CSC 402 – Internet Technology

Recap

- Benefits and drawbacks of Intranets
- Protocols, Structure and Scope of Networks
- Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources
- Intranet Implementation Guidelines
- Tunneling Protocols: VPN
- Tunneling Protocols: VPN Taxonomy
- Tunneling Protocols: VPN Security Protocols

Tunneling Protocols: VPN Security Protocols

- Confidentiality (aka Privacy) – to prevent eavesdropping of the tunnel data traveling through the Internet.
  - Cryptographic algorithms.
- Integrity – to ensure that the received tunnel data are identical to the sent data.
  - One-way hash functions.
- Authentication – to ensure that any request for tunnel creation comes from a legitimate client and to ensure that the data have originated from an authorized sender and have not been modified in the tunnel.
  - Digital signatures.
- Certification – to establish the identity of the tunnel peer entities before keys are exchanged.
  - Digital certificates issued by a trusted third party.
- Access control – tunnel endpoints must limit access to legitimate users.
  - Firewalls or other filtering mechanisms at the tunnel endpoints
- Key management – to have an efficient mechanism by which the keys are exchanged during a session.

Tunneling Protocols: VPN Security Protocols

- Several tunneling protocols have been developed for VPNs.
- They are broadly distinguished by the OSI layer at which they work:
  - Layer 2.
  - Layer 3.
  - Higher layers.
- Layer 2 tunneling protocols :
  - PPTP (Point-to-Point Tunneling Protocol).
  - L2F (Layer 2 Forwarding).
  - L2TP (Layer 2 Tunneling Protocol).
- Layer 3 tunneling protocols :
  - IPSec (IP Security).
- Higher-layers tunneling protocols :
  - SSL/TLS (Secure Sockets Layer/Transport Layer Security).
  - SSH (Secure Shell).

Tunneling Protocols: VPN Security Protocols

- Point-to-Point Tunneling Protocol (PPTP).
- PPTP – a layer 2 tunneling protocol that provides authenticated and encrypted access from desktops to remote-access servers.
- The protocol uses PPP (Point-to-Point Protocol) data link connections and comes in 2 operational modes:
  - In the first mode, the ISP's access server intercepts the remote user's PPP connection and builds a tunnel to the corporate network.
  - In the second mode, the VPN tunnel can be constructed all the way from the remote user to the corporate network.
- PPTP relies on the encryption and authentication mechanisms provided by PPP, namely:
  - For encryption: DES (Data Encryption Standard) and 3DES.
  - For authentication: PAP (Password Authentication Protocol).
  - CHAP (Challenge Handshake Authentication Protocol).

Tunneling Protocols: VPN Security Protocols

- Layer 2 Forwarding (L2F).
- Cisco proposed a proprietary layer 2 tunneling protocol called L2F as a competitor for PPTP.
- It uses PPP for encryption and authentication but extends authentication to support TACACS+ (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial-In User Service) authentication by using EAP (Extensible Authentication Protocol).
- While PPTP supports only IP, L2F can run on top of other layer 2 protocols such as ATM and Frame Relay.

Tunneling Protocols: VPN Security Protocols

- Layer 2 Tunneling Protocol (L2TP).
- In order to remove the non-interoperability limitation of L2F, it was combined with PPTP to produce the IETF and industry standard L2TP.
- This layer 2 protocol includes all the features of PPTP and L2F in addition to being interoperable.

Tunneling Protocols: VPN Security Protocols

- IP Security (IPSec)
- IPSec – a layer 3 tunneling protocol for IP proposed by the IETF as a set of open standards.
- It can provide per-packet, end-to-end, and segment-by-segment protection.
- Moreover, it accommodates a wide variety of strong cryptographic algorithms for privacy, integrity, and authentication and an effective key management procedure.
- While PPTP, L2F, and L2TP are mainly applicable to user-site VPNs, IPSec can be targeted for both site-site and user-site VPNs.

Tunneling Protocols: VPN Security Protocols

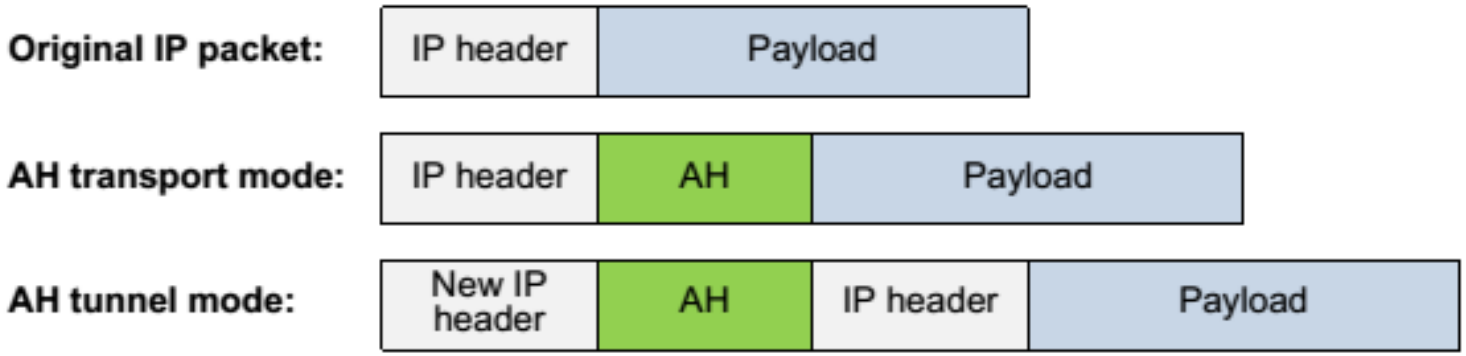
- In essence, IPSec is a framework (as opposed to a single protocol) for providing security services.
- As a framework, IPSec provides great freedom:
  - IPSec is highly modular, allowing users (system administrators) to select from a variety of encryption algorithms and security protocols.
  - IPSec allows users to select from a large number of security services, including privacy, integrity, authentication, etc.
  - IPSec allows users to control the granularity with which the security services are applied (e.g., allows to protect a particular data flow).
- IPSec operates at the network layer of the OSI model:
  - This makes IPSec more flexible, as it can be used for protecting both TCP and UDP traffic (in contrast to SSL/TLS).
  - An application does not need to be designed to use IPSec, whereas the ability to use SSL/TLS or another higher-layer tunneling protocol must be incorporated into the design of an application.
- IPSec is a mandatory part of IPv6, but is not an integral part of IPv4.
  - However, because of the slow deployment of IPv6, IPSec is most commonly used to secure IPv4 traffic.

Tunneling Protocols: VPN Security Protocols

- 3 main components of IPSec :
  - Authentication Header (AH).
  - Encapsulating Security Payload (ESP).
  - Internet Key Exchange (IKE).
- Authentication Header (AH).
- AH ensures integrity and authentication of the packet.
  - No encryption is provided with AH.
- AH contains:
  - Hashed message digest for the contents of the packet (HMAC-MD5, SHA-1).
  - Sequence number for prevention of replay attacks.
  - Security parameters index (SPI).
- SPI is a key to the security association (SA) database and is basically a pointer to the algorithm used (from the many in the set) for the calculation of the message digest.

Tunneling Protocols: VPN Security Protocols

- AH can be applied in 2 modes:
  - Transport
  - Tunnel
- The difference between them is that in the tunnel mode a new IP header is added in front of AH.
  - The new IP header has the tunnel endpoints as the source and destination addresses.
- Irrespective of which mode is applied, the entire packet is authenticated.

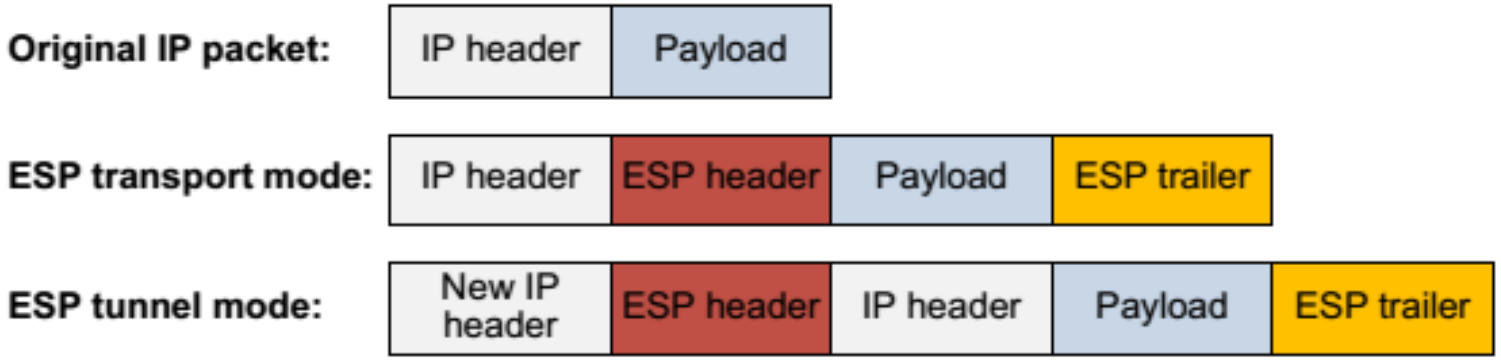


Tunneling Protocols: VPN Security Protocols

- In the transport mode , only the payload of the IP packet is encrypted and/or authenticated.
  - Thus, the routing is intact, since the IP header is neither modified nor encrypted.
  - However, when the authentication is used, the IP addresses cannot be translated by the routers along the path, as this will invalidate the hash value.
  - The transport and application layers are always secured by hash, so they cannot be modified in any way (e.g., by translating the port numbers).
  - Transport mode is used for host-to-host (i.e., end-to-end) communications.
- In the tunnel mode , the entire IP packet is encrypted and/or authenticated.
  - It must then be encapsulated into a new IP packet for routing to work
  - Tunnel mode is used mainly for network-to-network (i.e., gateway-to-gateway) communications.

Tunneling Protocols: VPN Security Protocols

- Encapsulating Security Payload (ESP).
- ESP ensures data privacy by encryption in addition to integrity and authentication.
- ESP contains:
  - Header chunk with the SPI, serial number, and other parameters.
  - Trailer chunk with the authentication data
- The packet portion between the ESP header and trailer gets encrypted.
- Like AH, ESP can also be applied in the transport and tunnel modes



Tunneling Protocols: VPN Security Protocols

- Internet Key Exchange (IKE).
- IPSec provides a robust and flexible key exchange architecture.
- The 2 peers setting up the IPSec VPN tunnel first set up a security association (SA).
- SA defines:
  - Encryption algorithm and its key
  - Authentication algorithm and its key
  - AH and ESP modes
  - Key lifetimes
  - Lifetime of the SA itself

Tunneling Protocols: VPN Security Protocols

- In order to generate a secret key for data transfer, the IKE process can be divided into 2 main phases.
- Phase 1:
  - Proposals for SA are sent and negotiated.
  - A Diffie-Hellman exchange is done to generate a master key.
  - Encrypted with the master key, digital signatures and certificates are exchanged to authenticate the peers.
- Phase 2:
  - A second Diffie-Hellman exchange is done to generate a private data exchange key.
  - This Diffie-Hellman exchange is protected by the master key.
  - The private data exchange key is used to transfer data (for ESP modes).
- Private keys can be refreshed every few minutes using encrypted Diffie-Hellman exchanges.

Tunneling Protocols: VPN Security Protocols

- Secure Socket Layer (SSL)
  - This protocol was developed by Netscape Communications to provide secure HTTP connections.
  - SSL operates on top of TCP and provides a secure connection for applications such as HTTP, FTP, Telnet, etc.
  - SSL v3.0 was submitted to the IETF standardization and, after some changes, led to the Transport Layer Security (TLS) protocol.
- Transport Layer Security (TLS)
  - TLS sits between the application layer and the transport layer.
  - The reason for calling it ”transport layer security” is that, from the application’s perspective, this protocol layer looks like a normal transport protocol, except for the fact that it is secure.
  - By running TLS on top of TCP, all of the normal features of TCP (reliability, flow control, etc.) are also provided to the application.
  - When HTTP is used over TLS, it is known as Secure HTTP (HTTPS).

Tunneling Protocols: VPN Security Protocols

- TLS protocol provides privacy, integrity, and authentication between 2 communicating applications.
- One advantage of TLS is that it is application protocol independent.
- TLS is composed of the 2 protocols:
  - TLS Record Protocol (at the bottom).
  - TLS Handshake Protocol (on the top).
- Book ”Computer Networking: A Top-Down Approach” by James F. Kurose and Keith W. Ross (2010).

Tunneling Protocols: VPN Security Protocols

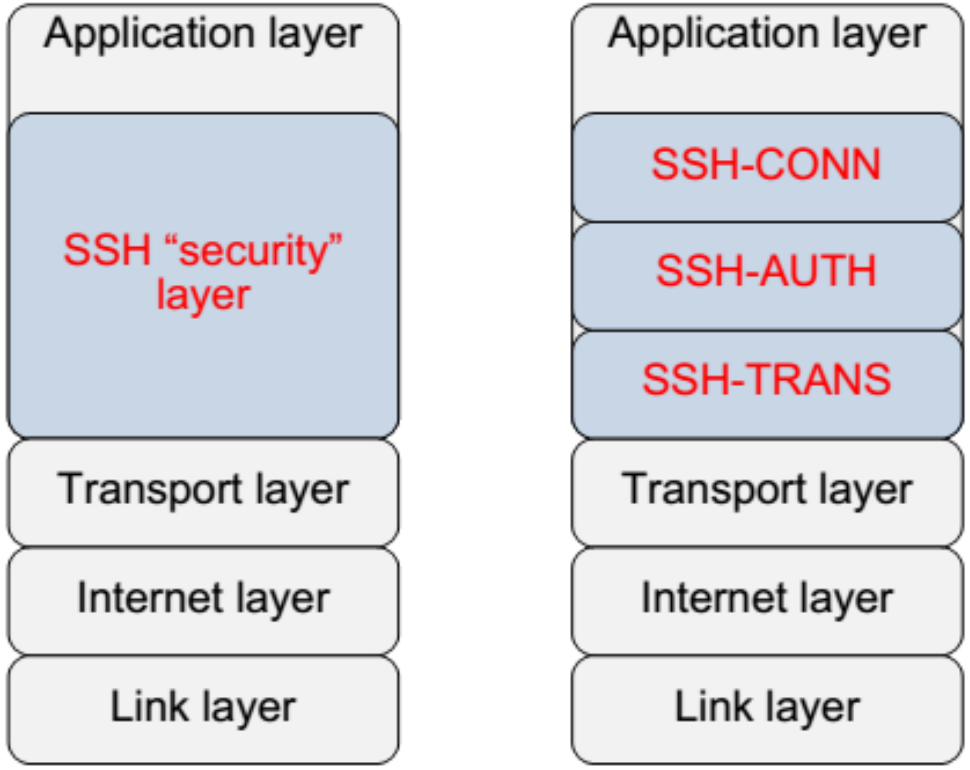
- TLS Record Protocol provides:
- Privacy
  - Symmetric cryptography is used for data encryption (e.g., DES)
  - The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol).
- Integrity
  - Message transport includes a message integrity check (e.g., MD5)
- Encapsulation of various higher-level protocols.
  - One such encapsulated protocol is the TLS Handshake Protocol.

Tunneling Protocols: VPN Security Protocols

- TLS Handshake Protocol provides:
- Authentication of peer's identity by using secret or public key cryptography.
  - This authentication can be made optional, but is generally required for at least one of the peers.
- Negotiation of a shared secret key is secure.
  - The negotiated secret key is unavailable to eavesdroppers, even by an attacker who can place himself in the middle of the connection.
- Negotiation is reliable.
  - No attacker can modify the negotiation communication without being detected by the parties to the communication.

Tunneling Protocols: VPN Security Protocols

- Secure Shell (SSH)
- SSH – a protocol and a program for secure remote login and other secure network services over an insecure network.
- In particular, it is used as a ”secure version of Telnet” or as a secure shell – a program which allows commands to be executed in a remote machine, for the transfer of files between machines, and other secure network services.
- It was invented by Tatu Ylonen, a researcher at Helsinki University of Technology, in 1995.
- In 1996, a revised version of the protocol, SSH-2, was designed, incompatible with SSH-1.
- SSH-2 consists of 3 protocols:
  - SSH-TRANS: a transport layer protocol (RFC 4253)
  - SSH-AUTH: an authentication protocol (RFC 4252)
  - SSH-CONN: a connection protocol (RFC 4254)



Tunneling Protocols: VPN Security Protocols

- SSH transport layer protocol provides:
  - Encryption.
  - Compression (if required).
- Typically, SSH transport layer protocol runs over a TCP connection (port 22).
- SSH authentication protocol provides:
  - Used by the client to authenticate itself to the server.
- It runs over the SSH transport layer protocol.
- SSH connection protocol provides:
  - Multiplexing of several logical channels into a single tunnel provided by the SSH transport and authentication protocols.

Tunneling Protocols: VPN Security Protocols

Feature	PPTP	L2F	L2TP	IPSec	SSL/TLS	SSH
Layer	2	2	2	3	Higher Layers	Higher Layers
Encryption	PPP – Based	PPP – Based	PPP – Based	DES, 3DES, IDEA	DES, 3DES, IDEA	DES, 3DES, IDEA
Authentication	PPP – Based	PPP – Based	PPP – Based	Certificates, public keys	Certificates	Certificates, passwords
Data Integrity	None	None	None	HMAC-MD5, SHA-1	MD5, SHA-1	HMAC-MD5, SHA-1
Main VPN type supported	User-site	User-site	User-site	User-site, site-site	User-site	User-site