ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (83-85), Month: July - September 2020, Available at: www.researchpublish.com

Digital Security through Data Encryption

Abdullah Alsaeed

Abstract: **Today, the information technology world approaches unprecedented era of digital interconnectivity. The digitally interconnected world ranges from applications, systems, computing infrastructures, cloud environments all the way to mobile and Internet of Things (IoT) devices. Therefore, the data security is essential for the optimal safe use of the information technology. Cryptography mechanisms are means to protect the digital data which is sensitive, high value, or vulnerable to unauthorized disclosure or modification during data transmission or at their residence storage. The document intents to discuss the cryptography mechanisms availed in the today's technology market in additions to the cryptographic challenges.**

Keywords: **Encryption, data protection, cybersecurity, data in-motion, data at-rest, key management, cryptography.**

1. INTRODUCTION

Cryptography is based upon a branch of mathematics. It consists of two fundamentals components: an algorithm and a key.

A cryptographic algorithm is a specified mathematical process for computation. It has its own set of rules which, when followed, will give a prescribed result.

A cryptographic key is a parameter used with a cryptographic algorithm during the cryptography process. The key determines algorithm operation in such a way key holder can reproduce or reverse the algorithm operation while an entity without knowledge of the key cannot.

Both the algorithm and key are used to implement cryptographic protection to data either encrypting or decrypting.

Algorithms of Cryptography

This section will describes three different cryptographic algorithms: hash functions, symmetric-key and asymmetric-key.

Hash Function Algorithm

A hash function algorithm is a cryptographic algorithm that yields a condensed representation of its input or a message. A hash function takes an input of arbitrary length and outputs a value with a predetermined length (known as a hash value or message digest.

The hash function algorithm has key features that distinguish it from other cryptographic algorithms. The hash function transform data of arbitrary length to a fixed length. The output is generally smaller than the input data. It does a compression to the input data resulting into a data digest. The output bits of the hash function generated ranges between 160 to 512 bits.

Common Hash Functions

Message Digest (MD) was used widely to hash the data. The MD comes with different versions such as MD2, MD4, MD5 and MD6. MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it. In 2004, collisions were found in MD5. An analytical attack was reported to successful in a matter of an hour by using computer cluster. This collision attack resulted in compromising MD5.

Secure Hash Function (SHA) come with structurally different forms: SHA-0, SHA-1, SHA-2, and SHA-3. The version SHA-0 was published by the National Institute of Standards and Technology (NIST) in 1993. It came with tis weaknesses and vulnerabilities. Hence, it was not popular in the information security community. It was restructured and resulted in introducing SHA-1 to eliminate and mitigate the known weaknesses. The SHA-1 hash function started to attract the attention and was employed widely in different applications and protocol such as the secure socket layer (SSL) security. The SHA-1 was evolved and improved yielding the SHA-2. In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

Whirlpool is hash function that is based on the use of a block cipher for the compression function. It is is a 512-bit hash function driven from Advanced Encryption Standard (AES). Whirlpool have three releases: WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

The hash function cryptographic algorithms applies into two direct uses: password storage and data integrity check. The former use is to store the logon password in a hashed format. That will provide an intrusion prevention measure in a case of the credential compromising. A successful intruder will only display a hashed password. The hashed password cannot be used for logon or derive the original password from a hash value because of the pre-image resistance property of the hash function algorithm.

Data integrity check is the second application for the hash function algorithm. It generates a checksums on data files. It provides an assurance about correctness of the data and detects any changes made to original file.

Symmetric Key Algorithm

Symmetric-key algorithms, also called secret-key algorithms, transform data in a way that is fundamentally difficult to reverse it with no knowledge of cryptographic key. The key is symmetric since the same key is used for a encrypting and decrypting the data.

Common Symmetric Key Algorithm

Data Encryption Standard algorithm (DEA) was developed by IBM in 1970s. The DEA had only a 56-bit key. The DEA key was not sufficiently secure against brute-forcing of the key using modern computers. Therefore, Triple-DES (commonly known as TDES, TDEA or 3DES) was introduced in with the use of the 3 keys bundle. That gives a nominal strength of 168 bits never the less at the price of slow performance.

Advanced Encryption Standard algorithm (AES) features a block size of 128 bits and three key length options: 128, 192 or 256 bits. Most today's applications embrace the use of the Advanced Encryption Standard algorithm (AES). They mostly use with 128 and 256-bit keys while the latter key length considered strong enough to protect highly classified data. A single 128-bit key will take billions of years to brute force using any classical computing technology today.

Asymmetric Key Algorithms

Asymmetric key algorithms use two related keys: public and private keys (key pair) in order to perform their encryption and decryption operations. The public key may be known by anyone. However, the private key is under the sole control of the entity that owns the key pair. The knowledge of the public key cannot be used to derive the private key. Because an asymmetric-key algorithm use one of the keys of the key pair apply cryptographic protection and the other key remove or verify that protection.

A variety of communication protocols depend on asymmetric cryptography. That includes the transport layer security (TLS) and secure sockets layer (SSL) protocols which make HTTPS possible. The asymmetric key algorithm is also considered a validation mechanism for a digital signature.

Increased data security is the primary benefit of asymmetric cryptography. It is the most secure encryption process because users are never required to reveal or share their private keys, thus decreasing the chances of a cybercriminal discovering a user's private key during transmission.

Asymmetric cryptography authenticates data through validating digital signatures. A digital signature is a mathematical technique used to validate the authenticity and integrity of data. The digital signature is an analogy for a handwritten signature or stamped seal.

Asymmetric key algorithms can be also utilized by application and systems for secure communication. A public key can encrypt an email communication and the recipient can then decrypt it through the private key. Cryptocurrencies rely on asymmetric cryptography as users have public keys that everyone can see and private keys that are kept secret. Bitcoin uses a cryptographic algorithm to ensure that only the legitimate owners can spend the funds.

Common Asymmetric Key Algorithms

The Rivest, Shamir and Adleman (RSA) asymmetric algorithm commonly used to provide secure communication. The RSA algorithm derives its security from the computational difficulty of factoring large integers that are the product of two large prime numbers.

Elliptic Curve Cryptography (ECC) has started to get favor with the cybersecurity community as another alternative to RSA algorithm. ECC is a public key encryption technique based on elliptic curve theory. It creates faster, smaller and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation.

Cryptographic Key Management

Cryptographic keys have a significant role in any data encryption mechanism. Those keys can be an analogy to a combination of a safe vault. When the safe combination is compromised, the toughest safe vault provides zero security against unauthorized access or penetration.

Therefore, an effective and efficient management of the cryptographic keys is essential to use cryptography for the cyber security. In contrast, improper cryptographic keys management leads to comprise the encryption algorithm.

2. CONCLUSION

Cryptographic attacks get stronger as new tools and techniques are developed. Algorithms that were once considered strong are today easy to break on a home PC. Even today's best algorithms will be weakened by quantum computing. New algorithms will continue to be developed to improve security and to target new applications with specific needs, such as IoT.

Quantum computing threatens to create a major upheaval in the next five years, and companies not wishing to be stuck on the back foot have to start planning now. All new applications should be designed with crypto-agility in mind – i.e. the ability to switch algorithms via simple, painless software upgrades. Ideally, this process should be controlled and managed centrally to save having to reach out to each and every application individually to upgrade it.

REFERENCES

[1] Hoffstein, J. Pipher, J. Joseph H. 2014. An Introduction to Mathematical Cryptography.

[2] Barke, L. 2020. Recommendation for Key Management. [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf]. Accessed on May 7, 2020.

[3] Rousea, M. 2019. Asymmetric cryptography (public key cryptography).[https://searchsecurity.techtarget.com/definition/asymmetric-cryptography]. Accessed on May 9, 2020

[4] Kessler, G. 2020. An Overview of Cryptography. [https://www.garykessler.net/library/crypto.html]. Accessed on June 3, 2020.

[5] Barke, L. 2020. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. [https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final]. Accessed on April 13, 2020.