SNIA

Education

STORAGE SECURITY TUTORIAL

With a focus on Cloud Storage

Gordon Arnold, IBM

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.

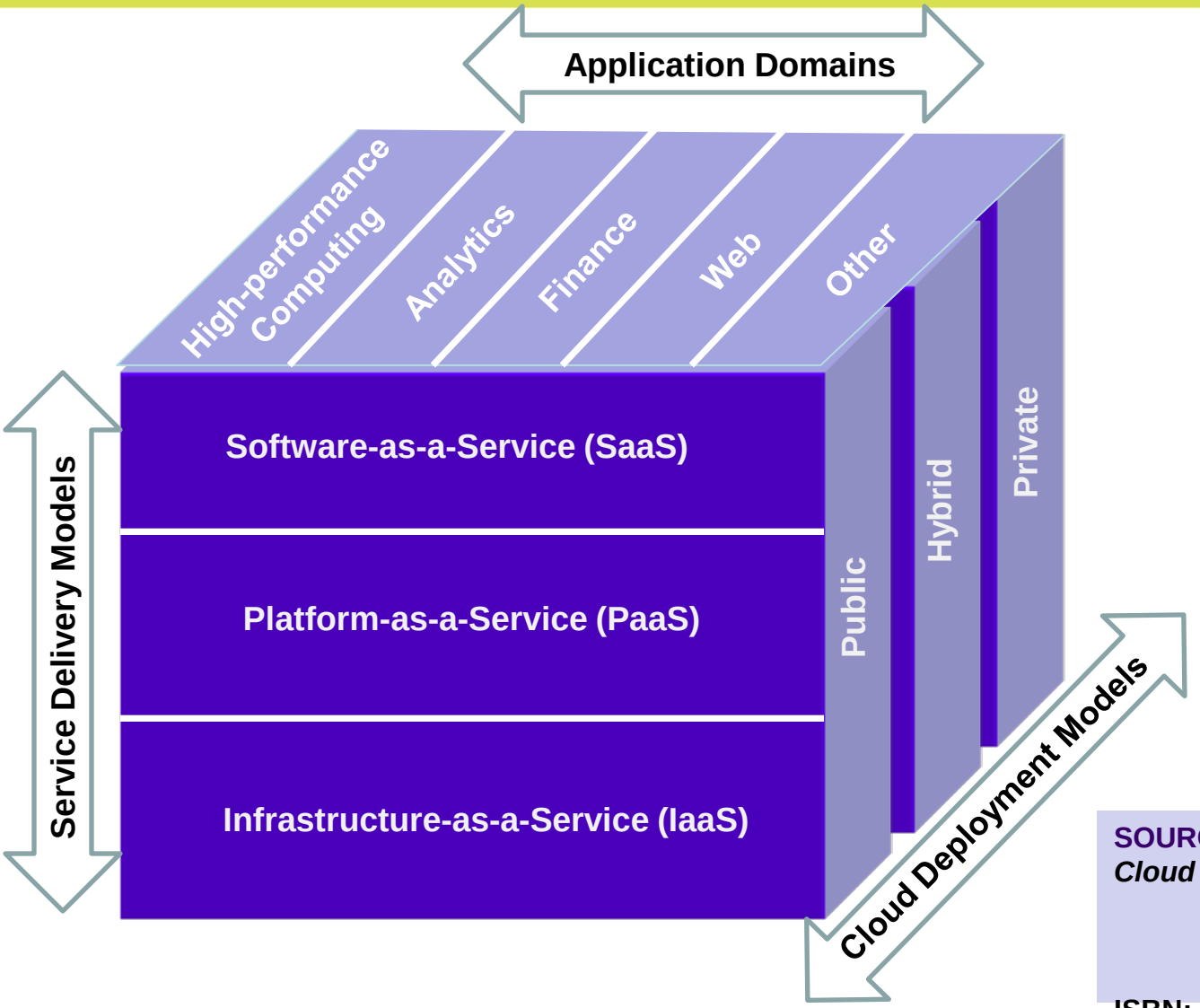
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Cloud Storage Security Introduction

- Introduction of computing and data services in a cloud service provider context exposes the customer's information to a new set of threats and vulnerabilities. This session provides an introduction to those threats and what techniques are available to mitigate the threats.

Cloud Models



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

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
- Trusting the cloud service providers

Cloud Security Concerns

- 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 becomes much more complicated

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 Computing 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 2.1, 2009, http://www.cloudsecurityalliance.org/guidance.

CSA Top Threats (1)

#1: Abuse and Nefarious Use of Cloud Computing

Impacted Services Models: IaaS & PaaS

Description: The illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process (that preserve anonymity)— has allowed spammers, malicious code authors, and other criminals to conduct their activities with relative impunity.

#2: Insecure Interfaces and APIs

Impacted Services Models: IaaS, PaaS, SaaS

Description: Software interfaces, exposed for customers to manage and interact with cloud services, interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

SOURCE: Cloud Security Alliance, *Top Threats to Cloud Computing*, Version 1.0, 2010, http://www.cloudsecurityalliance.org/topthreats.

CSA Top Threats (2)

Education SNIA

#3: Malicious Insiders

Impacted Services Models: IaaS, PaaS, SaaS

Description: The well known malicious insider threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure as well as little or no visibility into the hiring standards and practices for cloud employees, creating an attractive opportunity for an adversary.

#4: Shared Technology Issues

Impacted Services Models: IaaS

Description: IaaS vendors deliver their services in a scalable way by sharing infrastructure, which was not designed to offer strong isolation properties for a multi-tenant architecture, so appropriate security controls should be employed to ensure that individual customers do not impact the operations of other tenants and that customers do not have access to any other tenant's actual or residual data, network traffic, etc.

CSA Top Threats (3)

#5: Data Loss or Leakage

Impacted Services Models: IaaS, PaaS, SaaS

Description: The threat of data compromise (unauthorized access or corruption/destruction) increases in the cloud, due to the number of and interactions between risks and challenges, which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

#6: Account or Service Hijacking

Impacted Services Models: IaaS, PaaS, SaaS

Description: Although account or service hijacking is not new, cloud solutions add a new threat because a successful attacker (e.g., gains access to your credentials) can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites as well as use your account or service instances as a new base for the attacker, possibly leverage the power of your reputation to launch subsequent attacks.

CSA Top Threats (4)

#7: Unknown Risk Profile

Impacted Services Models: IaaS, PaaS, SaaS

Description: The features and functionality of a cloud service may be well advertised, but there may be few details (e.g., versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design) to help estimate your organization's security posture as well as little or no information on the cloud service provider's compliance of the internal security procedures, configuration hardening, patching, auditing, and logging. Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

CSA Cloud Control Matrix

- Control Area
  - Compliance - Audit Planning
    Compliance - Independent Audits
    Compliance - Third Party Audits
    Compliance - Contact / Authority Maintenance Compliance - Information System Regulatory Mapping
    Compliance - Intellectual Property
    Data Governance - Ownership / Stewardship Data Governance - Classification Data Governance - Handling / Labeling / Security Policy
    Data Governance - Retention Policy
    Data Governance - Secure Disposal
    Data Governance - Non-Production Data Data Governance - Information Leakage
- Scope Applicability
  - **SaaS PaaS IaaS Service Provider,**
  - Tenant
- Compliance Mapping
  - **COBIT 4.1**
  - **HIPAA / HITECH Act**
  - **ISO/IEC 27001-2005**
  - **NIST SP800-53 FedRAMP**
  - **PCI DSS v2.0**
  - **BITS Shared Assessments AUP v5.0 / SIG v6.0**
  - **GAPP (Aug 2009)**

Possible Security Benefits

- Centralized data
- Segregated 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.

- These are purported benefits of using cloud storage
- Can they be realized with the security challenges addressed?

Topics for Discussion

- Privileged user access
- Regulatory compliance
- Data location
- Data isolation and segregation
- Investigative support

Privileged User Access

- When your data is "in the cloud" instead of under your employee's direct control
  - Do you trust service providers to keep that data private and protected?
  - Once the data is in the cloud – can you even identify what administrators could potentially access or what data they could potentially alter?
    - For instance are they sub-contracting services
- You would like for the cloud to provide the services effectively without being able to read the sensitive or personally identifiable information in your data
  - Do your service level agreements cover who has access to your data?

Privileged User Access

- Do administrators of the cloud infrastructure have access to the customer data?
  - What storage administration tasks would expose customer data? – there should be a way to manage the data and recovery without being able to read the data
  - Separation of duties for different roles should be implemented
- One technical approach is to encrypt the data in transit and at rest
  - Is the data encrypted in the cloud and do the customers maintain control over the encryption keys?
    - This can be part of the solution
  - Can the encryption keys be safely and securely provided to encryption processes without an opportunity for compromise or the cloud having to retain those keys?
    - Often this results in customer management of keys for data stored in the cloud
- Can the cloud perform all the operations related to data availability and integrity without being able to read the data – except in encrypted form?
  - For instance can a copy of media be made without having to decrypt data?

Regulatory Compliance

- You and your customers will be subject to various regulations
  - Will the service provider be able to supply the necessary documentation for compliance?
    - Review the documentation and audit information which the service provider is able to provide
  - Is the documentation related to treatment of customer data sufficient to meet requirements for compliance?
    - For instance can a proof of encryption document be produced for any case of loss of physical storage media?
      - Ask if the documentation which would be provided is sufficient to invoke the safe harbor provisions of the privacy disclosure laws you may be subject to

Regulatory Compliance

- What is the documentation of compliance by the cloud provider and what are the compensating controls required to meet the compliance requirements?
  - How much trust can you put in representations – is the service agreement language sufficient to protect your interests?
- If the service provider is not able to meet your compliance requirements can you segregate the data and applications which can not be hosted in the cloud versus those you have to separate services?
  - You may be doing data classification to decide what data is appropriate for hosting in the cloud
  - You may take a granular approach (by application or business line) but fine grained classification can be a challenge

Data Location

- Do the customer's requirements limit where their data can be physically located?
  - Primary and any copies for recovery and availability
  - You may know about the primary data center location (or not) but there may be copies of the data outside of the country for recovery or archive functions
- National and regional laws may limit the ability to move data outside of national boundaries
  - EU privacy directive has specific restrictions on personally identifiable information being moved outside of the EU
  - State specific laws like those in Massachusetts and Nevada have specific restrictions on treatment of their citizens' data

Data Isolation and Segregation

- In the cloud – can different customers' data be isolated despite the shared infrastructure?
- Is the security implemented such that shared infrastructure or a multi-tenancy is supported without introducing compromises of the customer's data security?
- Do you pay extra for dedicated infrastructure or share infrastructure with the security able to partition the infrastructure?
  - virtual private cloud?

Data Isolation and Segregation

- Consider the workflow in the case where:
  - You want to rent computational capacity for business intelligence analytics on a monthly basis
  - You have to transfer the data to cloud for the processing
  - After the processing is complete how is the data cleansed from the cloud?
    - Data overwrites
    - Crypto erasure or shredding

Investigative Support

- When processing and storing the customer's data
  - Are there sufficient audit trails around creation, access, modification, destruction of data?
  - Can you attest to the accuracy of the data?
  - Is there a chain of custody defined for retrieval of data?
  - Is there a facility for a trusted third party for dispute resolution over data?
  - Is there a provision for snapshots of all customer data at a point in time?

Audit trails

- Are there sufficient audit trails around creation, access, modification, destruction of data?
  - Whenever anyone touches the data
    - Is there an audit record written?
    - Are those records kept in a tamper proof way?
      - Could a privileged used cover their tracks?
    - Is an attestation of data destruction available?

Data Provenance

- Can the accuracy of the data be attested?
  - Are digital signatures or hashes available to verify if data has been modified without the owner's knowledge?
    - Originator's application may support digital signatures,
    - Enterprises may provide an edge-of-enterprise gateway that adds digital signatures, or
    - The service provider may provide a hash of the data as it is ingested
  - Encryption may not be sufficient
    - Some encryption mode of operations (cypher blocking modes) may not be able to detect substitution of cypher blocks – need chaining

Chain of Custody

- Is there a chain of custody defined for retrieval of data?
  - Provenance
    - Can you prove who created the data and that the data retrieved was exactly the data supplied by the originator?
  - If there was a legal discovery or law enforcement request can you provide the data in a way that will satisfy a court?
    - You can't just pull the disk drives out of a common service…

Dispute resolution

- Is there a facility for a trusted third party for dispute resolution over data?
  - Is there the legal framework in place for a trusted third party to escrow and make data available in case there is a dispute?
    - Who sent what when?
    - Was it actually delivered – is the delivery receipt mechanism or proof of retrieval?
    - Is there an ability to restrict access to the matter in question?
    - Is there an ability to filter out PII or other data which may not be appropriate to disclose?
- This may come with cloud services where before there was not the possibility of the 3rd party being involved in a business to business transaction

Investigative Support

- Is there a provision for snapshots of all customer data at a point in time?
  - Fraud or other types of investigations may require a snapshot of the state of a company's representations, for instance
    - The state of messages which have flowed back and forth
    - The statements on a portal or web site
    - Files which may have been shared
    - Users' interactions with SaaS applications
  - For example – a dispute over an order when price, quantity, delivery dates, etc. are in question

Data Security Track Tutorials

- Including Storage Security Best Practices

Check out the other data security SNIA Tutorials:

Q&A / Feedback

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

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

- SNIA Education Committee

Gordon Arnold, IBM
Eric Hibbard, HDS
Larry Hofer, Emulex

SNIA Security TWG

SNIA Cloud TWG