ENCRYPTION SERVICES

What is Encryption?

ENCRYPTION

Encryption is the process of converting plain text to cipher text that is non-readable. The algorithmic schemes used to encrypt and decrypt the information are referred to as encryption algorithms.

The vulnerability of the data can be significantly reduced by encrypting the data or encrypting the transmission path taken by the data along the network. Encrypting the data is referred to as data-level encryption and encrypting the path is referred to as session encryption.[1]

"The vulnerability of data can be significantly reduced by encrypting data or encrypting the transmission path."

[1] A First Data White Paper A Primer on Payment Security Technologies: Encryption and Tokenization: https://files.firstdata.com/downloads/thought-leadership/primer-on-payment-security-technologies.pdf

WHAT CAN I ENCRYPT?

In data-level encryption, the encryption is applied to sensitive data elements. The process where the encryption is applied on the data elements determine if the data is protected from internal fraud and/or external fraud.

In session-level encryption, the communication path in which the transaction flows from source to destination is encrypted. The sensitive data inside the encrypted path/ tunnel may be a clear text. This method is used when the sender (of data) doesn't control the path all the way out to the receiver. e.g. E-commerce over the Internet. Using Secured Socket Layer (SSL) it is easy to establish encryption for the communication session between the end-user and the e-commerce web page.

If a user needs end-to-end protection of data, measures must be taken to keep it secure in all the three states: at rest, in use, and in motion. [2]

ENCRYPTION IN TRANSIT

Data is at its most vulnerable when it is in motion. Protecting information in transit requires specific capabilities. The best way to protect data in transit is to use an encryption platform that integrates with the users existing systems and workflows. Encrypted connections like HTTPS, SSL, TLS (the newer more secure and more versatile replacement for SSL), SFTP, etc. are used to protect the contents of data in transit.

The Transport Layer Security (TLS) protocol, Secure Sockets Layer (SSL) protocol, and the Private Communications Transport (PCT) protocol are based on public key cryptography. The Security Channel (Schannel) authentication protocol suite provides these protocols and it uses a client/server model. In the authentication process, a TLS client sends a message to a TLS server, and the server responds with the information that the server needs to authenticate itself. The client and server perform an additional exchange of session keys, and the authentication dialog ends. When authentication is completed, SSL-secured communication can begin between the server and the client using the symmetric encryption keys that are established during the authentication process.[3]

[2] Best Practices: Securing Data at Rest, in Use, and in Motion : https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/

[3] What is TLS/SSL?: https://technet.microsoft.com/en-au/library/cc784450(v=ws.10).aspx

TLS secures transmitted data using encryption, authenticates server, authenticates clients (optional) to prove the identities of parties engaged in secure communication and provides data integrity through an integrity check value. TLS can be used protect against masquerade attacks, man-in-the-middle or bucket brigade attacks, rollback attacks, and replay attacks. TLS works with most Web browsers and is often integrated in news readers, LDAP servers, and a variety of other applications. TLS provides options for the authentication mechanisms, encryption algorithms, and hashing algorithms that are used during the secure session Error! Bookmark not defined..

A Virtual Private Network (VPN) is designed to provide a secure, encrypted tunnel in a public network. Data is then transmitted between the remote user and the organisation's network using this tunnel. IPsec-based virtual private network (VPN) encrypts traffic between end points and can protect against eavesdropping, man-in-the-middle, and denial-of-service (DoS) attacks. Initially VPNs were set up using dedicated VPN hardware. As our systems have grown more sophisticated, software firewalls and VPN virtual appliances have become more commonplace. A VPN offers significant cost savings over hardware appliances and can be scaled up by new virtual instances. However, virtualised VPN appliances may share resources with other VMs, and availability may be affected during peak loads. [4]

ENCRYPTION AT REST

Data is at rest when it is stored on a hard drive. Perimeter-based defences methods such as firewalls and anti-virus programs are commonly used when data is at rest. However, for stronger protection, organisations need additional measures to protect sensitive data from intruders. Encrypting hard drives ensures the security of data at rest. Similarly, storing individual data elements in separate locations decrease the chances of attackers gaining all the important information.

Transparent encryption (on-the-fly encryption (OTFE)) is used by some disk encryption software and it automatically encrypts or decrypts data that is saved in the hard drive. The files in encrypted disk are accessible only using the correct key. [5]

[4] Securing Data in Transit: https://cdn2.hubspot.net/hub/407749/file-2454417150-pdf/Downloads/WP_Securing_Data_in_Transit.pdf?t=1452903009655

ENCRYPTION IN USE

Data in use is more vulnerable than data at rest. The keys to securing data in use are to control access as tightly as possible and to incorporate some type of authentication to avoid the use of stolen identities. Businesses should be able to track and report relevant information so they can detect suspicious activity and diagnose potential threats.

Major vulnerabilities are exploitable at the OS level and the best way to prevent OS level exploits is to use a web proxy and monitor and prevent malicious attachments via email.

Cogito Group is an award-winning ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies.