ITMR

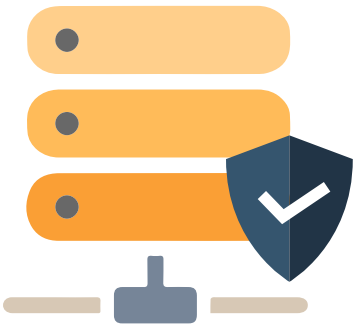
योगः कर्मसु कौशलम्

WHITE PAPER ON

Data Encryption

Prepared by **Mohammed Samiuddin**

Contents



Introduction

Data encryption is the act of changing electronic information into an unreadable state by using algorithms or ciphers. Data encryption refers to mathematical calculations and algorithmic schemes that transform plaintext into ciphertext, a form that is non-readable to unauthorized parties. The recipient of an encrypted message uses a key that triggers the algorithm mechanism to decrypt the data, transforming it to the original plaintext version. Before the evolution of Internet, data encryption was mostly used as military security tool. With the prevalence of online shopping, banking and other services, even basic home users are aware of data encryption. Nowadays, web browsers will automatically encrypt text when connecting to a secure server. A secure, encrypted website URL begins with "https", meaning Hypertext Transmission Protocol Secure.

Data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorisation. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message.

Need For Data Encryption

There are many factors contributing to the increased need for data encryption. Although the drivers vary, together they help illustrate the importance of implementing a proactive security strategy that features a comprehensive encryption solution.

Due Care

Due care is a legal concept that refers to the care a reasonable and prudent person would exercise in protecting organisation assets. It is the responsibility of the organisation to protect the private information of its customers. This holds even if the job of handling the data is managed by a third party. Hence, an organisation must have reasonable and appropriate measure available to meet the standards.

Reputational Risk

The significant factors determining the success of an organisation in today's world are consumer trust, brand image, reputation, etc. Data being one of the primary asset of any organisation, protecting them with encryption is a less expensive than paying for clean-up after a data breach or massive records loss.

Regulatory Risk

Regulatory noncompliance can also result in stiff financial consequences. Regulations like CA SB 1386, Gramm-Leach-Bliley and HIPAA are few among the powerful regulations which organisations must comply.

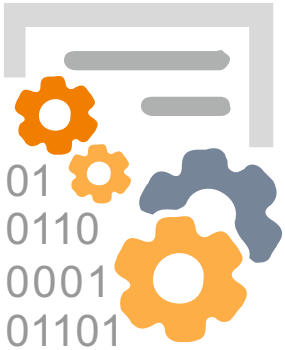
Types of Data encryption

Single Key Encryption

Single Key Encryption is also known as private key, single key, secret key, or symmetric encryption. It is one of the oldest encryption methodologies. This method suited only for communication between small groups of trusted people sharing a secret encryption key. In single key encryption, the sender and recipient of the data both holds the same key for translation. This single key is used to code and also decode information exchanged between two parties. Since the same key is used to encrypt and decrypt messages, the parties involved must exchange the key secretly and keep it secure from outsiders. Private Key encryption systems are usually faster than other types. However, in a situation where large group of people want to communicate securely (such as modern Internet commerce) it is impossible for everyone to share a 'secret' key. This problem was solved by the advent of asymmetric or public key Encryption.

Public Key Encryption

The second, and more commonly used data encryption system is known as a public key system. This approach involves pairs of keys: a 'public' key and a 'private' key. Once information has been encrypted with the public key, nobody but the holder of the private key can decrypt it. In reverse, if the private key is used for encryption, anyone with the public key can decrypt it. It is difficult to derive the private key from the public key. Public Key Encryption is widely used in electronic commerce. Public key encryption is slower than Single Key Encryption, even on fast computers, so most modern encryption uses a combination of both methods.



Standards

Data Encryption Standard (DES)

DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption determines the cipher type. DES is therefore a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time. The key size used is 56 bits; however, a 64 bit (or eight-byte) key is the actual input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily, and does not increase the security.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm for data encryption and decryption. The algorithm allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits.

AES was designed to have the following characteristics:

- Resistance against all known attacks
- Speed and code compactness on a wide range of platforms
- Design Simplicity

Data Encryption Modes of Operation

A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application. These can be used with any symmetric block cipher algorithm such as DES, 3DES or AES. The five modes of operation are:

1.Electronic Codebook (ECB) Mode

2.Cipher Block Chaining (CBC) Mode

3.Cipher Feedback (CFB) Mode

4.Output Feedback (OFB) Mode

5.Counter (CTR) Mode

Applications of Encryption

Encryption plays a major role in confidentiality, access control, integrity and non-repudiation. Some of the applications are:

1. Pretty Good Privacy (PGP) and S/MIME for e-mail encryption.

2. Secure Sockets Layer (SSL) is an encryption protocol that enables secure communications and user authentication over unsecured networks like the Internet.

3. An international security standard called Wi-Fi Protected Access (WPA2) applied to encrypt data sent over wireless networks.

4. Digital television providers control subscriber access by encrypting audio and video signals. Subscribers are equipped with a descrambling device comprising the decryption algorithm and decryption key, which together decrypt pictures and sound.

5. Digital signatures allow parties to sign e-mails or documents electronically. They can be used to verify integrity (to check who sent a document and to confirm that no-one else has modified it). They can also be used for non-repudiation: if a party digitally signs an electronic document, they cannot later deny this.

Conclusion

Encryption is one or the widely available tools to safeguard the electronic information and privacy. It is the responsibility of organisations to choose the right encryption solution or select an encryption vendor. However, sensitive information could still be vulnerable if the vendor's product is unreliable or ineffective. Today, most of the organisations have implemented strong encryption methodologies to protect their valuable data. With the evolution of the Internet commerce, the need for encryption has grown rapidly. Thus, there is a need for the organisations to constantly monitor the advances in the encryption technology to ensure their data is secured and protected.

Glossary

CA SB 138: California S.B. 1386 was a bill passed by the California legislature. It is Enactment for notification to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person.

The Gramm-Leach-Bliley Act (GLB Act or GLBA): This act is also known as the Financial Modernisation Act of 1999. It is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.

HIPAA: This is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

Data Encryption –

http://www.spamlaws.com/data-encryption.html

http://www.inc.com/encyclopedia/data-encryption.html

Data Encryption Types and Standards –

http://www.site.uottawa.ca/~chouinar/Handout_CSI4138_DES_2002.pdf

http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf

http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

http://www.vocal.com/cryptography/data-encryption-standard-des/

http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

Applications –

http://www.parliament.uk/documents/post/postpn270.pdf

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research

(Division of Mamta Trust)

2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.

Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,

Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349

Contact for More Information: training@htcitmr.ac.in