International Journal of Information Management 38 (2018) 42–44

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Case study

Analyze encryption and public key infrastructure (PKI)

Vincent Lozupone

Northcentral University, 2488 Historic Decatur Rd., San Diego, CA, 92106, United States

ARTICLE INFO

Keywords:
Symmetric encryption
Secret key
Private key
Cryptography
Digital signatures
Hash functions
Lockbox
Block ciphers

ABSTRACT

The researcher opens with a brief description of symmetric and asymmetric encryption systems. Then the researcher presents an analysis, comparisons of asymmetric and symmetric encryption schemes and advantages and disadvantages of PKI (Public Key Infrastructure). Asymmetric encryption systems use different transmitter and receiver keys, and it is very difficult to derive one key from the other. Symmetric systems use one shared key. PKI is a set of hardware, software, policies, and technicians to manage an environment using public key digital certificates. The researcher addresses security, PKI, and solutions within cloud technology.

1. Introduction

Symmetric encryption is the oldest and well-known technique. It uses a secret key that can be a number, word, or random letters. All the parties, the sender, and receiver need to have the key in their possession. There is a problem with the concept of a secret key. Having the knowledge of this secret key can decrypt the message. The solution to this issue is to use a key-pair. Use a public key, that anyone can hold, and a private key. A PKI system allows both encryption and digital signatures by a wide breadth and diverse set of applications (Entrust, 2017).

2. A critical analysis of similarities and differences between a symmetric and asymmetric encryption system

Gaining a strong understanding of cryptography requires a grasp of the four main areas of primitives. All the primitives are very closely related. The four primitives are random number generation, symmetric encryption, asymmetric encryption, and hash functions (Cole, 2008). There are three main goals that cryptographic systems attempt to attain. Confidentiality is one the objectives. If a user can decrypt the message without having a key, then this objective is not met. To assure the data has not been modified is the goal of the objective of integrity. Authentication, the third goal, is to assure that the source of the data is verified (Cole, 2008). Asymmetric encryption is more secure and more complex than symmetric encryption (Omar, Asif, Mahaboob, Ramana, & Shahid, 2012).

Asymmetric encryption uses private and public keys to encrypt and decrypt information as shown in Fig. 2. Cole (2008) stated that symmetric encryption or single key encrypt and decrypt data as illustrated in Fig. 1. A benefit of using a single key encryption is speed. Coincidently, symmetric key encryption used with asymmetric encryption also makes a fast transaction (Cole, 2008). One would use symmetric encryption when sending confidential information. It can also be used to offer integrity. An excellent analogy explaining this type of encryption is similar to a lockbox (Cole, 2008).

The equivalent to a key is a set of random bits. There are some block ciphers used for symmetric encryption, but the one that is the most popular is DES (Data Encryption Standard). It has a key of 56 bits. This value means that it would take 72, 057, 594, 037, 927, 936 varying keys to test to full exhaustion (Cole, 2008). Compared to symmetric encryption, asymmetric encryption needs two keys, a private key, and a public key. The public key is available to anyone who chooses to use it. Asymmetric encryption is slower than symmetric encryption because it uses number theory to increase its strength. Regardless of its slow speed, it does an excellent job of the difficulty of sharing keys.

Two mechanisms use asymmetric encryption, digital signatures, and hashes. A digital signature message is one that uses authentication to prove a certain person sent the message and used to meet important security goals (Villanueva, 2015). The authentication accomplishes by only encrypting a smaller section of the entire message, which then makes the process faster than encrypting the entire message (Cole, 2008). Hash functions are used to gain improved performance when large blocks of data are using with asymmetric encryption (Cole, 2008). Hashes have three properties that make them valuable. It is doubtful that the same messages can hash identically. With a known digest, it would be nearly impossible for a second message to create the same digest. Finally, it would also be almost impossible to locate the original

E-mail address: vlozupone@hotmail.com.

http://dx.doi.org/10.1016/j.ijinfomgt.2017.08.004
Received 22 April 2017; Received in revised form 9 August 2017; Accepted 25 August 2017

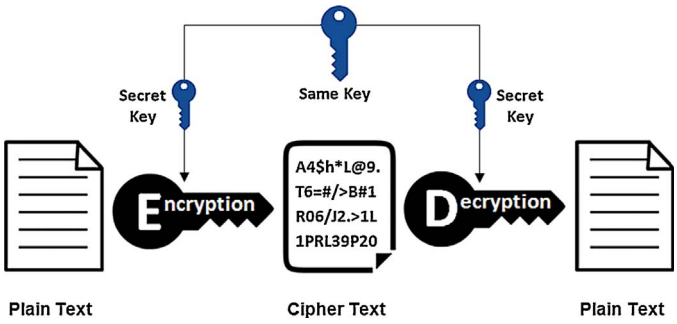

Fig. 1. Symmetric Encryption (Ssl2buy, 2017).

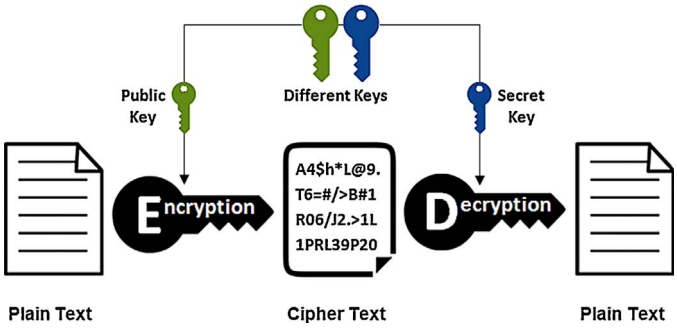

Fig. 2. Asymmetric Encryption (Ssl2buy, 2017).

message that created the known Digest (Cole, 2008). Hashing is also valuable in storing passwords and hashing ensuring integrity. A message remains the same regardless of the number of times it is computed. There was a vulnerability in hashing passwords until salting was used to prevent a dictionary attack. A dictionary attack uses common words in the dictionary to attempt a breach to discover a password. Salting is used to insert pseudo-random data into a message before being hashed (Cole, 2008).

3. An evaluation of the public key infrastructure used by modern organizations, the entities involved in PKI, and how PKI works

Entrust (2017) explained that PKI is an all-inclusive system that provides a public-key encryption and the use of digital signatures. PKI manages keys and certificates. By making use PKI, an organization can create and manage a dependable and trustworthy networking environment (Entrust, 2017). PKI is commonly synonymous with asymmetric encryption because it is more secure than symmetric encryption as depicted in Fig. 3. Two keys relate mathematically use a public and private key, one for encryption and the other for decryption. Everyone knows the public key, and only the owner knows the private key (Braun, Volk, Classen, Buchmann, & Mühlhäuser, 2014). The problem arises if a public key is used by a party that is not the actual owner of the public key. To avoid this issue, digital certificates verify the owner is making use of a CA (Certificate Authority) (Braun et al., 2014). A CA

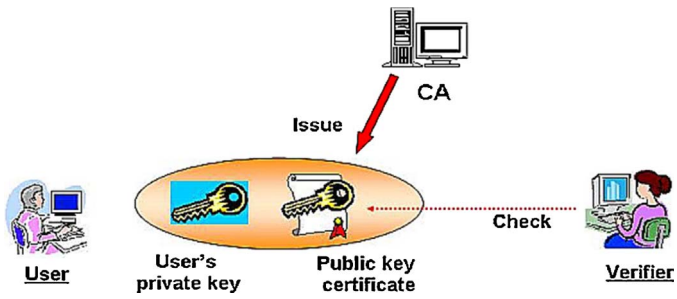

Fig. 3. Public Key Infrastructure (PKI, 2017).

can be a public third-party such as Verisign, Thawte or RSA. An organization can also create one for itself. To create a certificate, a PKI-enabled application is required. The CR (Certificate Request) contains a public key and information used to submit the type of certificate requested (Cole, 2008). The organization needs to decide the types of certificates required, and this would determine whether implementation of a public or private CA. If an organization chooses a private CA, then a choice has to be made of roles that are a Root CA, Intermediate CA, or an Issuing CA. It is prudent to design a system with multiple CAs to assure available and secure distributing points (Cole, 2008).

Another critical component of a PKI implementation is the certificate policy. Uahhab and Bakkali (2014) stated that it lays out the rules for leading key security, the process for issuing, renewing, revoking, and default life span of certificates. Private PKI's should institute precise policies to assure methods of identifying certificate holders, revocation of the certificates, and the methods of list distribution. Revocation is another critical component of PKI.

Upon request, the requestor sends a created pair to the CA. The signature must verify. The occasions of revocation are compromised key or an employee dismissal. The key revokes when a new certificate replaces a previous one, or the CA is decommissioned (Cole, 2008). The issuing enterprise CA publishes and distributes a list called a CRL (Certificate Revocation List) (Uahhab & Bakkali, 2014). The clients check the CLR before accepting a certificate. According to Jayapandian, Rahman, Radhikadevi, and Koushikaa (2016), businesses share data by way of cloud technology effectively on a worldwide basis. Organizations use various service models, i.e., Service and a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) in one or more of these deployment models (private, public, hybrid, and community) (Jayapandian et al., 2017). Encryption ensures originality of data and allows secure duplication and construction by proper encryption and decryption (Jayapandian et al., 2017). Jayapandian et al. (2017) stated that symmetric key encryption or secret key encryption prevent information from eavesdroppers.

According to the survey, Information Technology (IT) governance and security standards have an impact on the increased adoption of cloud technology (Paquet, 2013). Another study by International Data Corporation (IDC) reveals that 87.5% of the respondents mentioned that security is the top issue of cloud adoption (Paquet, 2013). According to Singh (2017), there are possible points of entry for an intruder into a cloud technology (a) insecure mobile phone access to data, (b) a web application with vulnerability, and (c) sharing a password of a cloud database. It is becoming harder to protect data hosted on cloud platforms. There is no key transmission outside the enterprise hence the private key is considered a secure tool protecting enterprise data (Singh, 2017). Considering Small and Medium Businesses (SMBs) which are lacking the financial and hardware resources to implement a PKI solution, Singh (2017) emphasized the use of a publicly offered OAuth standard, which is an open standard for access delegation. Singh (2017) stated that encryption would not stop attacks, but it does make them less likely. It is difficult for businesses to allow clients to manage cloud resources with passwords and various authentication methods (Singh, 2017). The solution is implementing Single Sign-On (SSO). After the customer validates, a ticket allows clients access to all permitted resources (Singh, 2017).

Two solutions for cloud security are PKI and the use of multiple cloud solutions. Singh's (2017) solution for cloud security is to assure that data is safe for internal and external data (suppliers, clients, and catalogs). Singh (2017) stated that a symmetric key algorithm applies so the customer has a high level of trust for their critical data and the personal key not shared. Therefore, this solution is for Public Cloud security that combines OAuth authentication along with encryption algorithms (Singh, 2017).

The second solution uses certificate-based authentication along with public key cryptography infused to the business confidential data applied before placing the data in the cloud (Singh, 2017). PKI requires a

company to sign keys, which some companies find hard to use. Companies have found another solution, which is to public key Secure Sockets Layer (SSL) or later variant Transport Layer Security (TLS) (Singh, 2017). It is the researcher's opinion and that of Singh (2017) that TLS with PKI is a better panacea because it allows cryptographically hardened methods of authentication in environments that are unsafe.

4. An analysis of the advantages and disadvantages associated with PKI

Oppliger (2014) stated that there are advantages and disadvantages associated with PKI. Some vendors are selling various versions of PKI solutions. If the vendor goes bankrupt, it is difficult to obtain service in the future. Fraudulently issued certificates substitute kernel software with malware that mimics code-signing certificates is another disadvantage (Oppliger, 2014). Another downside is a company breach that had issued the CA. Companies think that their information is private. Companies that cannot afford the cost or not willing to yield authority to a third party of a public CA would have to invest in an in-house solution.

Security is a major concern for all companies that transfer digital information. These transactions that may be confidential, government or private information need to be protected from falling into corrupt hands. PKI is probably the best solution for this problem. Considering the increased use and number of digital transactions by consumers, a high assurance requires confidence (Oppliger, 2014). PKI enables the business community to convey to the consumer that their transactions and privacy is secure and safe not only from the government but the prying eyes of organizations. A CA like a trusted third party can increase consumer confidence. Another significant advantage is cost. According to researchers, PKI will decrease costs attenuating the support of labor-intensive transactions. High speed and increased volume of transactions will reduce the cost per transactions. This would more than likely increase the business' market share. PKI also is one of the best methods of creating an infrastructure that is safe for Internet transactions and from hackers, theft of information (PI) Personal Information, and virus injection.

It is also important that there may be occasions where PKI is not necessary, and a secret encryption is sufficient. These may include an environment where users can meet in private. This may also include a closed bank system where a manager, single authority knows all the keys. PKI is usually not required in a single-user environment. Also, PKI does not replace symmetric encryption but to augment it to make it more secure.

5. Conclusion

Certificates provide businesses an attractive security model. The cost is almost nothing to create. It is lucrative if you can convince a party to purchase a certificate for about $5.00 per year. This proposition is even more lucrative if one can convince business to purchase a CA and pay a fee for every issued certificate. A CA means trust. Regarding cryptography, it means that it handles private keys well. Symmetric Key Algorithms run much faster than Asymmetric Key Algorithms, i.e. RSA and in addition, the former uses less memory than for latter. Furthermore, the security facet of Symmetric Key Encryption is far superior to the Asymmetric Key Encryption. In cloud platforms, TLS with PKI is a better solution because it allows cryptographically secured methods of authentication in environments that are unsafe.

References

Braun, J., Volk, F., Classen, J., Buchmann, J., & Mühlhäuser, M. (2014). CA trust management for the web PKI. *Journal Of Computer Security, 22*(6), 913–959. http://dx.doi.org/10.3233/JCS-140509.

Cole, E. (2008). *Network security fundamentals.* Hoboken, NJ: Wiley.

Entrust. (2017). What is PKI? Retrieved from http://www.entrust.com/what-is-pki/.

Jayapandian, N., Rahman, Z., Radhikadevi, S., & Koushikaa, M. (2016). Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption. *Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), World Conference on, 1*. http://dx.doi.org/10.1109/startup.2016.7583904.

Omar, M., Asif Irshad, K., Mahaboob Sharief, S., Ramana, M. V., & Shahid Ali, M. K. (2012). (2012). Secure communication using symmetric and asymmetric cryptographic techniques. *International Journal Of Information Engineering And Electronic Business, 2*, 36.

Oppliger, R. (2014). Certification authorities under attack: a plea for certificate legitimation. *IEEE Internet Computing, Internet Computing, IEEE, IEEE Internet Comput, 1*, 40. http://dx.doi.org/10.1109/mic.2013.5.

PKI. (2017). Public key infrastructure. Retrieved from http://itslab.csce.kyushu-u.ac.jp/research/pki.html.

Singh, N. (2017). Advanced security model for ensuring complete security in cloud architecture. *International Journal of Computational Intelligence Research, 13*. [ISSN 0973 1873 Retrieved from] https://www.ripublication.com/ijcir.htm.

Ssl2buy. (2017). Symmetric vs. Asymmetric encryption − what are differences? Retrieved from https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences.

Uahhab, Z., & Bakkali, H. (2014). *A comparative study of PKI trust models International conference on next generation networks and services (NGNS) Next generation networks and services (NGNS), 2014 fifth international conference,* 255. http://dx.doi.org/10.1109/ngns.2014.6990261.

Villanueva, J. (2015). *What is a digital signature?* Retrieved from, http://www.jscape.com/blog/what-is-a-digital-signature.