Introduction

• Russ McMahon
• Assoc Prof – UC (1999)
• College of Education, Criminal Justice, and Human Services
• Dept of IT – BSIT – ABET accredited
• Enjoy reading/researching about history of technology
  – Researched UC’s computing history
• IT User Group Evangelist
  – TechLife Cincinnati
  – ISSA
  – Infragard
  – OWASP
First Computer to Arrive in the Cincinnati Area

• March 1953
• IBM 701
• $17,000/month rental fee
• GE Evendale
• Dr Herb Grosch was the director
  – “Our whole technological civilization will be guided by this type of machine which will be doing the detail or dog work.”
  – GE had hoped to lure Dr Paul Herget from the UC Observatory
• Was the first large mainframe in the region
• 4 full-time IBM engineers on hand
• At that time a young computer programmer by the name of Donald Shell work for GE
  – Shell sort
  – IBM SHARE
What’s the Point

• “The whole point of cloud computing is economy: ...”
• “It has been shown .. . For computation to be done on encrypted data, which would prevent the person ... from using your information ...”
• “Current techniques could more than undo the economy gained by outsourcing and show little sign of becoming practical.”
• Whitfield Diffie
  – From an interview done by David Talbot, Nov 16, 2009 for Technology Review
  – Spoke at NKU back in Sept, 2011
• How Secure Is Cloud Computing?
  – http://www.technologyreview.com/computing/23951/
• “Much of this would result from care on the part of cloud computing providers--choosing more secure operating systems ... --and keeping those systems carefully configured. A security-conscious computing services provider would provision each user with its own processors, caches, and memory at any given moment and would clean house between users, reloading the operating system and zeroing all memory.”
Cloud Computing Concerns

- Illinois Institute of Technology presentation on Cloud Security by Ray Trygstad
- Governance, Risk Mgmt, & Compliance (GRC)
  - Has been described as "security in sheep's clothing," but primarily for defending the integrity of data and systems within the firewall

**Chart: Cloud Computing Concerns**

- Security defects in the technology itself: 54%
- Unauthorized access to or leak of our proprietary information: 51%
- Unauthorized access to or leak of our customers' information: 49%
- Application/system performance: 34%
- Business continuity/DR readiness of provider: 26%
- Business viability of provider; risk company will fail: 25%
- Vendor lock-in: 17%
- Features and general maturity of technology: 17%
- Unpredictable costs: 13%
- Other: 2%

*Note: Three responses allowed*

*Base: 310 respondents using, planning to use or considering using cloud computing*

*Data: InformationWeek Analytics 2010 Cloud GRC Survey of 518 business technology professionals, January 2010*
Hey! You! Get off of my cloud

• 1\textsuperscript{st} solution
  – Tightly controlled
  – Closed environment
  – Limits your ability to be mobile

• 2\textsuperscript{nd} solution
  – No security perimeter
    • Larger attack surface
    • You are more exposed
  – Lack of auditability, accountability, etc.
  – Regulatory compliance issues
  – What is hiding just behind the tree?
  – You may need an army behind you
It’s like déjà vu all over again

• Everything has changed; nothing has changed
• Timeshare Computing
  – class of remote, multi-access data processing systems which allow each user to utilize the full resources of the system while sharing the processor time with the other active users
  – Multics: ZARF is with you again
• Security Controls in the ADEPT-50 Time-sharing System, 1969, C. Weissman
  – 1. concurrent multiple users with different access rights operating remote from the shielded room
  – 2. multiple programs with different access rights co-resident in memory
  – 3. multiple files of different data sensitivities simultaneously accessible.
• System Techniques for Time Sharing, 1965, J. H. Morrissey
  – The user is concerned with security of his programs and data.
  – The “cloud provider” must also be constrained from security violations.
  – The first generation of “cloud” systems are currently in operation. They are not perfect, but they do work.
• Availability and security
NIST Cloud Computing Model

- Benefit of IT without the wait
  - Lower cost, risk, barrier to entry into new markets
- Infrastructure → Platform → Application
- IT → Developer → Business User
- IaaS – each app gets its own instance of the OS
- PaaS -- each app uses the same instance of the OS & platform
- SaaS – Application Service Provider
- Moving toward XaaS model
  - CaaS – Communication as a Service
    - Crime as a Service (Zeus botnet)
    - Cells as a Service (HP cloud security)
  - EaaS – Expertise as a Service
  - SECaas – Security as a Service
  - NaaS – Network as a Service
  - MaaS – Monitoring as a Service
  - Haas – Hardware as a Service
  - Daas – Data(base) as a Service

So then I typed GOTO the Cloud and here I am!
NIST and Cloud Security

- NIST standard as to what cloud computing is and is not
  - Computer Security Resource Center (CSRC)
  - SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
  - SP800-145 Definition of Cloud Computing
  - SP800-146 Cloud Computing Synopsis and Recommendations
  - SP500-293 US Govt Cloud Computing Technology Roadmap V1
  - NIST Cloud Computing Collaboration
    - NIST Cloud Computing Security Working Group (NCC-SWG)
  - 2009 presentation: Effectively and Securely Using the Cloud Computing Paradigm by Peter Mell and Tim Grance (NIST)
    - Tim Grance will speak at UC on April 11 from 3-4 in Swift Hall, Room 500
    - Sponsored by the Taft Research Center, the Department of Mathematical Sciences, and the Department of Political Science
    - [www.artsci.uc.edu/taft](www.artsci.uc.edu/taft)
  - NIST Cloud Guidelines Address Security, Privacy Concerns
    - Lee Badger & Tim Grance interview
NIST Top Cloud Security Working List

1. Potential Loss of Control/Ownership of Data
2. Data Integration, Privacy Enforcement, Data Encryption
3. Security Concerns are Identified Threats - CSA's Top Threats
4. Data Remanence after de-provisioning
5. Multi Tenant Data Isolation
6. Data Location Requirements (within national borders)
7. Hypervisor Security
8. Audit Data Integrity Protection
9. Ensuring Verification of Subscriber policies (including regulatory needs) through Provider controls
10. Certification/Accreditation Requirements for a given Cloud Service
NIST Impediments and Mitigations List

• Process Oriented
  – Confusion about Application of 800-53-style Controls, and Compliance
    • Recommended Security Controls for Federal Information Systems and Organizations
  – Lack of Cloud Audit Assurance and Log Sensitivity Management
  – Need Clear Certification and Accreditation Guidelines
  – Need Clear E-discovery Guidelines
  – Need Clear Privacy Guidelines
  – Need Clarity on Security Control Roles and Responsibilities
  – Need to Assess Trustworthiness of Cloud Operators
  – Business continuity and disaster recovery
  – Lack of Technical Continuous Monitoring Capabilities

• Focused Technical
  – Lack of Visibility for Customers
  – Lack of Control for Customers
  – Limited Data Protection
  – Risk of Account Hijack
  – Identity and Access Management (IAM) and Authorization not Deployed
  – Risk from Multi-tenancy
  – Cloud Based Denial of Service
## NIST Threat Sources

<table>
<thead>
<tr>
<th>Cloud Architecture Component</th>
<th>Security Threats</th>
<th>Security Functional Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualized</td>
<td>1. Unauthorized Access to Hypervisor</td>
<td>AILM</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>2. Presence of Malware in Hypervisor software</td>
<td>TVM</td>
</tr>
<tr>
<td>AILM = Access &amp; Identity Lifecycle Management</td>
<td>3. Starvation of Resources &amp; Denial of Services by some Rogue VMs</td>
<td>A</td>
</tr>
<tr>
<td>A = Availability</td>
<td>4. Unauthorized Access to VMs</td>
<td>AILM</td>
</tr>
<tr>
<td></td>
<td>5. Side-Channel Attack: One VM attacking another *</td>
<td>TVM</td>
</tr>
<tr>
<td></td>
<td>6. Presence of Covert Channel between VMs *</td>
<td>TVM</td>
</tr>
<tr>
<td></td>
<td>7. Unauthorized Access to VM Image repository *</td>
<td>AILM</td>
</tr>
<tr>
<td></td>
<td>8. Tampering of VM Images *</td>
<td>IALM</td>
</tr>
<tr>
<td></td>
<td>9. VM placed in an insecure state after a restart *</td>
<td>TVM</td>
</tr>
<tr>
<td>TVM = Threat &amp; Vulnerability Management</td>
<td>10. VM placed in an insecure state after migration to a new host</td>
<td>TVM</td>
</tr>
<tr>
<td>IALM = Integrity &amp; Access &amp; Lifecycle Management</td>
<td>11. A traffic meant for one VM is delivered to a wrong VM or to an outside entity</td>
<td>?</td>
</tr>
</tbody>
</table>
NIST Threat Analysis: Hypervisor Threats

• HT1: Starvation of Resources & Denial of Service for some VMs:
  – Some VMs hog most of the processing and memory resources of the hypervisor host resulting in starvation of resources or complete denial of services for other VMs.
  – Probable Causes:
    • (a) Badly configured Resource Limits for some VMs
    • (b) A Rogue VM having the capability to bypass resource

• HT2: VM Side-channel Attacks:
  – Malicious attack on one or more VMs residing in the same hypervisor host by a rogue VM.
  – Probable Causes:
    • (a) Lack of proper isolation of inter-VM traffic due to misconfiguration of the virtual network residing in the hypervisor.
    • (b) Limitation of packet inspection devices to handle high speed traffic (e.g., video traffic)
    • (c) Presence of VM Instances built from insecure

• HT3: Buffer overflow Attacks
NIST Threat Analysis: VM-Based Threats

• VM1: Deployment of Rogue or Insecure VMs:
  – Unauthorized users may create insecure instances from Images or may perform unauthorized administrative actions on existing VMs.
  – Probable Causes:
    • (a) Improper configuration of access controls on VM administrative tasks such as Instance Creation, launching, suspension, re-activation etc.

• VM2: Presence of Insecure and Tampered Images:
  – Due to lack of controls, the VM Image repository may contain insecure and tampered images.
  – Probable Causes:
    • (a) Lack of access control on who can put images into a repository
    • (b) Lack of mechanisms to verify the integrity of the images (e.g., digitally signed Image)
Cloud Computing Security

- Cloud Security Alliance (CSA)
  - Cloud Computing Security Risks
    - Security Guidance for Critical Areas of Focus in Cloud Computing
    - Trusted Cloud – CSA Guidance for Identity & Access Mgmt
  - Top Threats to Cloud Computing
    - Abuse and Nefarious Use of the Cloud
    - Insecure APIs (Weakest Link Security)
    - Insider Threat
    - Shared Technology Vulnerabilities
    - Data Loss/Leakage
    - Account/Service and Traffic Hijacking
    - Unknown Risk Profile
- CloudSecurity.org -- cloudsecurity.org/ (*seems stale)
  - Project Skylab
    - The Skylab Project is aimed at IT and IT security professionals that are “cloud curious” and want to get their hands dirty in a relatively safe way (i.e. no business data involved). You could say its for the hobbyist security geek.
  - Brucon 2010
  - GoGrid Security Breach
  - What Does PCI Compliance in the Cloud Really Mean?
Cloud Computing Security

• PKI – Public Key Infrastructure
  – NIST SP800-32 Introduction to PKI and FPKI
    • http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/index.html
    • src.nist.gov/groups/ST/crypto_apps_infra/pki/index.html
  – PKIX Working Group
    • goal of developing Internet standards to support X.509-based PKIs
    • http://datatracker.ietf.org/wg/pkix/charter/
  – 10 Risks of PKI
    • www.schneier.com/paper-pki.html

• European Network & Information Security Agency (ENISA)
  – Governmental Cloud in the EU-New Agency Report
  – SecureCloud
    • Sponsored by ENISA, CSA, ISACA
  – Cloud Computing video
  – Presentation on Cloud Security & Identity

• Forum of Incident Response and Security Teams (FIRST)
  – international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs
Cloud Standards Related Orgs

- Distributed Management Task Force (DMTF)
  - is developing a set of standards to improve cloud management interoperability between service providers and their consumers and developers
    - includes short talks from NIST, DMTF, SNIA, & CSA
  - The State of Cloud Standards (Feb 10, 2012)
  - Cloud Auditing Data Federation (CADF) Work Group

- Open Cloud Computing Interface (OCCI)
  - comprises a set of open community-lead specifications delivered through the Open Grid Forum (OGF – Applied Distributed Computing). OCCI is a Protocol and API for all kinds of Management tasks
  - OpenNebula.org – open source toolkit for cloud computing

- Object Management Group (OMG)
  - to develop, with our worldwide membership, enterprise integration standards that provide real-world value
  - UML, Model Driven Arch (MDA), Interface Defn Lang (IDL)
  - Can submit specifications directly into ISO’s fast-track adoption process
Cloud Standards Related Orgs

- **Storage Networking Industry Assoc (SNIA)**
  - develop robust solutions for storing and managing the massive volumes of information generated by today’s businesses
  - CompTIA Storage+

- **Org for the Advancement of Structured Info Std (OASIS)**
  - drives the development, convergence and adoption of open standards for the global information society (SMGL, XML, SAML)
  - IDtrust
    - where government agencies, companies, research institutes, and individuals work together to advance the use of trusted infrastructures, including PKI
  - IDCloud webcast -- [www.oasis-idtrust.org/node/75](http://www.oasis-idtrust.org/node/75)

- **Cloud Computing Interoperability Forum (CCIF)**
  - A key focus will be placed on the creation of a common agreed upon framework / ontology that enables the ability of two or more cloud platforms to exchange information in an unified manor

- **OpenCrowd Taxonomy**

- **Open Group - Jericho Forum - Cloud Cube Model**
CSA’s Security Guidance for Critical Areas of Focus in Cloud Computing

- Cloud Computing Architectural Framework
- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability
- Traditional Security, Business Continuity, and Disaster Recovery
- Data Center Operations
- Incident Response, Notification, and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
CSA’s Cloud Controls Matrix (CCM)

• Specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider
• Part of their GRC stack (Governance, Risk Mgmt, Compliance)
• Control Areas (in a form of an Excel spreadsheet)
  – Compliance
  – Data Governance
  – Facility Security
  – Human Resources
  – Information Security
  – Legal
  – Operations Management
  – Risk Management
  – Resiliency
  – Security Architecture
Mapping the Cloud Model to the Security & Compliance Model

- From the CSA Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, Dec 2009
How Security Gets Integrated

- Pg 26 Figure 7 of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing

The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.
Data Security Lifecycle in the Cloud →

- Pg 40-41 of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing
Data Security Lifecycle in the Cloud

• Data security

• Location of the data
  – There must be assurance that the data, including all of its copies and backups, is stored only in geographic locations permitted by contract, SLA, and/or regulation

• Data remanence or persistence
  – Data must be effectively and completely removed to be deemed ‘destroyed.’

• Commingling data with other cloud customers

• Data backup and recovery schemes for recovery and restoration

• Data discovery

• Data aggregation and inference
  – there are added concerns of data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information

• Encryption issues esp involving computations on data
For IaaS Cloud Solutions

- Pg 47-48 of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing
- Understand how virtual machine images can be captured and ported to new cloud providers, who may use different virtualization technologies.
- Identify and eliminate (or at least document) any provider-specific extensions to the virtual machine environment.
- Understand what practices are in place to make sure appropriate deprovisioning of VM images occurs after an application is ported from the cloud provider.
- Understand the practices used for decommissioning of disks and storage devices.
- Understand hardware/platform based dependencies that need to be identified before migration of the application/data.
- Ask for access to system logs, traces, and access and billing records from the legacy cloud provider.
- Identify options to resume or extend service with the legacy cloud provider in part or in whole if new service proves to be inferior.
- Determine if there are any management-level functions, interfaces, or APIs being used that are incompatible with or unimplemented by the new provider.
For PaaS Cloud Solutions

• When possible, use platform components with a standard syntax, open APIs, and open standards.
• Understand what tools are available for secure data transfer, backup, and restore.
• Understand and document application components and modules specific to the PaaS provider, and develop an application architecture with layers of abstraction to minimize direct access to proprietary modules.
• Understand how base services like monitoring, logging, and auditing would transfer over to a new vendor.
• Understand control functions provided by the legacy cloud provider and how they would translate to the new provider.
• When migrating to a new platform, understand the impacts on performance and availability of the application, and how these impacts will be measured.
• Understand how testing will be completed prior to and after migration, to verify that the services or applications are operating correctly. Ensure that both provider and user responsibilities for testing are well known and documented.
For SaaS Solutions

• Perform regular data extractions and backups to a format that is usable without the SaaS provider.
• Understand whether metadata can be preserved and migrated.
• Understand that any custom tools being implemented will have to be redeveloped, or the new vendor must provide those tools.
• Assure consistency of control effectiveness across old and new providers.
• Assure the possibility of migration of backups and other copies of logs, access records, and any other pertinent information which may be required for legal and compliance reasons.
• Understand management, monitoring, and reporting interfaces and their integration between environments.
• Is there a provision for the new vendor to test and evaluate the applications before migration?
CSA Final Considerations

• There is tremendous potential for misguided decisions and detrimental outcomes.
  – Unless cloud providers can readily disclose their security controls and the extent to which they are implemented to the consumer, and the consumer knows which controls are needed to maintain the security of their information

• First one classifies a cloud service against the cloud architecture model.
  – Then it is possible to map its security architecture; as well as business, regulatory, and other compliance requirements; against it as a gap-analysis exercise.

• Cloud computing is about gracefully losing control
  – By maintaining accountability

• ISO/IEC 27001 certification

• Trust, but verify (Ronald Reagan to Mikhail Gorbachev)
Recent Research Topics & Talks

• ACM Conference on Computer and Communications Security Workshop (CCSW) (Oct 19, 2011)
  – Cloud Security – Myth or Reality by Tim Brown (legal-contract issues)
  – What’s Different about Security in a Public Cloud by Charlie Kaufman
  – Clouds and Their Discontents by John Manferdelli

• Security Analysis of Cloud Mgmt Interfaces (Somorovsky et al)
  – All Your Clouds are Belong to us
  – Security analysis of a large Public Cloud (Amazon) and a widely used Private Cloud software (Eucalyptus) – they can be successfully attacked
  – Cross Site Scripting (XSS) is an issue (see OWASP Top 10)

• Who Can You Trust in the Cloud? (Roberts & Al-Hamdani)
  – Security issues with Cloud Based Computing and Cloud Oses
    • Google’s Chrome OS – open source cloud based OS

• Managing a Security Program in a Cloud Computing Environment (Townsend)

• Ontological Approach toward Cybersecurity in Cloud Computing (Takahashi et al)
Recent Research Topics & Talks

• Cloud Application Logging for Forensics (R. Marty)
• Intrusion Detection System in Cloud Computing Environment (Dhage et al)
• Eliminating the Hypervisor Attack Surface for a More Secure Cloud (Szefer et al)
  – NoHype system
• Functional Components for a Security Manager within Future Inter-Cloud Environments (Kretzschmar et al)
• A Stealth Approach to Usable Security (Parkin et al)
  – Users are not the Enemy (Adams & Sasse – 1999)
• Detecting Fraudulent Use of Cloud Resources (Idziorek et al)
• Towards Incident Handling in the Cloud (Grobauer & Schreck)
• Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds (Bleikertz et al)
• On Securing Untrusted Clouds with Cryptography (Chen & Sion)
  – Diffie was right (for the time being)
Emerging Technologies, Topics, Issues

• OASIS Security Assertion Markup Language (SAML) (SP800-63)
• OpenID
• Trusted Cloud Computing Platform (TCCP)
  – Max Planck Institute for Software Systems
• TrustCube – manage the authentication infrastructure (using OpenID)
• Digital Death, Thanatosensitivity, and Identity Inheritance
• Model Driven Security Accreditation (MDSA)
• JeOS – Just Enough OS – a new advancement in directing users to only using browsers for running apps
  – Google Chrome OS
• Fraudulent Resource Consumpption (FRC) attack (free-rider)
• eXtensible Access Control Markup Language (XACML)
• Security Content Automation Protocol (SCAP ) (NIST)