The 10th International Scientific Conference
“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”
Braşov, November 13th 2015

CRYPTOGRAPHIC KEY MANAGEMENT IN CLOUD COMPUTING

Maj. Florin OGÎGĂU-NEAMȚIU

Regional Department of Defense Resources Management Studies/Braşov/Romania

Abstract:

Cloud security has gained increasingly emphasis in the research community, with much focus primary concentrated on how to secure the operation system and virtual machine on which cloud system runs on. Companies considering moving to a cloud based infrastructure need to understand various aspects of specific encryption and key management – regulation guidelines, the impact of key status on application performance and the differences between the software and hardware key management implementations.

Key words: cryptography, key management, encryption, cloud computing, security protocols, standards

1. Introduction

Cloud computing is the technology that uses network connectivity and central remote servers to store and manage data and to run applications. Since its appearance cloud computing proved its ROI advantages to managers and has become an important business model where computational resources are rented to customers by providers. The key term for cloud computing is the virtualization technology, not a new one but a “reinvented" one with the full advantages of the hardware and software developments which appeared since its discovery.

Since its appearance, even if the technology promised great advantages to stakeholders, cloud computing spread has been limited by the security risks implied by outsourcing data to third party infrastructure. Traditional network architecture with its local data storing and manipulation mechanisms and corresponding security mechanism has been quickly forgotten and data storage, manipulation, and even computer and networking hardware has been moved to the cloud. This poses a tremendous new challenge to the cloud security developers to ensure the security of data as a typical cloud user doesn’t know the exact location of their data or the other sources of the data collectively stored with theirs and he can’t apply most of the tradition defense mechanisms.

To mitigate the data security risks (confidentiality, integrity, availability) and to increase cloud computing acceptance developing companies, organizations, and specialists proposed various systems and procedures based on the different cloud computing implementation model.

The main method of limiting access to information is through encryption and selective distribution of keys used to encrypt group information. A data encryption system takes input data (e.g. a group message) and performs some transformations on it using cryptographic primitives and a cryptographic key. This process generates a ciphered text. There is no easy way to recover the original message from the ciphered text other than by using a specific algorithm and the right key [Schneier 1996].

All data encryption systems are comprised of the following three elements:

- The data: the object or objects to encrypt. The nature of the data to be encrypted (fixed size or stream) and the place where it is located influence the way the encryption system in developed;
- The encryption engine: is the core of the system. He is responsible for the actual scramble of original data based on implementation of cryptographic primitives and some other manipulation algorithms. It can be implemented at a software level or at the hardware level of the system.
- The key manager: the component that handles the keys and passes them to the encryption engine.

Encryption key management solutions have the primary goal of managing and protecting encryption keys and making them available to authorized applications in a secure fashion. Key management solutions vary greatly in the complexity of the key retrieval process. The more complex the key retrieval interface, the greater the challenge for the enterprise IT team in deploying key retrieval in applications. Understanding this fact can help IT decision makers assess different vendor solutions and determine the approximate costs of deploying a solution in their companies.

Many key management providers developed their own particular solutions to address the key management process as software products sometimes, in order to achieve superior performance and reliability, even implemented it on a dedicated hardware infrastructure HSM (Hardware Security Module). In cloud computing key management software can be deployed as a service. Even the HSM platform can be virtualized and provided as a service by cloud providers like currently Amazon Web Services and Microsoft Azure do. Having so many products to the key management security problem each one with different approaches and implementations was another obstacle in cloud acceptance. The diversity of approaches generated confusion and lack of application interoperability.

However in the latest years some standards are being established in the industry by specific organizations. In this direction NIST (National Institute of Standards and Technology) developed requirements and standards for cryptography modules that include both hardware and software components FIPS 140-2 standard and OASIS organization (Open Standards for the Information Society) proposed the Key Management Interoperability Protocol (KMIP) which stands as a basis for achieving interoperability between cryptographic systems by defining message formats for the manipulation of cryptographic keys on a key management server.

1. Key Management attributes

Successful key management is critical to the security of a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. Cryptographic systems may use different types of keys, with some systems using more than one. These may include symmetric keys or asymmetric keys.

The following are the important key management attributes:

• **Generate Key:** The generation of good-quality keys is critical to security. Keys for a cryptographic algorithm should be generated in cryptographic modules that have been approved for the generation of keys for that algorithm.

• **Bind Key and Metadata:** A key may have associated data, such as the time period of use, usage constraints (such as authentication, type of encryption, and/or key establishment), domain parameters, and security services for which they are used, such as source authentication, integrity, and confidentiality protection.

- **Activate Key:** This function transitions a key to the active state. It is often done in conjunction with key generation.
- **Deactivate Key:** This function is generally done when a key is no longer needed for applying cryptographic protection. For example, when a key has expired, or is replaced by another key.
- **Backup Key:** A key is backed by the owner, the key management infrastructure, or a third party in order to reconstitute the key when it is accidentally destroyed or otherwise unavailable.
- **Recover Key:** This function is complementary to the key backup function and is invoked when the key is unavailable for some reason and is required by the authorized parties. Key backup and recovery generally applies to the symmetric and private keys.
- **Modify Metadata:** This function is invoked when metadata bound to key needs to be changed. The renewal of a public key certificate is an example of this function where the validity period for the public key has expired and the time period has to be changed or another key has to be generated.
- **Rekey:** This function is a critical one used to replace the existing key with a new key because the old key is obsolete. In traditional cryptographic systems many times the delivery of the new key is done by encrypting it with the old key. However when the current key is compromised or in modern cloud computing systems which are based on secure group communication the rekeying process of the group key can’t be based on the old group key and some other protocol has to be developed.
- **Suspend a Key:** This function is used to temporarily cease the use of a key. It is similar to reversible revocation. This function may need to be invoked if the status of a key is undetermined or if the key owner wishes to temporarily suspend its use (e.g., for extended leave). For secret keys, this can also be accomplished via key deactivation. For public keys and the companion private key, this is generally done using suspension notification of the public key.
- **Restore a Key:** This function is used to restore a suspended key once its secure status is ascertained. For secret keys, this can also be accomplished via key activation. For public keys and the companion private keys, this is generally done using a revocation notification where the revoked public key entry is deleted implying the key is valid.
- **Revoke a Key:** revoking a key or certificate is the process of invalidates the key or certificate as a trusted security credential. There are a number of reasons why a certificate, as a security credential, could become untrustworthy prior to its expiration. Examples include: compromising, fraudulent usage, changes in the status of the owner,
- **Archive a Key:** This function is used to store a key in long-term storage after it has been deactivated, expired, and/or compromised.
- **Destroy a Key:**In cryptography, zeroisation is the practice of erasing sensitive parameters (electronically stored data, cryptographic keys) from a cryptographic module to prevent their disclosure. This is generally accomplished by altering or deleting the contents to prevent recovery of the data.
- **Manage TA Store:** This function is used by the relying party to determine what trust anchors to trust and for what purpose. A trust anchor is a public key and its associated metadata that the relying party explicitly trusts and uses to establish trust in other public keys via transitive trust, such as a public-key certification path that is a series of public key certificates where the digital signature in one certificate can be used to verify the digital signature on the next certificate.

CRYPTOGRAPHIC KEY MANAGEMENT IN CLOUD COMPUTING

2. Risks Associated with Key Management

The ability to manage security operations built on cryptography—such as digital signing or data encryption—depends directly on the ability to manage effectively the cryptographic keys that govern these processes. Cloud computing implementations brings new paradigms and key management challenges areincreasing as cryptography is employed more broadly within an organization's IT infrastructure, driving up the number and diversity of keys to be managed. The understanding of different approaches to key management, key management best practices, and technology alternatives for implementing those practices are critical to a good implementation of a company cryptographic security system.

Key management is not just an operational challenge. As regulatory bodies become more aware of the importance of key management, the security and audit requirements specific to these processes are becoming more stringent. In addition, standards such as the OASIS Key Management Interoperability Protocol (KMIP) are maturing and will improve key management interoperability between different devices and systems. Given these trends, organizations need to consider, operational, security, and audit requirements when building a key management strategy.

The risks associated with key management are the followings:

- Keys compromising – keys can fall into the wrong hands, giving unauthorized persons or applications access to sensitive or high-value information. Data breaches can result in embarrassing disclosures, risk of customer identity theft, and perhaps fines or legal challenges;
- Unavailability of cryptographic services – if a cloud key management solution as a service is used then the unavailability of the service can be devastating for the activities of a company;
- Cryptographic keys can become lost or unrecoverable, rendering data unreadable. Depending on the specific nature of the data, key loss can result in major problems for the business in the form of interruptions to business operations, lost customers, or legal consequences;
- The limited protection offered by the key management system can leave sensitive keysand the data they protect vulnerable to attack;
- Lack of interoperability between key management systems protocols and the proliferation of fragmented key management systems can increase the complexity and cost of security management, resulting in business processes that are difficult to manage and to scale;
- Poorly documented key management activities can increase the burden of compliance reporting activities.

3. Cloud key manager solutions:

Townsend Security Alliance Key Manager - is an application that helps organizations meet compliance requirements with FIPS 140-2 compliant encryption key management. The symmetric encryption key management solution creates, manages, and distributes 128-bit, 192-bit, and 256-bit AES keys for any application or database running on any Enterprise operating system. It can be implemented as a standing application, as a virtual instance or as a physical hardware security module (HSM). It was thoroughly investigated by one of the main cloud solution providers and has achieved VMware's highest level of endorsement: VMware Ready status.

Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services running on Microsoft Cloud platform: AZURE. Key Vault can be used to encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs (keys never leave the HSM boundary). The HSMs are FIPS 140-2 Level 2 validated. Developers can create keys for development and testing in minutes, and then seamlessly migrate them to production keys. Security administrators can grant (and revoke) permission to keys, as needed.

Amazon Web Services (AWS) Key Management Service (KMS) is an encryption and key management service used in the Amazon Cloud Platform. KMS keys and functionality can be used by other AWS services and can provide security mechanisms for protecting data but also be integrated in applications.

The IBM Distributed Key Management System (DKMS) provides online key management to the Integrated Cryptographic Service Facility (ICSF) as well as to IBM cryptographic products on other platforms. ICSF is a software element of z/OS that works with hardware cryptographic features and the Security Server to provide secure, high-speed cryptographic services in the environment. ICSF provides the application programming interfaces by which applications request the cryptographic services.

DKMS offers centralized key management for symmetric and asymmetric keys and for certificates. DKMS automates the key management process, and exchanges and replaces keys and certificates on demand. Further, to assure continuous operation DKMS maintains backup copies of all critical keys.

4. Conclusion

Public and private organizations which want to take advantage of cloud-based solutions to reduce costs and improve business performance have to implement security mechanisms in order to secure their data. The basis for this process is the encryption process and the critical point in this process is the key management solution. Cloud services providers like Amazon, Microsoft, IBM, VMware and other companies saw the importance of this and developed or adopted different key management solutions.

5. References:

[1] Cryptographic Key Management Issues & Challenges in Cloud Services ,Ramaswamy Chandramouli ,Michaela Iorga ,Santosh Chokhani , September 2013;

[2] A Group Key Management Approach For Multicast Cryptosystems, M .V. Vijaya Saradhi, BH. Ravi Krishna, Journal of Theoretical and Applied Information Technology, 2010;

[3] https://solutionexchange.vmware.com/store/products/alliance-key-manager-for-vmware

[4] https://en.wikipedia.org/wiki/Key_management#References

[5] https://azure.microsoft.com/en-us/services/key-vault/