Practical Advice for Cloud Data Protection

Ulf Mattsson
CTO, Protegrity

Ulf.Mattsson@protegrity.com

protecting your data.
protecting your business.
UlF Mattsson, Protegrity CTO

- Cloud Security Alliance (CSA)
- PCI Security Standards Council
  - Cloud & Virtualization SIGs
  - Encryption Task Force
  - Tokenization Task Force
- ANSI X9
  - American National Standard for Financial Services
- IFIP WG 11.3 Data and Application Security
  - International Federation for Information Processing
- ISACA (Information Systems Audit and Control Association)
- ISSA (Information Systems Security Association)
“It’s clear the bad guys are winning at a faster rate than the good guys are winning, and we’ve got to solve that.”

- 2014 Verizon Data Breach Investigations Report

“...Even though security is improving, things are getting worse faster, so we're losing ground even as we improve.”

- Security expert Bruce Schneier

Key Topics

- What are the Concerns with Cloud?
- What is the Guidance for Cloud Data Security?
- What New Data Security Technologies are Available for Cloud?
- How can Cloud Data Security work in Context to the Enterprise?
- What are the Common Use Cases?
- How can Search and Indexing be Performed?
What are the Concerns with Cloud?
What Is Your No. 1 Issue Slowing Adoption of Public Cloud Computing?
82%

Of organizations currently (or plan to) transfer sensitive/confidential data to the cloud in the next 24 mo.
Lack of Cloud Confidence

Number of survey respondents that either agree or are unsure that the cloud services used by their organization are NOT thoroughly vetted for security.

2/3
Stopped or Slowed Adoption

Cloud computing applications that are not vetted for risks are not used
- 41%
- 51%

Assessment of the affect of cloud computing on the ability to protect confidential information
- 44%
- 50%

IT leaders are concerned about the security of cloud computing resources
- 51%
- 48%

Proactive assessments of information that is too sensitive be stored in the cloud
- 38%
- 43%

Audits or assessments of cloud computing resources are conducted before deployment
- 36%
- 43%

Cloud computing presents a more secure environment than on-premises computing
- 29%
- 35%

Source: The State of Cloud Security

Blue: Most recent data
Data Loss & Insecure Interfaces

Number of Cloud Vulnerability Incidents by Threat Category
What is Cloud Computing?

Computing as a Service:
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Delivered Internally or Externally to the Enterprise:
- Public
- Private
- Community
- Hybrid
Public Cloud
Public Cloud

Cloud Consumers accessing the cloud over a network.
On-site Community Cloud

Organizations providing and consuming cloud resources.

Organizations consuming cloud resources.
Outsourced Community Cloud
Hybrid Cloud
Service Orchestration

- **Software as a Service (SaaS)**
  Typically web accessed internet-based applications ("on-demand software")

- **Platform as a Service (PaaS)**
  An internet-based computing platform and solution stack. Facilitates deployment of applications at much lower cost and complexity

- **Infrastructure as a Service (IaaS)**
  Delivers computer infrastructure (typically a virtualized environment) along with raw storage and networking built-in
The Conceptual Reference Model

Cloud Provider

- Service Orchestration
  - Service Layer
    - SaaS
    - PaaS
    - IaaS
  - Resource Abstraction and Control Layer
  - Physical Resource Layer
    - Hardware
    - Facility

Cloud Service Management

- Business Support
- Provisioning/Configuration
- Portability/Interoperability

Security

Privacy

Cloud Broker

- Service Intermediation
- Service Aggregation
- Service Arbitrage

Cloud Consumer

Cloud Auditor

- Security Audit
- Privacy Impact Audit
- Performance Audit

Cloud Carrier
Governance, Risk Management and Compliance
Trust vs. Elasticity

Trust

Corporate Network

Private Cloud

Public Cloud

Elasticity
Consumers have no control over security once data is inside the public cloud. Completely reliant on provider for application and storage security.
Private Cloud – Limited Control

Outsourced Private Cloud

Consumer has limited capability to manage security within outsourced IaaS private cloud.

On-site Private Cloud

Cloud Consumers accessing the cloud from within the enterprise network.
Threat Vector Inheritance

- SAAS Tenant 1
- SAAS Tenant 1
- SAAS Tenant 1

- Traditional Web Threats / Vulnerabilities

- Additional Threat Vectors
Virtualization Concerns in Cloud

- Virtual machine guest hardening
- Hypervisor security
- Inter-VM attacks and blind spots
- Performance concerns
- Operational complexity from VM sprawl
- Instant-on gaps

- Virtual machine encryption
- Data comingling
  - Virtual machine data destruction
  - Virtual machine image tampering
- In-motion virtual machines
<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>Example responsibility assignment for management of controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
<td>IaaS</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>Both</td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
<td>Both</td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
<td>Client</td>
</tr>
<tr>
<td>5. Use and regularly update anti-virus software or programs</td>
<td>Client</td>
</tr>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
<td>Both</td>
</tr>
<tr>
<td>7. Restrict access to cardholder data by business need to know</td>
<td>Both</td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access</td>
<td>Both</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
<td>CSP</td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data</td>
<td>Both</td>
</tr>
<tr>
<td>11. Regularly test security systems and processes</td>
<td>Both</td>
</tr>
<tr>
<td>12. Maintain a policy that addresses information security for all personnel</td>
<td>Both</td>
</tr>
<tr>
<td>PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</td>
<td>CSP</td>
</tr>
</tbody>
</table>
Mapping the Cloud Model to Security Control & Compliance

Cloud Model
- Presentation Mobility
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content
- Integration & Middleware
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities

Find the Gaps!

Security Control Model
- Applications
  - SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- Information
  - DLP, CMF, Database Activity Monitoring, Encryption
- Management
  - GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- Network
  - NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- Trusted Computing
  - Hardware & Software RoT & API's
- Compute & Storage
  - Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
- Physical
  - Physical Plant Security, CCTV, Guards

Compliance Model
- PCI
  - Firewalls
  - Code Review
  - WAF
  - Encryption
  - Unique User IDs
  - Anti-Virus
  - Monitoring/IDA/IPS
  - Patch/Vulnerability Management
  - Physical Access Control
  - Two-Factor Authentication...
- HIPAA
- GLBA
- SOX
Governance, Risk Management and Compliance

An Integrated Suite of Four CSA Initiatives

Cloud Audit
The A6 Working Group

Cloud Controls Matrix

Consensus Assessments Initiative

Cloud Trust Protocol
Cloud Gateways Provide Enterprise Control

- Cloud Encryption Gateways
  - SaaS encryption

- Cloud Security Gateways
  - Policy enforcement
    - Cloud Access Security Brokers (CASBs)
    - Cloud Services Brokerage (CSB)
    - Secure Email Gateways
    - Secure Web gateway
Public Cloud Gateway – SaaS Example
Security Gateway Deployment – Application Example
Example of Cloud Security Gateway Features

- High-Performance Gateway Architecture
- Enterprise-extensible platform
- Tokenization and encryption
- Enterprise-grade key management
- Flexible policy controls
  - File or Field Security
  - Advanced function & usability preservation
- Comprehensive activity monitoring & reporting
- Support for internal, remote & mobile users
- Multiple deployment options
Security Gateway Deployment – Database Example

Corporate Network

Backend System

Cloud Gateway

RDBMS

Enterprise Security Administrator

Security Officer
Security Gateway Deployment – Indexing

Corporate Network

Backend System

Query re-write

Cloud Gateway

Index

RDBMS

Index

Enterprise Security Administrator

Security Officer
Security Gateway Deployment – Search

Corporate Network

Backend System

Cloud Gateway

Query re-write

Enterprise Security Administrator

Security Officer

RDBMS

Order preserving encryption

ORACLE

protegrity

037
Where is Encryption Applied to Protect Data in Cloud?

- Your organization encrypts data during its transfer through networks: 38%
- Your organization encrypts data before it is transferred to a cloud provider: 35%
- Your organization selectively encrypts at the application layer within the cloud environment: 16%
- Your cloud provider encrypts stored data as a service to your organization: 11%
How Data-Centric Protection Increases Security in Cloud Computing and Virtualization

- Rather than making the protection platform based, the security is applied directly to the data, protecting it wherever it goes, in any environment.

- Cloud environments by nature have more access points and cannot be disconnected – data-centric protection reduces the reliance on controlling the high number of access points.
Encryption Guidance from CSA

- Encrypting the transfer of data to the cloud does not ensure the data is protected in the cloud.
- Once data arrives in the cloud, it should remain protected both at rest and in use.
- Do not forget to protect files that are often overlooked, but which frequently include sensitive information.
  - Log files and metadata can be avenues for data leakage.
- Encrypt using sufficiently durable encryption strengths (such as AES-256).
- Use open, validated formats and avoid proprietary encryption formats wherever possible.
Data Anonymization and De-identification

- This is where (for example) Personally Identifiable Information (PII) and Sensitive are stripped before processing.

Utilizing access controls built into the database
## De-identification / Anonymization

<table>
<thead>
<tr>
<th>Field</th>
<th>Real Data</th>
<th>Tokenized / Pseudonymized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Joe Smith</td>
<td>csu wusoj</td>
</tr>
<tr>
<td>Address</td>
<td>100 Main Street, Pleasantville, CA</td>
<td>476 srtacoe, cysieondusbak, CA</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>12/25/1966</td>
<td>01/02/1966</td>
</tr>
<tr>
<td>Telephone</td>
<td>760-278-3389</td>
<td>760-389-2289</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td><a href="mailto:joe.smith@surferdude.org">joe.smith@surferdude.org</a></td>
<td><a href="mailto:eoe.nwuer@beusorpdqo.org">eoe.nwuer@beusorpdqo.org</a></td>
</tr>
<tr>
<td>SSN</td>
<td>076-39-2778</td>
<td>076-28-3390</td>
</tr>
<tr>
<td>CC Number</td>
<td>3678 2289 3907 3378</td>
<td>3846 2290 3371 3378</td>
</tr>
<tr>
<td>Fingerprint</td>
<td><img src="image" alt="Fingerprint" /></td>
<td>Encrypted</td>
</tr>
<tr>
<td>Photo</td>
<td><img src="image" alt="Photo" /></td>
<td>Encrypted</td>
</tr>
<tr>
<td>X-Ray</td>
<td><img src="image" alt="X-Ray" /></td>
<td>Encrypted</td>
</tr>
<tr>
<td>Healthcare / Financial Services</td>
<td>Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities</td>
<td>Protection methods can be equally applied to the actual data, but not needed with de-identification</td>
</tr>
</tbody>
</table>
Data Tokenization

- De-identification / Pseudonymization / Anonymization
- Replaces real data with fake data – “Tokens”
- Data is protected before it goes to the cloud

Benefits:
- Eliminates data residency issues
- Data remains usable in applications without modification
- Vaultless tokenization
  - No data replication/collision issues
  - High scalability
## Significantly Different Tokenization Approaches

<table>
<thead>
<tr>
<th>Property</th>
<th>Dynamic</th>
<th>Pre-generated</th>
<th>Vaultless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footprint</td>
<td>Large, Expanding</td>
<td>Large, Static</td>
<td>Small, Static</td>
</tr>
<tr>
<td>Replication</td>
<td>Complex replication</td>
<td>No replication required</td>
<td>No replication required</td>
</tr>
<tr>
<td></td>
<td>required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collisions</td>
<td>Prone to collisions</td>
<td>No collisions</td>
<td>No collisions</td>
</tr>
<tr>
<td>Latency / Performance</td>
<td>Will impact performance</td>
<td>Will impact performance</td>
<td>Little or no latency</td>
</tr>
<tr>
<td></td>
<td>and scalability</td>
<td>and scalability</td>
<td>Fastest tokenization in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Faster than the</td>
<td>industry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traditional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dynamic approach</td>
<td></td>
</tr>
<tr>
<td>Tokenizing many data categories</td>
<td>Potentially impossible</td>
<td>Potentially impossible</td>
<td>Can tokenize many data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>categories with minimal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or no impact on footprint</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or performance</td>
</tr>
</tbody>
</table>
The company received trade files from customers daily, containing sensitive Card Holder Data (CHD), making them subject to Payment Card Industry Data Security Standard (PCI DSS) regulations.
Use Case - Increasing Pressure from International Data Protection Regulations
Enterprise Data Security Policy

What
What is the sensitive data that needs to be protected.

How
How you want to protect and present sensitive data. There are several methods for protecting sensitive data. Encryption, tokenization, monitoring, etc.

Who
Who should have access to sensitive data and who should not. Security access control. Roles & Users

When
When should sensitive data access be granted to those who have access. Day of week, time of day.

Where
Where is the sensitive data stored? This will be where the policy is enforced.

Audit
Audit authorized or un-authorized access to sensitive data.
Centralized Policy Management - Example

Enterprise Security Administrator

RDBMS
- Audit Log

MPP
- Audit Log

Big Data
- Audit Log

IBM Mainframe Protector
- Audit Log

HP NonStop Base24
- Audit Log

File Servers
- Audit Log

Gateway Servers
- Audit Log

Protection Servers
- Audit Log

Gateway
- Audit Log

Cloud
- Audit Log

Security Officer

Application

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log

Audit Log
Summary

- What are the Concerns with Cloud?
- How is Cloud Computing Defined?
- What is the Guidance for Cloud Data Security?
- What New Data Security Technologies are Available for Cloud?
- How can Cloud Data Security work in Context to the Enterprise?
Thank you!

Questions?

Please contact us for more information

www.protegrity.com

Ulf.Mattsson@protegrity.com