SNIA

Education

Securing The Cloud

Russ Fellows,
Managing Partner -
Evaluator Group Inc.

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

- Securing The Cloud – Using Cloud Computing without risking data security
  - Security has always been a critical aspect of IT Storage. However, the proliferation of networking technologies and protocols, combined with the emergence of Cloud Storage has made security more important and difficult than ever. In this presentation, we will examine some of the technologies and standards that are available to solve these issues, and show how companies can utilize these technologies to design an architecture that is scalable and secure. You will learn how to establish security practices that accommodate multiple networking technologies, including FCoE, IB, iSCSI and FC networks. Securing data in both public and private clouds is covered, with an examination of the issues around securing Cloud and other storage services. This session will focus on the data-center requirements for implementing a successful encryption strategy that secure data both in-flight and at-rest. Issues such as when and where to encrypt data, products to use and the all-important key-management question are addressed.

Agenda

- Introduction
  - Cloud Provider Models
  - Cloud Security Overview
  - Elements of Security
- Security Issues
  - Cloud Specific Issues
  - Privacy and Compliance
  - Encryption and Key Management Issues
- SNIA CDMI Security
  - CDMI Overview
  - Security Capabilities
- Recommendations
  - Questions for Cloud Providers
  - Security for IaaS, Paas and SaaS
  - Recommendations
  - Summary

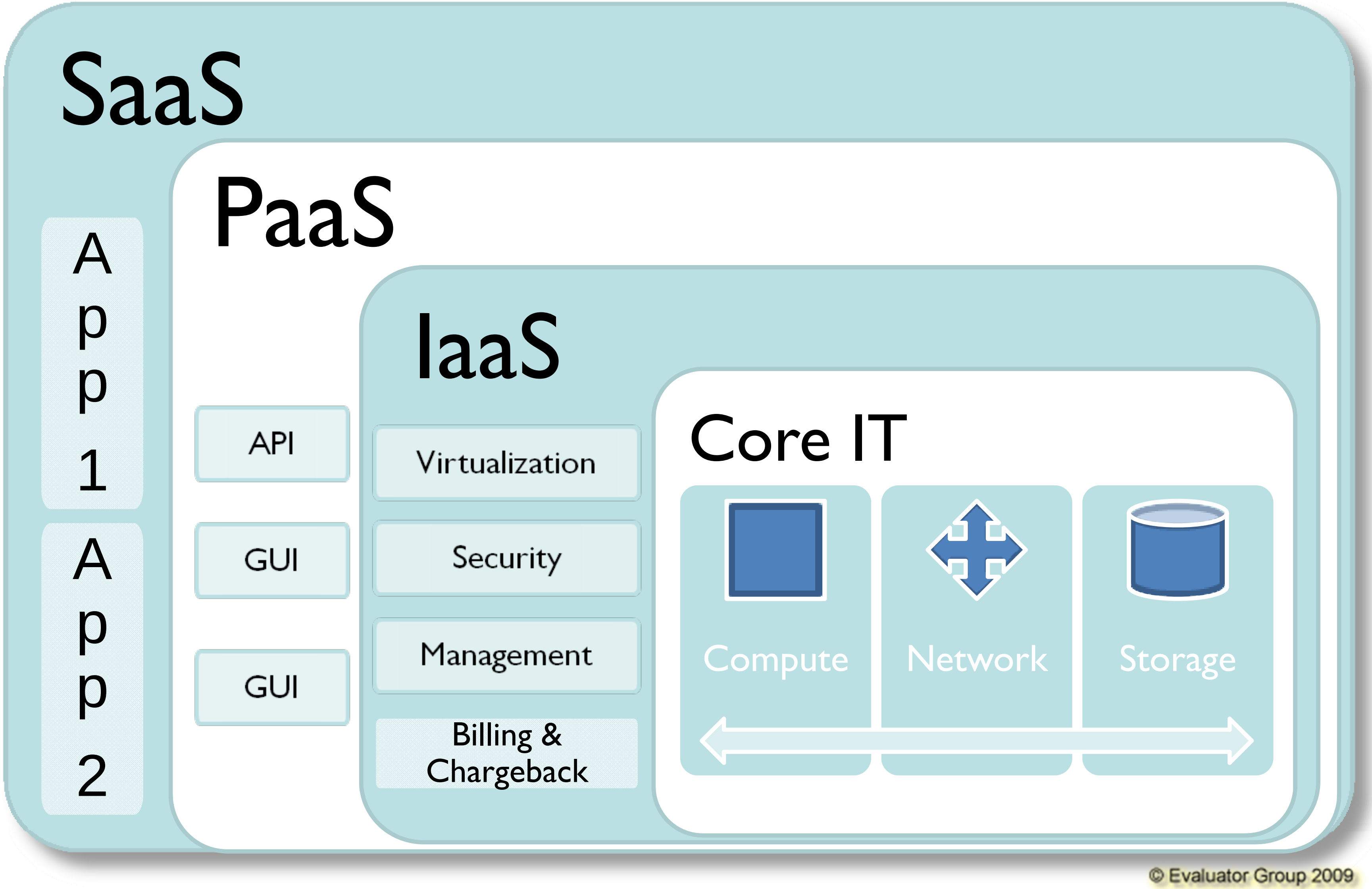
Cloud Computing

- “The Network *really* is the Computer”
- Features:
  - Scalable, Infinite, Instant Resource
  - Capacity on Demand
  - High Level – Abstract Resources
  - Fault Tolerant
- Key Enabler
  - *Secure* multi-tenancy

Cloud Computing Issues

- Understand Infrastructure
- Understand Legal and eDiscovery implications
- Understand Compliance and Audits
- Understand impact of ILM and data migration
- Understand BC & DR Impact
- Understand impact on operations
- Investigate security, including key management, identity management & access control

Cloud Provider Models



© Evaluator Group 2009

Why Cloud Security is a Concern

- The lack of security is the #1 reason why CIO's, CTO's and IT departments don't trust Clouds
- Requires more effort than securing internal IT
- Security only as good as weakest link
- In practice, will require user managed encryption
- Still requires diligence on other issues
  - Denial of Service (DoS)
  - Application security
  - Encryption and key management, etc.

Regulations Drive Security

BSI PD08

NIST 800-26 & 53 NASD 3010 & 3110

EU Richtlinie AML

GDPdU & GoBS HIPAA OSHA GAO

Sarbanes-Oxley SEC Rule 17a-4

C cGxP & 21 CFR Part 11 CAN-SPAM

BS-179

Hong Kong Data Protection Act SEC Rule 240.17

DOD 5015 EU WEEE

RoHS GAMP4 Gramm-Leach Bliley Act

UEE Act

OSHA Basel II

ISO 17799 & 13335 11MEDIS-DC

EU GMP BS 7799-2

Why Cloud Security is Different

- Physical security is impossible –
  - "There is no there, there"
- Requires architectural and operational diligence
- Providers only enable <u>the ability</u> to secure services
- Many services are insecure out of the box
- Perimeter security models must evolve to secure virtual perimeters
  - No (or limited) direct control over resources
  - Resources are virtual (or fungible)
- Service Contracts drive features – nothing is free

Elements of Security

- Confidentiality
  - Information released only to authorized entities
- Integrity
  - Information should be unaltered
- Authorization
  - Policy to determine who has access to information
- Authentication
  - Requires identification of systems and users
- Availability
  - The system must be available for use

Ensuring Confidentiality

- Without physical control of resources
- Without perimeter control
- With access by unknown personnel
- In an inter-networked environment
- With unknown virtual image management
- There is only one practical method of providing confidentiality –

- Encryption is the only viable option

What to Encrypt

- Any regulatory protected data
  - SSN, Name, DOB, etc
- Any “Unique Identifiers” used by interact with Cloud Services
  - UID is in essence a private key, meaning securing the key is essential to securing access
  - The “key”, “oid”, “bucket” or other identifier must be secured at all times, just as a private key
  - Best practices dictate using public key encryption with certificates to secure, transfer and store identifier

Communications Security

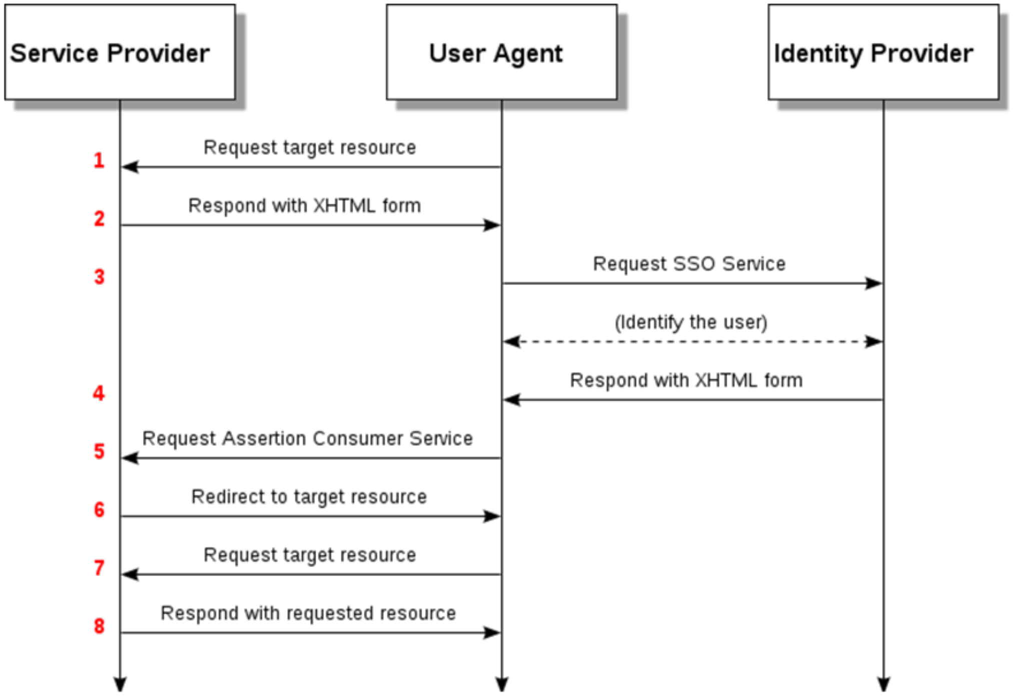
- Communication Security is a Pre-Requisite in Cloud Computing
- Authentication and Identification information is often required by Cloud Services
- Authentication and Identification are two areas most often compromised in security
  - Lost, stolen or misplaced login credentials
  - Examples: Login ID's, passwords, Java cards, etc.

Authentication and Identity

- Authentication
  - TLS (Successor to SSL) has two modes
    - Unilateral (Server is authenticated, but client is not)
    - Bilateral (Both Server and Client are authenticated)
  - Look to own authentication process
    - Provides more flexibility, SSO, VPN portals, etc
  - Authentication requires Certificates
    - May require creating certificates in some cases
  - SNIA CDMI may support bilateral authentication
    - Important if implicit trust is not possible by one party
- Identifying information must be protected
  - Requires a secure transport (e.g. TLS)

Leading Identity Protocols

- SAML, WS-Federation and OpenID
- SAML uses XACML (XML Access Control Meta Language)
- SAML Model



CLOUD SECURITY ISSUES

Cloud Storage Specific Issues

- "Cloud Security is a Nightmare"
  - Cisco CEO John Chambers – April 2009 RSA Conference
- Some Recent Cloud Outages
  - Twitter, Phising Jan. 2009, DoS Aug. 2009
- All services are potentially vulnerable
- Using any non secure protocol is risky
  - Packet sniffing can detect sensitive data

Privacy & Compliance Concerns

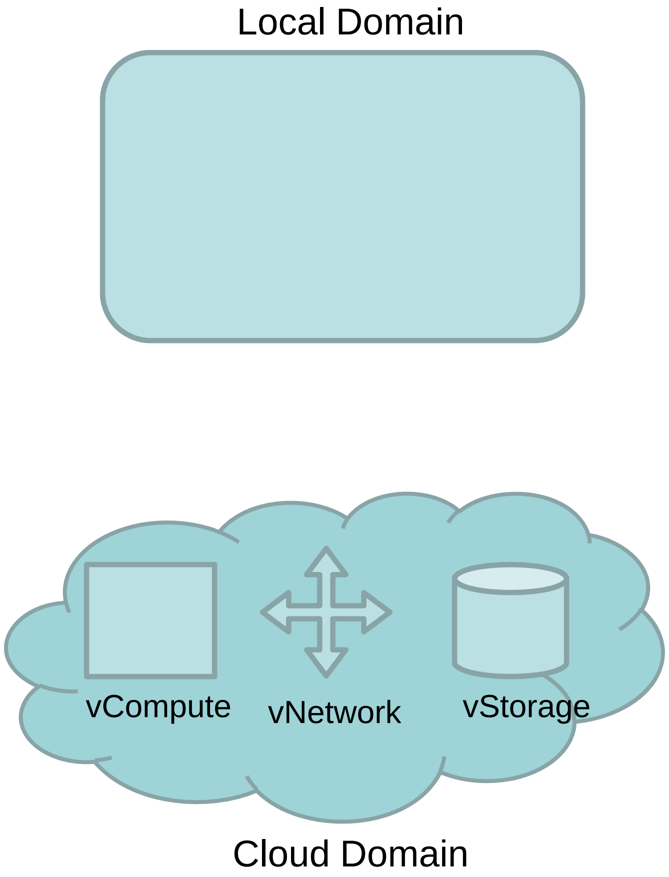
- EU data privacy and data protection laws severely restrict transfer of data outside the EU to the US
  - Based on EU Directive 95/46/EC
    - Enforcement becoming more widespread
    - Fines have been imposed against firms violating member countries laws, including UK and France
  - Safe-harbor or other EU approved programs may provide a method for compliant data transfer
- The US is pre-disposed to compel release of information vis-à-vis the Patriot Act
  - Provides significant ability for law enforcement to search telephone, e-mail, medical, financial, and other records

Many Organizations and Standards

- Cloud Security Group:
  - Cloud Security Alliance
- There are many standards bodies:
  - ACM, IEEE, IETF, NIST, ISO, OASIS, SNIA, PCI, etc
- Even more standards
  - NIST FIPS 140-2, IEEE P1619, ISO/IEC 27002,
  - OASIS SAML and KMIP, PCI-DSS, etc. etc.
- Who is Responsible? – You

Issues with Encryption

- Where to provide encryption?
  - Host, Network or Storage
- Storage encryption focus
  - Current efforts place encryption on storage devices: disks and tapes
  - This model is difficult in a multi-tenant, virtual data-center cloud
- Encryption perimeter
  - Data must be encrypted whenever leaving local domain
  - Key retention and management also must be local



Key Management Overview

- Key management is essential for Cloud Computing

Check out SNIA Tutorial:

Introduction to Key Management – Walt Hubis

- Several efforts underway
  - IEEE P1619.3
    - Part of P1619 focus on storage encryption
    - In process for several years, now aligned with OASIS KMIP
  - OASIS KMIP
    - Comprehensive Key and Certificate Policy Framework
    - Most Large Storage Vendors Participating
      - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

Issues with Key Management

- Many groups, bodies and efforts underway
- Critical to using encryption
- Without standards, vendor lock-in is likely
- Where are the Key Management Standards headed?
- (Note: Author’s Opinion)
  - Vendors appear ready to commit now
  - OASIS KMIP appears to have momentum
  - Standards still in progress, may be reality in 2010
  - Early interoperability problems likely (as with all new standards)

Check out SNIA Tutorial:

Cloud Storage Standards Overview

by Mark Carlson

SNIA CDMI SECURITY OVERVIEW

What is CDMI?

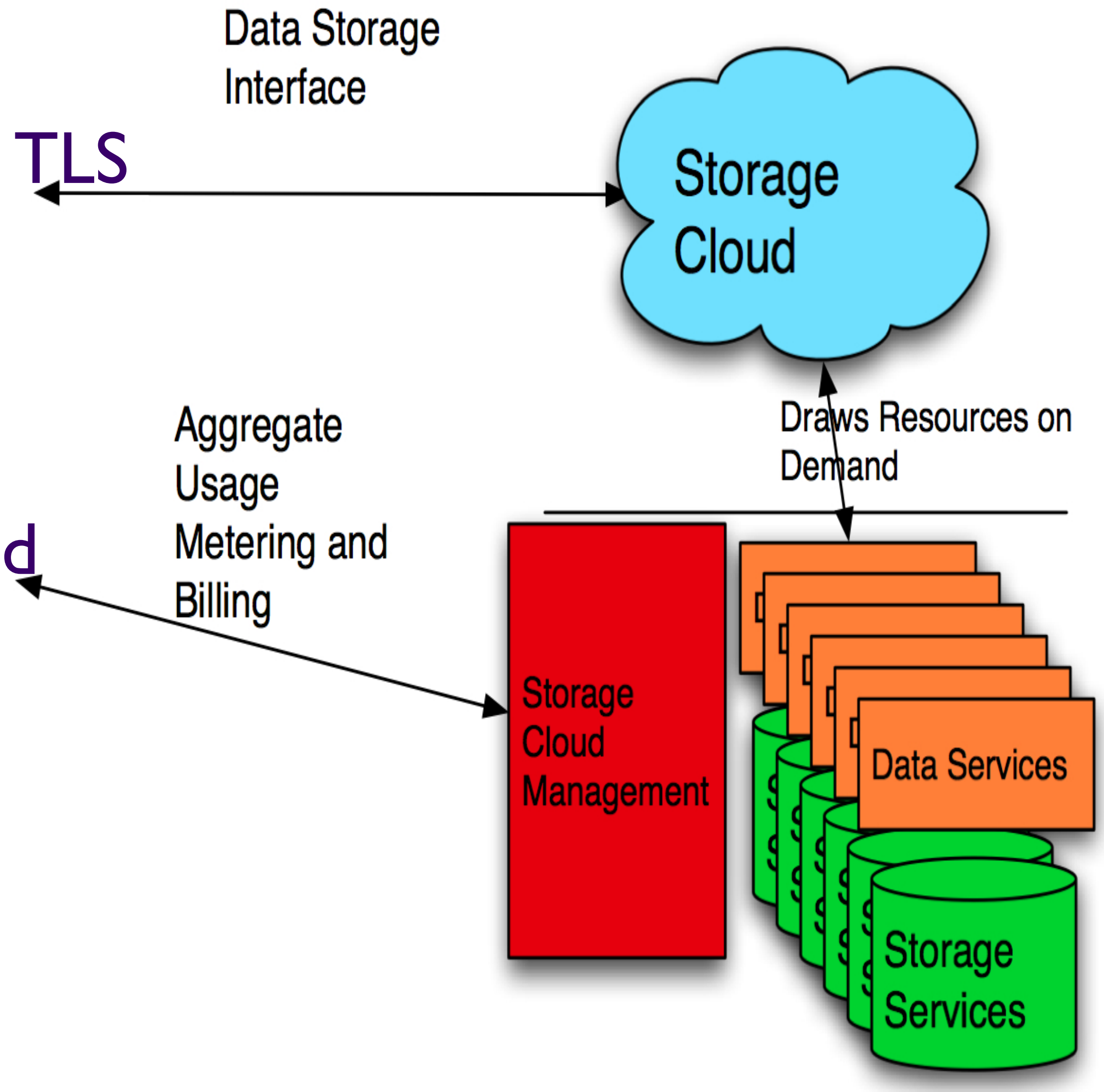
- CDMI is SNIA's Cloud Data Management Interface
  - A standards based mechanism for Cloud Storage
- Includes both management and data access
- Cloud Storage access through multiple methods
- Management interfaces
  - Proprietary, Web UI, SMI-S
- Billing & Chargeback
  - Based on allocated space and QoS parameters

SNIA CDMI Access

- Stored data can be accessed using native protocols:
  - HTTP, CIFS, NFS, iSCSI, SQL, etc.
- Data may also be accessed using CDMI as a standards based interface
  - Cloud-to-cloud migration
  - Cloud federation, backup, search and more
- Desired characteristics can be associated with stored data:
  - Replication, Compression, Placement, Retention, QoS, etc.

CDMI Security Example

- All Transfers utilize TLS encrypted sessions
- At a minimum, all regulatory protected information is encrypted locally



Data Storage Interface

Storage Cloud

Aggregate Usage Metering and Billing

Draws Resources on Demand

Storage Cloud Management

Data Services

Storage Services

SNIA CDMI Authenticated Access

- Example of account access with certificate

```
HTTP connection established to http://cloud.example.com/ port 80

>> GET /myaccount/cdmi_account_members/jdoe HTTP/1.1<CR><LF>
>> host: cloud.example.com<CR><LF>
>> <CR><LF>
<< HTTP/1.1 200 OK<CF><LF>
<< Date: Mon, 20 Jul 2009 05:58:29 GMT<CF><LF>
<< Content-Type: text/plain
<< Content-Length: 522
<< <CR><LF>
<< {
<<     “cdmi_member_name” : “jdoe”,
<<     “cdmi_credentials_type” : “certificate”,
<<     “cdmi_credentials” : “-----BEGIN CERTIFICATE-----
          MIIC2DCCAkGgAwIBAgIDEL90MA0GCSqGSIb3DQEBBAUAMGwxCzAJBgNVBAYTAlVT ...
          -----END CERTIFICATE-----”,
<<     “cdmi_acl_name” : “jdoe”,
<<     “cdmi_groups” : [ “”, ],
<<     “cdmi_privilages” : [ “administrator”, ],
<<     “cdmi_quota” : “1000000000”,
<< }

HTTP Connection closed
```

Practical ways to secure data using Cloud Services

CLOUD SECURITY RECOMMENDATIONS

Tenants of Cloud Security

- Moving to a virtual data center implies no physical perimeter or physical controls
- Requires an equally greater reliance on information security
- Must assume Cloud Resources are publicly accessible for compliance laws
  - Security = Authentication, Authorization, Access, Audit
  - Access typically uses encryption as enforcement

Cloud Storage Provider Questions

- What is the storage architecture
- What controls are used during provisioning to partition multiple customers
- What data search capabilities
- How is data destroyed in a multi-tenant environment
- Can data be seized by a third party or government entity
- How are multi-tenant encryption and keys managed (single key, multiple, who has keys?)
- Support for long term archiving
  - Will data be available in 10 years, will the decryption still be useable?

Security for SaaS

- Similar to many applications => Few Security Controls
- Typical Controls:
  - User creation / deletion
  - Login / authorization
  - Password reset
  - Audit log access

	Login	Admin	Read	Write
Vendor A	Some	No	No	Yes
Vendor B	Yes	Yes	No	Yes
Vendor C	No	No	No	Yes

Security for PaaS

- More threats than SaaS, but fewer than IaaS
- In addition to steps taken for SaaS consider additional security issues
- Some Examples:
  - CSRF (Cross Site Request Forgery – Sidejacking)
  - XSS (Cross Site Scripting)
  - SQL Injection

Security for IaaS

- About the same as for any publicly accessible data center
  - OS Weaknesses
  - Hypervisor Issues
  - Management Interfaces
  - Network access and DoS
  - Storage and long term retention
  - Patch management, etc.
- How to protect secret data (private keys, etc.)

IaaS Issues

- Virtualization & Hypervisor Attacks
- Management Interfaces
  - Limited TLS and SSH access, limited audit logs
- Networking
  - Limited VPN, IP filters only
- Storage
- Management
  - Private keys, Identifiers, Password files, etc.

IaaS Security Example

- OS Security:
  - OS root access gives full control over ports and processes
- Virtualization Level Security:
  - Security with Triple-A (Authentication, Access Control and Audit)
- Physical Security:
  - Physical servers in data center with bio-metric access control
- Network Security:
  - Traffic can be isolated and restricted to dedicated VLANs
- Instances Persistence:
  - Virtual systems persist with local storage and static IP
- Storage Security:
  - Unencrypted local storage or encrypted NAS
- Firewall:
  - Built into HA load balancers

Detailed IaaS Security Checklist

- Ensure the system key is encrypted at start-up
- Use Security Groups
- Never allow password authentication for shell access
- Encrypt all network traffic to the Cloud
- Encrypt everything stored in cloud
- Encrypt file systems for Block devices

- Open only the minimum required ports
- Remove authentication information from all system images
- Never store keys in the cloud
- Install host based intrusion detection
- Backup VI's and store them securely

Cloud Security – Where to Start

- Create architecture and review
- Understand the Security Checklist
- Ask your Cloud provider for detailed answers
- Follow best practices guidelines by providers
- No need to wait for standards
- Many encryption and key management product options available

Summary

- Cloud Security is Possible
- Understand how security is unique in Cloud environments
- Requires attention to security issues + extra concerns
- Deployments are possible without waiting for standards

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Thanks to the following individuals
for their contributions to this tutorial.

- SNIA Members:

Russ Fellows
Eric Hibbard
Larry Hofer
Mark Carlson