INTERNET SECURITY

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Types of security

Network layer security

TCP/IP can be made secure with the help of cryptographic methods and protocols that have been developed for securing communications on the Internet. These protocols include SSL and TLS for web traffic, PGP for email and IPsec for the network layer security.

IPsec Protocol

This protocol is designed to protect communication in a secure manner using TCP/IP. It is a set of security extensions developed by IETF and it provides security and authentication at the IP layer by using cryptography. To protect the content, the data is transformed using encryption techniques. There are two main types of transformation that form the basis of IPsec the Authentication Header (AH) and Encapsulating Security Payload (ESP). These two protocols provide data integrity, data origin authentication and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

The basic components of the IPsec security architecture are described in terms of the following functionalities :

- Security protocols for AH and ESP
- Security association for policy management and traffic processing
- Manual and automatic key management for the internet key exchange (IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays and confidentiality. The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

Security Token

Some online sites offer customers the ability to use a six digit code which randomly changes every 30-60 seconds on a security token. The key on the security token have mathematical computations built-in and manipulate numbers based on the current time built into the device. This means that every thirty seconds there's only a certain possible array of numbers which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that devices' serial number and therefore would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that would work in that given 30-60 second cycle. After the 30-60 seconds the device will present a new random six-digit number which can log into the website.

Electronic Mail Security (E-mail)

Email messages are composed, delivered,hes composing the message and sends it, the message is transformed into a standard format an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur recipient server identification, connection establishment and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

Pretty Good Privacy (PGP)

PGP provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such Triple DES or CAST-128. Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of its sender.
- Encrypting the body of an email message to ensure its confidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both the message body and message header.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other. For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.