Securely Managing Cryptographic Keys used within a Cloud Environment

Dr. Sarbari Gupta
sarbari@electrosoft-inc.com
703-437-9451 ext 12

2012 NIST Cryptographic Key Management Workshop
September 10-11, 2012
Introduction

- Federal government moving computing/storage to Cloud
  - Vivek Kundra’s Cloud First Strategy
  - OMB M-10-19 – FY 2012 Budget Guidance

- Cloud Computing has unique security challenges
  - Remote operations, Co-tenancy, Distributed Management

- Cryptography essential to secure cloud operations
  - Use of sound Key Management Practices is critical
  - Yet, limited visibility into Cloud Key Management

- FedRAMP streamlines Cloud Authorizations
  - Does it provide enough visibility or assurance for Cloud Key Management?
Cloud Service Provider (CSP) - Models

- Cloud Service Models
  - Software as a Service (SaaS) - Access to applications and services hosted in cloud
  - Platform as a Service (PaaS) - Building blocks to rapidly develop/host cloud applications
  - Infrastructure as a Service (IaaS) - processing power, storage

- Cloud Deployment Models
  - Public Cloud
  - Private Cloud
  - Community Cloud
  - Hybrid Cloud

- Not all Clouds are created equal!
Cloud Based Systems – Uncertainties

- **Processor**
  - Where is my process running?
  - Am I sharing the processor with other users/organizations?

- **Data Storage**
  - Where does my data reside?
  - Is my data co-resident with other users’ data?

- **Communication**
  - How does my CSP know who I am?
  - How is my connection to cloud components protected?

- **Administration**
  - Who administers the Cloud Infrastructure?
  - Who has access to my data? My activity history?

- **Key Management**
  - Where and how are keys: Generated? Stored?
  - How are keys: Distributed? Protected?
  - How are keys and data recovered if lost?
  - When and how are keys destroyed?
Cloud Systems – Dependence on Browser

- **Browser is integral to Cloud Systems**
  - User Interface – Presentation
  - Data input and output from Cloud
  - Communication with Cloud Components

- **Browsers have significant vulnerabilities**
  - Weak implementation of security protocols
  - Man-in-the-middle (MITM) and other attacks
  - Browser contamination from other websites

- **Browser represents inherent weakness!**
Cryptography Integral to Cloud Operations

- Supports strong authentication of remote Users, Administrators
- Implements strong communication protocols between User (browser) and cloud
- Partitions User data in co-tenancy environments
- Provides data confidentiality (even from Administrators)
- Supports data integrity (tamper-detection)
Cryptographic Key Management – Basics (I)

- Cryptographic Keys - Core Functions
  - Confidentiality
  - Integrity
  - Source Authentication

- Key Management - Scope
  - Key Generation
  - Key Storage
  - Key Distribution
  - Key Recovery
  - Key Destruction
Cryptographic Key Management – Basics (II)

- Key Management - Critical Dimensions
  - *Key Type, Algorithms, Strength, Crypto-period, Metadata*
  - *Key Generation, Acquisition*
  - *Key Use, Users, Applications*
  - *Key Establishment, Agreement, Distribution*
  - *Key Material Protection (storage, transit)*
  - *Key Access Control*
  - *Key Backup, Recovery*
  - *Key Renewal, Revocation, Destruction*
Cloud Cryptography – Visibility and Control

- Remote Authentication; Secure Communication with Cloud
  - Some Visibility
    - Use of Third Party Credential Providers; Standard Communication Protocols (TLS/SSL)
  - Some Control
    - User may select own Credential Provider, Configure Browser settings

- Cloud Data Protection (Confidentiality, Integrity)
  - SaaS - no visibility; no control
    - CSP implements all crypto – opaque to Cloud User
  - PaaS – limited visibility; limited control
    - CSP implements crypto in lower layers – opaque to Cloud User
    - May provide toolset (building blocks) for application development
  - IaaS – limited visibility; more control
    - CSP implements infrastructure level crypto – opaque to Cloud User
    - Cloud User controls key management for virtualized IT components
FedRAMP Control for Key Management (based on SP 800-53 R3)

- **SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
  - **Control:** The organization establishes and manages cryptographic keys for required cryptography employed within the information system.
  - **Control Enhancements for MODERATE baseline:**
    - (2) The organization produces, controls, and distributes symmetric cryptographic keys using [NIST-approved] key management technology and processes.
    - (5) The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key.

- **SC-13 USE OF CRYPTOGRAPHY**
  - **Control:** The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
  - **Control Enhancements for MODERATE baseline:**
    - (1) The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.
FedRAMP Weaknesses for Key Management

- No minimum requirements for key parameters
- No explicit requirement for Key Management Policy (KMP)
- No explicit requirement for Key Management Practices Statement (KMPS)
- No requirement for key recovery

Result – Cloud User has:
- Little visibility into cloud key management
- Limited assurance of soundness of key management policies, practices and operations
Way Forward

- **Establish Federal Profile for Cloud Key Management**
  - *Based on SP 800-152 (being developed)*
  - *More stringent requirements due to Cloud Environment*

- **FedRAMP require that CSPs**
  - *Follow Federal Profile for Cloud Key Management*
  - *Develop Key Management Plan (KMP) and Key Management Practices Statements (KMPS)*
    - NIST SP 800-57– Part 2: Best Practices for Key Management Organization
  - *Have Mandatory 3rd Party Auditing against KMP/KMPS*
Dr. Sarbari Gupta – Electrosoft

- **Email:** sarbari@electrosoft-inc.com
- **Phone:** 703-437-9451 ext 12
- **LinkedIn:** [http://www.linkedin.com/profile/view?id=8759633](http://www.linkedin.com/profile/view?id=8759633)