Network Security

Information Security Principles

tgeng@email.sc.edu

October 27, 2021

Outline

- Network concepts
- Threats to network
- Wireless network
- DoS
- DDoS
- **Cryptography in network**
- Network defense tools
- Network management
- Network testing

Part V

Cryptography in network

Outline

- Network Encryption
- Browser Encryption
- Onion Routing
- IPsec
- VPN

Cryptography

Chapter 2:

- Symmetric encryption
  - bulk encryption of large quantities of data
  - perfectly fits network traffic
- Asymmetric encryption
  - establishing a trustworthy relationship between two parties not met before
  - suitable for network connection

Network Encryption

- Encryption protects only what is encrypted
- Designing encryption algorithm is best left to professionals
- Encryption is no more secure than its key management
- Encryption is not a panacea or silver bullet

In network applications, encryption can be applied:

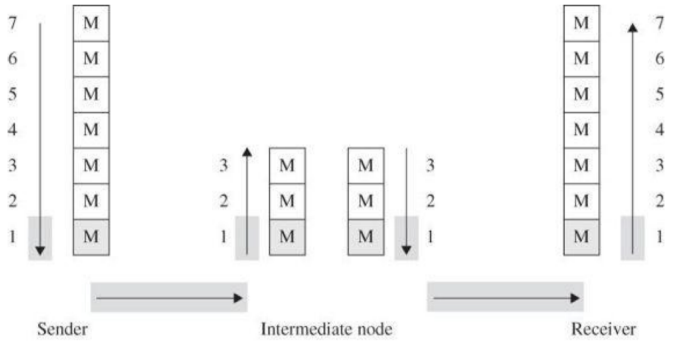
- between two hosts (link encryption)
- between two applications (end-to-end encryption)

Modes of Network Encryption

- These two modes of network encryption perform different functions and have different strengths and weaknesses.
- They can even be used together, even somewhat redundantly

Link Encryption

In link encryption, data are encrypted just before the system places them on the physical communication link.



Link encryption covers a communication from one node to the next on the path to the destination.

Link Encryption

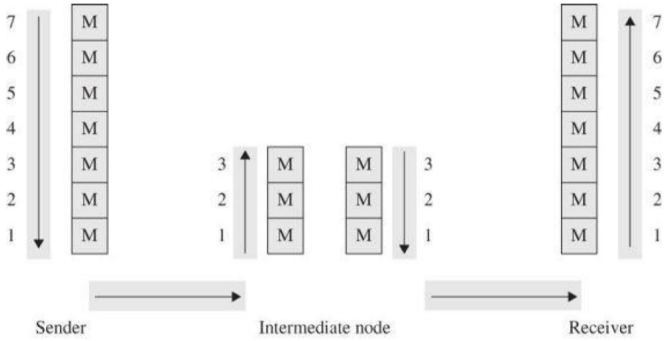
- Encryption protects the message in transit, but the message is in plaintext inside the hosts
- If we have good physical security and we trust the software implements the upper-layers functions, this potential vulnerability is not a big concern

Link Encryption

- Link encryption is transparent to the user and OS
- The header and optional trailer are appended before the encryption
  - Headers and trailers in upper layers will be encrypted also
  - The encryption will be removed when arrived the destination
- Link encryption is suitable for the insecure communication medium
  - Several parties share on link
  - Sensitive transmission

End-to-end Encryption

End-to-end encryption provides security from one end of a transmission to the other.



- The encryption could be applied between the user and the host by a hardware device
- The encryption can also be done by software running on the host computer
- The encryption is usually performed in level 7 (highest), but sometimes 5 or 6
- End-to-end encryption is also called application-level encryption.

End-to-end Encryption

- The encryption occurs typically in application layer
- The encryption precedes all the routing and transmission processing of the layer (header, trailer)
- Only the data portion of the message is protected

- Headers and trailers are not encrypted
  - Advantage: the intermediate nodes doesn't need to decrypt. This prevents the data leak in the intermediate nodes.
  - Disadvantage: sometimes the header and trailer contains the information about data, possibly sensitive

Comparison of Encryption Methods

Link Encryption	End-to-end Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Dat partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application knows the encryption
Host administrators selects encryption	User application selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Can be done in software or hardware, but usually by software
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

SSL, SSH and IPSec

- Security can be implemented at many layers
  - SSL and SSH are implemented at the application layer
  - No need to change the OS
  - Applications must be specially designed to work with SSL or SSH
  - IPSec is implemented at the transport layer
  - Inside the OS
  - More transparent to user

SSL and TLS

- SSL can enhance the security of web browser
- SSL provides a secure transport connection between applications, usually client and server
- SSL encryption covers communication between a browser and the remote web server
- SSL (Secure Socket Layer) was originally proposed by Netscape
- SSL 3.0 was specified in an Internet Draft (1996)
  - was been widely implemented in web browsers and web servers (Netscape navigator, MS Internet Explorer)
- TLS (Transport Layer Security) (1999)
  - "SSL 3.1"
  - TLS is not compatible with SSL 3
  - TLS 1.0 and TLS 1.1 were deprecated by Apple, Google, Microsoft, and Mozilla in October 2018
  - TLS 1.3 (2018)

Components

- SSL Handshake Protocol
  - negotiation of security algorithms and parameters
  - key exchange
  - server authentication, and client authentication
- SSL Change Cipher Spec Protocol
  - a single byte message, indicates end of SSL handshake
- SSL Record Protocol
  - fragmentation
  - compression
  - message authentication and integrity protection
  - encryption
- SSL Alert Protocol
  - error messages

Important Concepts

SSL works in terms of connection and sessions between client and server:

- SSL Session:
  - An association between a server and a client
  - Stateful
    - ⋆ cryptographic security parameters
  - Can be multiple sessions between parties (but not common)
  - Sessions are created by the handshake protocol
- SSL Connection
  - Peer-to-peer relationship, transient
  - Every connection is associated with a session
  - A session can have multiple connection

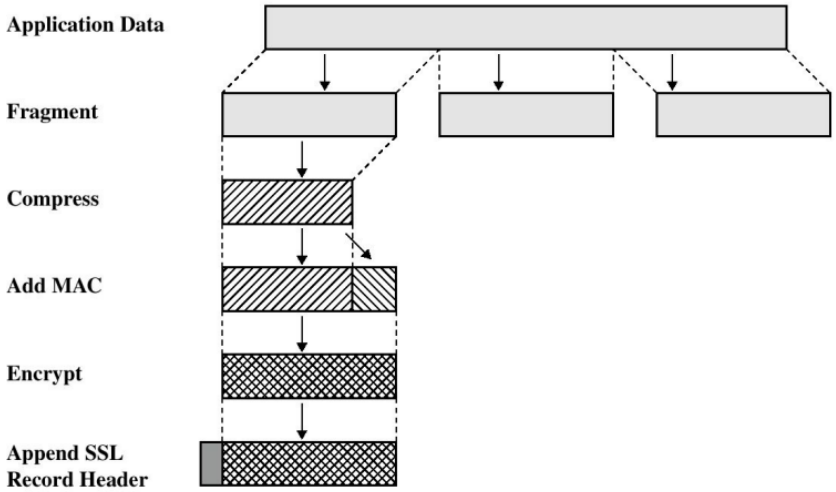
Lower Layer: SSL Record Protocol

- Receive message from upper layer
- Breaks messages into blocks
- Compresses blocks
- Computes MAC for each block
  - Each block has implicit sequence number to prevent reordering
- Encrypts blocks
  - If encryption and MAC key not selected, then no encryption or MAC used
- Adds header

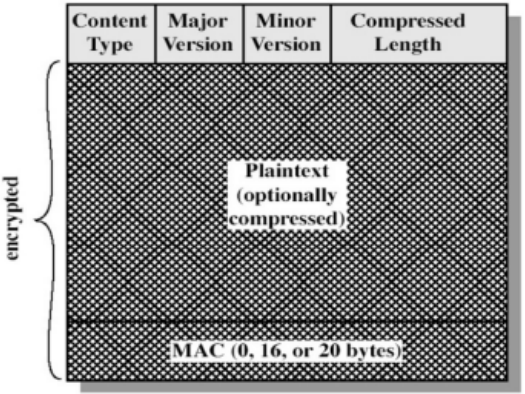
This protocol provides two services for SSL connections:

- Confidentiality - using conventional encryption
- Message Integrity - using a Message Authentication Code

SSL Record Protocol Operation



SSL Record Format



SSL Handshake Protocol

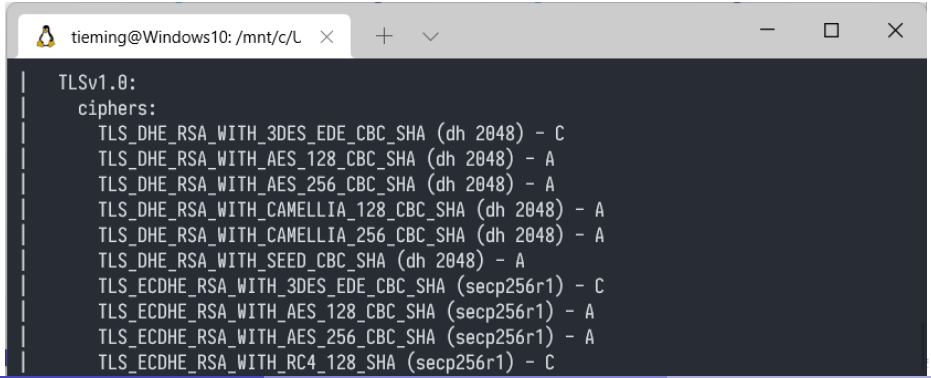
- The most complex part of SSL
- Authenticate both server and client
- Negotiate cipher suite (encryption, MAC algorithm, and cryptographic keys)
- Used before any application data are transmitted

Cipher Suite

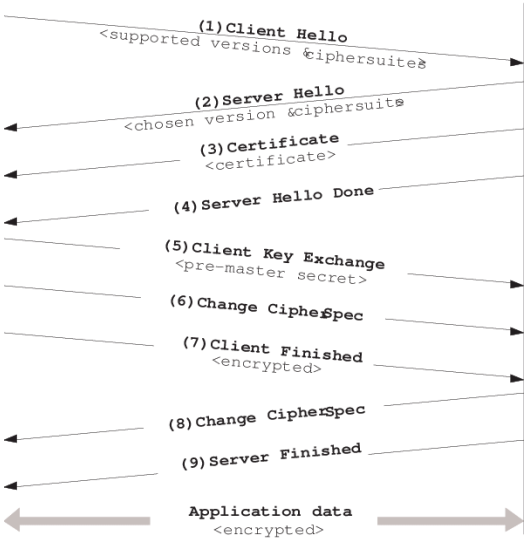
The algorithms for authentication, session encryption, and hashing.

Key Exchange Authentication Cipher (algorithm, strength, mode) Hash or MAC

ECDHE-ECDSA-AES128-GCM-SHA256



SSL Handshake Protocol



SSL Certificate

- Serial Number: Used to uniquely identify the certificate
- Subject: The person, or entity identified
- Signature Algorithm: The algorithm used to create the signature
- Signature: The actual signature to verify that it came from the issuer
- Issuer: The entity that verified the information and issued the certificate
- Valid-From: The date the certificate is first valid from
- Valid-To: The expiration date
- Key-Usage: Purpose of the public key (encipherment, signature...)
- Public Key
- Thumbprint Algorithm: The algorithm used to hash the public key certificate
- Thumbprint (fingerprint): The hash itself, used as an abbreviated form of the public key certificate

SSL Change Cipher Spec Protocol

- Sent by both the client and the server to notify the other party that the following records will be protected using the just negotiated CipherSpec and keys
- Consists of single message, a single byte with the value 1
- The purpose of the message is to updates the cipher suite to be used on the connection

SSL Alert Protocol

- Used to convey SSL-related alerts to the peer entity
- Alert messages are compressed and encrypted
- The message is two bytes:
  - 1 byte: warning (1) or fatal (2)
  - 1 byte: status of the certificate or other specific alerts

Second Byte of SSL Alert Protocol

fatal alert:

- unexpected message
- bad record MAC
- decompression failure
- handshake failure
- illegal parameter

warning alert:

- no certificate
- bad certificate
- unsupported certificate
- certificate revoked
- certificate expired
- certificate unknown

In case of a fatal alert, the connection is terminated, and Session ID is invalidated

- No new connection can be established within this session

SSH

Secure Shell

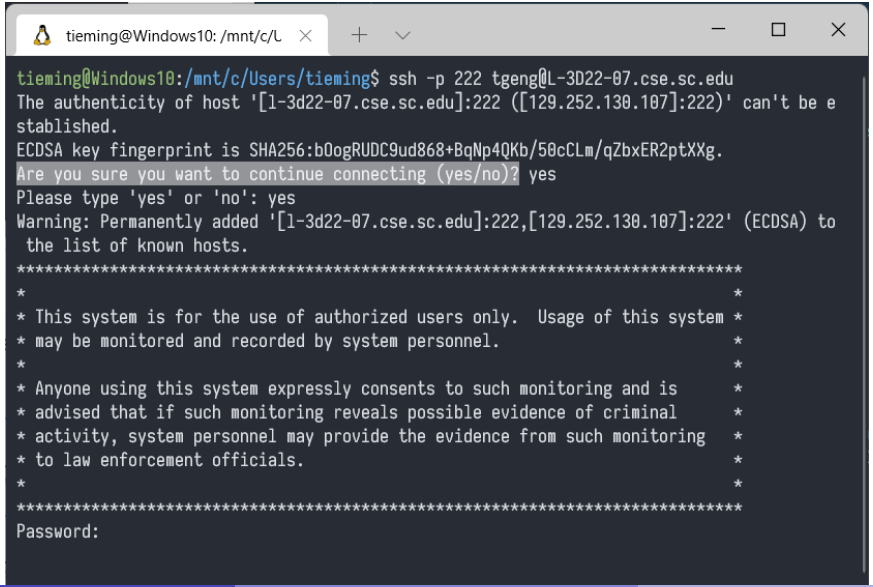
- Provides confidentiality
  - Credential used for login
  - Content of the remote login session
- SSH provides security at Application Layer
  - Secure copying of files between client and server
  - Also can be used for tunnelling other protocols

SSH

SSH authenticates both the client and the server

- Server: public and private key pair
  - client uses a locally stored public key of the server to verify the server's signature
- Client
  - username and password
  - asymmetric key pair, the server needs to know the public key

SSH


tieming@Windows10: /mnt/c/L
tieming@Windows10:/mnt/c/Users/tieming$ ssh -p 222 tgeng@L-3D22-07.cse.sc.edu
The authenticity of host '[l-3d22-07.cse.sc.edu]:222 ([129.252.130.107]:222)' can't be e
stablished.
ECDSA key fingerprint is SHA256:bOogRUDC9ud868+BqNp4QKb/50cCLm/qZbxER2ptXXg.
Are you sure you want to continue connecting (yes/no)? yes
Please type 'yes' or 'no': yes
Warning: Permanently added '[l-3d22-07.cse.sc.edu]:222,[129.252.130.107]:222' (ECDSA) to
the list of known hosts.
* This system is for the use of authorized users only. Usage of this system *
* may be monitored and recorded by system personnel. *
* Anyone using this system expressly consents to such monitoring and is *
* advised that if such monitoring reveals possible evidence of criminal *
* activity, system personnel may provide the evidence from such monitoring *
* to law enforcement officials. *
Password:

SSH Applications

- SFTP
- SSH git

SSH Architecture

- SSH Connection Protocol
- SSH Authentication Protocol
- SSH Transport Layer Protocol

Port Forwarding

- Tunneling: a way to forward TCP traffic through SSH
  - e.g: securing POP3, SMTP and HTTP connections (insecure connections)
  - The client-server applications will run their normal authentication over the encrypted tunnel
- There are two types of port forwarding:
  - local (outgoing tunnel)
  - remote forwarding (incoming tunnel)

Port Forwarding

Local Port Forwarding:

- Forwards traffic coming to a local port to a specified remote port
- `ssh -L 1234:localhost:23 username@host`
  - traffic to port 1234 on the client (localhost) will be forwarded to port 23 on the server(host)

Remote Port Forwarding:

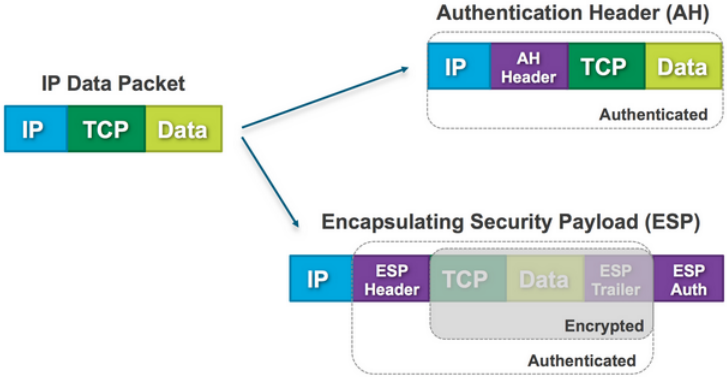
- Remote port forwarding does opposite
  - forwards traffic coming to a remote port to a specified local port
  - `ssh -R 1234:localhost:23 username@host`
    - ★ traffic that comes from port 1234 on the server (host) will be forwarded to port 23 on the client (localhost)

IPsec

- Protection of communication between:
  - hosts
  - gateways
  - a host and a gateway
- Comparison with SSL, TLS, SSH:
  - These are at higher layer of OSI
  - Applications must be altered to incorporate these
- IPSec provides application-transparent security
  - network services that use IP (telnet, FTP) or user application that uses IP (TCP, Socket) can use IPSec without modification

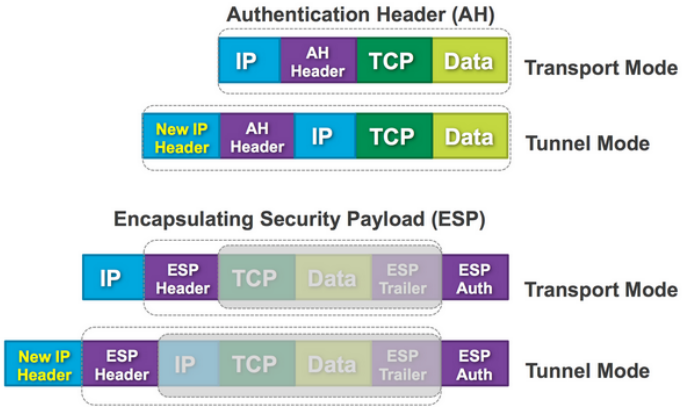
IPSec Methods

- Authentication header (AH)
  - provides data integrity and authentication
- Encapsulating Security Payload (ESP)
  - provides encryption, data integrity, and authentication



IPSec Modes

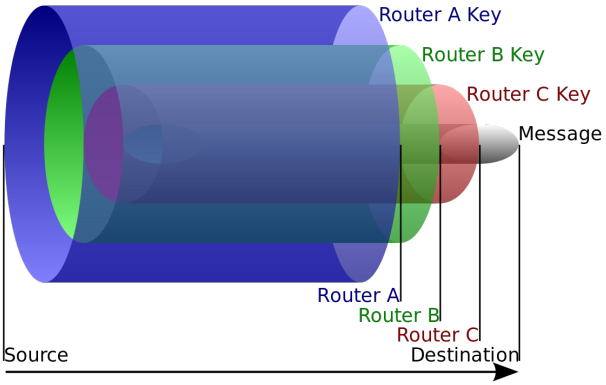
- Transport mode: preserves original IP header, typically used for remote-access VPN
- Tunnel mode: encapsulates the entire IP datagram within a new header, typically used for site-to-site VPn



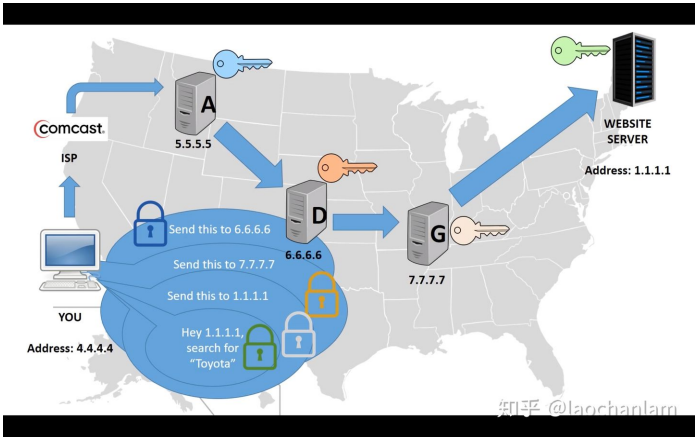
Onion Routing

- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network
- This is particularly helpful for evading authorities, such as when users in oppressive countries want to communicate freely with the outside world
- Uses asymmetric cryptography, as well as layers of intermediate hosts, so that
  - The intermediate host that sends the message to the ultimate destination cannot determine the original sender, and
  - The host that received the message from the original sender cannot determine the ultimate destination

Onion Routing



Onion Routing



VPN

A virtual private network simulates the security of a dedicated, protected communication line on a shared network.

- Remote access
  - A host-to-network configuration is analogous to connecting a computer to a local area network.
- Site-to-site
  - A site-to-site configuration connects two networks. This configuration expands a network across geographically disparate offices, or a group of

VPN

VPN

- PPTP
- L2TP
- OpenVPN
- SSL VPN