Identify Components of Key Management

Chimene Tchokoko Diboma

School or Institution Name (University at Place or Town, State)

**Identify Components of Key Management**

**Introduction:**

Modern businesses rely on information technologies for business continuity and operations. Most of the business operations require processing of sensitive information such as personally identifiable information in healthcare institutions and corporations. This type of information is highly valuable for hackers to compromise for monetary benefits. Given to the fact that information technology systems are playing the role of a utility in every aspect of life, cyber-criminals are always creating new and sophisticated attacks to compromise such systems. It is the responsibility of the organization dealing with the data to protect its systems against cyber-attacks (Lei et al., 2017). Therefore, cybersecurity must be a part of the business plans and aligned with the business goals with the primary purpose of ensuring the confidentiality, integrity, availability, and non-repudiation of data. Several systems and frameworks have designed by experts for organizations to achieve these security goals. One such system is known as the cryptographic system that protects the confidentiality and integrity of data. The report describes the cryptographic systems for the healthcare organization to secure personally identifiable information of clients and different components of the key management system.

**Discussion:**

Cryptography can be considered as the basic requirement for securing confidential data against cyber-attacks. In cryptographic systems information is encoded using some algorithm so, that it can be retrieved only by the intended recipient of the information. A simple cryptographic system can be described as a substitution algorithm. For example, a specific plain text message is to be protected from prying eyes, then certain letters in that message can be substituted with different letters. A popular substitution cryptographic algorithm is known as Caesar cipher. Caser cipher replaces every letter in a message with the corresponding third letter from English alphabets. The resulting text is known as the ciphertext that can be converted back to plain text by performing the exact reverse operation (Sciancalepore, Capossele, Piro, Boggia, & Bianchi, 2015). There are some key components in any cryptographic system known as the cryptographic algorithm, cryptographic key, and key management system. In the example rotation of three letters is the key of encryption. The resulting ciphertext cannot be decoded by any criminal or anyone unless the key of encryption is not known. Such systems are known as symmetric encryption systems.

**Symmetric Encryption:**

A symmetric encryption system is one that uses the same keys for encryption and decryption of the data. The key is then considered to be the symmetric keys. Symmetric encryption is also referred to as the encryption scheme for data at rest. It can be used for protecting the data when it is being stored in the database storage system. It will protect the storage system against un-authorized access ensuring the confidentiality of the data. As in symmetric key cryptographic systems, the same key is used for encryption and decryption of data, it is the most critical part of the system (Kurihara, Kikuchi, Imaizumi, Shiota, & Kiya, 2015). Data will be as secure as the encryption key used to encrypt the data regardless of the encryption algorithm used. Therefore, a key management system is required to protect the key of encryption from unauthorized access. If the key is compromised then all of the logical security measures will be breached.

Symmetric encryption is mainly used for storage devices such as in full disk encryption programs instead of transferring the encrypted data. The reason behind the use of symmetric encryption for local security is that in case of data transfer, the key must be transmitted separately via some secure communication channel because the recipient of the data will not be able to decrypt the data without having the same key. As it is very difficult to securely transmit the encryption key using available communication systems, the system is mainly used for local disk or database encryption.

**Triple DES:**

Data encryption standard (DES) is an encryption algorithm that uses the same keys for encryption and decryption of the data. It was designed in 1970 as the standard for securing digital information against cyber-attacks. It is a block cipher meaning that it operates over a block of plaintext information and convert that plaintext information into the corresponding ciphertext. As in the previous example the encryption key length was 3 bits because the letters were rotated three places. Key length is important in cryptographic systems because when researchers are designing sophisticated encryption algorithms, the criminals are also trying to exploit such systems at the same time (Kumar, Roth, Rubin, Seigle, & Tirdad, 2016). Being a block cipher DES uses a key length of 64-bits. A block of data is encrypted using 64-bit keys of encryption and it can encrypt the data in different modes. In simple mode, each block of data can be encrypted using the independent key. The second mode of operation is in which the blocks of data are encrypted such that each block of encrypted data depends on the previous block of encrypted data.

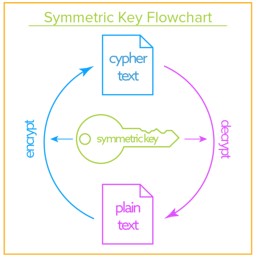
Regardless of the mode of operation of the algorithm the data can be retrieved by performing the exact reverse operation following the reverse order of encryption. DES was prone to brute force attacks. A brute force attack uses all the possible combination of keys to decrypt the message until a correct key is found. The length of the key determines the total number of attempts for such an attack to be successful. In reality DES was not using 64-bit keys, instead, the data was encrypted using 56-bit keys while rest of the bits reserved for parity checks. Depending on the key length it will only take a total of 256 attempts to decrypt the message encrypted using DES. At the time of introduction and implementation of this algorithm considerable computing power as required to try such a large number of keys on a single block of data. However, with the exponential increase in computing power available today DES system is not feasible anymore. To overcome the weakness of the DES algorithm, its successor was introduced known as triple-DES (Baek, Vu, Liu, Huang, & Xiang, 2015). Triple DES uses three rounds of DES to encrypt the data increasing the key length from 56 bits to 168 bits. However, due to the intermediate attacking mechanism, the effective length of the key was only 112 bits. Soon after the introduction, severe flaws were discovered by the researchers in the Triple DES algorithm and it was replaced by the modern encryption system known as advanced encryption standard (AES). AES is currently the most secure encryption standard being used by the governments as well.

**AES:**

Advance encryption standard (AES) is the successor of DES. It is also a block cipher like the predecessor of it but uses a different approach for encryption and decryption of the data. It uses a block of 256 bits for data to be encrypted but with a variable length of key such as key lengths of 128 bits, 192 bits, and 256 bits. AES is the most secure cryptographic algorithm available today and being used as a data encryption standard. The federal government of the United States has approved AES as an encryption standard to encrypt the classified information. AES uses a substitution-permutation network as compared to the DES. Currently, AES encryption is being used in conjunction with the asymmetric cryptography.

**Symmetric Key Systems:**

As it is evident by the explanation that any encryption system is as secure as the key of encryption used in the algorithm. Therefore, a key management system is utilized by organizations that secure the key of encryption from being stolen or compromised by the targeted attacks on information technology infrastructure. There are several components o symmetric key management system as well. The key primarily used to encrypt and decrypt the data is known as the data encryption key. Then a key is used to encrypt the data encryption key and is known as the key encryption key. An application interface is used to provide lengthy encryption keys to the clients requesting the keys from a server and known as the key management application program interface. A server that hosts the key management software is known as the key management system. The following figure shows the working of a symmetric key cryptography system.



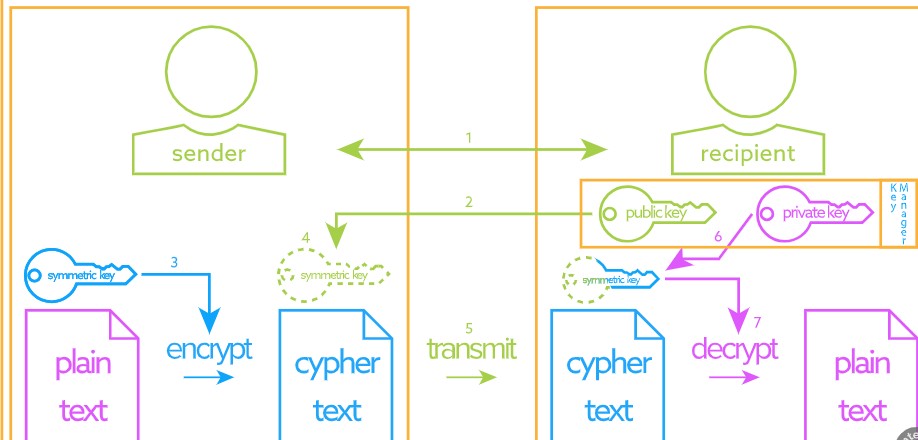
When a client has to access a protected data resource the direct key of encryption is not provided to the client to ensure the security of the key. The request is forwarded to the above mentioned key management system. The client sends a request for the data encryption key to the application interface that connects the client with the server housing the database of encryption keys along with the key management software. Certificate of the client will be verified by initiating a transport layer security session with the client. If the certificate of the client is verified by the server then the key encryption key is used to retrieve the original data encryption key on behalf of the requesting client. The data encryption key is then provided to the requested database or file storage system that decrypts the required resource using that key and provide the client with plain text information (Rodgers et al., 2017). The file system or database may store the key temporarily in memory for decryption purpose but that will be cleared after a set interval of time. Implementation of such key management system will help the organization to secure its critical information systems against cyber-attacks. The clients will be accessing the encrypted data without explicitly requiring access to the key itself. The access to the symmetric key in this key management system is protected by the public key cryptographic system also known as the public key cryptography system.

**Asymmetric Cryptography:**

As it is evident by the name asymmetric cryptography use different keys for encryption and decryption. It uses a pair of public and private keys for encryption and decryption. The key pairs of public and private keys are based on the large prime number factorizations. None of the keys can be extracted from each other meaning that the public key cannot be used to extract the public key in any way. The public key, as the name suggests, is known to the public. Whenever a person needs to send a message to some then the message is encrypted by using the public key of the recipient as the recipient is the only entity that has the corresponding private key to decrypt the message. In the organizational situation, a public key cryptographic infrastructure is used for key management and handling of public keys (Al Salami, Baek, Salah, & Damiani, 2016). The certification authority issues digital signatures or digital certificates that can be used by individuals or organizations to prove their identity providing the confidentiality and integrity of the data. A digital signature or certificate is just the public key of an individual with some additional details such as the expiry date of the certificate. The certification authority keeps the identification record of the individual and matches the public keys with corresponding private keys. It verifies the owner of a legitimate public key for authentication and authorization purpose.

**Asymmetric Key Systems:**

In public key cryptographic systems implemented by the healthcare organization, each party owns a digital certificate provided by the certification authority. The sender of the information sends its certificate to the receiver for verification. The receiver then checks the validity and authenticity of the received certificate with its certification authority by sending it to the corresponding server hosting the validation data. When the certificate of the sender is verified then the receiver sends its certificate for verification and acceptance. After acceptance of digital certificates and having shared corresponding public keys a symmetric session key is created for an added layer of security. The session key is unique for each session to rule out the possibility of a man in the middle attacks in which an attacker can masquerade as the original sender by intercepting the initial validation communication between the parties. The sender encrypts the session key with the public key of the receiver. The receiver, on the other hand, decrypts the content of the message using the corresponding private key. Following flow chart describes the working of an asymmetric key cryptographic system.



The encryption scheme is implemented by the organization to secure its critical information infrastructure from cyber-attacks. The system utilizes a combination of asymmetric and symmetric cryptography to ensure the integrity, non-repudiation, availability, and confidentiality of the data. Key generation and storage take place on a dedicated server. On local hosts, the integrity of system files verified using the local encryption keys stored in trusted platform module device that cannot be accessed by software solutions making difficult target for attackers. Any client requesting for a protected resource is required to first prove the identity using public key cryptography system employing the digital certificates and then provided with the encrypted resource.

**Benefits and Risks:**

Any information technology system cannot be guaranteed to be 100% secure against targeted and advance persistent attacks. Cryptographic systems can also be tampered using techniques such as frequency analysis for stream ciphers and major cryptanalysis techniques for other encryption standards. Protection of the key itself is a challenging job in all of the cryptography system. The proposed implementation of the system uses encryption to encrypt the key as well as obfuscating the information and making it hard for cracking the original key (Vasilomanolakis et al., 2015). Normal keys and symmetric keys of shorter lengths can be cracked using brute force attacks. In the case of public key infrastructure the session keys can be collected by the attackers intercepting the network traffic. Such attacks are considered to be the man in the middle attacks. If an attacker has access to the session key then he will be able to communicate with the server to retrieve the encryption key. A successful attack can compromise the entire system even if the resources are encrypted. Therefore, encryption of session keys with public keys rules out the possibility of such attacks.

**Conclusion:**

Cryptographic systems are considered to be the primary line of defense for organizations against digital dark arts. As it is an established fact that any cryptographic system is as secure as the corresponding keys of encryption being used by the system. Therefore, securing the encryption keys is an inevitable task for the security teams of organizations dealing with sensitive information such as healthcare organizations. The best way of implementation of a cryptographic system is to aid the implementation with a key management infrastructure. It will help organizations in legal scenarios as well because if a key is lost and misused then the court of law may ask whether or not the organization was using a key management system. Even if it is not a legal or standardized requirement it will add value to the business.

**Enterprise Key Management Policy**

The goal of information security technology systems is to ensure the security of critical information systems. While designing security infrastructure, security teams have to find the balance between security and usability of the system. There is always a tradeoff between the security and usability of the system in information technology infrastructure. A most secure system will be one that is not connected to anything including the power source. But at the same time, the system will be the most useless system as well because it cannot be accessed by anyone. In the case of the cryptographic systems, strict security policies will make the system useless due to the complexity of operations involved. However, the system can still be protected if a key management system along with a comprehensive key management policy is deployed. Following are the key management rules implemented in healthcare organizations for the cryptographic system installed.

As a single encryption key cannot be used for data protection for an extended period of time. The key management system will use a key manager to ensure the rollover of existing keys and activation of new keys. For example when a new key of activation is generated the system will restrict the encryption activity using the previous key. Encryption operations will only be allowed using the newly activated encryption key. However, it will not be feasible for the system to re-encrypt all of the existing data with the new key because it will create a lot of processing overhead rendering the overall system useless (Barker & Barker, 2018). Therefore, the key manager will allow the previous key to be used for the decryption operation of existing data but not for the encryption. Similarly, the key manager can also revoke a key for both encryption and decryption operation in emergency conditions. The key manager will be required to maintain a list of all of the key operations along with the revocation list of keys.

Escrow keys also known as the backup keys must be maintained even after the expiration of their crypto period. Achieved keys must be protected against accidental deletion and corruption. It is required to decrypt the backup of data in case of a large-scale breach of data happens or hardware failure. On the other hand, the key manager is also authorized to securely delete an entire encryption key along with all of its instances or only selected instances if the key is compromised. The operation will make it impossible for attackers to reconstruct the encryption key and use it to exploit the protected systems. Even if the encrypted data is compromised, the deletion of the key will ensure that the data is completely secure and cannot be recovered at all. As per the framework of the national institute of standards in technology, key generation roles will be segregated between three parties. Meaning that no single person will know about the entire structure of the key. Each person will only be aware of a certain part of the key making the key generation secure against insider attacks.

In addition, the operation of the entire key management system will be divided between at least two persons. It will ensure that no single entity has complete control of the system. It is also a requirement of the NIST framework. Physical security of the key management system will also be ensured as per the federal information protection standards. It is inevitable for any organization to have an adequate physical defense in place along with the logical measures. Because if a system can be physically breached and compromised then all of the logical protection measures will fail too.

References

Al Salami, S., Baek, J., Salah, K., & Damiani, E. (2016). Lightweight encryption for smart home. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 382–388. IEEE.

Baek, J., Vu, Q. H., Liu, J. K., Huang, X., & Xiang, Y. (2015). A secure cloud computing based framework for big data information management of smart grid. *IEEE Transactions on Cloud Computing*, *3*(2), 233–244.

Barker, E., & Barker, W. (2018). *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*. National Institute of Standards and Technology.

Kumar, S., Roth, G. B., Rubin, G. A., Seigle, M. C., & Tirdad, K. (2016). *Redundant key management*. Google Patents.

Kurihara, K., Kikuchi, M., Imaizumi, S., Shiota, S., & Kiya, H. (2015). An encryption-then-compression system for jpeg/motion jpeg standard. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *98*(11), 2238–2245.

Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, *4*(6), 1832–1843.

Rodgers, R. S., Eatherton, W. N., Beesley, M. J., Dyckerhoff, S. A., Lacroute, P. G., Swierk, E. R., … Rajagopal, S. (2017). *Method and system for key management*. Google Patents.

Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., & Bianchi, G. (2015). Key management protocol with implicit certificates for IoT systems. *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, 37–42. ACM.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the security and privacy of Internet of Things architectures and systems. *2015 International Workshop on Secure Internet of Things (SIoT)*, 49–57. IEEE.