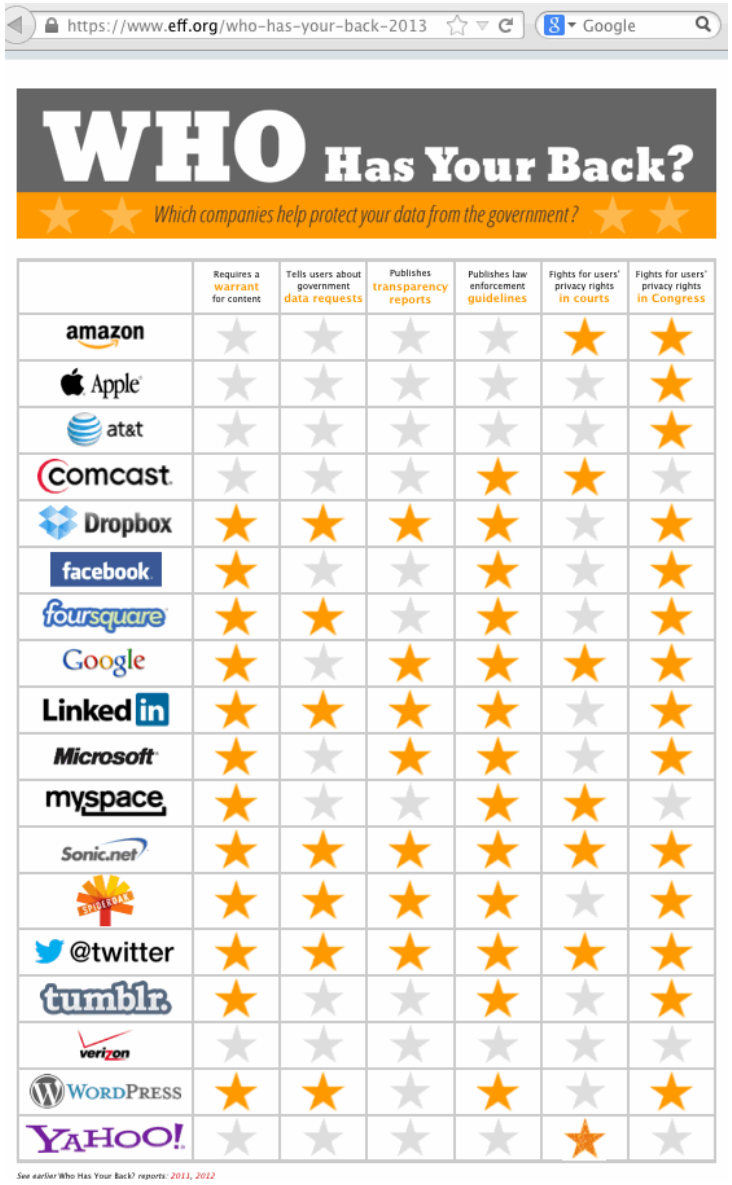
  -- If I store my confidential data in the cloud, will it end up disclosed to unauthorized parties?

- Or compliance:

  -- If I use the cloud, will I inadvertently violate some compliance requirement, and get fined or otherwise penalized?

- Not all cloud providers treat privacy issues the same way

EFF's "Who Has Your Back?" Privacy Graphic



Those columns of stars are, from left to right:

Requires a **warrant** for content

Tells users about government **data requests**

Publishes **transparency reports**

Publishes law enforcement **guidelines**

Fights for users' privacy rights **in courts**

Fights for users' privacy rights **in Congress**

Privacy Concerns May Also Shift Some Users Away From American Cloud Providers

- ITIF reported in August **2013** that one consequence of the NSA's PRISM interception program is that "**On the low end, U.S. cloud computing providers might lose $21.5 billion over the next three years. This estimate assumes the U.S. eventually loses about 10 percent of foreign market to European or Asian competitors** and retains its currently projected market share for the domestic market." http://www2.itif.org/2013-cloud-computing-costs.pdf
- BUT, the Cloud Computing Security Alliance, reporting on a survey of cloud adoption post-Snowden, reported that "**56% of non-US residents were now less likely to use US-based cloud providers**, in light of recent revelations about government access to customer information." https://cloudsecurityalliance.org/media/news/official-csa-snowden-nsa-patriot-act-survey/

Is Europe *Really* Any Better, Privacy-Wise?

- Europe was once fairly famous (notorious?) for having stringent data protection requirements, see http://ec.europa.eu/justice/data-protection/ but consider:

- "The FRA law (FRA-lagen in Swedish) [...] authorizes the Swedish Defence Radio Authority to warrantlessly wiretap all telephone and Internet traffic that crosses Sweden's borders. It [...] took effect on January 1, 2009." http://en.wikipedia.org/wiki/FRA_law
- "BND lässt sich Abhören von Verbindungen deutscher Provider genehmigen," [BND (the Federal Intelligence Service) can authorize [the] interception of German provider connections], http://www.spiegel.de/spiegel/vorab/bnd-laesst-sich-abhoeren-von-verbindungen-deutscher-provider-genehmigen-a-926221.html
- "UK government is one of the world's top pryers into user data on Facebook and Twitter," http://blogs.spectator.co.uk/coffeehouse/2013/08/uk-government-is-one-of-the-worlds-top-pryers-into-user-data-on-facebook-and-twitter/

Speaking of "European" Cloud Security

- I don't mean in any way to make light of the extremely serious events that took place during WW II, but there's a humorous spoof on cloud security that was put together by Marcus Ranum that's too good to overlook:

- http://www.youtube.com/watch?v=VjfaCoA2sQk

Some Potential Compliance Hurdles

- Depending on the sort of stuff you're working with, other applicable compliance regimes could include:
  -- Breach notification laws (47 different state laws!)
  -- CAN-SPAM (anti-spam laws)
  -- DIACAP (a DOD compliance thing)
  -- FERPA (higher education privacy)
  -- FIPS 140-2 (crypto standards)
  -- FISMA (federal contractors)
  -- GLBA (certain financial data)
  -- HIPAA/HITECH (health data)
  -- Human Subjects Research Data Protection
  -- ITAR (export controlled technologies and research)
  -- PCI (payment cards)
  -- SOX (accuracy of financial information)
  -- etc., etc., etc.

Just ONE Compliance Area: HIPAA

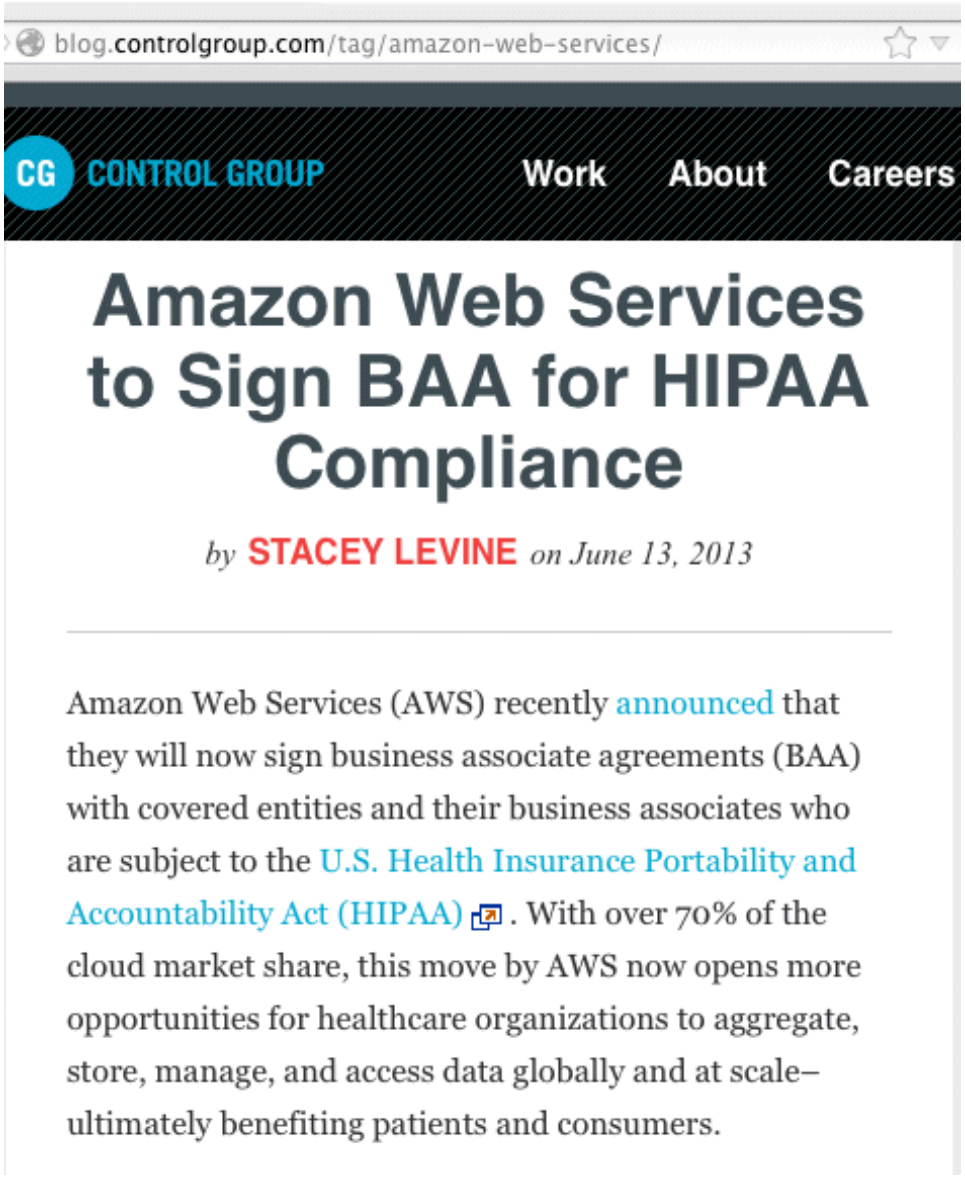
- Covered entities must be in compliance with the HIPAA Omnibus Rule as of 9/23/2013, see http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf (138 pps)
- As part of that the so-called "conduit exception" has been clarified to NOT include "data storage companies"

  … We note that the conduit exception is limited to transmission services (whether digital or hard copy)… In contrast, **an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information…**the difference between the two situations is the transient versus persistent nature of that opportunity. **For example, a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis.** (emphasis added) [PDF page 8, FedReg page 5572]
- To store Protected Health Information (PHI) in the cloud, you WILL need a BAA (Business Associate Agreement).

Will **Cloud Providers Execute BAAs?**

- If you want to use a cloud provider for PHI, and the cloud provider won't execute a BAA, compliance requirements will stall your cloud deployment.
- Why might a cloud provider "balk" at executing a BAA? Many cloud providers try to maintain a strict demarc, with security and compliance responsibilities split between the provider and the customer at the demarc.
- BAA's potentially drag the cloud provider back "across that demarc," and may entangle them in expensive PHI breaches caused by factors over which they ultimately have little or no control. Penalties for HIPAA security violations can run up to $1.5 million per year per incident.
- But, if you aren't willing to do BAAs, you're probably going to have to forego a lot of health-care-related customers...

One Cloud-as-Infrastructure Provider…



blog.controlgroup.com/tag/amazon-web-services/

CG CONTROL GROUP Work About Careers

Amazon Web Services to Sign BAA for HIPAA Compliance

by **STACEY LEVINE** *on June 13, 2013*

Amazon Web Services (AWS) recently announced that they will now sign business associate agreements (BAA) with covered entities and their business associates who are subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA). With over 70% of the cloud market share, this move by AWS now opens more opportunities for healthcare organizations to aggregate, store, manage, and access data globally and at scale– ultimately benefiting patients and consumers.

Another Timing Factor: Some Standards Are Still Being Developed; Maybe You Should Chime In/Help With This Work?

- **ISO/IEC 27017** […] **This standard will provide guidance on the information security elements/aspects of cloud computing, recommending cloud-specific information security controls** supplementing those recommended by ISO/IEC 27002 and indeed other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards covering information security in general. […] **The standard is at Working Draft stage. Publication is very unlikely before 2014, quite possibly not until 2015.** Over 200 pages of detailed comments from national bodies are being digested and integrated into the next draft. The comments are generally positive and helpful, but it inevitably takes time to discuss and agree so many through in-person committee meetings […] SC 27 decided NOT to progress a separate cloud information security management system specification standard, judging that ISO/IEC 27001 is sufficient. **Therefore, there are no plans to certify the security of cloud service providers specifically.**

  http://www.iso27001security.com/html/27017.html

III. What *Is* Cloud Computing?

Now That We Know People Worry About Security (and Privacy, and Compliance) In "The Cloud," What Exactly *Is* "The Cloud?"

- Infrastructure (compute cycles, storage, database, etc.) available on demand from a pre-provisioned pool (example: Amazon AWS, see http://aws.amazon.com/), sometimes referred to IAAS ("infrastructure as a service")
- Apps that run somewhere "out there" on infrastructure you don't run or rent (example: Google Apps for Education, see http://www.google.com/enterprise/apps/education/), often called SAAS ("software as a service")
- And then, largely for developers, there's "platform as a service" (PAAS) outfits; one example of this would be RedHat's OpenShift, see https://www.openshift.com/ , running somewhere in between IAAS and SAAS

I'm Renting a Server From A Hosting Company. Am I Using "The Cloud?"

- No. Just outsourcing the hosting of a server isn't enough to make you a user of "the cloud."
- Why? Most notably, your capacity isn't "highly elastic." If you get /.'d and temporarily need a lot more capacity, you can't quickly get it, you may need to enter into a year long contract, and if you no longer need the contracted server after a few weeks, well, that's too bad.
- You may also still need to administer the system from the "bare iron" on up, which again is inconsistent with "cloud" concept. In the cloud, you don't need to worry about actual infrastructure devices.
- You may even know where "your" server is located (example: server 26, rack 209, datacenter foo, Dallas, TX)

I'm An End User Using Gmail. Am I Using "The Cloud"?

- Yes. Gmail (and associated applications such as Google Apps for Education) are in many respects a perfect example of "software as a service."

- Another very common example of a cloud-based SAAS application is a file sharing service, such as Box or DropBox.

- Peer-to-peer file sharing services, on the other hand, such as BitTorrent, wouldn't typically be considered to be "in the cloud."

I'm Backing Up Stuff From My Smartphone Online Somewhere. Am *I* Using the Cloud?

- Yes. Backups of content from mobile devices (such as smart phones and tablets) would be a prime example of how users may be engaging with the cloud.

- In fact, mobile devices largely REQUIRE cloud-based backups because on-device storage may be limited, and opportunities for external expansion may be limited (typically, at best, you might be able to plug in something like a 32GB MicroSDHC card).

- Backups are particularly important for mobile devices given that mobile devices disproportionately often end up lost, stolen, or broken...

My Campus Is Running a "Private Cloud" – Surely *I'm* Using "The Cloud," Aren't I?

- From my POV, it depends. Some people just call a local compute cluster a "Private Cloud" because "private cloud" sounds cool/trendy.

- To *really* qualify as a cloud service, I'd be looking for:
  -- substantial pool of resources shared among many users with plenty of headroom for handling peaking loads
  -- an interface that's compatible with things like the Amazon EC2 public cloud (two examples: Ubuntu's OpenStack and the nimbusproject.org)

- Things like "publicly hosted" "private clouds" make my head hurt, definitionally-speaking. :-)

I'm Using XSEDE for Scientific Computing. What About Me? Am I Using "The Cloud?"

- XSEDE, the follow-on project to the TeraGrid, certainly has many "cloud-like" characteristics, but typically the XSEDE folks treat "the Cloud" as being something that they themselves are not.

- So I'd say, "not."

- See for example: "XSEDE Cloud Survey Report," https://www.ideals.illinois.edu/bitstream/handle/2142/45766/XSEDE%20Cloud%20Survey%20Report%20final.pdf?sequence=2

IV. So What Are The Risks If We "Go To The Cloud?"

Availability...

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

- As I'm sure everyone knows, computer and network security is fundamentally about three goals/objectives:

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

- **<u>Availability</u> 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...

Some Major Cloud Outages in 2013 (as of 1 July)

- Nice summary from InfoWorld, "Worst Cloud Outages of 2013 (So Far)," http://www.infoworld.com/slideshow/107783/the-worst-cloud-outages-of-2013-so-far-221831#slide1
- Amazon, January 31st, less than an hour
- Dropbox, January 10th, 16 hours
- Facebook, January 28th couple of hours
- MS Bing, February 2nd, couple of hours
- MS Office 365/Outlook, February 1st, couple of hours
- MS Azure, February 22nd, over 12 hours
- Google Drive, March 18-19th, 17 hours total
- CloudFlare, March 3rd, about an hour
- Dropbox, May 30th, about an hour and a half
- Twitter, June 3rd, about 45 minutes

www.geekwire.com/2013/vine-instagram-stop-working-time-users-freak-twitter/

GW | Jobs | Calendar | GeekWire Events | Startup Resources | Startup List

Instagram, Vine stop working at same time; people use Twitter to freak out

August 25, 2013 at 1:28 pm by Taylor Soper 7 Comments

Share this: Email Like 126 Tweet 164 Share 4 +1 68

New post: *AWS server issues take down Instagram, Airbnb, Flipboard*

Original post:

If you want to Instagram another selfie or post a hilarious Vine video, it looks like you'll need to wait as both Instagram and Vine are currently out-of-order.

It appears both social media hubs went down sometime around 1 p.m. PST. Both Vine.co and Instagram.com are down, as confirmed by Down For Everyone Or Just Me.

Facebook (which owns Instagram) still works, and Twitter (which owns Vine) is also working. Instagram has more than 100 million users, while Vine has 40 million.

I was actually trying to post a photo to Instagram a few minutes ago and got a little frustrated when it kept stalling, even after restarting my phone.

But there seem to be some people on Twitter — which is still up and running just fine — quite a bit more angry than me (see below).

Amazon.com went down for 40 minutes last week, presumably costing the Seattle online giant millions in sales. Two days before that, all of Google's services went down for five minutes. The New York Times also went down for two hours two weeks ago, and GitHub also experienced outages.

A More Dire Thing: Provider Bankruptcies

blogs.wsj.com/venturecapital/2013/10/01/nirvanix-files-for-chapter-11-bankruptcy/

October 1, 2013, 6:11 PM

Nirvanix Files for Chapter 11 Bankruptcy

Article | Comments (4)

Email | Print

By DEBORAH GAGE CONNECT

Cloud storage company Nirvanix Inc. on Tuesday filed for Chapter 11 bankruptcy in Delaware federal court, the culmination of a startling flop for what was once seen as a high-flier among cloud startups.

The filing comes on the heels of a notice the company posted on its website last week saying that it was working with International Business Machines Corp. to either return customers' data or help them move it to another cloud storage provider and would try to be available through October 15.

Kharisma Tarigan/Agence France-Presse/Getty Images

Nirvanix had raised more than $70 million in venture capital since its founding in 2007, according to VentureWire records. In May 2012 after the last funding round, which was $25 million, former Chief Executive Scott Genereux told VentureWire that Nirvanix was growing and headed toward profitability and a possible IPO.

Its largest equity holders are Khosla Ventures and TriplePoint Capital, which may

The Three Cloud Bankruptcy Issues...

- If you prepaid (to lock in prices/get a multiyear discount), is that prepaid money in escrow somewhere (and able to be refunded), or is it flat out gone?

- Can you find a replacement provider that will be able to take over when it comes to providing the same service your former cloud provider delivered? (standardized services will obviously be easier than unique applications)

- Perhaps most critically: can you get your data out, and in format that's usable elsewhere?

Cloud Lock-In: If You Want To Exit The Cloud, Will You Have the Local Expertise You Need?

- One risk of letting someone else do the heavy lifting for you for a while is that if you need to resume doing that work yourself, it can be a lot harder to get back up to speed than you might think.

- Will you still have key staff?
- Will you still have critical facilities?
- Can you deliver the professional quality of the services or application you got from the cloud? (It's not uncommon for some parts of a cloud service to be terrific, while others may drive you nuts)

Digging Down On A Specific Technical Availability Risk: Network Connectivity

- In the (public) cloud computing model, users are local but critical resources are hosted elsewhere.
- Connectivity thus is of paramount importance: if the network is "down," you won't be able to reach "the public cloud." Some things to think about:
  - What might cause a network outage? Fiber cut? DDoS? Other?
  - Is the outage local, remote, or somewhere in between?
  - How much network IS "in between" me and my cloud provider?
  - How long might an outage last? Minutes? Hours? Days?
  - What would we do while we're down?
  - Do I need more network redundancy?
  - **If I need to buy more redundancy, what will that cost?**

Network Quality

- Besides just being available, you should also think about the quality of your network connections. Will they be good enough to support the cloud app you're thinking of fielding? Depending on the app this may mean confirming:
- Do I have enough aggregate bandwidth?
- What sort of throughput can a single user achieve?
- Are there latency issues?
- Are there jitter issues?
- Am I going to be NAT'd, or will I have publicly addressable IPs? Are those addresses "clean," or do those addresses have reputation issues from previous users?
- Can I get IPv6 connectivity if I want or need it?
- Can I get jumbo frames if I need them? (9K MTU)

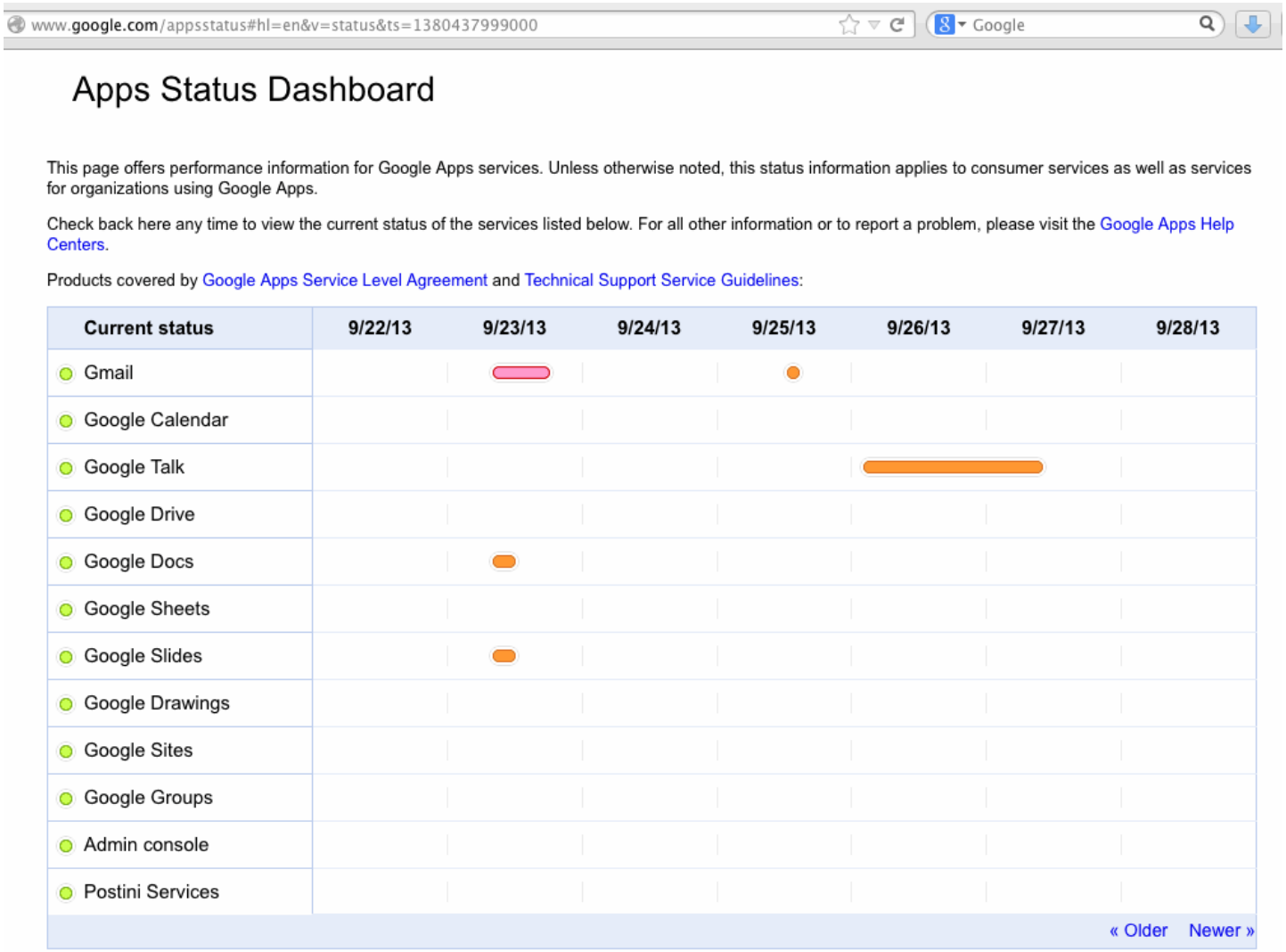
Mitigating Cloud Computing Availability Issues

- 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 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.

SLAs

- Cloud providers may be willing to help you meet whatever service level agreements you need. For example, if availability is of critical importance, you may be helped to configure the cloud service you're providing so that it has a high level of redundancy.
- However, as the saying goes, "You can get whatever level of redundancy you need, but you're going to pay for what you request."
- The "more 9's" you need (e.g., 99% availability, 99.9% availability, 99.99% availability, etc.), the more you're going to pay because handling the weirdest potential corner cases that can impact availability becomes increasingly difficult (and thus expensive).
- 99.99 availability ==> 52+ minutes downtime/yr...

Cloud Application Availability Reporting



Gmail - Service Details

Apps Status Dashboard

This page offers performance information for Google Apps services. Unless otherwise noted, this status information applies to consumer services as well as services for organizations using Google Apps.

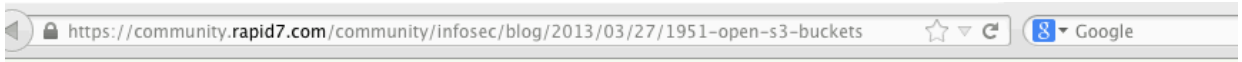
Check back here any time to view the current status of the services listed below. For all other information or to report a problem, please visit the Google Apps Help Centers.

Time	Description
9/23/13 7:00 PM	The problem with Gmail should be resolved. We apologize for the inconvenience and thank you for your patience and continued support. Please rest assured that system reliability is a top priority at Google, and we are making continuous improvements to make our systems better. As of 1600 Pacific Time, Gmail message delivery and attachment download is functioning normally for all users. We apologize for the duration of today's event; we're aware that prompt email delivery is an important part of the Gmail experience, and today's experience fell far short of our standards. We have analyzed the data on user impact and are providing a preliminary assessment of what occurred: Between 0554 and 1530 Pacific Time today, 29.1% of messages received by Gmail users were delayed. The average (median) delay was just 2.6 seconds, but some mail was more severely delayed. However, this issue did not affect users' access to the Gmail page or other functionality.
9/23/13 4:00 PM	Gmail service has already been restored for some users, and we expect a resolution for all users in the near future. Please note this time frame is an estimate and may change. Gmail message delivery delays and attachment download issues have been corrected for most affected users. A majority of the delivery backlog has also been cleared. We hope to clear the backlog completely in the very near future.
9/23/13 1:00 PM	Gmail service has already been restored for some users, and we expect a resolution for all users within the next 3 hours. Please note this time frame is an estimate and may change. Gmail message delivery delays and attachment download issues have been corrected for most affected users. We expect a small and declining number of messages to still be affected for the next 3 hours as the remaining delivery backlog is cleared. We are working on several options to accelerate the process and will provide more information when we have an updated time estimate.
9/23/13 12:00 PM	Gmail service has already been restored for some users, and we expect a resolution for all users within the next 1 hours. Please note this time frame is an estimate and may change.
9/23/13 11:45 AM	Our team is continuing to investigate this issue. We will provide an update by 9/23/13 12:45 PM with more information about this problem. Thank you for your patience.
9/23/13 11:05 AM	Our team is continuing to investigate this issue. We will provide an update by 9/23/13 12:05 PM with more information about this problem. Thank you for your patience. The email delays are affecting less than 50% of Gmail users.
9/23/13 10:45 AM	Our team is continuing to investigate this issue. We will provide an update by 9/23/13 11:45 AM with more information about this problem. Thank you for your patience.
9/23/13 9:43 AM	Our team is continuing to investigate this issue. We will provide an update by 9/23/13 10:45 AM with more information about this problem. Thank you for your patience.
9/23/13 8:45 AM	Our team is continuing to investigate this issue. We will provide an update by 9/23/13 9:45 AM with more information about this problem. Thank you for your patience. The delivery of some messages is being delayed and attachments may fail to download. This issue is affecting less than an estimated 0.024% of the Gmail user base.
9/23/13 7:25 AM	We're investigating reports of an issue with Gmail. We will provide more information shortly.

V. Confidentiality...

Data Confidentiality and Breaches

- But let's not get rat holed on availability.
- CIOs don't get fired for services going down (at least as long as they don't go down for TOO long). CIOs do get fired for big data breaches involving PII.
- Therefore, most CIOs worry a lot about the security of private data, including its security if stored off-site.
- Should they? In some cases, yes.
- A couple of examples...



The Research

My role at Rapid7 is providing penetration testing services for organizations that want to test the effectiveness of their security practices and identify potential areas of risk, as well as the likely impact of attacks in those areas. Having found public buckets on a number of assessments, and used them as part of my attack strategy, I was curious how common this issue of public buckets is, and what sorts of data we would find in exposed buckets.

Later on in the research process I discovered that someone else had already discussed the dangers of public buckets. Robin Wood previously blogged on the issue and published a tool to check the openness of buckets. Robin's work is excellent as usual and we tried to take it a bit further focusing on enterprises and buckets identified in web crawling results.

The Results

We discovered 12,328 unique buckets with the following breakdown:

```
Public:  1,951
Private:  10,377
```

Approximately 1 in 6 buckets of the 12,328 identified were left open for the perusal of anyone that's interested.

These 12,328 buckets were skewed towards those we could identify based on domain name, word list, or use within web sites. From the 1,951 public buckets we gathered a list of over **126 billion files**. The sheer number of files made it unrealistic to test the permissions of every single object, so a random sampling was taken instead. All told, we reviewed over 40,000 publicly visible files, many of which contained sensitive data.

Some specific examples of the data found are listed below:

- Personal photos from a medium-sized social media service
- Sales records and account information for a large car dealership
- Affiliate tracking data, click-through rates, and account information for an ad company's clients
- Employee personal information and member lists across various spreadsheets
- Unprotected database backups containing site data and encrypted passwords
- Video game source code and development tools for a mobile gaming firm
- PHP source code including configuration files, which contain usernames and passwords
- Sales "battlecards" for a large software vendor

Much of the data could be used to stage a network attack, compromise users accounts, or to sell on the black market. Although more subtle, one of the other concerns was the number of publicly available log files.

talkincloud.com/saas-software-service/adobe-data-breach-will-skeptical-cloud-users-exit

Adobe Data Breach: Will Skeptical Cloud Users Exit?

Chris Talbot | *Talkin' Cloud* *Oct. 4, 2013*

EMAIL COMMENTS 0

Adobe's Creative Cloud and Revel customers are among the worst affected by a data breach that has left the personal data of 2.9 million Adobe customers open to hackers. Exactly who and what was affected by the breach are still unknown, but it looks like Adobe's cloud services may have been hit hardest.

This was the last thing Adobe needed: Another blemish to tarnish the reputation of its cloud services. As Adobe tries to shift customers to cloud services like Creative Cloud, the company has suffered a setback. Hackers have exposed approximately 2.9 million users' personal data.

Although it's not yet clear how many of those users were cloud users, the Internet gossip is that Creative Cloud and Revel users are among the worst affected by the data breach. What seems to have happened is hackers broke into Adobe's servers to swipe software source code, and according to a blog post by Brad Arkin, Adobe's chief security officer, Adobe has been attracted more and more attention from cyber-attackers.

And things look pretty bad.

"Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders," Arkin wrote.

Protecting Data Confidentiality in the Cloud

- Protecting data in the cloud is often largely a matter of how you encrypt private data at rest, and how you encrypt it when it is in transit/on the wire.
- For web based applications, encryption of data on the wire normally involves use of SSL/TLS ("https").
- While all SSL/TLS web sites may look more or less the same, the quality of the encryption used by any given web site may vary dramatically.
- I'd encourage you to check the SSL/TLS practices of sites you care about using https://www.ssllabs.com/ssltest/ (caution: sometimes you will be disappointed!)
- You may also want to see an earlier talk of mine that's at http://pages.uoregon.edu/joe/hardlook/hard-look.pdf

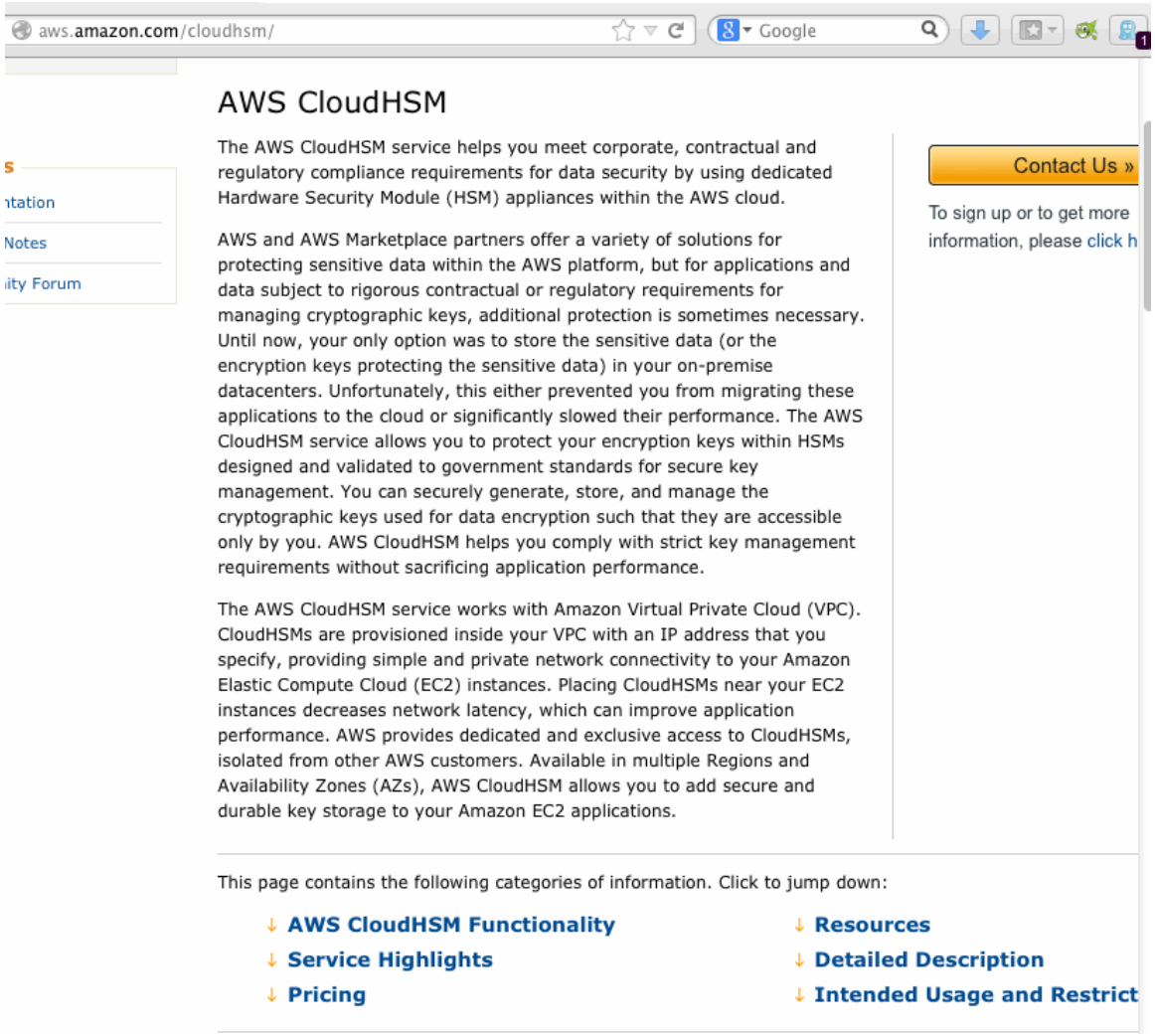
Protecting Data at Rest

- Protecting data at rest is often trickier.

- Some sites may do whole disk encryption when the system is quiescent, but leave all data decrypted once the system has booted up. If your worry is just theft of hardware, WDE may be all you need, but in most cases the value of your data >> value of the hardware it is sitting on.

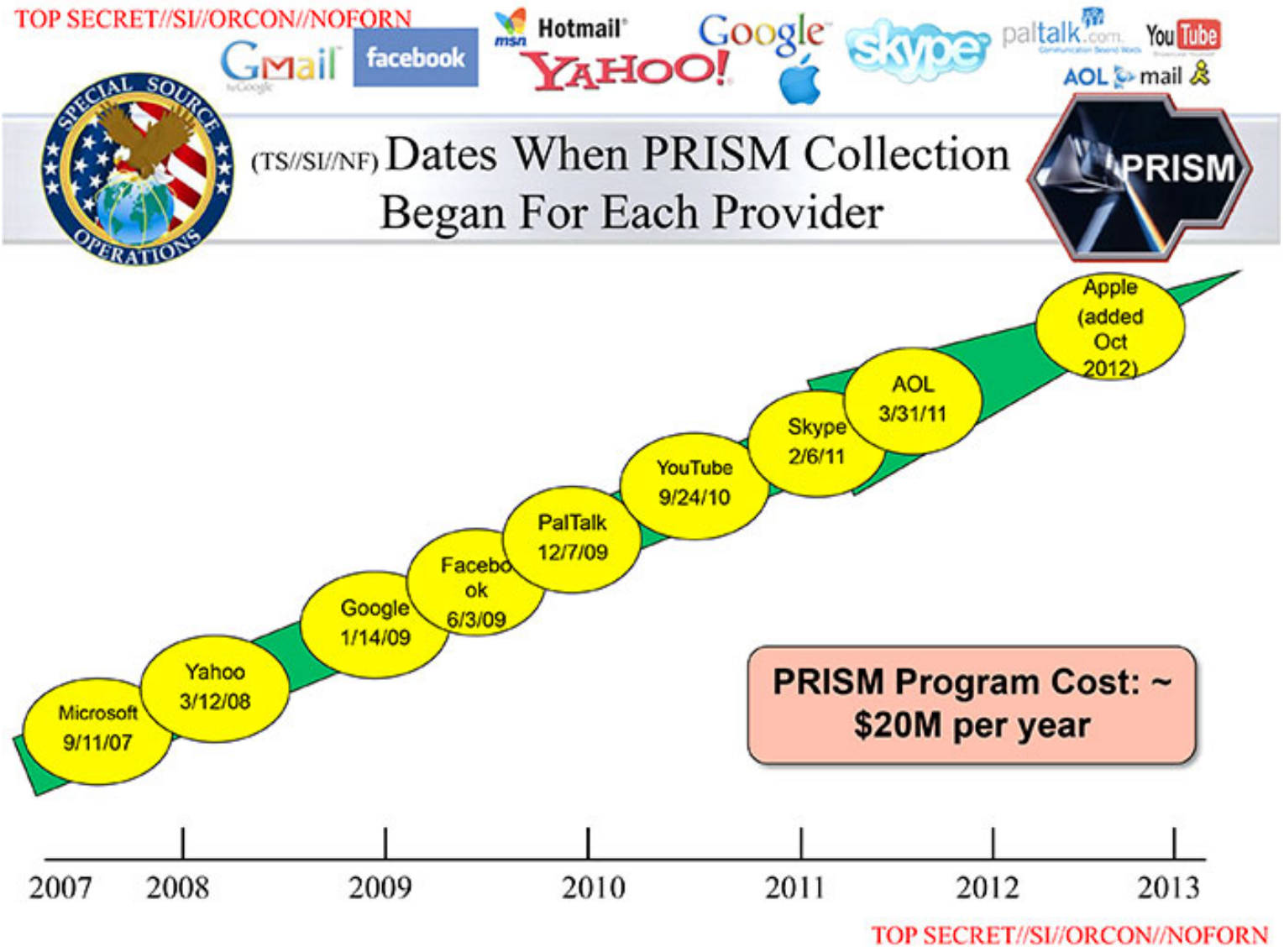
- Therefore, strive to encrypt everything as much as possible, as routinely as possible, and be sure to think about secure cryptographic key storage (e.g., use a hardware security module when possible). See an example of a service that's offering HSM service in the cloud on the next slide.

Amazon's CloudHSM Service



Compulsory Access to Your Data

- Cloud providers may, under some circumstances, be required to provide government authorities with access to your data. This may be due to a court order, or as a result of national security program, as was revealed in Edward Snowden's recent leaks (see next slide)
- You may not be notified of government access, particularly if the order served on your cloud provider prohibits the provider from even disclosing the existence of that order to you.
- As is true for other potential confidential vulnerabilities, your best bet is to use strong encryption so that your cloud provider doesn't have the ABILITY to disclose confidential information in unencrypted form.



http://upload.wikimedia.org/wikipedia/commons/c/c7/Prism_slide_5.jpg

VI. Integrity...

What About Data Integrity in The Cloud?

- Data integrity often seems to be the "red-headed step child" of cyber security: many people seem to pretend this issue doesn't exist.
- How do we rigorously know that the GB (or TB!) worth of files we have stored are correct and un-tampered-with?
- Some of us may checksum critical files, but do we religiously check those file checksums to ensure that nothing's changed? And what about all the files we DON'T check, eh?
- Some might ask is data integrity really that big a deal?
- Sure it is. We just don't think about it as "data integrity" or "files being tampered with," we tend to run into it as "sites getting hacked" or "defaced" or maybe systems getting hit with "ransomware"

WordPress Plugin Issues As A Path To Unauthorized File Modifications

Executive Summary

Checkmarx's research lab identified that more than 20% of the 50 most popular WordPress plugins are vulnerable to common Web attacks, such as SQL Injection. Furthermore, a concentrated research into e-commerce plugins revealed that 7 out of the 10 most popular e-commerce plugins contain vulnerabilities. This is the first time that such a comprehensive survey was prepared to test the state of security of the leading plugins. In total, 8 million vulnerable WordPress plugins were downloaded.

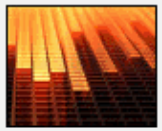
The impact? Hackers can exploit these vulnerable applications to access sensitive information such as personally identifiable information (PII), health records and financial details. Other vulnerabilities allow hackers to deface the sites or redirect them to another attacker-controlled site. In other cases, hackers can take control of the vulnerable sites and make them part of their botnet heeding to the attacker's instructions.

http://www.checkmarx.com/wp-content/uploads/2013/06/The-Security-State-of-WordPress-Top-50-Plugins3.pdf

vBulletin CMS Exploit → Full Control

www.net-security.org/secworld.php?id=15743


WhatsApp encryption flaw revealed, POC code published


Dangerous vBulletin exploit in the wild


The cost and frequency of cyber attacks on the rise


Several IT workers among "Operation Payback" indicted suspects


What can we learn from ICS/SCADA security incidents?


Linux command line cheat sheet

Top IT predictions for 2014 and

Dangerous vBulletin exploit in the wild

Posted on 09 October 2013.

vBulletin is a popular proprietary CMS that was recently reported to be vulnerable to an unspecified attack vector. vBulletin is currently positioned 4th in the list of installed CMS sites on the Internet. Hence, the threat potential is huge.

Although vBulletin has not disclosed the root cause of the vulnerability or its impact, we determined the attacker's methods. The identified vulnerability allows an attacker to abuse the vBulletin configuration mechanism in order to create a secondary administrative account. Once the attacker creates the account, they will have full control over the exploited vBulletin application, and subsequently the supported site.

Initial analysis

Although vBulletin has not disclosed the root cause of the vulnerability or the impact on customers, they did provide a workaround in a blog post encouraging customers to delete the /install, /core/install in vBulleting 4.x and 5.x respectively.

Additionally, on vBulletin internal forums a victimized user shared his server's Apache log, providing some visibility into the attacker's procedure:

```
"GET /forum/core/install/upgrade.php HTTP/1.1" 404 613 "-" "-"
"GET /forum/install/upgrade.php HTTP/1.1" 404 613 "-" "-"
```

The Feds Have Begun Paying Attention to Server-Side Security Vulnerabilities

- For example, there's a new FCC Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group that is specifically focused on DoS attacks that come from servers rather than botted PCs.

- I view that as a particularly positive sign that people are increasingly coming to realize that servers have some unique risks of their own, due to things like their high level of connectedness (e.g., gigabit links are common), and pressures on administration practices (if you're selling services at dirt cheap rates, you may not have a lot of money available to vet customers, much less process abuse complaints or do extensive security reviews).

Recovering From Data Corruption Issues

- The most common approach to recovering from data corruption/unauthorized file modifications -- once they're somehow detected -- is to restore data from a trusted backup. When you're running systems locally, you also probably arrange for them to be backed up, periodically testing those backups for usability, etc.

- But what about in the cloud? Are you backing up data that's there, too, somehow? Or are you trusting your cloud vendor to do it for you?

- Data loss may be more common than you think...

finance.yahoo.com/news/cloud-computing-users-losing-data-205500612.html

Home Mail News Sports Finance Weather Games Groups Answers

YAHOO! FINANCE Search Finance

Cloud Computing Users Are Losing Data, Symantec Finds

INVESTOR'S BUSINESS DAILY Investor's Business Daily – Wed, Jan 16, 2013 3:55 PM EST

Email Recommend 18 Tweet Share +1 Print

RELATED QUOTES

Symbol	Price	Change
SYMC	24.63	-0.11

AMZN	297.45	-5.78

Cloud computing is a ticket to losing data for two in five companies, a new study finds.

"It's really kind of astounding," said Dave Elliott, a cloud marketing manager at storage and security company Symantec (SYMC). The company polled more than 3,200 organizations to gauge hidden costs of the cloud and ways to mitigate problems.

"Forty-three percent of respondents have lost data in the cloud and have had to recover from backups," Elliott said. And the recovery process has failed at least once for most.

Specific Example: T-Mobile's Sidekick Service, 2009

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

Another Example: Amazon 2011

www.businessinsider.com/amazon-lost-data-2011-4

BUSINESS INSIDER | Tech | Finance | Politics | Strategy | Li

Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data

HENRY BLODGET | APR. 28, 2011, 7:10 AM | 92,221 | 75

EMAIL | MORE

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's huge EC2 cloud services crash permanently destroyed some data.

Um...

The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is.

(And a small loss on a percentage basis for Amazon, obviously, could be catastrophic for some companies).

Amazon has yet to fully explain what happened when its mission-critical and supposedly bomb-proof systems crashed, but the explanation will be

When You Start Looking at Cloud Backup

- Be sure to distinguish between backing up data TO the cloud, and backing up what you currently have IN the cloud.
- Remember that our worry is "What happens when the data you've got that was in the cloud that needs to be restored?" Depending on what caused data to be lost or corrupted, some strategies may not save you (example: mirrored data can perfectly mirror data corruption caused by an application flaw, right?)
- Some cloud providers have chosen to specifically focus on cloud backup as a core competency, see for example:
  http://aws.amazon.com/backup-storage/
  http://www.windowsazure.com/en-us/services/backup/
  http://www.rackspace.com/cloud/backup/

VII. "Integrating" With The Cloud: Another Area of Potential Concern

Campus Authentication

- In addition to the big three issues of availability, confidentiality and integrity, you may also see more subtle cloud-related security risks. For example, some cloud providers may not do a very clean job of integrating with your campus identity management system (e.g., they do NOT do federated SAML-based authentication ala Shibboleth and InCommon)
- Some providers may want to do something really, really broken, like periodically syncing a copy of your credential store to their systems (ooh, not good, not good at all), or using your campus LDAP servers (also not a good model).
- Other providers may substitute their own identity management system as a replacement for yours (hello, OpenID providers).

We're Not Going To Rehash The Step-By-Step Process By Which OpenID Works

- If you want a nice step-by-step summary of how OpenID works, see the discussion and diagrams that are available at https://developers.google.com/accounts/docs/OpenID

- I also rather like:
  "Single Sign-On For the Internet: A Security Story,"
  https://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Whitepaper/bh-usa-07-tsyrklevich-WP.pdf

  While this is a 2007 document, it does a nice job of summarizing not just how OpenID is meant to work, but some of the ways that OpenID could potentially be abused (at least if people are casual about how they implement/use it)

https://developers.google.com/accounts/docs/OpenID

Federated Login for Google Account Users

Third-party websites and applications can now let visitors sign in using their Google user accounts. Federated Login, based on the OpenID standard, frees users from having to set up separate login accounts for different web sites--and frees web site developers from the task of implementing login authentication measures. OpenID achieves this goal by providing a framework in which users can establish an account with an OpenID provider, such as Google, and use that account to sign into any web site that accepts OpenIDs. This page describes how to integrate Google's Federated Login for a web site or application.

> **Note:** If you are planning to provide a "sign-in with Google" feature, we recommend using Google+ Sign-in, which provides the OAuth 2.0 authentication mechanism along with additional access to Google desktop and mobile features.

Google supports the OpenID 2.0 protocol, providing authentication support as an OpenID provider. On request from a third-party site, Google authenticates users who are signing in with an existing Google account, and returns to the third-party site an identifier that the site can use to recognize the user. This identifier is consistent, enabling the third-party site to recognize the user across multiple sessions. Google also supports the following extensions:

OpenID Attribute Exchange 1.0 allows web developers to access, with the user's approval, certain user information stored with Google, including user name and email address.

OpenID User Interface 1.0 supports alternative user experiences for the authentication process. The default experience requires the web application to redirect users away from the application site to Google's authentication pages. This extension allows web developers to open Google authentication in a popup window and includes favicon support for a smoother experience.

OpenID+OAuth Hybrid protocol lets web developers combine an OpenID request with an OAuth authentication request. This extension is useful for web developers who use both OpenID and OAuth, particularly in that it simplifies the process for users by requesting their approval once instead of twice.

Google Is Not the Only OpenID Provider, But It's Probably the Most Widely Used One

- There are literally hundreds of OpenID providers out there, although just a handful account for the vast majority of OpenID logins, see http://janrain.com/blog/what-are-most-popular-networks-social-login-and-sharing-web/ which quotes the values:

Google:	***38%***	***38%*** (cumulative %)
Facebook:	27%	65%
Yahoo:	14%	79%
Twitter:	7%	86%
Windows Live:	6%	92%
Other:	8%	100%

- That same article notes that OpenID provider popularity varies with the type of web site that's being accessed.

Surprise! You may already have an OpenID.

If you use any of the following services, you already have your own OpenID. Below are instructions on how to sign in with each of the following providers on an OpenID enabled website. (When you see bold text, you should replace it with your own username or screenname on that service.)

Google

Look for the "Sign in with a Google Account" button or use your Google Profile URL.

YAHOO!

Look for the "Sign in with Yahoo" button.

YAHOO! JAPAN

Look for the "Yahoo! JAPAN IDでログイン" button.

LIVEJOURNAL

Enter "**username**.livejournal.com"

Hyves

Click the "Sign in with Hyves" button.

Blogger

Enter your blog URL: "**blogname**.blogspot.com"

flickr™

Look for the "Sign in with Yahoo" button or use your photostream URL

orange™

Click the "Sign in with Orange" button or enter "orange.fr"

mixi

mixi is a web service that allows users to communicate with their friends and acquaintances.

myspace

Look for the "Login with MySpaceID" button or enter "www.myspace.com/**username**"

Wordpress

Enter your WordPress.com URL, for example: "**username**.wordpress.com"

Aol.

Look for a "Sign in with AOL" button or enter "openid.aol.com/**screenname**"

Other Well Known & Simple Providers

In addition, there are several dedicated OpenID providers that are generally recommended by various members of the community. While not a comprehensive list, each of these providers offers a free and secure OpenID to use across the web.

Not All OpenID Providers Will Necessarily Work The Way Originally Intended...

- For example, imagine an OpenID provider that provides a redirection layer between an OpenID, concealing/protecting a user's real email address from disclosure...

- This is not a hypothetical service – this is exactly what LiquidID does, see http://liquidid.net/home.php (does this remind you of privacy/proxy domain name registrations? It sure strikes a chord for me in this respect...)

- Even more "interestingly," imagine an OpenID provider that offers completely anonymous "throw away" OpenID credentials, much in the way that Mailinator offers completely anonymous throw away email addresses...

openid.anonymity.com

Anonymous OpenID

brought to you by...

Your disposable OpenID

http://openid.anonymity.com/ClraHoG

What is this?

In short: automatic, anonymous, registration-less & disposable OpenID log-ins.

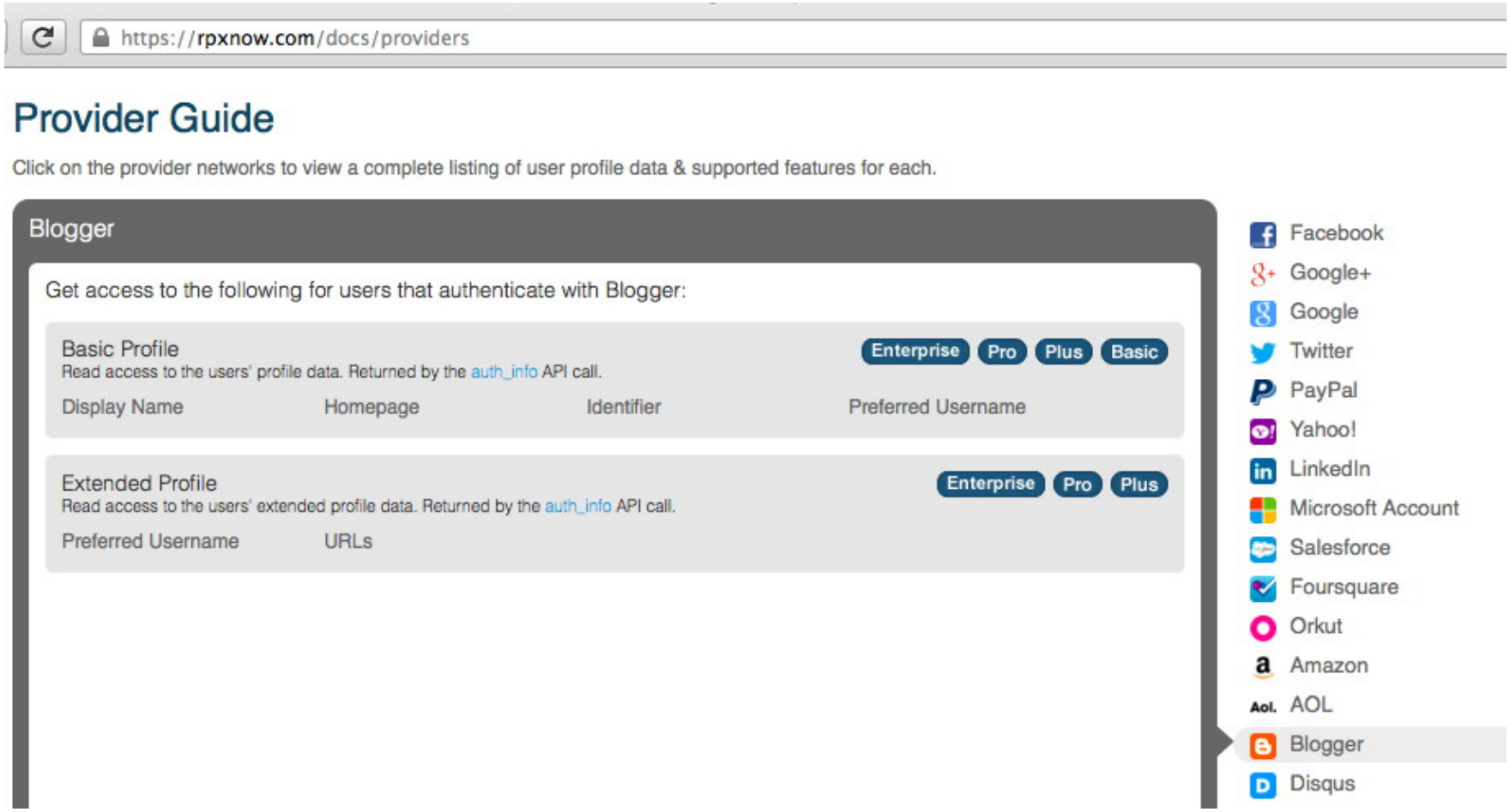
OpenID is a solution to the problem of having to keep track of usernames and passwords for sites that require log-ins. Many sites are now OpenID enabled and allow visitors to log in using only the URL of their profile on an OpenID provider such as AOL, Blogger and so on.

OpenID.Anonymity.com is an OpenID provider just like them, but we do it differently. No one has got a fixed profile here, and you don't have to sign up or register any accounts whatsoever. Rather, any OpenID profile given such as *http://openid.anonymity.com/anythingHere* will automatically be validated for you as an authentic log-in by Anonymity.com. If the site that you log in to ask for a name, we simply give it a randomized name such as "AnonEceSAqo." In short, OpenID.Anonymity.com is to OpenIDs what Mailinator is to e-mails.

How do I use it?

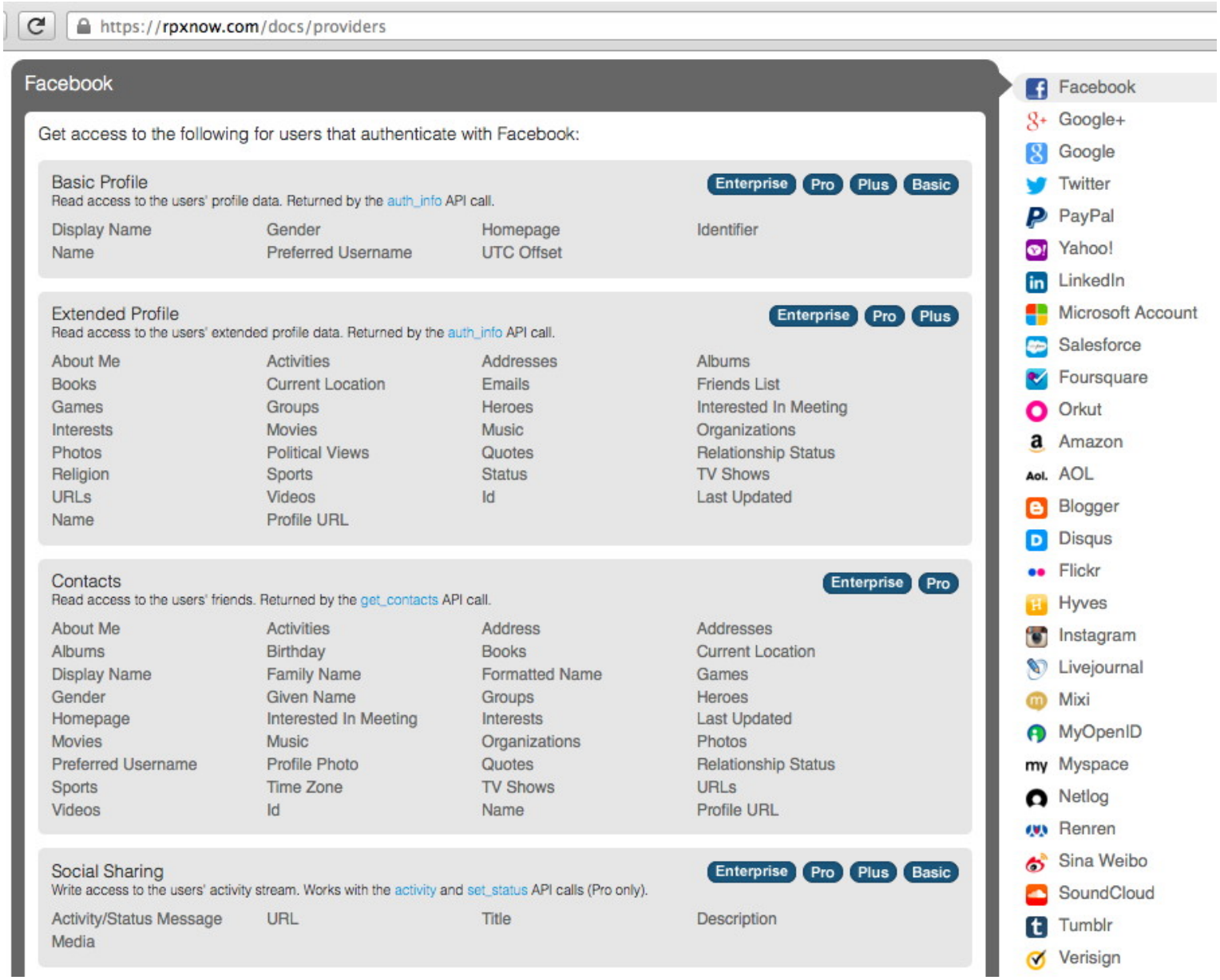
When you would like to log in to a site that you would rather not give your online identity to, look for the OpenID icon or an option to log in using OpenID. If the site accepts OpenID, it should ask you for the URL to your OpenID-enabled profile (provider). Now, rather than giving up your AOL or LiveJournal URL, simply type in *http://openid.anonymity.com/whateverhere*, substituting the *whateverhere* part with any letters and numbers of your choosing. Submit, enter in the characters on the captcha image, submit again, and that's it! The site should now recognize you as a logged in account under a fictitious name indicating your anonymity.

So What DOES Gets Shared When OpenID Is Used? Answer: It Varies By Provider.



"Display Name, Homepage, Identifier, Preferred Username, URLs "

Facebook? LOTS More Gets Shared

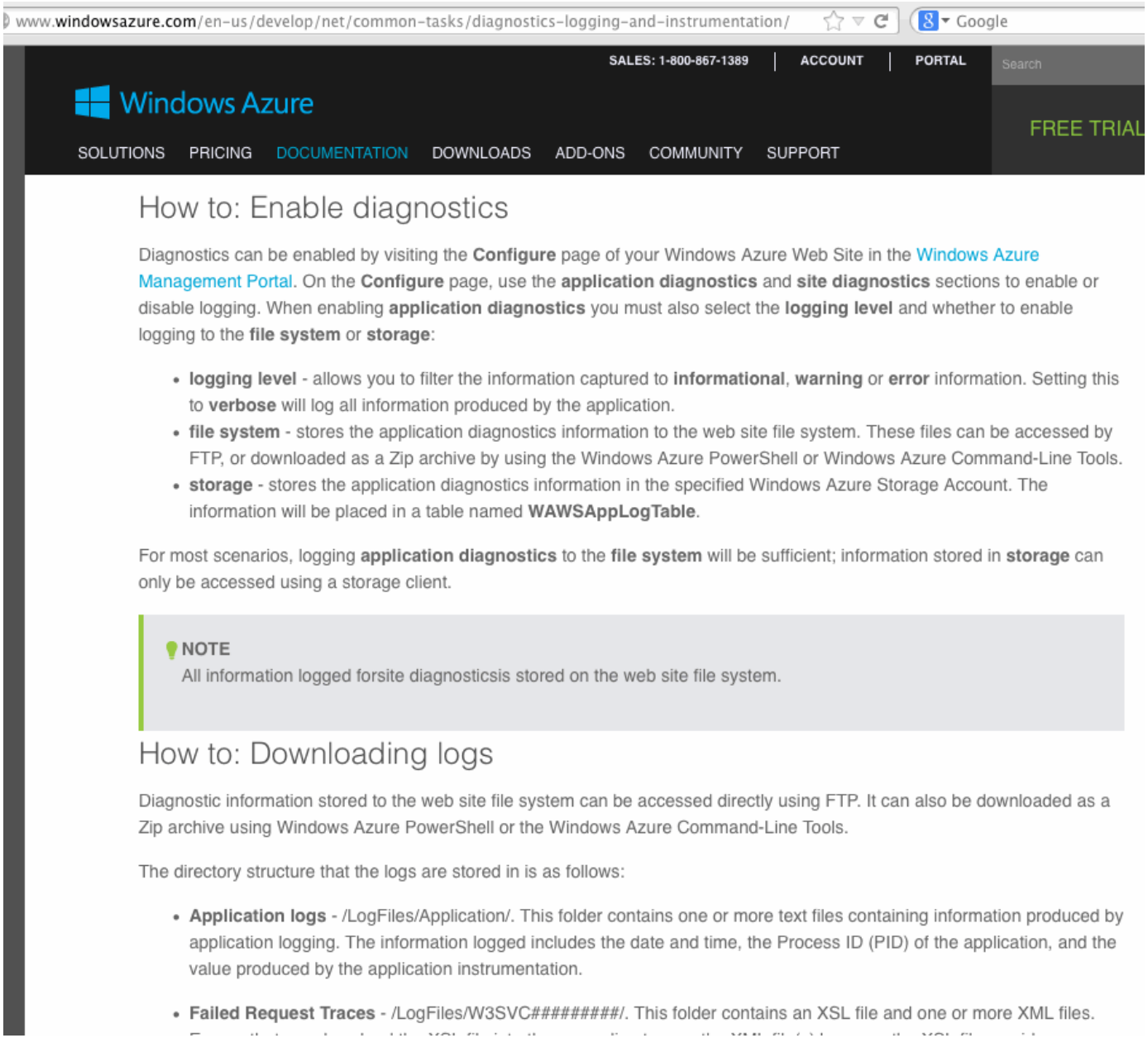


Is Disclosing More Information About Users A Good Thing, or A Bad Thing?

- If a legitimate service is relying on an OpenID for authentication, having more information about a user helps them to potentially identify and manage problematic users.
- On the other hand, if I'm a bad site attempting to leverage OpenID to mine information about users, the more information that gets shared with them, the bigger the potential risk to user privacy.
- Presumably privacy-aware users would prefer to use whatever OpenID identity provider releases the LEAST information about me (while still being acceptable to the services I use), but most users just don't seem to know/care.
- One more point: virtually all of these user attributes are "self-asserted"/"user-supplied" – should you even bother paying attention to them anyway? What if users simply choose to lie?

Using The Cloud -- Losing Your Logs?

- One of the really useful things you get when you run services locally is log files. You get to see how your service is used, and how people attempt to abuse it. Hopefully you're doing that logging to a central log server.
- In some cases, when you move to the cloud, you may lose access to those sort of log files, and that can really hurt when it comes to your situational awareness. A major attack may be going on, and you might not ever know (until it is potentially too late).
- In other cases, logs are available for web-based review, but not for centralized sysloging.
- Sometimes logs are available, but only if you specifically ask for them to be made available...


www.windowsazure.com/en-us/develop/net/common-tasks/diagnostics-logging-and-instrumentation/
Google
SALES: 1-800-867-1389
ACCOUNT
PORTAL
Search
Windows Azure
FREE TRIAL
SOLUTIONS
PRICING
DOCUMENTATION
DOWNLOADS
ADD-ONS
COMMUNITY
SUPPORT
How to: Enable diagnostics
Diagnostics can be enabled by visiting the Configure page of your Windows Azure Web Site in the Windows Azure Management Portal. On the Configure page, use the application diagnostics and site diagnostics sections to enable or disable logging. When enabling application diagnostics you must also select the logging level and whether to enable logging to the file system or storage:
logging level - allows you to filter the information captured to informational, warning or error information. Setting this to verbose will log all information produced by the application.
file system - stores the application diagnostics information to the web site file system. These files can be accessed by FTP, or downloaded as a Zip archive by using the Windows Azure PowerShell or Windows Azure Command-Line Tools.
storage - stores the application diagnostics information in the specified Windows Azure Storage Account. The information will be placed in a table named WAWSAppLogTable.
For most scenarios, logging application diagnostics to the file system will be sufficient; information stored in storage can only be accessed using a storage client.
NOTE
All information logged forsite diagnosticsis stored on the web site file system.
How to: Downloading logs
Diagnostic information stored to the web site file system can be accessed directly using FTP. It can also be downloaded as a Zip archive using Windows Azure PowerShell or the Windows Azure Command-Line Tools.
The directory structure that the logs are stored in is as follows:
Application logs - /LogFiles/Application/. This folder contains one or more text files containing information produced by application logging. The information logged includes the date and time, the Process ID (PID) of the application, and the value produced by the application instrumentation.
Failed Request Traces - /LogFiles/W3SVC########/. This folder contains an XSL file and one or more XML files.

End User Support and the Cloud

- You are probably used to locally support users of local applications. One of the trickiest things to get used to is recognizing that in the cloud, support may be a fully (or at least partially) delegated responsibility.
- If a user has a problem, you may not be able to answer their question. You may need to refer the user to a cloud provider's support infrastructure, and that support may be outsourced to a third party in the third world.
- Your users may or may not get good support as a result, and in some cases that may negatively impact the security of the work they do.
- You will also need to learn to live with not being able to have direct access to a ticketing system operated by the cloud provider...

VIII. Stepping Back For a Second... What's The Basic Question Again?

Oh Yeah... "Should We Go Ahead With Cloud Provider Foo, Or Not?"

And How Do We Decide?

"Should We Go Ahead With Cloud Provider Foo Or Not?" -- Simple Question, Right?

- Only two basic answers, after all, "Yes," or "No."

- Presumably you make comparable go/no-go decisions for non-cloud-related technologies all the time:
  -- Is the campus data center secure enough?
  -- What operating systems should we recommend (or ban)?
  -- How can we mitigate the risks arising from malware?
  -- Is our learning management system FERPA-compliant?
  -- Do we need a new policy to deal with unencrypted data on desktops or laptops?

- For stuff <u>not</u> in the cloud, you have myriad sources of local data to help you reach a decision...

Investigating Local Security Concerns

- For stuff that's NOT in the cloud, it's easy to locally find out what's going on:

  -- Look at your logs
  -- Check your passive monitoring infrastructure
  -- Actively scan the relevant systems
  -- Reach out via phone/email/IM
  -- Have meetings with coworkers and users
  -- Consult the campus IT ticketing system
  -- Walk over and pick up a compromised system for forensic review
  -- Talk to local developers
  -- Discuss issues with university counsel or internal audit

- This is the sort of stuff you're used to doing every day.

Security Concerns In The Cloud

- It's a little trickier when stuff's "in the cloud:"
  - You don't run the gear.
  - You don't hire the staff (often you don't even know who the staff are!)
  - You (often) can't scan the cloud installation.
  - You don't monitor the internal cloud provider network.
  - You (normally) don't get to set the cloud provider's policies.
  - Terms and conditions may be a take-it-or-leave-it matter.
  - etc., etc., etc.

That Said, 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. There are no special new physical security requirements which suddenly appear simply because a facility is supporting "cloud computing"

Physical Security at an Oregon Cloud Provider

Cloud As A "Tycho Magnetic Anomaly"

- The cloud may normally be represented by a fluffy white blob, but the cloud's is actually more like a "black box." You end up needing to figure out what's happening inside of it without being able to open it up or even touch it.
- Remember Arthur Clarke's *Space Odyssey* books? If not, see http://en.wikipedia.org/wiki/Monolith_%28Space_Odyssey%29
- **Think of a cloud provider as being just like one of Clarke's black monoliths: even though it may have some sort of mysterious force field that keeps you from directly touching it, you still have to decide what it means, if it's safe to have around, and what (if anything) you need to do about it.**
- When you get right down to it, the primary way you're going to do that is by **asking questions.**

Asking Q's About Cloud Provider Security

- But do you actually want to directly ask questions of the cloud provider? Or are you willing to just "take the cloud provider's word for what they're doing," perhaps by just reviewing documentation they've already written?
- If you do want to ask questions of the providers, do you want to ask a bunch of questions that you yourself personally dreamed up, perhaps uniquely well tailored to probe unique security aspects of that particular provider?
- Or would you prefer that a qualified auditor/external assessor asked questions, and you just got to see an audit report? (Would you be willing to sign an NDA to get it?)
- Or do you want to ask questions of others who currently use that cloud-based service? (But what if it's a brand new service, and you are one of the first users of it?)

Taking the Provider's Word For It....

- If you're tempted to try this route, you might hear...

- "Check out their security website. It's all there, and they won't tell us anything beyond what's on it anyhow, so I guess we'll just have to take their word for it."
- "Millions of other users trust these guys, so it's probably safe for us to do so too, right? They're really big, and they seem really smart, so surely they wouldn't screw up anything important about their security, would they?"
- "They're much cheaper (or "free!"), so it's worth taking a chance on them -- heck we couldn't afford to do [insert service name] ourselves if we couldn't get it from them..."
- "Legal okayed it. Don't second guess the attorneys. If something goes go wrong, they'll sue them for us."

Asking Your Own Set of Questions...

- If you try this route, hypothetically you might hear...

- "We'll schedule a conference call, and you can ask any security questions you might have then."
- "[on the call] Let's just start with your half dozen biggest questions. We don't want to get hung up over 'hundreds' of 'techy' security questions..."
- "[next call] What? You've got still more questions? I thought we took care of all those during the last fifteen minutes of the last call... it isn't fair to just keep coming up with new security question after question..."
- "[by email] Look. We've got thousands of customers. We can't answer long lists of unique security questions for each customer... We'd have to charge 100X what we do..."

"We'll Review Their Audit Reports"

- What exactly will you be looking for? **What would be a "deal breaker,"** if you saw it in an audit report?
- Some new providers may NOT have been audited at all. Getting audited "just for you" may be expensive, and not something they're interested in doing. What then?
- Not all audit reports are the same, so which one(s) do you want? For example, assume your choice is SOC-1, SOC-2, or SOC-3? (FWIW, AWS offers all three SOC reports, see https://aws.amazon.com/compliance/#third-party)
- Providers may be reluctant to share a non-redacted audit report with you (although a major potential customer who is willing to sign an NDA to get access to an audit report may have better luck than a smaller-scale customer who is not willing to sign an NDA)
- How often will any audit need to be repeated?

"Checking References"

- Asking others who may be using the cloud service may give you some insights into what they've seen, but...
- Your site and the reference site(s) may not have the same infrastructure, or the same planned usage, or the same tolerance for risk, etc.
- Pesky NDA terms may limit a colleague's ability to candidly share what they've learned (at least "on the record"/for attribution)
- Just like talking to references for a new potential employee, you usually end up getting referred to those who have positive opinions (for some reason)
- Oral reports are not very comparable, if you're trying to evaluate multiple potential options side-by-side.

IX. "I Highly Support Standards. That's Why We All Use Our Own."

Using a Standardized Security Framework

- Another option: If we want to do a systematic review of cloud provider security, maybe it would make sense to use some sort of **standardized security framework?**
- If we all agree to use the **same one**, a provider would only need to complete one framework, and because the framework would be standardized, we could:
  -- Be comfortable that we haven't overlooked anything
  -- Easily compare the responses from provider A with the responses from provider B
  -- Not have to wait while a provider answers a newly written set of security questions
- If we all agreed to use the same security framework, providers could just complete that one, confident that it would handle the lion's share of the questions from users.

Whose Security Framework Should We Use?

- Cloud security frameworks have been developed by many agencies/organizations, including:

  -- Cloud Security Alliance

  -- ENISA

  -- GSA

  -- ISO

  -- Jericho Forum

  -- NIST

Which Security Framework Should We Use?

- Even if we pick a particular organization, such as the Cloud Security Alliance, they may still have multiple security frameworks available. For example, CSA has the Consensus Assessments Initiative Questionnaire (CAIQ) as well as the Cloud Controls Matrix (CCM).

- Even if we pick the CSA CCM, there may be multiple versions of it in circulation:

  -- CSA CCM v1.4
  https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v1.4.xlsx
  -- CSA CCM v3.0
  https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

The "Goldilocks Problem"

- Just like Goldilocks and the Three Bears, some cloud security frameworks may be too simple, other cloud security frameworks may be too complex.

- The trick is finding one that's "just right."

- What about FedRAMP? It may be an example of a framework that's TOO tough, with just ten FedRAMP-certified cloud services to-date.

Just 10 FedRAMP-Certified Services

CSA STAR Registry

- On the other hand, there are 37 companies listed on the CSA STAR (Security, Trust & Assurance Registry) list, see: https://cloudsecurityalliance.org/star/#_registry
- Listing on the STAR registry is based on completion of a relatively simple self-assessment, the CSA CAIQ (pronounced "CAKE"). Many of these items may end up being responded to with just a "Yes" or "No" response (you can review CAIQ self-assessments for providers of interest on the web site).
- If a provider makes just a *pro forma* yes/no response to each item, in my opinion, that's really not very helpful. It's *too* much of just a "checklist" approach.
- We need something in between FedRAMP (too much), and CSA STAR (too little). Fortunately, there's the CSA CCM.

CSA Cloud Controls Matrix

- The CSA Cloud Controls Matrix (CSA CCM) is the security framework that I've previously suggested Internet2 use with its NET+ providers.
- Sometimes folks wonder how the CSA CAIQ and the CSA CCM relate... While the CSA CAIQ aligns with what the CSA CCM also covers, the CAIQ is basically a checklist while the CCM provides an outline for preparation of a narrative whitepaper covering relevant security topics in depth
- The CSA CCM approach also avoid any problems that may be associated with completing a checklist but NOT FIXING any issues that may be exposed as a result. If you complete a CSA CCM-based whitepaper talking about your approach to security, it becomes quite difficult to gloss over/ignore areas where deficiencies may exist.

CSA CCM 1.4 vs. CSA CCM 3.0

- The version of the CSA CCM that I originally recommended, v1.4, had just under a hundred questions. Candidly, one of the reasons I liked it was that it was relatively brief (you might not think I like succinct paperwork given the length of my talks, but really, I do)
- Community-wide experience with the 1.4 version of the CSA CCM lead to the realization that it didn't cover everything. Thus, the most recent version of the CSA CCM, v3.0, released in late September, now has 136 items, obviously a significant expansion.
- Internet2 is currently considering whether it wants to move to CSA CCM v3.0 (my recommendation would be that we do so). In fact, my recommendation would be that we routinely roll to new versions of the CSA CCM, as they may be released.

What Controls ("Rows") are in CSA CCM?

- To see, download a copy at https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx

- Its 136 rows ("controls") are grouped into 16 topical areas:
  1) Application & Interface Security
  2) Audit Assurance & Compliance
  3) Business Continuity Management & Operational Resilience
  4) Change Control & Configuration Management
  5) Data Security & Information Lifecycle Management
  6) Datacenter Security
  7) Encryption & Key Management

  [continued on the next slide]

What Controls ("Rows") are in CSA CCM? (2)

- 8) Governance and Risk Management
  9) Human Resources
  10) Identity & Access Management
  11) Infrastructure & Virtualization Security
  12) Interoperability & Portability
  13) Mobile Security
  14) Security Incident Management, E-Discovery & Cloud Forensics
  15) Supply Chain Management, Transparency and Accountability
  16) Threat and Vulnerability Management

- Many of the items in each of these areas are pretty basic "common sense" items.

Items From One of Those 16 Areas: Threat and Vulnerability Management

- **TVM-01, Anti-Virus / Malicious Software:**

  Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

Items From One of Those 16 Areas: Threat and Vulnerability Management (2)

- **TVM-02, Vulnerability/Patch Management:**
  Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed (physical and virtual) applications and infrastructure network and system components, applying a risk-based model for prioritizing remediation through change-controlled, vender-supplied patches, configuration changes, or secure software development for the organization's own software. Upon request, provider shall inform customer (tenant) of policies and procedures, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

Items From One of Those 16 Areas: Threat and Vulnerability Management (3)

- **TVM-03, Mobile Code:**

  Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

The Columns In the CSA CCM

- When you look at the CSA CCM and scroll across, you'll see that there are also multiple columns in the spreadsheet:
  -- A: Major control area and control name (e.g., "Threat and Vulnerability Management: Mobile Code")
  -- B: Control ID number (e.g., TVM-03)
  -- C: Control specification (narrative text of the control)
  -- D-I: Architectural Relevance (compute? storage? net?)
  -- J: Corp Governance Relevance?
  -- K-M: Cloud Service Delivery Model Applicability (Software as a Service? Platform as a Service? Infrastructure as a Service?)
  -- N-O: Supplier Relationship (Service Provider? Tenant/Consumer?)
  [continued]

The Columns In the CSA CCM (2)

- -- P: AICPA TS Map
  -- Q: AICPA Trust Service Criterial SOC 2SM Report)
  -- R: BITS Shared Assessments AUP v5.0
  -- S: BITS Shared Assessments SIG v6.0
  -- T: BSI Germany
  -- U: CCM V1.X
  -- V: COBIT 4.1
  -- W: CSA Enterprise Architecture/Trust Cloud Initiative
  -- X: CSA Guidance v3.0
  -- Y: ENISA IAF
  -- Z: FedRAMP Security Controls, Low Impact Level
  -- AA: FedRAMP Security Controls, Moderate Impact Level
  [continued]

The Columns In the CSA CCM (3)

- -- AB: GAAP
  -- AC: HIPAA/HITECH Act
  -- AD: ISO/IEC 27001
  -- AE: Jericho Forum
  -- AF: NERC CIP
  -- AG: NIST SP800-53 R3
  -- AH: NZISM
  -- AI: PCI DSS v2.0

- The columns from P-AI are particularly helpful because they allow you to see how the controls present in the CSA CCM map to the requirements of most of the other popular security frameworks you might encounter.

The CSA CCM Does Not Highlight Controls OTHER Frameworks Require That Are Missing

- If you were to take SP 800-53 R3, and build a new spreadsheet where each row was one control required by SP 800-53, you could then check to see which of those controls are (or aren't) covered by the CSA CCM.
- You CAN'T get that information from the current CSA CCM spreadsheet because the ONLY controls listed in the CSA CCM are the ones that the CSA CCM ALREADY HAS.
- That is, the CSA CCM lets us answer the question, "Is what the CSA CCM requires consistent with what other security frameworks require?" (And the answer would be largely "yes")
- It does NOT help us answer the OTHER (perhaps more interesting) question, "Are there things the other frameworks require that are missing from the CSA CCM?"

Are There Things That Are Missing From Even v3.0 of the CSA CCM?

- Sure. What's missing depends on what you care about/ where you're coming from.
- For example, when I first recommended that Internet2 use the CSA CCM, Bob Brammer was very concerned that the CSA CCM might not include everything that higher education cared about. For example, the CSA CCM has no controls specifically focused on FERPA-related issues (probably because FERPA's not a big deal for most folks outside of higher education). I'm also not seeing anything about SAAS accessibility (e.g., for blind or deaf users).
- Does this mean that the CSA CCM is a failure, or can't be used by higher ed? No, it's just an example of an area where supplemental compliance items may be required to cover areas of specific interest to our sector.

What's A "Passing Score" on the CSA CCM?

- For example, does a site need to have all controls perfectly addressed? 90% of them? A majority of them in some form or another? What if they're all just TBD/in progress?
- There's no right or wrong answer to any item, and many different approaches could work. A stronger response to one item might offset a weaker response to another.
- Sometimes, just seeing HOW a company responds to a CSA CCM item can be very instructive -- do they take the process seriously? Do they just try to get it out of the way as quickly as they can, treating it as if it were a checklist? Do they have answers that appear to be internally inconsistent?
- Higher ed understands grading essay exams, theses, and disserations. :-)

Every Site's Needs May Be Different

- Another reason why we don't want to have a "passing score" on the CSA CCM is that even if we agree on the set of questions we're going to ask, what's an acceptable answer to those questions may vary from site-to-site.
- For example, site A may be interested in offering an easy-to-use free application for student recreational use, and they may have minimal security concerns as a result.
- Site B, on the other hand, might want to deploy a mission-critical application for use in their medical facility, triggering significant worries about availability, data privacy, compliance, etc.
- Different sites, different requirements, different thresholds for what's acceptable.
- One uniform passing score wouldn't work for everyone.

The Goal: Give YOU The Data You Need

- Because every site's different, the goal is to give you at least most of the data you need to make an informed decision, without making you pry it out of the cloud provider yourself.
- Ideally, the data should even be publicly available so you don't even need to screw around requesting it, you should just be able to click on the data you need in a public repository. (If a provider's reluctant to publicly share their CSA CCM results, that might be something worth exploring, too).
- If something doesn't look right to you, you can follow up with the cloud provider directly, digging in on the issue of concern to you. Maybe the issue is just a matter of a misunderstanding, and something that can be easily rectified.

CSA CCM and "Recursive Cloud Providers"

- We also quickly came to realize as we worked with the CSA CCM that some parts of it are not applicable to (or even easily answered by!) a cloud application vendor that is hosting their cloud app on cloud infrastructure.
- For example, when it comes to the "Data Center Security" section of the CSA CCM, a typical cloud application vendor may have no idea how to respond to those items, because they don't run the data center they're using, some other cloud provider does.
- They may still be RESPONSIBLE for how that data center works, but they may need to rely on what they're told by their cloud infrastructure provider, but now we're getting recursive, and infrastructure providers may not be willing to "open the kimono" for non-customer review.

Giant Clouds and Teeny-Tiny Clouds

- Another rapid discovery: some cloud providers are giants, with huge staffs (including entire (LARGE!) teams focused on security and compliance and privacy).
- Other cloud providers, particularly entrepreneurial cloud app vendors, might be tiny. If their total staff amounted to half a dozen people, it was unlikely that one of them would be devoted entirely to security/compliance/privacy.
- This difference in security "maturity" impacts the security processes the vendor may have, and the amount of help they may need when it comes to completing a framework like the CSA CCM.
- It also shows up in things like "division of responsibility" requirements: tiny entrepreneurial cloud providers may not have enough staff to divide up roles and responsibilities the way large firms do.

Note: You May Have Limited Luck Seeking Major Changes From a Huge Cloud Provider

- Cloud providers are all about offering standardized services at scale.
- As such, they may not be willing (or even able) to consider modifying their service (or their practices/procedures) to meet your preferences/needs.
- If they did make changes to meet your needs, they might find those changes aren't welcomed by an equal number (or more!) existing customers, customers who liked how the provider traditionally did things. Therefore, you may need to live with "off the rack" rather than custom tailored outfits.
- Small entrepreneurial cloud providers, on the other hand may be much more potentially flexible.

Couldn't a Provider Just Lie When Doing Their CSA CCM Writeup?

- That's always a possibility, but if they've provider a written statement describing what they're doing, and that statement subsequently proves to be factually inaccurate or intentionally misleading, you likely have a good basis for talking with legal counsel if things go awry.

- I discuss this and more in a draft two page document "Using the CSA CCM with Net+" document you can retrieve from:

  http://pages.uoregon.edu/joe/using-the-ccm-with-net+.docx

- If you're really worried, you can always ask for audits (but if you really don't trust them, well...)

X. Wrap Up

Thanks For the Chance to Talk Today

Are there any questions?

If you'd like a copy of these slides, they're available online at

http://pages.uoregon.edu/joe/nwacc-security-2013/