Communications Security Protocols

This lecture describes some protocols that are used to secure communications.

SSL and TLS

This protocol, first known as SSL (Secure Sockets Layer), was defined in 1994 by Netscape for securing communication between web browsers and servers. The current version is called Transport Layer Security (TLS) and is probably the most common security protocol.

TLS operates at the "session" layer because it encrypts a TCP connection (this corresponds to a "session" in OSI terminology). TLS provides secrecy, authentication and integrity. It is most often used for securing access to web sites using the HTTP (Hypertext Transport Protocol), but can also be used for secure versions of other TCP-based protocols such as FTP (file transfer) and SMTP (mail transport).

A TLS session begins with a negotiation of compatible ciphers (both public-key and symmetric) and hash algorithms. The server then sends it's public key in a certificate and the client checks it and verifies that the server knows the private key by asking the server to decrypt a random value that is encrypted with the server's public key. This randomly-chosen value is then used to derive session keys.

Various public-key and symmetric encryption algorithms and hash functions can be used, including RSA, AES and SHA-1 described previously.

Since access to a web site may involve many connections over a short period of time, a session ID can be used to recall previously-negotiated encryption parameters.

S/MIME

S/MIME (secure multipurpose internet mail extensions) is an IETF protocol for securing e-mail. It can provide authentication, secrecy and also digital signatures.

S/MIMIE is based on public-key encryption and uses a certificate format called PKCS7. For authentication, a user can obtain a certificate signed by a CA that has verified their identity.

Once a user receives a public key from an initial signed but un-encrypted message the public key can be used to encrypt a reply. This typically includes the repllying party's own certificate and from then on the exchange can happen securely.

IPSec

IPSec is another IETF security protocol similar to TLS whose purpose is to encrypt connections on IP networks. However, while the TLS protocol is implemented in an application (e.g. a web browser), IPSec is typically used to set up secure connections that are used by unmodified applications. IPSec can use private ("pre-shared") keys as well as public keys. The main application of IPSec today is VPNs.

VPNs

A VPN (Virtual Private Network) is a way to emulate a private connection between two endpoints, typically two routers. A typical application is to connect a remote office to a corporate LAN. All IP traffic passed between the two routers is passed through a secure "tunnel" that ensures the endpoints are authenticated and that traffic is encrypted. Since all IP traffic (including DHCP and DNS) can be passed over the tunnel, devices connected to the remote router appear to be connected to the central LAN.

SSH

SSH (Secure SHell) is a remote terminal application that is primarily used to connect to a shell program (command interpreter) on a remote computer. However, SSH can also be used to transfer files (by piping data between processes on the two ends) and also allows a user to set up tunnels that connect TCP ports on the two ends.

SSH supports various authentication mechanism including public-key authentication and passwords. Various encryption algorithms can be negotiated.

802.1x

802.1x is a standard for authenticating users before they are allowed to use a LAN (or WLAN) interface on a bridge (typically also a router). It requires the use of authentication server that stores credentials (often passwords) for authorized users.

A client (e.g. a PC, called a "supplicant") that want to communicate through the router exchanges messages with the router ("authenticator") which in turn verifies the supplicant's with an authentication server. The most common protocol for this is EAP (Extensible Authentication Protocol) which allows for many different authentication algorithms. Examples include EAP-PSK (a pre-shared key), PEAP (EAP protected by TLS) and EAP-TLS which uses the TLS authentication mechanisms including a client certicate.

802.1x allows (requires) a centralized authentication database and so is used when there are many different users connecting to many different devices. It avoids the need to have a single access password shared between all users and avoid having to embed authentication information in each router.

The authentication server typically uses a protocol called RADIUS (Remote Authentication Dial In User Service). Authentication is performed using a sequence of challenges to verify the authenticity of the supplicant. Typically this involves having the supplicant respond with a hash of the password, possibly combined with a challenge.