Education

A HYPE-FREE STROLL THROUGH CLOUD STORAGE SECURITY

Eric A. Hibbard, CISSP, CISA, ISSAP, ISSMP, ISSEP, SCSE
Hitachi Data Systems

Author: Eric A. Hibbard, Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- 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

A Hype-free Stroll Through Cloud Storage Security

Cloud storage is emerging as a cloud offering that has appeal to a potentially broad set of organizations. Like other forms of cloud computing, the security must be addressed as part of good governance, managing risks and common sense. The Cloud Security Alliance (CSA) guidance on cloud computing security can be used as a starting point for what some believe is a make-or-break element of cloud storage.

This session provides an introduction to cloud computing security concepts and issues as well as identifying key guidance and emerging standards. An overview of the current CSA materials and activities is also provided. The session concludes by providing a security review of the SNIA Cloud Data Management Interface (CDMI) specification, which includes protective measures employed in the management and access of data and storage.

Cloud Computing 101

Key Attributes of Cloud
(All Must Be Met)

- *Offsite, by third-party provider* - "In the cloud" execution (offsite, location-agnostic)
- *Accessed via the Internet* - Standards-based, universal network access though this doesn't preclude security or quality-of-service value-add
- *Minimal/No IT skills to "implement"* - Online, simplified specification of services and no lengthy implementation of on-premise systems
- *Automated Provisioning* - Self-service requesting, near real-time deployment, dynamic & fine-grained scaling
- *Fine-Grained Pricing* - Usage-based pricing capability though some providers mask this granularity with long-term, fixed price agreements
- *User Interface* - browser & successors
- *System Interface Via Web Services APIs* - Providing a standards-based framework for accessing and integrating with and among cloud services
- *Shared resources/common versions* - Some ability to customize "around" the shared services, via configuration options within the service

Source: ***IDC on The Cloud*** (http://blogs.idc.com/ie/?p=189)

Cloud Computing Characteristics

- *On-demand self-service* – automated provisioning scenario in which capabilities such as server time and network storage can be obtained as needed, without requiring human interaction with the service's provider
- *Broad network access* – style of interaction in which capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms
- *Resource pooling* – aggregation of a provider's computing resources to serve multiple consumers using a multitenant model, with physical and virtual resources dynamically assigned and reassigned on demand
- *Rapid elasticity* – quick scaling of resources and capabilities to meet expansion and contraction of demand
- *Measured Service* – metered dispensation of resources appropriate to a given type of service (e.g., storage, processing, bandwidth, and active user accounts), such that usage can be monitored, controlled, reported and billed

Cloud Service Models

- *Software as a Service (SaaS)* – delivery over a network, on demand, of the use of an application
- *Platform as a Service (PaaS)* – delivery over a network of a virtualized programming environment, consisting of an application deployment stack based on a virtual computing environment
- *Infrastructure as a Service (IaaS)* – delivery over a network of an appropriately configured virtual computing environment, based on a request for a given service level
- *Data Storage as a Service (DaaS)* – over a network of appropriately configured virtual storage and related data services, based on a request for a given service level

SOURCE: SNIA Dictionary, http://www.snia.org/dictionary

Cloud Deployment Models

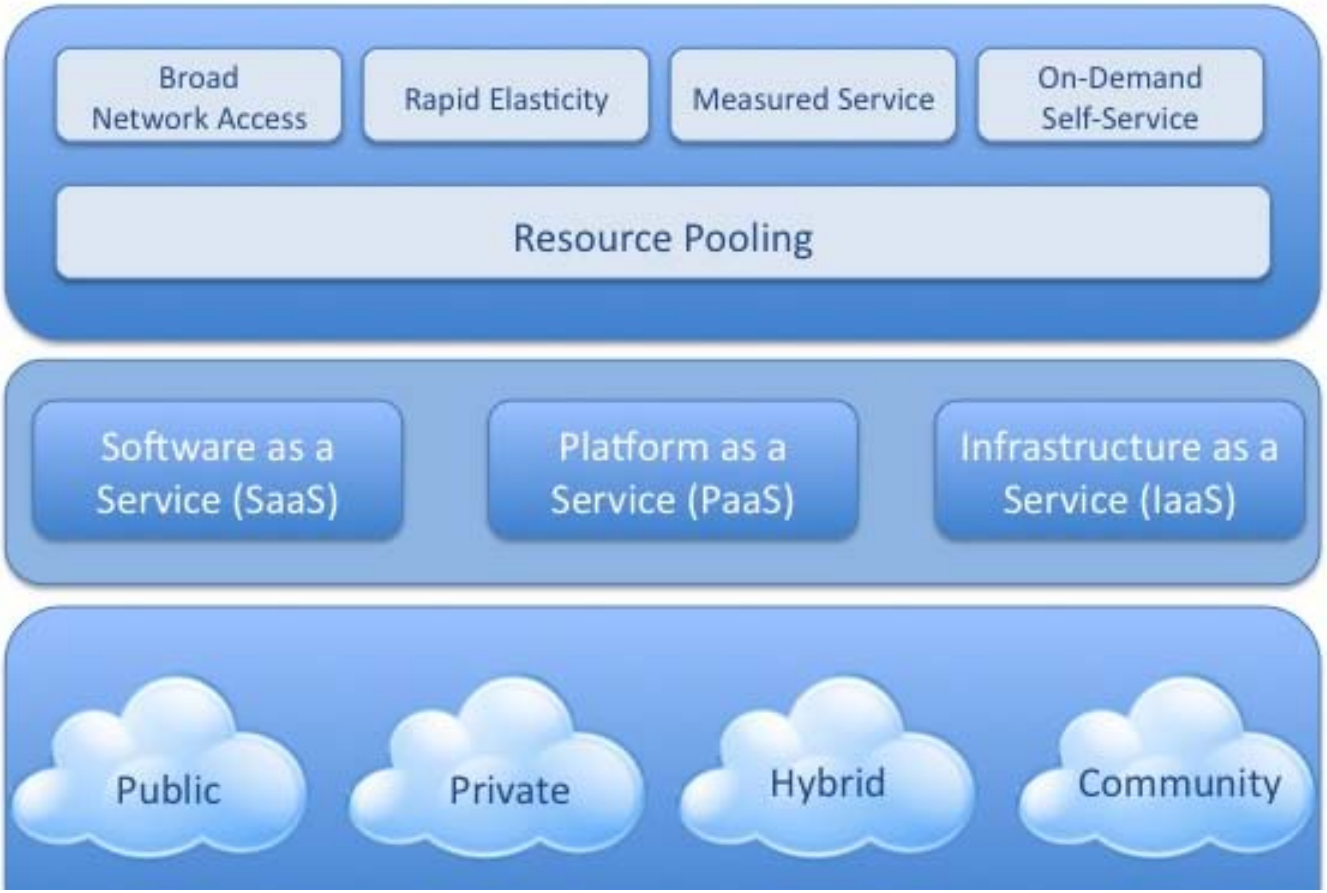
- *Private cloud* – delivery of SaaS, PaaS, IaaS and/or DaaS to a restricted set of consumers, usually within a single organization
- *Public cloud* – delivery of SaaS, PaaS, IaaS and/or DaaS to a relatively unrestricted set of consumers
- *Community cloud* – cloud infrastructure shared by several organizations and supporting a specific community that has shared concerns
- *Hybrid cloud* – composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

SOURCE: SNIA Dictionary, http://www.snia.org/dictionary

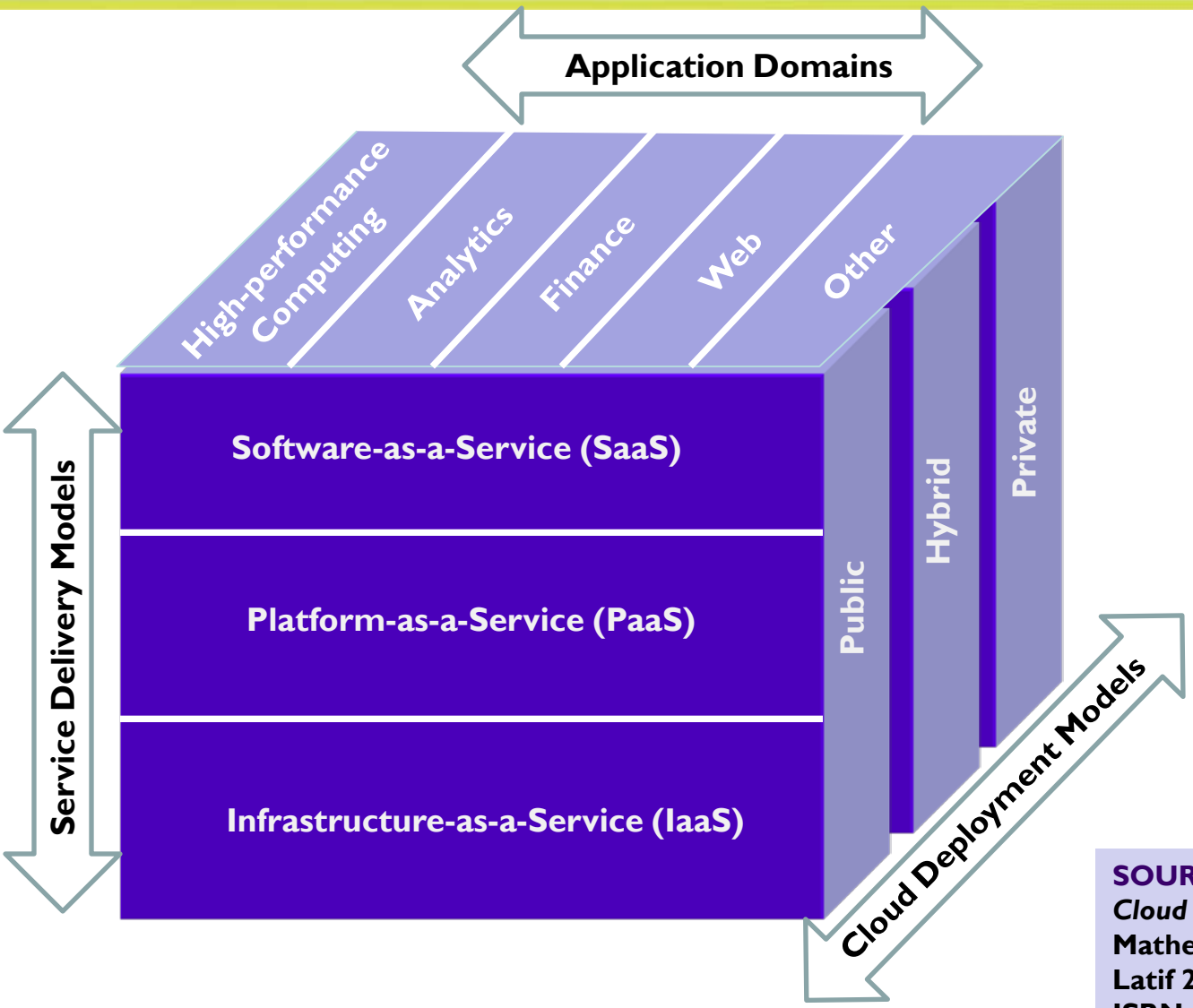
NIST View of the Cloud

Education SNIA

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



An Application View of Cloud



SOURCE:
***Cloud Security and Privacy*, Mather, Kumaraswamy and Latif 2009, O' Reilly, ISBN: 978-0-596-80276-9.**

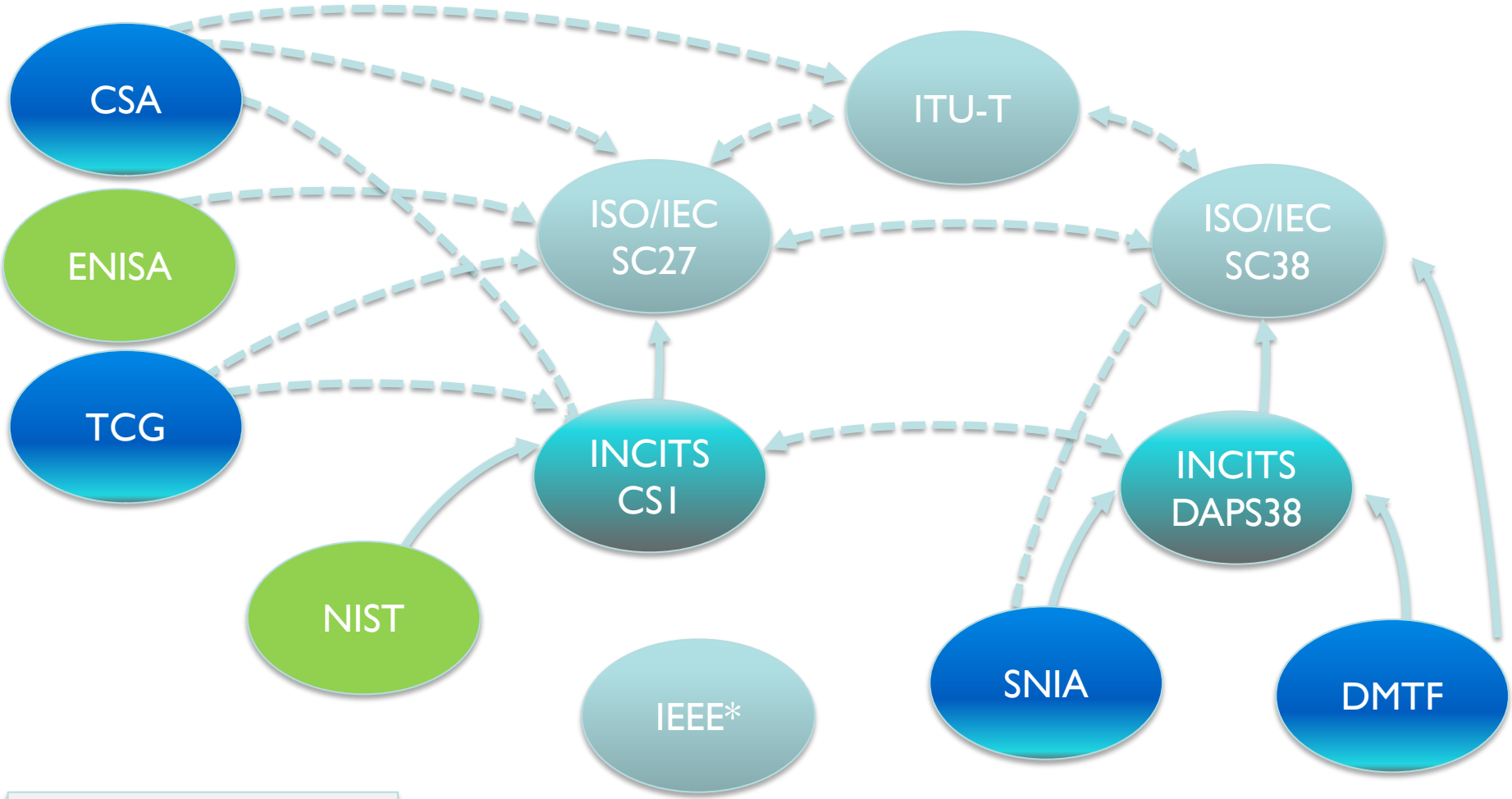
Standards & Specifications (1)

- *Cloud Security Alliance (CSA)* develops security guidance for the use and implementation of cloud computing
- *Distributed Management Task Force (DMTF)* has released whitepapers on cloud management and interoperability
- *IEEE P2302* develops standards covering topology, functions, and governance for cloud-to-cloud interoperability and federation.
- *ISO/IEC JTC 1 Subcommittee 27 (SC27) IT Security Techniques* develops international standards covering information security management systems, cryptography and security mechanisms, security evaluation criteria, security controls and services, and Identity management and privacy technologies
- *ISO/IEC JTC 1 Subcommittee 38 (SC38) Distributed Application Platforms and Services (DAPS)* develops international standards covering Web services, SOA, and cloud computing

Standards & Specifications (2)

- *Object Management Group (OMG)* is modeling cloud deployments for portability, interoperability & reuse
- *Open Cloud Consortium (OCC)* has developed a benchmark and is working on a reference model for large data clouds
- *Open Grid Forum (OGF)* has published an Open Cloud Computing Interface (OCCI) to standardize cloud management tasks
- *Storage Networking Industry Association (SNIA)* develops specifications for storage related technologies, including storage management (SMI-S) and cloud storage (Cloud Data Management Interface or CDMI)

Sample Cloud SDO Relationships



Security & Legal Issues for Cloud Computing

Top Security Concerns with Cloud

- Understanding how cloud services provide for the following:
  - Preserving confidentiality, integrity and availability
  - Maintaining appropriate levels of identity and access Control
  - Ensuring appropriate audit and compliance capability
- Dealing with loss of control
  - Physical and
  - Logical access
- Trusting the cloud service providers

Cloud Security (or Insecurity)

- Core Information Assurance issues to address:
  - Confidentiality
  - Integrity
  - Availability
  - Possession
  - Authenticity
  - Utility
  - Privacy
  - Authorized use
  - Non-repudiation
- Data loss and/or leakage measures become even more important
- Data aggregation changes the risk equation
- Legal and compliance forces require additional due diligence
- Forced exits and data disposition have to be carefully thought out
- Incident management become much more complicated

Possible Security Benefits

- Centralized data
- Segmented data and applications
- Better logging/accountability
- Standardized images for asset deployment
- Better resilience to attack & streamlined incident response
- More streamlined audit and compliance
- Better visibility to process
- Faster deployment of applications, services, etc.

Litigating in the Cloud

- Privacy and the Cloud
  - Sensitive information is potentially moving around the Internet within the cloud in violation of law
  - Data protection and security dependent on contractual terms and service level agreements
  - Data may be crossing national boundaries (possibly multiple jurisdictions)
- Digital Evidence and the Cloud
  - Amassing the forensic data from the various sources could be a serious challenge
  - Real-time nature of cloud services may reduce the amount and nature of digital evidence
  - The integrity and authenticity of data may be questionable (for example, inadequate protections against attacks)
- Electronic Discovery and the Cloud
  - Organizations will have additional challenges identifying relevant data because business units are directly leveraging the Cloud
  - Relevant data could be within the hands of a large number of third parties (suppliers to suppliers)

Jurisdictional Fog

- It has been said that possession is nine tenths of the law…that may not be the case for cloud
- It is often the situation that an entity has to have some physical presence in a country in order for a government to obtain access to the entity's data
- In the era of the cloud, however, all that may be required is a physical presence of the "cloud provider"
- This is not limited to just the U.S. Patriot Act (other law enforcement authorities have invoked similar provisions)

Cloud Security Resources

- SNIA Cloud Storage Initiative, http://www.snia.org/cloud
- Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Focus in Cloud Computing*, *Cloud Controls Matrix*, *Top Threats to Cloud Computing*, http://www.cloudsecurityalliance.org
- European Network and information Security Agency (ENISA), *Cloud Computing – Benefits, risks and recommendations for information security*, http://www.enisa.europa.eu/
- Information Systems Audit and Control Association (ISACA), *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, http://www.isaca.org
- *Cloud Security and Privacy*, Mather, Kumaraswamy, Latif, 2009, O' Reilly Publishing, ISBN: 978-0-596-80276-9

Key Activities in Cloud Computing Security

Cloud Security Alliance (CSA)

- CSA is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing
- The CSA objectives:
  - Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.
  - Promote independent research into best practices for cloud computing security.
  - Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.
  - Create consensus lists of issues and guidance for cloud security assurance.

CSA Cloud Security Guidance

Governance	Operations
Governance and Enterprise Risk Management	Traditional Security, Business Continuity and Disaster Recovery
Legal and Electronic Discovery	Data Center Operations
Compliance and Audit	Incident Response, Notification and Remediation
Information Lifecycle Management	Application Security
Portability and Interoperability	Encryption and Key Management
	Identity and Access Management
	Virtualization

NOTE: The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

SOURCE: Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, Version 3.0, 2011, http://www.cloudsecurityalliance.org

CSA Cloud Controls Matrix v1.2

- Provides mappings on
  - Architectural relevance (Physical, Network, Compute, Storage, Application, Data and Corporate Governance)
  - Delivery Models (SaaS, PaaS, IaaS)
  - Supplier relationships (Service Provider and Tenant)
- Not currently aligned with the CSA guidance v3
- Will be aligned with FedRAMP

- Compliance [6]
- Data Governance [8]
- Facility Security [8]
- Human Resources [3]
- Information Security [34]
- Legal [2]
- Operations Management [4]
- Risk Management [5]
- Release Management [5]
- Resiliency [8]
- Security Architecture [15]

CSA Top Threats v1.0

Education SNIA

#1: Abuse and Nefarious Use of Cloud Computing

#2: Insecure Interfaces and APIs

#3: Malicious Insiders

#4: Shared Technology Issues

#5: Data Loss or Leakage

#6: Account or Service Hijacking

#7: Unknown Risk Profile

ITU-T Study Focus Group on Cloud
(Threats for Cloud Security)

- For Cloud Service Users
  - Responsibility Ambiguity
  - Loss of Governance
  - Loss of Trust
  - Service Provider Lock-in
  - Cloud Service User Remote Access
  - Lack of Information/Asset Management
  - Data loss and leakage
  - Loss of Account/Service management

- For Cloud Service Providers
  - Responsibility Ambiguity
  - Protection Inconsistency
  - Evolutional Risks
  - Business Discontinuity
  - Supplier Lock-in
  - License Risks
  - Bylaw Conflict
  - Bad Integration
  - Unsecure Administration API
  - Shared Environment
  - Hypervisor Isolation Failure
  - Service Unavailability
  - Data Unreliability
  - Abuse Right of Cloud Service Provider

FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP)
- US Government-wide program
  - provides a standardized approach to security assessment,
  - authorization, and
  - continuous monitoring for cloud products and services.
- Relevant for
  - Cloud Service Providers (CSPs),
  - Third Party Assessment Organizations (3PAOs),
  - government employees and contractors working on FedRAMP projects, and
  - any outside organizations that want to use or understand the FedRAMP assessment process.
- More information at:

  http://www.gsa.gov/portal/category/102371

FedRAMP Security Controls

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Assessment & Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical & Environmental Protection (PE)
- Planning (PL)
- Risk Assessment (RA)
- System & Services Acquisition (SA)
- System & Communications Protection (SC)
- System & Information Integrity (SI)

NOTE: Security controls were selected from the NIST catalog of controls and enhancements as described in Special Publication 800-53 as revised

Cloud Storage

Cloud Storage in a Nutshell

- *"Cloud storage is a model of networked online storage where data is stored on virtualized pools of storage which are generally hosted by third parties."* - Wikipedia
- Cloud storage is:
  - made up of many distributed resources that act as one
  - fault tolerant through redundancy and distribution of data
  - durable through the creation of versioned copies
  - data replicas eventually consistent
- Advantages include:
  - Only pay for storage used
  - No need to install physical storage devices (credit card IT)
  - Relieved of storage management/maintenance/protection tasks
  - Immediate access to a broad range of resources and applications
  - Maybe…improved data security

Security Issues for Cloud Provider

- **Data confidentiality** – Is data encrypted at-rest? In transit? If so, who manages the keys?
- **Data segmentation assurances** – What are the assurances they provide which ensure that a tenant's data is kept isolated from others?
- **Data replication** – Are there locality controls on where data can or cannot physically reside?
- **Data sanitization policies** – Can they get rid of a tenant's data on demand? How long will that process take?
- **Incident Management** – How are security incidents handled? Who does breach notifications?
- **Independent assessment** – A 3rd party assessment that validates the provider's policies and claims would be mandatory

Security Summary of SNIA CDMI (ISO/IEC 17826)

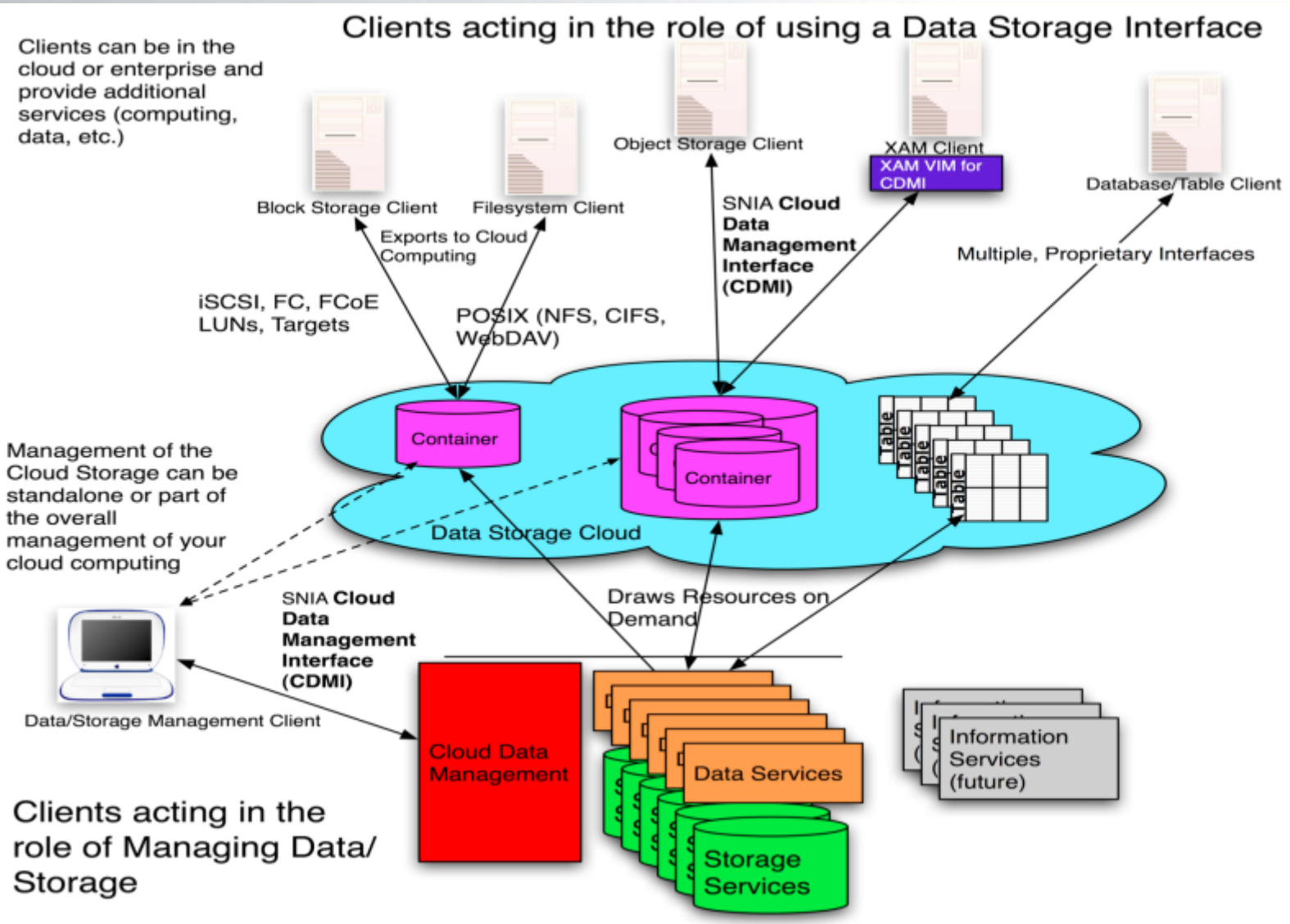
Cloud Data Management Interface

- Applicable to three types of cloud storage:
  - Cloud storage for cloud computing
    - Whitepaper at snia.org/cloud – the management interface for the lifecycle of storage in a compute cloud
  - Public storage cloud
    - Both a data path for the cloud and a management path for the cloud data
  - Private cloud storage
    - As well as hybrid clouds
    - An API for storage vendors selling into cloud based solutions
- Semantics
  - Simple containers and data objects with tagged metadata
  - Data system metadata expresses the data requirements
- Protocol
  - RESTful HTTP as "core" interface style
  - JSON (JavaScript Object Notation)– format of the representations are extensible

CDMI Data Objects

- Stored data can be accessed using native protocols:
  - HTTP, CIFS, NFS, iSCSI, SQL, etc.
- Stored data can also be accessed using CDMI as a Data Path in a standardized manner. This facilitates:
  - Cloud-to-cloud migration
  - Cloud federation
  - Cloud backup
  - Cloud virus scanning
  - Cloud search
  - And more.
- Desired cloud storage characteristics can be associated with stored data:
  - Replication, Compression, Placement, Retention, QoS, etc.

The Complete CDMI Picture



CDMI Security Summary

- Security refers to the protective measures employed in managing and accessing data and storage.
- Security measures:
  - Include transport security, user and entity authentication, authorization and access controls, data integrity, data and media sanitization, data retention, protections against malware, data at rest encryption, and security capability queries.
  - Take the form of mandatory, optional, and vendor extensions
- The transport security and security capability queries are mandatory for all implementation; all other security mechanisms are optional to implement.
- Client use of security is always optional, but encouraged.

CDMI Security Objectives

- Provide a mechanism that assures that the communications between a CDMI client and server cannot be read or modified by a third party
- Provide a mechanism that allows CDMI clients and servers to provide an assurance of their identity
- Provide a mechanism that allows control of the actions a CDMI client is permitted to perform on a CDMI server
- Provide a mechanism for records to be generated for actions performed by a CDMI client on a CDMI server
- Provide mechanisms to protect data at rest
- Provide a mechanism to eliminate data in a controlled manner
- Provide mechanisms to discover the security capabilities of a particular implementation

Exploiting the Mandatory and Optional Features

- Always check the security capabilities of your cloud service provider's CDMI implementation
  - Ensure it has adequate protective measures
  - Make a "risk" based decision to use a particular implementation
- Secure the communications
  - Use Transport Layer Security (TLS), preferably TLS 1.2
  - Authenticate CDMI entities (certificates for servers; HTTP authentication for clients)
  - Encrypt sensitive information communicated between CDMI entities.

Exploiting the Mandatory and Optional Features (cont.)

- Use Domains to provide a place for authentication mappings to external authentication providers
- Audit logging within the context of CDMI
  - Establish logging queues and restrict access
  - Capture messages for all security and data management events
  - Make sure the CDMI client retrieves the messages on a regular basis

Exploiting the Mandatory and Optional Features (cont.)

- Align the automatic deletion capability with the organization's data retention policy
- Prior to using Holds, understand the process and mechanism for lifting the Holds
- For cryptographic functionality, it is always important to verify that the implementation has complied with the requested algorithm; something other than what was requested may be used

Final Thoughts

Summary

- It is *possible* to engineer solutions across most cloud services today that meet or exceed the security provided within the enterprise…however, the capability to execute may not be a reality!
- The various value propositions of cloud (agility, low cost, scalability, security) are often conflated, suggesting all four can be achieved simultaneously and in equal proportions; this is a fallacy because trade-off are almost always required.

Cloud Security Tips

- Cloud-based security is not a substitute for existing ICT security…think defense in depth
- Understand the Terms of Service…this is the best you can expect
- Don't put anything in the cloud you wouldn't want someone else to see (government, competitor, or a private litigant)
- Placing consumer data in the cloud could put you at risk of violating the law…where is it?

Final Thoughts

- Security and legal issues will persist as challenges for organizations that choose to use cloud computing, but there are promising signs that some of these issues will be addressed.
- It is, however, extremely important to understand the risks and to enter the cloud with your eyes wide open (i.e., select a cloud service provider that offers an appropriate set of contractual terms and conditions as well as demonstrable risk mitigations).

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Other SNIA Security Tutorials

- Thursday (April 5th @ 8:30): *Storage Security - The ISO/IEC Standard*
- Thursday (April 5th @ 11:15): *Implementing Stored-Data Encryption*

Q&A / Feedback

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

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Eric A. Hibbard, CISSP, CISA

SNIA Security TWG

Subhash Sankuratripati

SNIA Cloud Storage TWG