Cryptography: A Security Measure

Archana Chhikara
Assistant Professor,
Deptt .of Computer Science,
Hindu College,
Sonepat

Amita Gandhi
Assistant Professor,
Deptt .of Computer Science,
Hindu College,
Sonepat

Abstract

The security of network is a big issue for network security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. Network security consists of the provisions and techniques adopted by a network administrator to prevent and monitor unauthorized access (confidentiality), misuse, modification (integrity), or denial of a computer network (availability) and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network security administrator. Each and every client who is working on the internet wants security of information but sometimes he or she do not know that someone else may be a intruder is collecting the information. Information is an asset that must be protected. Network security is the process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability. To secure the information and the entire network system, one specific methodology is required which can be capable of providing the complete security solutions. In a layered security model, it is often necessary to implement one final prevention control wrapped around sensitive information: Encryption. Cryptography, a word with Greek origins, means "secret writing". However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred only to the encryption and decryption of message using secret keys. Now a days, Cryptography defined as involving three distinct mechanisms: Symmetric-Key encipherment, asymmetric-Key encipherment and hashing. Encryption is not a security solution. It will not solve all your data-centric security issues. Rather, it is simply one control among many. In this paper we look at cryptography's history and its role in security architecture.

Keywords: Encryption, Integrity, Confidentiality, Availability.

Introduction

Cryptography is a science and art that applies complex mathematics and logic to design strong methods for encryption. Achieving strong encryption, the hiding of data's meaning, also requires spontaneous leaps that allow creative application of known or new methods. So cryptography is also an art. Cryptology as a science started many years ago. Cryptography is most often related with the confidentiality of information that it provides. Four basic functions of Cryptography are: Confidentiality, Authentication, Integrity and Non repudiation.

History of Cryptology

The Manual Era

Manual cryptography was the first and starting period of manual cryptography, and continuing through World War I. In this era cryptography was limited only to the efficiency of operator who use simple mnemonic devices. As a result, encrypted text were limited in size and achieved limited security.

The Mechanical Era

Mechanization of cryptography is the second period, which began shortly after World War I and continues till now. In this period, the rotor machines replaced the manual operator of the Manual Era. These machines could perform complex operations and they could encrypt and decrypt faster, with less chance of error. The U.S. government designed and fabricated a single silicon chip implementation of the Data Encryption Standard (DES) in 1999. The Advanced Encryption Standard (AES) can be implemented in a single silicon chip to handle on an Internet. The volume of cipher text that had to be dealt with on a communication channel had increased almost billion fold, and it increases continuously.

The Modern Era

Modernization of cryptography is the third period, in which - the dramatic extension of cryptology to the information age: digital signatures, authentication, shared or distributed capabilities to exercise cryptologic functions.

Techniques of Cryptography

Symmetric Key cryptography

Symmetric Key Cryptography is referred by some other terms such as **secret key cryptography** or **private key cryptography**. In symmetric key cryptography, only one secret key is used for both encryption and decryption. The keys represent a shared secret between sender and receiver that can be used to maintain privacy while sharing data. The main drawback of symmetric key encryption is **key distribution** or **key management** and shared secret key between sender and receiver. Symmetric-key encryption can use either stream ciphers or block ciphers.

Asymmetric Key Cryptography

Asymmetric key Cryptography is referred by the term **public key cryptography.** In asymmetric key cryptography, two different are used, among them one key is used for encryption and the other corresponding key is used for decryption. One of which is *secret* (or *private*) and one of which is *public*. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. Asymmetric key cryptography solves the **key distribution** problem of symmetric key cryptography because only one pair of key is needed for communicating with any number of communicating parties. Moreover, it is practically impossible to deduce the private key from the known public key.

RSA (Ron Rivest, Adi Shamir & Leonard Adleman (MIT, 1977)) Algorithm is used in Asymmetric key Cryptography.

Cryptography Hash Function

Cryptography Hash Function is a function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the message, and the hash value is often called the message digest or simply the digest.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (*digital*) *fingerprints*, *checksums*, or just *hash values*, even though all these terms stand for more general functions with rather different properties and purposes.

Risk Factors for Cryptography Systems

Unpredictability of Keys

To prevent key generation from being predictable, keys must be generated randomly. However, keys that are generated by computer software are never generated in a truly random manner. At best, software-key generators use pseudo-random processes to ensure that virtually no one can predict what keys are going to be generated. However, if an attacker can predict the major variables that are used in key generation, he or she also can predict what keys will be generated. To provide maximum protection of highly valuable information, consider deploying security solutions that provide truly random, hardware-generated keys.

Length of Public Key

A key of the same length, public key cryptography generally is more susceptible to attack than symmetric key cryptography, particularly to factoring attacks. In a factoring attack, the attacker tries all of the combinations of numbers that can be used with the algorithm to decrypt cipher text. Factoring attacks are similar to key search attacks, but the number of possible factors varies with each algorithm and with the length of the public key and private key that are used. In general, for a given key length, a factoring attack on a public key requires fewer attempts to be successful than a key search attack on a symmetric key.

Lifetime of keys

Key length is only one factor in the strength of both symmetric key and public key cryptography algorithms. The longer that a secret key or private key is used, the more susceptible it is to attack. The longer a key is used, the greater the amount of information that is encrypted with the key. In addition, a longer key lifetime also gives attackers more time to exploit weaknesses in the cryptography algorithm or its implementation.

Strength of the Security Technology

The strength of cryptography-based security depends on the strength of the encryption algorithm and the technology that implements the security. A weak algorithm or a poorly implemented security technology can be exploited to decrypt any cipher text that it produces. For example, a weak algorithm can produce cipher text that contains hints or patterns that greatly aid cryptanalysis. A poorly implemented security technology might also provide unintentional backdoors that attackers can discover and exploit. For example, a poorly implemented security technology might provide a way for attackers to obtain secret keys from memory caches.

Storage of Private Keys

The security of private keys is crucial for public key cryptosystems. Anyone who can obtain a private key can use it to impersonate the rightful owner during all communications and transactions on intranets or on the Internet. Therefore, private keys must be in the possession only of authorized users, and they must be protected from unauthorized use.

Length of Symmetric key

Symmetric key encryption is subject to key search attacks (also called brute force attacks). In these attacks, the attacker tries each possible key until the right key is found to decrypt the message. Most attacks are successful before all possible keys are tried.

Strength of Security Protocols

Cryptography-based security technologies are implemented by using security protocols. For example, secure mail systems can be implemented by using the S/MIME protocol, and secure network communications can be implemented by using the IPSec suite of protocols. Likewise, secure Web communications can be implemented by using the TLS protocol. Standards for security protocols, however, whether proprietary or open standards, often contain weaknesses or limitations that attackers can exploit (for example, to launch denial of service attacks). Even the best implementations of protocol standards contain the weaknesses and limitations that are inherent in the standards.

Conclusion

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication.

References

1. Cipher-block chaining. (2012). In *wikipedia.org*. Retrieved from http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Cipher-block_chaining_.28CBC.29
2. Electronic codebook. (2012). In *wikipedia.org*. Retrieved from http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Electronic_codebook_.28ECB.29
3. enStratus. (2012). *enStratus Security Architecture.* Retrieved May 21, 2012, from enStratus Networks, Inc.: http://enstratus.com/media/document/1/security_architecture.pdf
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications* (Kindle ed.). Indianapolis, IN: Wiley Publishing.
5. Key escrow. (n.d.). In *Webopedia.* Retrieved from http://www.webopedia.com/TERM/K/key_escrow.html
6. Microsoft. (2005, December). *Data Confidentiality*. Retrieved May 16, 2012, from MSDN: http://msdn.microsoft.com/en-us/library/ff650720.aspx
7. Mogull, R. (2005, August). *Management Update: Use the Three Laws of Encryption to Properly Protect Data.* Retrieved February 4, 2006, from Gartner: http://www.gartner.com
8. NIST. (2001, November 26). *Advanced Encryption Standard.* Retrieved May 15, 2012, from NIST Computer Security Resource Center: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
9. NIST. (2010, February 16). *Block Cipher Modes*. (N. I. Technology, Producer) Retrieved May 15, 2012, from Computer Security Resource Center: http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html
10. Olzak, T. (2006, February). *Data Storage Security.* Retrieved May 19, 2012, from Adventures in Security: http://adventuresinsecurity.com/Papers/Data_Storage_Security.pdf
11. Ortiz, C. E. (2005, September). *The Security and Trust Services API (SATSA) for J2ME: The Security APIs*. Retrieved 18 2012, May, from Oracle Sun Developer Network: http://developers.sun.com/mobility/apis/articles/satsa2/
12. RSA. (2009). *Securing Sensitive Data with Tokenization: An Emerging Technology.* Retrieved May 19, 2012, from RSA Security Inc.: http://rsa.com
13. Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Kindle ed.). New York: Anchor Books.
14. Vormetric. (2010). *Vormetric Data Security Architecture.* Retrieved May 19, 2012, from Vormetric, Inc.: http://enterprise-encryption.vormetric.com/wp-vormetric-data-security-architecture.html
15. Zim, H. S. (1962). *Codes and Secret Writing.* Scholastic Book Services.
16. Zimmerman, P. (1994, October 11). *PGP User's Guide, Volume 1: Essential Topics*. Retrieved May 19, 2012, from Michigan State University: http://www.pa.msu.edu/reference/pgpdoc1.html#section-4