Key Management Issues in the Cloud Infrastructure

Dr. R. Chandramouli (Mouli) mouli@nist.gov

Dr. Michaela Iorga – michaela.iorga@nist.gov

(Information Technology Lab, NIST, USA)

ARO Workshop on Cloud Computing

March 11-12, 2013

George Mason University, Fairfax, VA, USA

Key Management - background

- SP 800-57-part1 describes twenty different key types;
  - **Main Categories**: encryption, authentication, authorization, signature, key wrapping, key transport, key agreement, master key, RNG.
- SP 800-130: Key &Metadata Management
  - **Main Key Functions**: generation, registration, storage, (de)activation, revocation, establishment, deletion, recovery, validation, archiving

Challenges in the Cloud

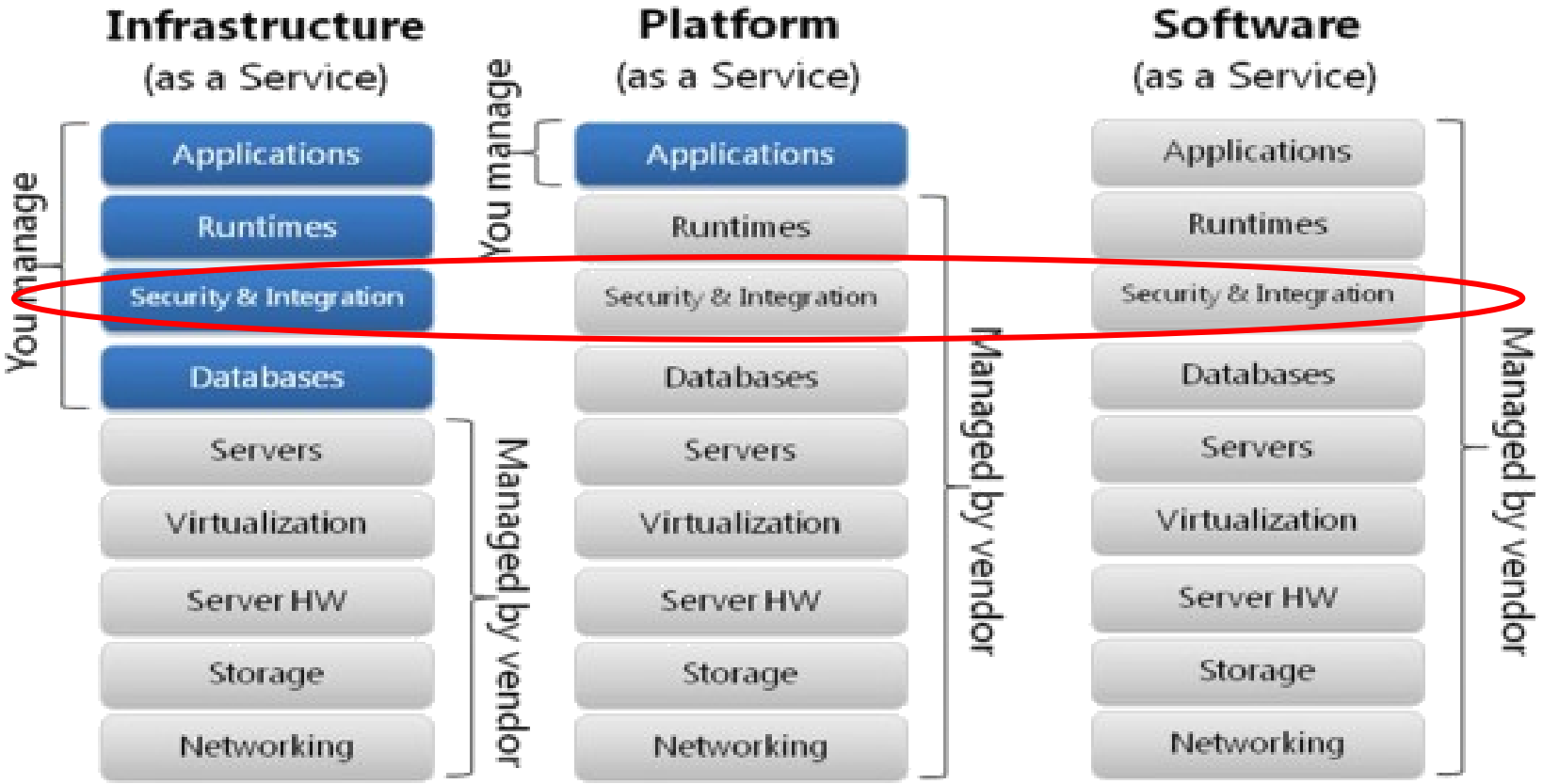
- Data protection (confidentiality & integrity) and privacy in multi-tenancy environment requires encryption **at rest** & **in transit**
- ID Authentication and Authorizations is as strong as **Key Management** is
- Backup Data Protection (confidentiality & integrity) - encryption prevents data misuse & protects when media is lost or stolen

Challenges in the Cloud

- Secure key stores
- Access to key stores
- Key backup and recoverability
- Protecting the keys from theft when they are in use
- Storing and managing the encryption keys
- Managing the encryption process
- Securing the data lifecycle

Who can do it?

Cloud Service Models and Data Protection



Courtesy of CIO Research Council (CRC)

Key Management Issues in Cloud Infrastructures – Outline

(*Cloud Consumer Perspective*)

- Cryptographic Operations within Overall Cloud Data Protection
- Encryption Requirements for Data in the Cloud
- Message Authentication Codes & Digital Signatures - Scope
- Common Cryptographic Operations in Cloud Use Cases
- Cryptographic Operations in SaaS, PaaS & IaaS Use Cases
- KM Issues for IaaS Cloud Consumers
- Contacts & Questions (?)

Cryptographic Operations within Overall Cloud Data Protection

Cloud Data Protection Approaches

(1) Network-Centric Approaches – Firewalls, IDS/IPS etc

(2) **Data Encryption –** Making Data unreadable & unusable

(3) Access Control Mechanisms – MAC, DAC, RBAC etc

(4) Security Monitoring – Alert Generation & Log Analysis (DAP, SIEM etc)

(5) **Attaching Digital Signatures & Message Authentication Codes** while delivering Data (*sometimes not considered as part of Data Protection Approaches per se*)

Encryption Requirements for Data in the Cloud

- Encryption should be applied **to**
  - Data at Rest (e.g., Encryption of Data in Virtual Disks used by Virtual Machines (VMs))
  - Data in Transit (e.g., Encryption of Data while Cloud Consumers send data from their from in-house sources or download data from Cloud-based Servers)
  - Data that is backed up and Archived

Encryption Requirements for Data in the Cloud (Contd..)

- Encryption of Data at Rest should include
  - Structured Data – (e.g., Transparent encryption within Databases)
  - Unstructured Data (e.g., Encryption of Files, File Folders, Disk Volumes, other forms of Data Repositories)

Message Authentication Codes & Digital Signatures - Scope

- Attached to Data transmitted over insecure communication channels
- Also needed for certain classes of stored data to obtain assurance about their source and integrity (e.g., Cloud Infrastructure Logs)

  - To ensure that log entries were generated by a certified Log Generation System
  - To ensure that log entries have not been tampered to obscure attack patterns or illegal insider access

Common Cryptographic Operations in Cloud Use Cases

- **CCO-UC-1**: *Certificate-based Authentication of Cloud Clients to Cloud Servers* – **Key Management not an Issue – Private Keys Under the control of Cloud Customer**

- **CCO-UC-2:** *Setting up secure communication session between Cloud Clients and CSP-Managed Cloud Servers* (Setting up Session Keys after one-way or two-way authentication using certificates – e.g., SSL/TLS) – **Key Management not an Issue as the KMS is fully under the control of respective parties – Cloud Consumer and CSP.**

Cryptographic Operations in SaaS Use Cases

SaaS-UC-1: Bulk Upload/Download feature provided by some SaaS providers

- If this feature supported with encryption, long lived symmetric keys are needed (Joint KM responsibility)

SaaS-UC-2: CSP uses database encryption for storing SaaS application Data

- ***KMS processes*** *(Quality of Keys, Key Storage & Key Recovery Mechanisms (customer data at stake) are of concern)* – ***CAN ONLY BE ADDRESSED USING SLAs***

Cryptographic Operations in PaaS Use Cases

PaaS-UC-1: Authenticated Access to CSP-Managed Cloud Servers used for Application Development - *Certificate-based Authentication of Cloud Clients to Cloud Servers (CCO-UC-1) – No KM Issues (Private keys under control of Cloud Consumer)*

PaaS-UC-2: Setting up a Secure Session with CSP-Managed Cloud Servers used for Application Development - *Setting up secure communication session between Cloud Clients and CSP-Managed Cloud Servers (CCO-UC-2) – No KM Issues*

Cryptographic Operations in Platform as a Service Use Cases (contd..)

PaaS-UC-3: Authenticated Access to Cloud Consumer's Development VM Instances - *Certificate-based Authentication of Cloud Clients to Cloud Servers (CCO-UC-1) – No KM Issues*

PaaS-UC-4: Setting up a Secure Session with Cloud Consumer's Development VM Instances –

KM is an Issue as the Cloud Consumer needs to run a KMS in the Cloud Infrastructure

Cryptographic Operations IaaS Use Cases

- **IaaS-UC-1: Authenticated Access to Cloud Consumer's Running VM Instances** - *Certificate-based Authentication of Cloud Clients to Cloud Servers (CCO-UC-1) – No KM Issues*
- **IaaS-UC-2: Encryption of Data traveling inside CSP network** (between a Web Server VM and Database Server VM)
- **IaaS-UC-3: Encryption of Data for storage in a Database**
- **IaaS-UC-4: Digitally signing a data sent as response to a Query from Cloud Customer**

(***For the last three Use Cases, KM is an Issue as the Cloud Consumer needs to run a KMS in the Cloud Infrastructure***)

Common Cryptographic–Related Operation in all IaaS Use Cases

- **IaaS-UC-O: Cloud Consumer Programs retrieve Keys from Key Store for use in all Cryptographic Operations** (e.g., Encrypting/Decrypting Data, Generating Digital Signature)

  - **KM is an Issue**

  - How to counter the threat of Key Exposure when keys are retrieved, loaded and used in the memory of Cloud Consumer's VM Instances

KM Issues for IaaS Cloud Consumers

- **It is obvious that IaaS Cloud Consumers need to run a KMS in the Cloud Infrastructure**

  - Run a KMS version in each VM (where keys are used) **OR**

    Run a Centralized KMS in a dedicated VM

  - Where can the HSM support for KMS come from

  - If a Centralized KMS is run

    - VMs needing the keys become the client of KMS

    - Need for a standardized Key Management Interoperability Protocol (KMIP) that must be provably Secure

Contacts & Questions

- **Contacts**:

  Dr. Ramaswamy Chandramouli (mouli@nist.gov)

  Dr. Michaela Iorga (michaela.iorga@nist.gov)

  Computer Security Division – Information Technology Lab

  National Institute of Standards and Technology

  Gaithersburg, MD, USA

- **Questions (?)**: