

Lecture 14

Security Protocols

SSL: Session State

- Session identifier
- Peer certificate (may be null)
- Compression method
- Cipher Spec
 - bulk data encryption algorithm
 - hash algorithm
 - hash size
- Master secret - 48 bytes
- Is resumable

SSL: Connection State

- Server and client random
- Server write MAC secret
- Client write MAC secret
- Server write key
- Client write key
- Initialization vectors
- Sequence numbers ($0..2^{64}-1$,
reset after `change_cipher_spec`)

SSL: Encryption Algorithms

Block cipher		Stream cipher	
Algorithm	Key size	Algorithm	Key size
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

SSL: Alert Types (1)

Fatal alerts

- unexpected message
- bad record mac
- decompression failure
- handshake failure (an acceptable set of security parameters could not be negotiated)
- illegal parameter

SSL: Alert Types (2)

Other alerts

- close notify = no more messages sent on this connection
- no certificate = no appropriate certificate available
- bad certificate = certificate was corrupt
- unsupported certificate
- certificate revoked
- certificate expired
- certificate unknown

SSL Handshake: Client Hello Message

- Version - highest SSL version understood by the client
- Random = 32-bit timestamp + 28-byte nonce generated by the client
- Session ID - non-zero for existing session zero to open a new session
- Compression method = list of methods supported by the client
- Cipher Suite
list of supported algorithms in decreasing order of preference
each item = Key Exchange Method + Cipher Spec

SSL Handshake: Server Hello Message

- Version - highest SSL version supported by both client & server
- Random = 32-bit timestamp + 28-byte nonce generated by the server
- Session ID - if client session ID non-zero, the same if client session ID zero, a new session ID
- Compression method = a single method selected by the server from the list suggested by the client
- Cipher Suite
a single cipher suite selected by the server from the list suggested by the client
Key Exchange Method + Cipher Spec

SSL Handshake: Key Exchange Methods

- RSA
 - static
 - ephemeral
- Diffie-Hellman
 - anonymous
 - fixed
 - ephemeral
- Fortezza = Key Exchange Algorithm

SSL Handshake: Cipher Spec

- Cipher algorithm
- MAC algorithm: MAC based on MD5 or SHA-1
- Cipher Type: Stream or Block
- Is Exportable: True or False
- Hash size: 0, 16 (for MD5), 20 (for SHA-1)
- Key material: used in generating write keys
- IV size: IV for CBC encryption

SSL Handshake: Certificate Request

- Certificate Type
 - RSA, signature only
 - DSS, signature only
 - RSA for fixed Diffie-Hellman
 - DSS for fixed Diffie-Hellman
 - RSA for ephemeral Diffie-Hellman
 - DSS for ephemeral Diffie-Hellman
 - Fortezza
- Certificate Authorities

Master Secret Creation

```
Master secret = MD5 (pre_master_secret ||
    SHA('A' || pre_master_secret ||
        ClientHello.random ||
        ServerHello.random)) ||
    MD5 (pre_master_secret ||
    SHA('BB' || pre_master_secret ||
        ClientHello.random ||
        ServerHello.random)) ||
    MD5 (pre_master_secret ||
    SHA('CCC' || pre_master_secret ||
        ClientHello.random ||
        ServerHello.random))
```

Generation of Cryptographic Parameters

```
Key block = MD5 (master_secret ||
    SHA('A' || master_secret ||
        ServerHello.random ||
        ClientHello.random)) ||
    MD5 (master_secret ||
    SHA('BB' || master_secret ||
        ServerHello.random ||
        ClientHello.random)) ||
    MD5 (master_secret ||
    SHA('CCC' || master_secret ||
        ServerHello.random ||
        ClientHello.random)) || .....
```

Major differences between SSL 3.0 and TLS 1.0

1. Verion Number

	SSL	TLS
Major version	3	3
Minor version	0	1

2. Cipher Suites

TLS does not support Fortezza (KEA + Skipjack)

Major differences between SSL 3.0 and TLS 1.0

3. Message Authentication Code - MAC

```
SSL    hash(MAC_write_secret || pad2 ||
        hash(MAC_write_secret || pad1 ||
            seq_num || SSLCompressed.type ||
            SSLCompressed.length ||
            SSLCompressed.fragment))

TLS    hash(MAC_write_secret+ ⊕ opad ||
        hash(MAC_write_secret+ ⊕ ipad ||
            seq_num || TLSCompressed.type ||
            TLSCompressed.version ||
            TLSCompressed.length ||
            TLSCompressed.fragment))
```

Major differences between SSL 3.0 and TLS 1.0

4. New pseudorandom function used to generate master secret and cryptographic parameters

TLS

$$\text{PRF}(\text{secret}, \text{label}, \text{seed}) = \text{P_MD5}(\text{S1}, \text{label} \parallel \text{seed}) \oplus \text{P_SHA-1}(\text{S2}, \text{label} \parallel \text{seed})$$

$$\text{master_secret} = \text{PRF}(\text{pre_master_secret}, \text{"master secret"}, \text{ClientHello.random} \parallel \text{ServerHello.random})$$

$$\text{key_block} = \text{PRF}(\text{master_secret}, \text{"key expansion"}, \text{SecurityParameters.server_random} \parallel \text{SecurityParameters.client_random})$$

Major differences between SSL 3.0 and TLS 1.0

5. New alert codes

Always Fatal Alerts

- decryption failed
- record overflow (ciphertext > 18 kB)
- unknown CA
- access denied
- decode error (field out of range)
- export restriction
- protocol version (not supported)
- insufficient security
- internal error

Major differences between SSL 3.0 and TLS 1.0

6. Padding

SSL

Padding length = minimum amount that results in a total length that is a multiple of the cipher's block length

TLS

Padding length = any amount up to 255 bytes that results in a total length that is a multiple of the cipher's block length

Goal: frustrate attacks based on the message length analysis
