KUS KIHIS TEKIB TURVALINE SIDEKANAL?

1) kanali kihis **–** näit. “taevakanalite” skrämblerid

2) võrgu kihis – näit. *IP Security*

3) transpordi kihis – näit. *TLS*

4) rakenduskihi ja transpordikihi vahel – näit. *SSL, SSA*

5) rakenduskihi objektis – näit. *turvaline elektronpost*

IPSEC – IP Security

RFC 1826 - IP Authentication Header

RFC 1827 - IP Encapsulating Security Payload (ESP)

TLS (Transport Layer Security) Protocol.

Version 1.0 RFC 2246

The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the **TLS Record Protocol** and the **TLS Handshake Protocol.**

At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- The connection is private. Symmetric cryptography is used for data encryption (e.g., DES [DES], RC4 [RC4], etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.

- The connection is reliable. Message transport includes a message integrity check using a keyed MAC (*Message Authentication Code*). Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

The TLS Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties:

- The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA [RSA], DSS [DSS], etc.). This authentication can be made optional, but is generally required for at least one of the peers.

- The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.

- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

One advantage of TLS is that it is application protocol independent. Higher level protocols can layer on top of the TLS Protocol transparently. The TLS standard, however, does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers and implementors of protocols which run on top of TLS.

Goals

The goals of TLS Protocol, in order of their priority, are:

1. **Cryptographic security**: TLS should be used to establish a secure connection between two parties.

2. **Interoperability**: Independent programmers should be able to develop applications utilizing TLS that will then be able to successfully exchange cryptographic parameters without knowledge of one another's code.

3. **Extensibility**: TLS seeks to provide a framework into which new public key and bulk encryption methods can be incorporated as necessary. This will also accomplish two sub-goals: to prevent the need to create a new protocol (and risking the introduction of possible new weaknesses) and to avoid the need to implement an entire new security library.

4. **Relative efficiency**: Cryptographic operations tend to be highly CPU intensive, particularly public key operations. For this reason, the TLS protocol has incorporated an optional session caching scheme to reduce the number of connections that need to be established from scratch. Additionally, care has been taken to reduce network activity.

SSL – Secure Sockets Layer
(Netscape – avalikud võtmed)

How SSL Works
http://developer.netscape.com/tech/security/ssl/howitworks.html

SSA – Secure Sockets Agent
http://www.cyber.ee/infoturve/tooted/ssa/index.html