Lecture 26 (E-Mail Security and TLS)

1 Confidentiality

1. Alice generates a symmetric key
2. Encrypt the email using this key
3. Encrypt the key using Bob's public key
4. Send both the encrypted email and key to Bob

2 Integrity

1. Hash of the email is encrypted with Alice's private key and then with they symmetric key
2. Everything is sent to Bob

3 Transport Layer Security (TLS)

1. Secure Socket Layer (SSL) has been deprecated in 2015
2. TLS provides confidentiality, integrity and authentication
3. Works on port 443 of HTTP

3.1 What's Needed

1. Handshake
2. Key derivation
3. Data transfer
4. Connection closure

3.2 Initial Handshake

1. Standard TCP SYN-ACK happens and TLS hello is done along with ACK of SYNACK
2. Alice sends public key certificate to Bob
3. Bob returns $K_A^+(MS) = EMS$ (Master Secret key) aftere verifying the public key
4. We have 3 RTTs before any data sharing can happen

3.3 Keys

1. K_c: encryption key for data from client to server
2. M_c: Message Authentication Code (MAC) for data from client to server
3. K_s: encryption key for data from server to client
4. M_s: MAC key for data from server to client
5. They are derived from MS using a Key Derivation Function (KDF)

3.4 Data Transfer

1. Break stream into a series of records
2. Each record carries a MAC encrypted using M_c
3. The entire record is encrypted using K_c
4. TLS sequence numbers are used
5. Similar procedure is used for server-to-client

3.5 Connection Closure

1. Record type is used
2. Type 0 for data and type 1 for closure

3.6 TLS: 1.3 Ciper Suite

1. Limited cipher suite choice than TLS 1.2
2. Only 5 choices rather than 37 choices
3. Requires Diffie-Hellman (DH) for key exchange, rather than DH or RSA
4. Combined encryption and authentication algorithm
5. HMAC (Hashed MAC) uses SHA

3.6.1 Steps - 1 RTT for Handshake

1. Client TLS hello message

- Guesses key agreement protocol, parameters
- Indicates cipher suites it supports

1. Server hello

- Selected cipher suite
- DH key agreement protocol, parameters

3.6.2 Steps - 0 RTT for Handshake

1. Client hello

- Resume previous conversation using the same keys and send encrypted application data

1. Server hello

- Reply to the application data

1. Client and server still send the same information as in the previous part too
2. This is no longer used since this is prone to replay attacks

3.7 QUIC

1. Used hy HTTP/3
2. Alternative to TLS and quicker

4 IP Security - IP Sec

It is of two types:

1. Transport mode - only datagram payload is encrypted
2. Tunnel mode - entire datagram is encrypted, encrypted datagram is encapsulared in new datagram with new IP header and tunneled to destination

4.1 Protocols

1. Authentication Header (AH) - authentication, data integrity but not confidentiality
2. Encapusulation Securty Protocol (ESP) - provides all three including confidentiality

4.2 Security Associations (SAs)

1. We need handshake before sending data, i.e., SA (which is directional)
2. Sending and receiving entities maintain state information about SA
3. This is different from IP which was connectionless
4. Data stored is:

a. 32-bit identifier - Security Parameter Index (SPI)
b. Origin SA interface
c. Destination SA interface
d. Encryption key
e. Type of encryption used
f. Type of integrity check used
g. Authentication key

4.3 IP Sec Datagram

1. new IP header
2. ESP header - SPI and sequence number
3. original IP header
4. original IP datagram payload
5. ESP trailer - padding, pad length, next header

6. ESP auth - MAC with shared secret key (acts as payload)

IP section along with ESP trailer is encrypted

4.4 IPsec Sequence Number

1. For new SA, sequence number is initialised to 0
2. This prevents sniffing and replaying packet

4.5 IPsec Security Databases

1. Security Policy Database

- For given datagram, sender needs to know if it should use IP sec
- Policy is stored in Secure Policy Database
- SPD: what to do

1. Security Association Database

- Endpoint holds SA state in SAD
- When sending IPsec datagram, router accesses SAD to determine how to process datagram
- On receiving datagram, router examines SPI and indexes SAD with SPI and processes datagram accordingly
- SAD: how to do it

5 Internet Key Exchange

1. Establishing IPsec SAs for multiple nodes is impractical in VPN or similar situations
2. Instead IPsec IKE is used