Fact Sheet

Cogito Group

Encryption Services

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

What Can I Encrypt?

In data-level encryption, the encryption is applied to sensitive data elements. The process where encryption is applied to the data elements determine if data is protected from internal 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 clear text.

This method is used when the data sender doesn't control the path all the way to the receiver, often seen in e-commerce transactions. The use of Secured Socket Layer (SSL) eases the establishment of 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 that data secure in all 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 uses a client/server model. In the authentication process, the TLS client sends a message to the TLS server, and the server responds with the information that the server needs to authenticate itself.

The client and server then 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]

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. It can be used to protect against masquerade attacks, man-in-the-middle or bucket brigade attacks, rollback attacks, and replay attacks. TLS works with most Web browsers and it often integrated in news readers, LDAP servers, and a variety of other applications. It provides options for the authentication mechanisms, encryption algorithms, and hashing algorithms that are used during the secure session.

A Virtual Private Network (VPN) is designed to provide a secure, encrypted tunnel in a public network. Data is transmitted between the remote user and the organisation's network using this secure, encrypted tunnel. An IPsec-based 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, beneficial for environments that were static and when hosts were on the same network.

Today, software firewalls and VPN virtual appliances are the more common solutions to these problems. They offer significant cost savings over hardware appliances and can be scaled up by new virtual instances. Virtualised VPN appliances, however, 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. 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 important information.

Transparent encryption, also known as On-The-Fly Encryption (OTFE), is used by some disk encryption software and automatically encrypts or decrypts data that is saved in the hard drive. The files in encrypted disk are accessible only through using the correct key.[5]

Encryption in use

Data in use is more vulnerable than data at rest. The key to securing data in use are to control access as tightly as possible, and to incorporate a form of authentication to avoid the use of stolen identities. Organisations 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 most effective prevention against OS level exploits is the use of a web proxy, and the monitoring of and prevention against malicious attachments via email.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated 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. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.

[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

[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

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

[5]TrueCrypt User's Guide: https://www.grc.com/misc/truecrypt/TrueCrypt%20User%20Guide.pdf