• "Copyright Eric Weakland and Randy Marchany 2010. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author."
Cloud Computing: Clear Skies or Rain?

Randy Marchany, VA Tech IT Security, marchany@vt.edu
Eric Weakland, AU Information Security, eric@american.edu
60 Minutes: Lots to do!

- Review- What is Cloud?
- How do I help my Organization evaluate cloud options, leverage the benefits without undue risk?
- Examples:
  - AU Student Email to Gmail
  - VT Alumni Mail to Gmail
- Forecast
- Examples For Discussion
The journey to the cloud is inevitable and we’re going to have to secure it... **Cloud infrastructures will catapult us forward because they force enterprises to focus on their security policies and processes – and not just on security technology**....In short... the cloud will turn the way we deliver security inside out....Cloud computing will indeed complete the transformation of IT infrastructures unleashed by the Internet. As security practitioners, we must lead, not follow. -- Art Coviello, RSA President

Why are we talking about this?

- October 2009 - Randy’s talk at VASCAN
- Drinks at Guapos
- Shared dissatisfaction with:
  - Clear definitions of what Cloud computing meant to vendors/consumers/security practitioners
- Difference of opinion on:
  - Geographic fault tolerance/availability
  - Are cloud providers “Secure” enough (CIA)
  - “We’ve been providing cloud all along”
- Hey – we should give a talk!
The Definition is evolving

– Cloud computing is still an evolving paradigm. Its definitions, use cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time.

  — The NIST Definition of Cloud Computing
  • Authors: Peter Mell and Tim Grance
  • Version 15, 10-7-09

– The Network is the Computer (Sun Microsystems, 1997)
Definition of Cloud

• NIST defines cloud computing by:
  – 5 essential characteristics
  – 3 cloud service models
  – 4 cloud deployment models
Essential Characteristics

- **On-demand service**
  - Get computing capabilities as needed automatically
- **Broad Network Access**
  - Services available over the net using desktop, laptop, PDA, mobile phone
- **Resource pooling**
  - Provider resources pooled to server multiple clients
- **Rapid Elasticity**
  - Ability to quickly scale in/out service
- **Measured service**
  - control, optimize services based on metering
Service Models

• Software as a Service (SaaS)
  – Provider supplies the apps, os and a place to run them all
  – Salesforce.com, Google Apps, Microsoft Online Services

• Platform as a Service (PaaS)
  – Provider brings the toolkit and the server, Customer takes care of the apps
  – Google App Engine, Azure Services Platform, Force.com

• Infrastructure as a Service (IaaS)
  – Provider is responsible for the infrastructure, Customer for everything else
  – Amazon’s EC2, Rackspace Cloud, and GoGrid

• “The key takeaway for security architecture is that the lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.”
  – Security Guidance For Critical Areas of Focus In Cloud Computing V2.1, p19
Deployment Models

- **Public**
  - Cloud infrastructure is available to the general public, owned by org selling cloud services

- **Private**
  - Cloud infrastructure for single org only, may be managed by the org or a 3rd party, on or off premise

- **Community**
  - Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rd party

- **Hybrid**
  - Combo of >=2 clouds bound by standard or proprietary technology
Cloud Security Alliance has great guidance on considering moving a service to the cloud

• Clear guidance on the potential pitfalls
• Step by step way to evaluate if you want to move the asset to the could, what type of cloud offering would best suit the asset
• What domains need to be considered when reviewing your service contract
• Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
What, When, How to Move to the Cloud

• Identify the asset(s) for cloud deployment
  – Data
  – Applications/Functions/Process

• Evaluate the asset
  – Determine how important the data or function is to the org
Evaluate the Asset

• How would we be harmed if
  – The asset became widely public & widely distributed?
  – An employee of our cloud provider accessed the asset?
  – The process of function were manipulated by an outsider?
  – The process or function failed to provide expected results?
  – The info/data was unexpectedly changed?
  – The asset were unavailable for a period of time?
Map Asset to Models

• 4 Cloud Models
  – Public
  – Private, internal, on premise
  – Private, external
  – Community
    • Hybrid

• Which cloud model addresses your security concerns?
Map Data Flow

• Map the data flow between your organization, cloud service, customers, other nodes
• Essential to understand whether & HOW data can move in/out of the cloud
  – Sketch it for each of the models
  – Know your risk tolerance!
Cloud Domains

• Service contracts should address these 13 domains
• Architectural Framework
• Governance, Enterprise Risk Mgt
• Legal, e-Discovery
• Compliance & Audit
• Information Lifecycle Mgt
• Portability & Interoperability
Cloud Domains

- Security, Business Continuity, Disaster Recovery
- Data Center Operations
- Incident Response Issues
- Application Security
- Encryption & Key Mgt
- Identity & Access Mgt
- Virtualization
Virgina Tech Google Apps

- [http://start.google.vt.edu/](http://start.google.vt.edu/)
- Goal: remove 62k alumni email accounts from core email system
- Goal: allow alumni to keep their same email address and aliases
  - name@vt.edu
- Opt in or lose it
- Not comfortable with moving active University members to gmail
Welcome to the Virginia Tech Google service.

Select service below:

- **Mail** - Check your VT Google E-mail
- **Docs** - Make Spreadsheets, Presentations, Documents
- **Calendar** - Your VT Google Personal Calendar
- **Sites** - Make your own VT Google Web Page
- **Contacts** - Manage your VT Google Addressbook

New to the VT Google Service? See our help for an introduction.
Don't have your VT Google Service account yet? Click here to get started.

You may add personal gadgets to your start page in the area below.
Welcome to Virginia Tech

Two ways to access this site at Virginia Tech

1. Use your Virginia Tech account and password
2. Sign in with a different account
   If you don’t have a Virginia Tech account, no problem.
   • You may be able to sign in with an account outside Virginia Tech.
   • You can create a Google Account.

Welcome to American University

Sign in to your account at American University

Username: @student.american.edu
Password: 
[Stay signed in] [Sign in]
Can't access your account?

Less spam, plenty of space and access from anywhere.

Welcome to your email for American University, powered by Google, where email is more intuitive, efficient and useful.

- Keep unwanted messages out of your inbox with Google's powerful spam blocking technology
- Keep any message you might need down the road, and then find it fast with Google search
- Send mail, read new messages and search your archives instantly from your phone

New! One-stop information sharing with Google Sites
Building a site is as simple as editing a document, and you don't need anyone's help to get started.
Check out these example sites: Company intranet, Team project, Employee profiles, Classroom

©2010 Google Privacy Policy - Terms of Service
AU student Gmail – May 2008

- AU offered 11000+ student email accounts previously with Lotus notes
- Goal was to move students to Google, retire servers, work
- Gmail was free! (more about this later)
- A large portion of our students were already forwarding to Gmail
- Working group of 12+ people – admins, programmers, customer service, contracts
- Google ID separate from your AU user id
  - <userid>@student.american.edu
  - Solve account lifecycle later
- Opt out available
- Success!
Shared Outcomes

• There were some things that we didn’t like, that we knew about
  – Lack of management visibility (no reports on usage etc.)
  – Broken AU account lifecycle (why delete the accounts, they’re FREE, right??)
  – Lack of leverage

• Some that we didn’t anticipate
  – Who said they could create team sites?
  – Calendaring compatibility issues
  – New services just popped up:
    • Tripit Manymoon Offisync Aviary
  – Several (brief) outages, security vulnerabilities
Unknown Unknowns

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

Donald Rumsfeld
Forecast for the future

• Definitions/Technology changing so fast
  – New Vulnerabilities
    – Abusing WCF to Perform Remote Port Scans
    – Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds
  – Legal questions
    • Multi-tenancy, 3rd party possession
    • 3rd Party subpoena
      – No requirement to notify.
  – Recoverability – how do I get my data back/make sure it is destroyed
  – Availability (are they really cloud, or are they in one datacenter?)
  – Visibility
  – Leverage – “Nailing jello to the wall.”

• Things that don’t belong in the cloud
  – PII/Core data not currently a good target
There are great/innovative things we can do!

- Cloud isn’t appropriate for everything, but it doesn’t mean you shouldn’t do it at all
- Be VERY concerned if you hear “We’ve got to get into the cloud”
  – Clouds aren’t free
- Find Assets/Services where the benefits of moving to the cloud far outweigh the risks
People are working on the problem!

- Cloud Security Alliance
  - Top Threats to Cloud Computing
  - CSA Cloud Controls Matrix
    - Coming soon!
  - Jericho forum commandments
Interesting Cloud Applications

- Potential move of staff Gmail
  - discoverable archive one strong driver
- “Cloud Raid” solution
  - http://www.tegile.com
  - No more Iron Mountain
- Distributed Web application firewall
  - http://www.artofdefence.com/
- Log management in the cloud
  - http://www.loggly.com
  - Central Syslog in the cloud
- Private Cloud for disaster recovery
  - One edu as the cloud for another
Credits

• Virginia Tech IT Security
  – http://security.vt.edu

• AU Information Security
  – http://www.american.edu/oit/security/index.cfm

• Flying Instruments-Only: Legal and Privacy Issues in Cloud Computing

• Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds
  – http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf

• Abusing WCF to Perform Remote Port Scans
  – http://www.gdssecurity.com/l/b/2010/02/12/abusing‐wcf‐to‐perform‐remote‐port‐scans/

• Chris Hoff’s blog
  – http://www.rationalsurvivability.com/blog/

• Various cloud working groups
  – Open Cloud Computing Interface Working Group, Amazon EC2 API, Sun Open Cloud API, Rackspace API, GoGrid API, DMTF Open Virtualization Format (OVF)