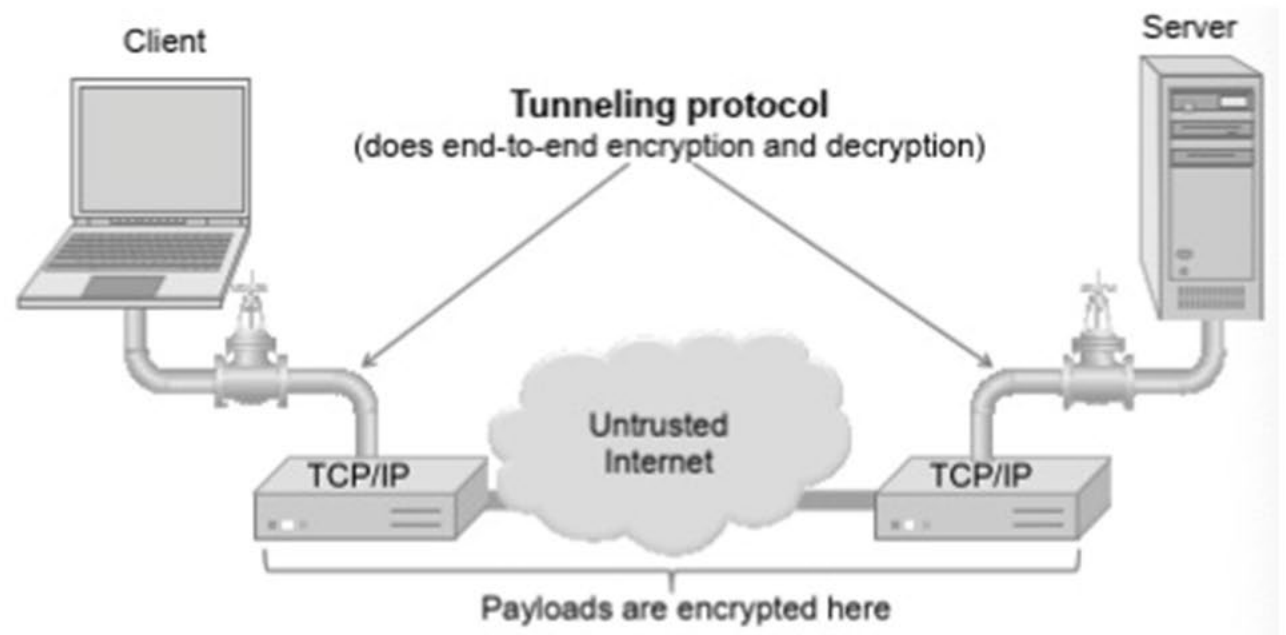


Tunneling

➤ SSH, VPN, SSL, TLS, IPSec

As the Internet is not secure by default, if someone is eavesdropping on a TCP connection, they can often see the complete contents of the payloads in this session. One way to prevent such eavesdropping without changing the software performing the communication is to use a tunneling protocol.



SSH, SSL, HTTPS?

- All form encrypted tunnels.
- SSH - secure sockets handler
 - specifies the protocols that occur in the encrypted tunnel.
 - includes multiplexing and **user authentication**
 - an application which replaces Telnet (sort-of application layer).
- SSL - Secure Sockets Layer
 - uses certificate (X.509)-based key exchange
 - encrypts **data only** (sort-of transport layer)
- HTTPS
 - HTTP tunneled through SSL (now referred to as TLS)
 - <http://security.stackexchange.com/questions/1599/what-is-the-difference-between-ssl-vs-ssh-which-is-more-secure>

SSH

- Secure Shell (SSH), secure copy protocol (SCP) and secure file transfer protocol (SFTP)
- Application layer protocol that encrypts application layer payload and then sends it by TCP.
- Uses a range of crypto (keys, certificates)
- Nullifies sniffing attacks. **BUT requires chain of trust**
- Can use server-side certificates only (like https) or server and client certificates.
- Built-in username/password authentication


SSL..

1. TCP connection established
2. Client requests connection to server
3. Server sends **certificate (X509)** and **public key**
4. Client compares key with those in its cache, CA.
User asked to accept/cache key
5. Client creates session key and sends it to server encrypted with server's public key
 - Server may request client public key (**optional**)
 - Server may check client's public key (cache/CA)
6. All subsequent traffic encrypted by session key

SSH vs SSL

- SSH: Encrypt-then-MAC

- Send ciphertext and MAC
- Proves integrity
- Encryption is a bit weaker
(easier to brute-force key)



Message
Authentication
Code
Think:
Checksum

- SSL: MAC-then-Encrypt

- MAC added to plain text and then both are encrypted
- Vulnerable to some known plain text attacks (BEAST attack).

SSL Vulnerability

- Heartbleed (2014)
 - Affects some OpenSSL libraries
 - Problem with the "Heartbeat" keep-alive packet
 - Allows user to scrape 64kB of RAM **before authentication.**
 - Get other people's logins
- Fix:
 - Patch OpenSSL or use a different SSL library.
- See Podcast, Slides (Blackboard)

IP Security (IPsec)

- Suite of protocols from Internet Engineering Task Force (IETF) providing encryption and authentication at the IP layer
 - Arose from needs identified in RFC 1636
 - Specifications in:
 - RFC 2401: Security architecture
 - RFC 2402: Authentication
 - RFC 2406: Encryption
 - RFC 2408: Key management
- Objective is to encrypt and/or authenticate all traffic at the IP level.

IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
 - TLS for Web, S/MIME for email, SSH for remote login
- IPsec aims to provide a framework of open standards for secure communications over IP
 - Protect every protocol running on top of IPv4 and IPv6

IPsec Benefits

- Provides a level of security for all applications.
 - Allows deployment of new/emerging applications that may not have their own security.
- Transparent to transport layer.
- Transparent to end-users.
 - No need for training, key issue, key revocation, etc.
- Can be provided to individual users where needed (e.g. off-site workers).
- Extensible to new, stronger, cryptographic methods as these become available.

IPsec Drawbacks

- Processing performance overhead
 - Protection is applied to all traffic, though only a small portion may be security-sensitive
- Blocks access to non-IPsec hosts
- Hosts must have security association
 - Not great for short-lived connections
- Not practical for broadcast

Uses of IPsec

- Virtual Private Network (VPN) establishment
 - For connecting remote offices and users using public Internet
- Low-cost remote access
 - e.g. teleworker gains secure access to company network via local call to ISP
- Extranet connectivity
 - Secure communication with partners, suppliers, etc.

VPN

- Virtual Private Network
- Tunnels all traffic (all packets) over a public network.
- Works with non-routable packets
- Encrypts IP packets and sends them over public TCP/IP as encrypted payloads.
- Many implementations, some vulnerable
 - PPTP (point to point tunneling protocol)
 - L2TP (layer 2 tunneling protocol)

VPN

- Tunneling provides separation between the outside of the tunnel (internet) and the inside (trusted private network).
- Provides no protection within the private network.
- If an **endpoint gets infected**, malware can pass through the tunnel to the rest of the private network without any barriers.
- Equivalent to LAN access to the trusted network.