Cloud Security – An Overview

OWASP

Presented by,
Ezhil Arasan Babaraj
Ezhilarasan.babaraj@csscorp.com
CSS Corp Labs
CSS Corp Pvt Ltd.

The OWASP Foundation
http://www.owasp.org

Acknowledgement

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

What is Cloud computing?

Cloud Computing Is Many Different Things to Many Different People

Some Generally Accepted Characteristics

- Most people would agree that true cloud computing is
  - 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
  - cloud computing leverages economies of scale

Cloud Computing Building Blocks

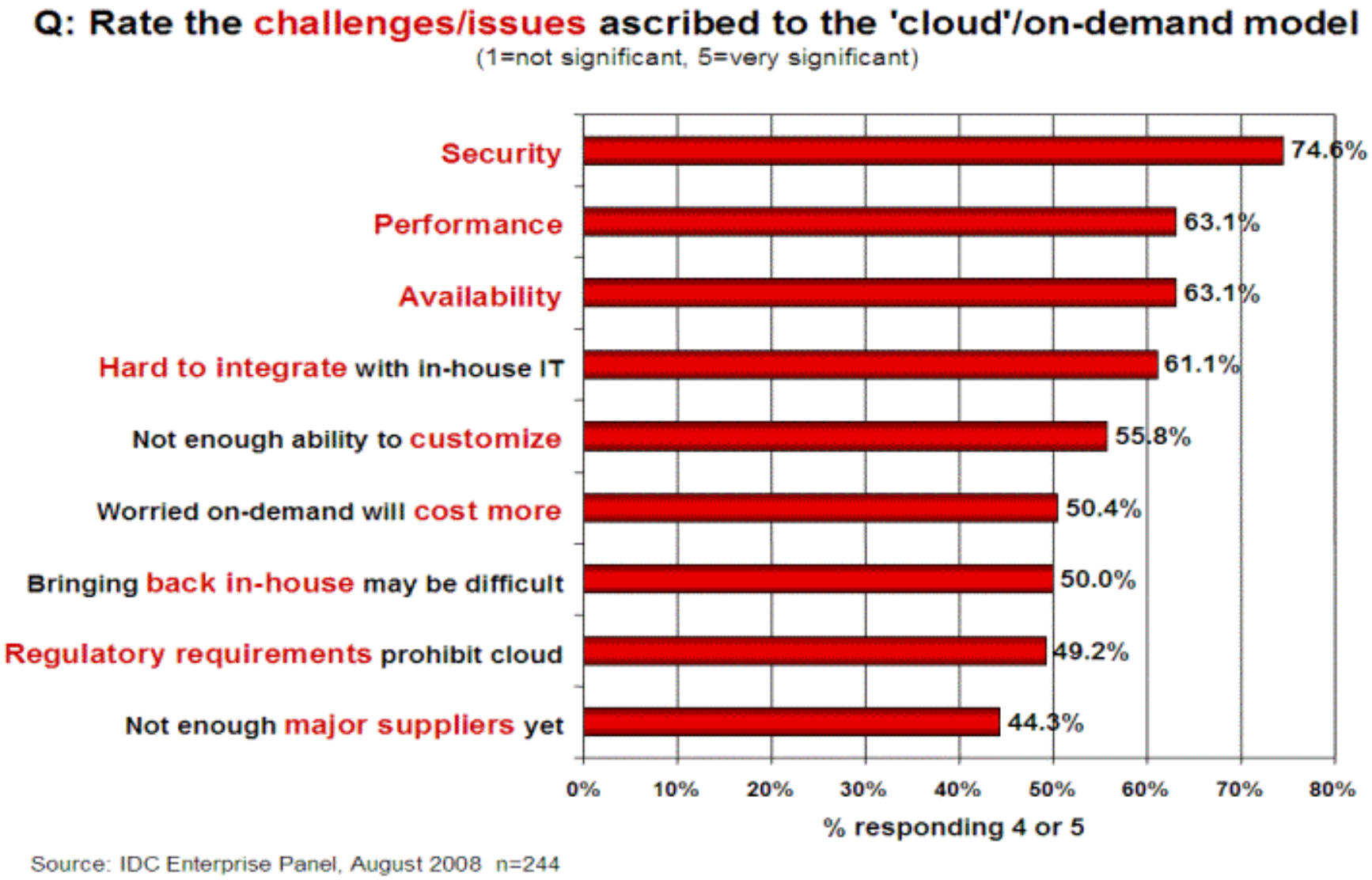
- IaaS
- PaaS
- SaaS

What's Driving Cloud Computing?

- Thought leaders
  - Amazon, Google, Microsoft and many
- The economy
  - Capex Vs Opex
- The Feds
  - Govt, Enterprise, Innovators (startups)

Cloud computing Challenges

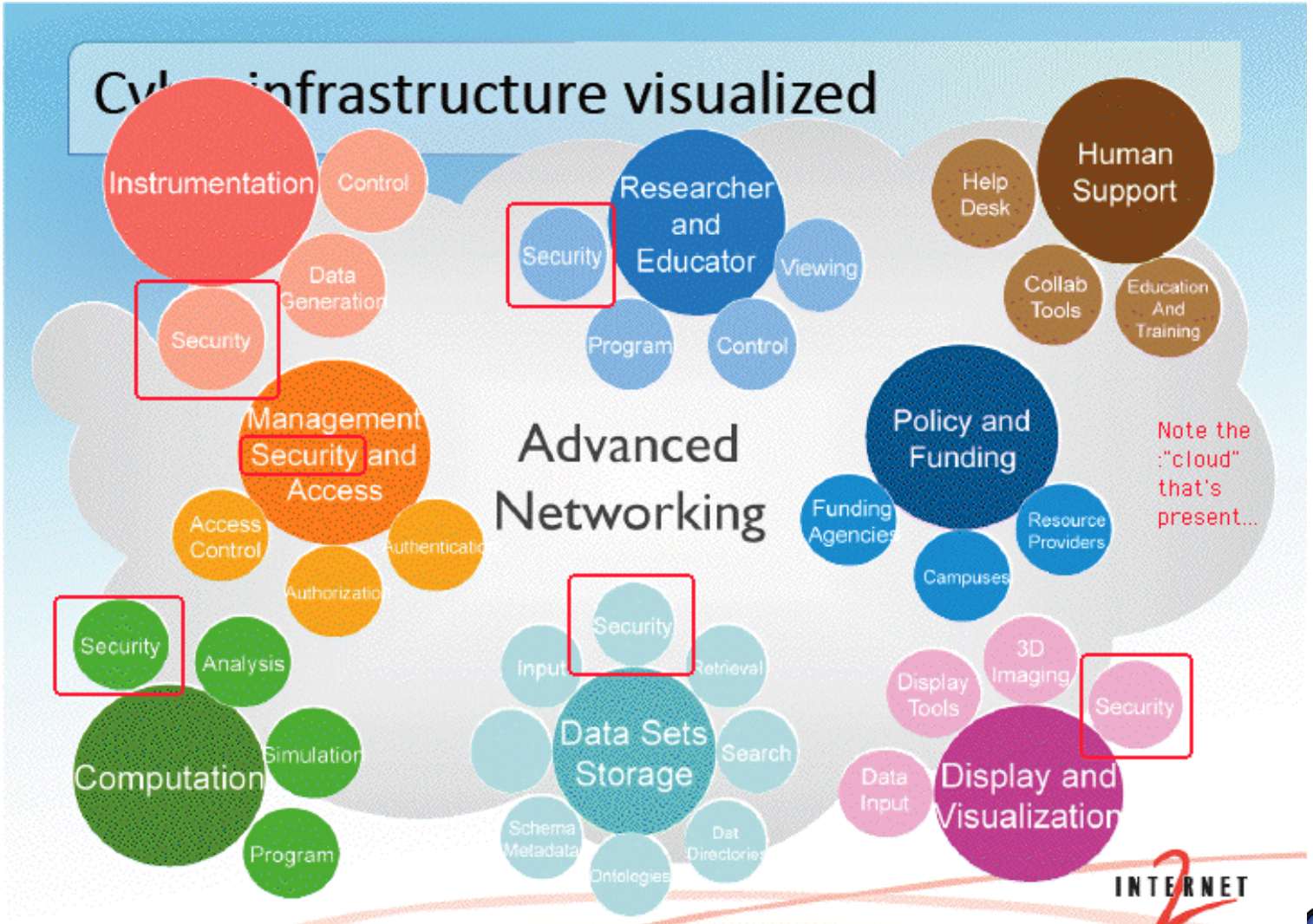
Cloud Computing Challenges



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

"Cyber infrastructure Visualized"

A Cloud, With Lots of "Security" References



What is Cloud computing Security?

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

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

- Contracting for Cloud Services
- Compliance, Auditing and eDiscovery

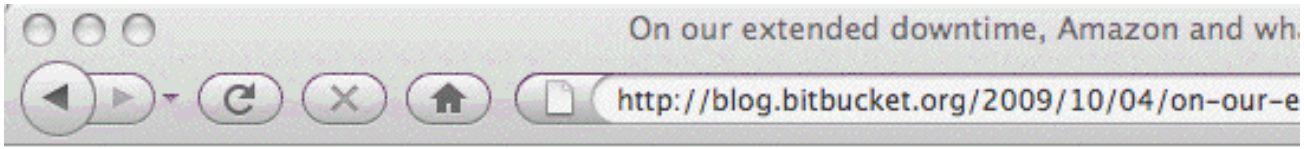
So what are some cloud-related security issues?

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 Key Issue**

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 [illegible] 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

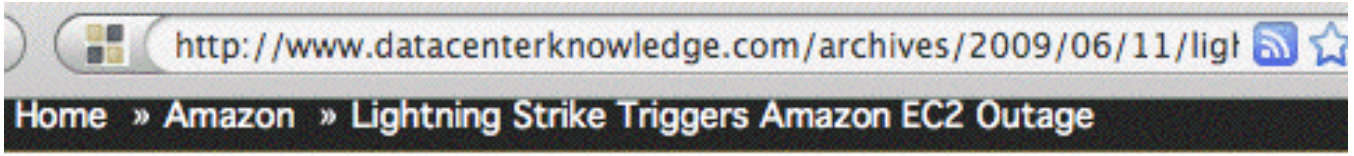
BREAKING

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.

Other Security Related Issues

- Firewalls
- IDS/IPS
- Virtualization Security
  - Noisy tenant, Instance Spoofing, Network & I/O Blocking
  - Gaining Access to Local Storage
- Network Spoofing

Issues with the 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.

Issues with Cloud Provider Location

- Location of the Cloud with respect to storage & computing
  - Due to competition of Cloud Pricing, they always look for low cost data centers
  - 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 someplace overseas.
- 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?

Other Issues

- What If your cloud provider has careless or untrustworthy system administrators, the integrity/privacy of your data's at risk
- willingness to disclose its security practices ?
- Is your Cloud Provider Financially stable?
- Some security Incident at your corporate . How will you find the root cause?
- What if your system ends up being the origin of an attack?

Mitigating the Risk Involved in Cloud Computing

Mitigating Cloud Computing Availability

- Multi Cloud Strategy
- Single Cloud Provider with Multiple Region Cloud
- Hybrid Cloud Strategy

- Finally be cautious, 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 (Data Availability)

- Off site backup
- Backup to an another Cloud or Region

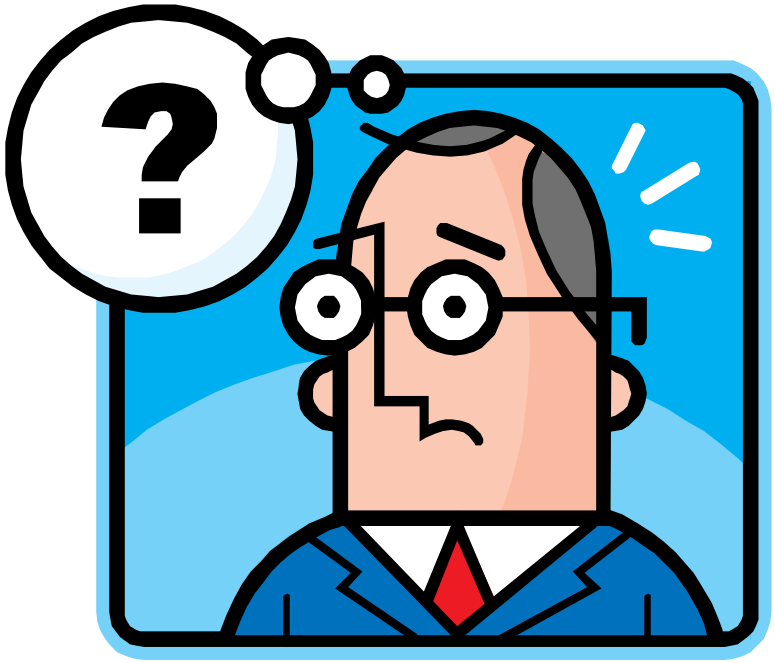
Understand the Employee Risk

- How can you tell if your cloud provider has careful and trustworthy employees? 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?

Mitigating Transparency related issues

- Your provider should not treat the security practices as a confidential or business proprietary thing
- Remember: "Trust, but verify." [A proverb frequently quoted by President Reagan during arms control negotiations]
- Be like Amazon & Microsoft

Q & A



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