Network Security
Security Services

CME451 Tutorial 7

Hao Zhang
(Graduate Teaching Fellow)

Department of Electrical & Computer Engineering
University of Saskatchewan

Feb 17, 2017

*Most contents are from William Stallings, *Data and Computer Communications*, 8th edition, 2007 Pearson Education Inc.

Network Encryption

- Encrypt messages against passive attacks.
- Symmetric encryption:
  - Sender and receiver share the encryption key.
  - DES, 3DES, AES, ...
  - Key distribution.
- Asymmetric encryption (public-key encryption)
  - Public key made for others to use.
  - Private key known only to its owner.
  - RSA, ...
  - Sender encrypt message using receiver's public key.
  - Receiver decrypt the message using private key.
  - Help key distribution of symmetric encryption.

Network Authentication and Digital Signature

- Protect messages against active attacks.
- Encryption can realize authentication.
- Message authentication code(MAC):
  - Shared secret key.
  - Append a block to message.
  - Receiver check MAC match.
- Hash functions:
  - Variable size of message.
  - Fixed size message digest.
  - No secret keys.
  - MD5, SHA-1, SHA-256, ...
- Digital signature:
  - Another way of using asymmetric encryption.
  - Sender sign the message with private key.
  - Receiver verify the message with public key.
  - Sign the hash code instead of whole message.

- Symmetric Encryption:
  - `des = DES.new('01234567', DES.MODE_ECB)`
- Asymmetric Encryption:
  - `key = RSA.generate(1024, random_generator)`
- Hash function:
  - `hash_md5 = MD5.new(b'CME451 Course').digest()`
- Digital signature:
  - `signature = privatekey.sign(hash_of_message, '')`
  - `publickey.verify(hash_of_decrypted, signature)`

Network Security Services

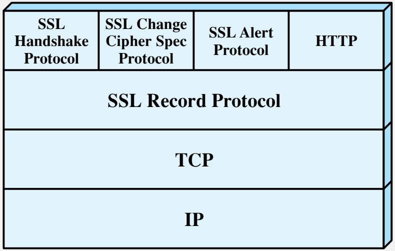
Overview

- Security services implement a set of protocols.
- Transport Layer:
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
- Network Layer:
  - Internet Protocol Security (IPSec)
- WiFi:
  - WiFi Protected Access (WPA)

SSL and TLS

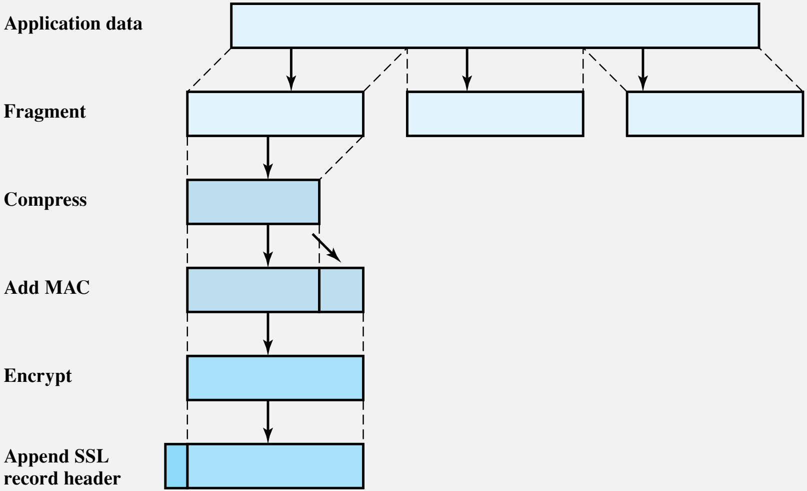
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Make use of TCP to provide reliable secure services.
- Protocol suites.
- Many web browsers are equipped with SSL.
- Most web servers support SSL protocols.

SSL and TLS



- SSL: two-layers of protocols.
- **SSL connection**: one transport, transient, associated with one session.
- **SSL session**: association between client and server, define a set of security parameters which are shared among multiple connections.
- Session avoids negotiation of security parameters for each connection.

SSL Record Protocol



SSL Record Protocol

- SSL Record Protocol Header
  - **Content Type (8-bit)**: The higher layer protocol used to process the enclosed fragment.
    - change_cipher_spec
    - alert
    - handshake
    - application_data
  - **Major Version (8-bit)**: Major version of SSL. For SSLv3, it is 3.
  - **Minor Version (8-bit)**: Minor version of SSL. For SSLv3, it is 0.
  - **Compressed Length (16-bit)**: Length in byte of compressed fragment.

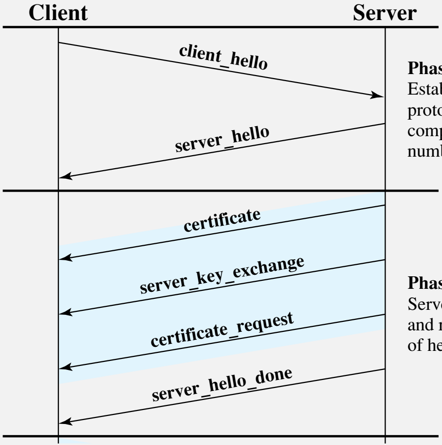
SSL Change Cipher Spec and Alert Protocol

- SSL Change Cipher Spec Protocol:
  - Consist of a single byte of value 1 in a single message.
  - Cause a pending state to allow the connection to update the cipher suite.
- SSL Alert Protocol:
  - Used to convey SSL-related alerts.
  - Consist of two bytes:
  - First byte: warning (1) or fatal (2).
    - Fatal: terminates the connection and no new connection on this session.
  - Second byte: specific alert message.
    - Fatal alert: incorrect MAC.
    - Non-Fatal: close connection when communication ends.

SSL Hand Shake Protocol

- Allow the server and the client to authenticate each other.
- Negotiate encryption and MAC algorithm, key...
- Used **before** any application data transmission.

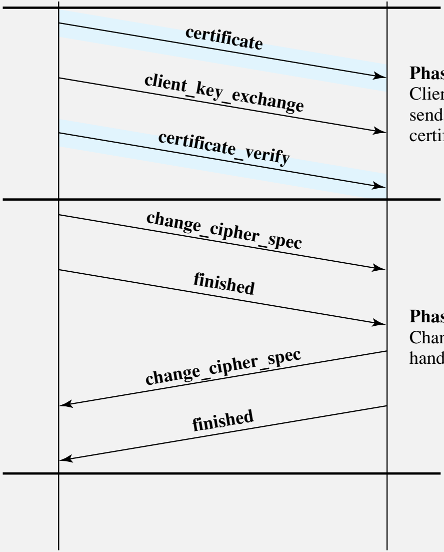
SSL Hand Shake Protocol



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

SSL Hand Shake Protocol



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

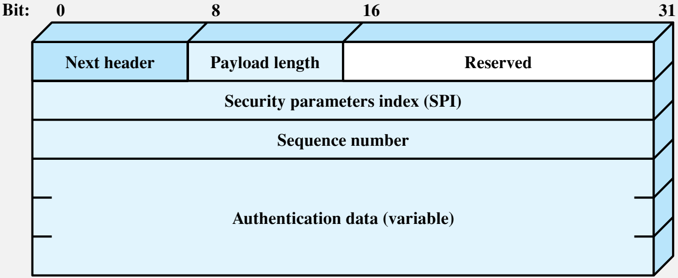
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

IPSec

- IPSec is designed to encrypt and authenticate all traffic at the IP level.
- Distributed applications can be secured:
  - remote login
  - email
  - file transfer
  - web access
- Scope:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - key exchange function

IPSec Authentication Header

- AH provides support for data integrity and authentication of IP packets.
- Based on MAC code, need a secret key.



Bit: 0 8 16 31

Next header | Payload length | Reserved

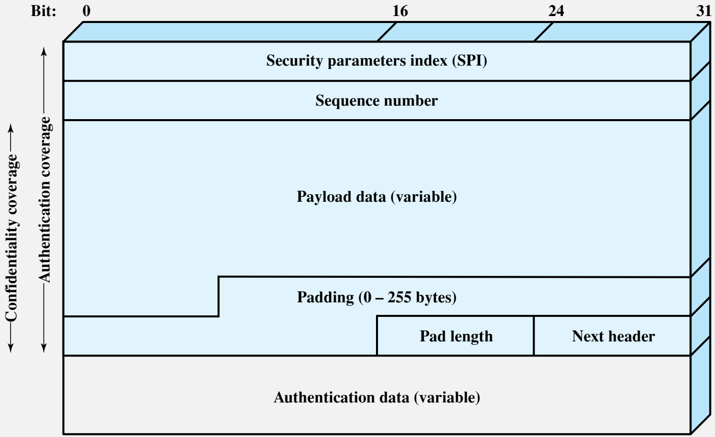
Security parameters index (SPI)

Sequence number

Authentication data (variable)

IPSec Encapsulating Security Payload

- ESP provide confidentiality services.



Bit: 0 16 24 31

Security parameters index (SPI)

Sequence number

Payload data (variable)

Padding (0 – 255 bytes)

Pad length

Next header

Authentication data (variable)

Confidentiality coverage

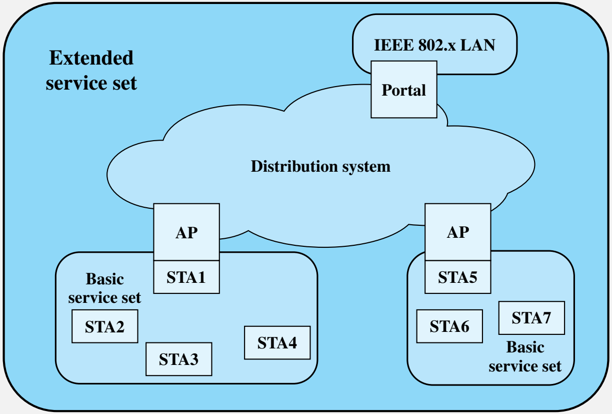
Authentication coverage

WiFi Protected Access

- WPA is involved in IEEE 802.11i.
- Address three security areas:
  - Authentication.
    - Authentication server (AS) and robust protocol.
  - Key management.
    - Authentication server (AS).
  - Data transfer privacy.
    - Encryption schemes: AES, ...

WiFi Protected Access

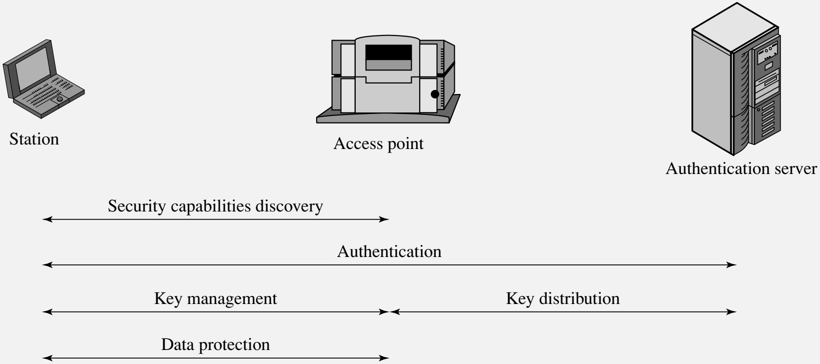
- Overview of 802.11 architecture:



STA = station
AP = access point

WiFi Protected Access

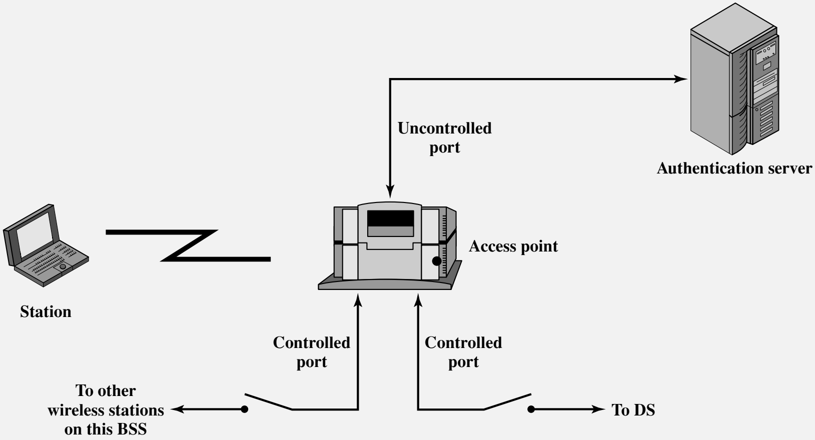
- Overview of 802.11i operation:



WiFi Protected Access

Access Control

- IEEE 802.1X Port-Based Network Access Control.


Uncontrolled port
Authentication server
Station
Access point
Controlled port
Controlled port
To other wireless stations on this BSS
To DS