RV College of Engineering®

Go, change the world

Unit 5- Transport Layer Security and Wireless Network Security

Contents

- Web Security Considerations.
- Secure Socket Layer.
- Transport Layer security.
- HTTPS.
- Wireless Network Security: Wireless Security, Mobile Device Security
- IEEE 802.11 Wireless LAN overview.
- IEEE 802.11i Wireless LAN Security – Services, Phases of operation.

Web Security Considerations

- The characteristics of Web usage that suggest the need for tailored security tools:
  - Web browsers and servers are easy to use and configure. Web content is easy to develop. The underlying software is complex, this complex software may hide many potential security flaws.
  - A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex.
  - Casual and untrained (in security matters) users are common clients for Web based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Web Security Threats

- Security threats may be active or passive:
  - Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
  - Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site.

Web Security Threats

- Security threats may come based on location:
  - Web server
  - Web browser
  - Network traffic between browser and server.

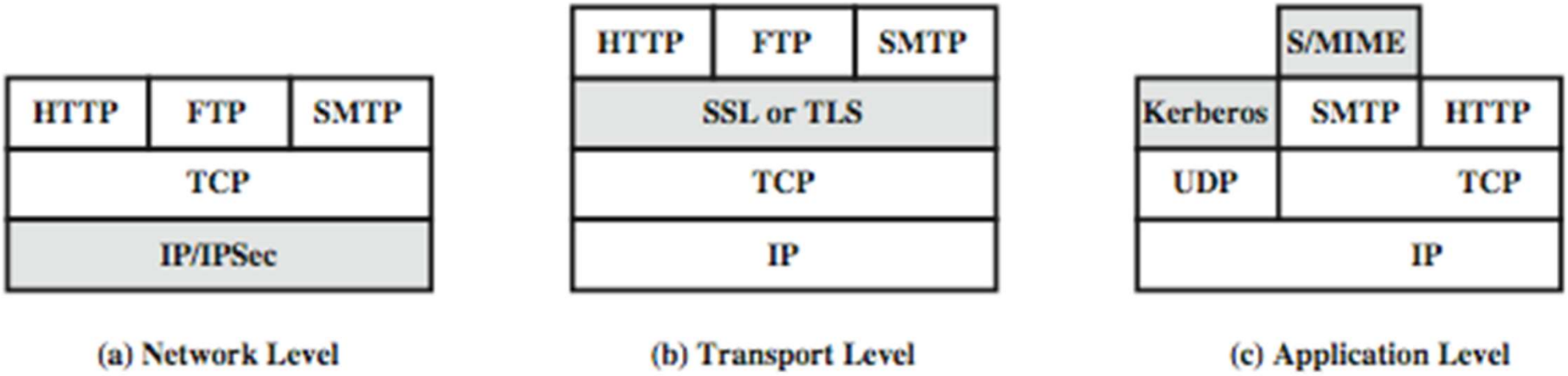
Web Security Threats: A Comparison of Threats on the Web

	Threats	Consequences	Counter measures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies

Web Security Threats: A Comparison of Threats on the Web

	Threats	Consequences	Counter measures
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Web Traffic Security Approaches



- IPSec: transparent to end users and applications and provides a general-purpose solution.
- SSL/TLS: provided as part of the underlying protocol suite and therefore be transparent to applications
- Application-specific security services are embedded within the particular application.

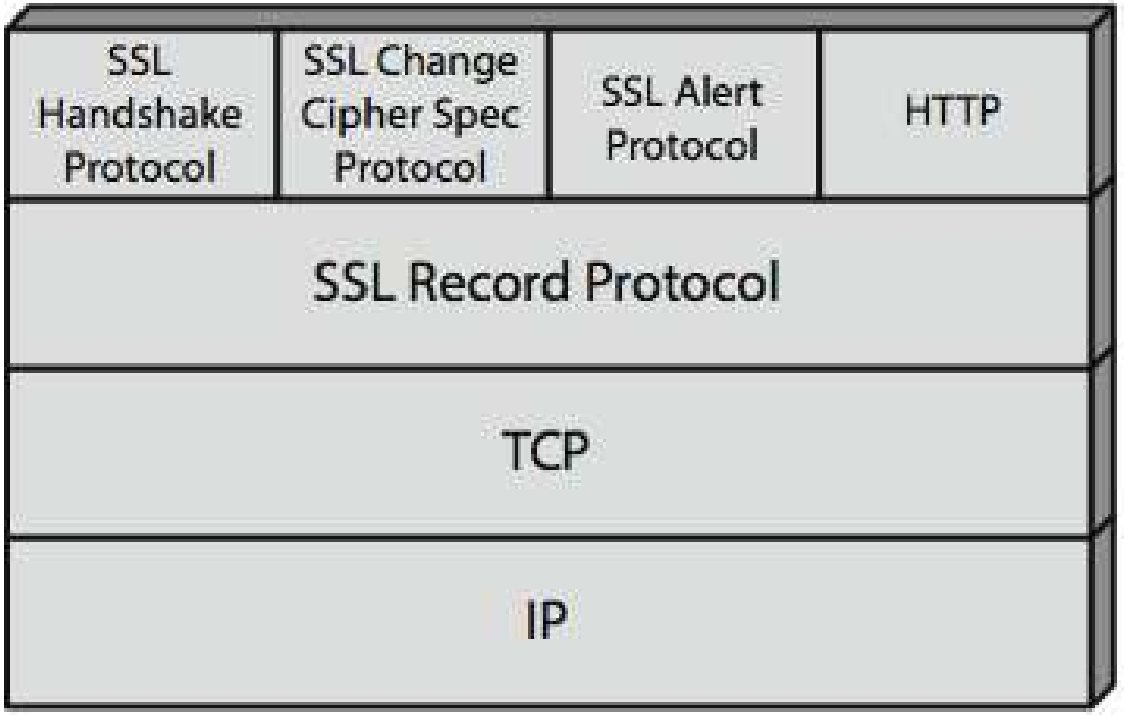
Secure Socket Layer

- One of the most widely used security services.
- SSL is a general-purpose service implemented as a set of protocols that rely on TCP
- Two implementation choices:
  - SSL/TLS: provided as part of the underlying protocol suite and therefore be transparent to applications
  - Application-specific security services are embedded within the particular application- browsers come equipped with SSL, and most Web servers have implemented the protocol.

SSL Architecture

- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols

SSL Architecture



SSL, TLS, HTTP, HTTPS Explained - YouTube

SSL Architecture

- The SSL Record Protocol provides basic security services to various higherlayer protocols.
- Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL.
- Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, The Change Cipher Spec Protocol, and the Alert Protocol. These SSL-specific protocols are used in the management of SSL exchanges

Two important SSL concepts are the SSL session and the SSL connection,

1. SSL connection

- a transient, peer-to-peer, communications link
- associated with 1 SSL session

2. SSL session

- an association between client & server
- created by the Handshake Protocol
- define a set of cryptographic parameters
- may be shared by multiple SSL connections

SSL Session State is defined by following parameters:

- **Session identifier**: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate**: An X509.v3 certificate of the peer. This element of the state may be null.
- **Compression method**: The algorithm used to compress data prior to encryption.
- **Cipher spec**: Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size.
- **Master secret**: 48-byte secret shared between the client and the server.
- **Is resumable**: A flag indicating whether the session can be used to initiate new connections.

SSL connection State is defined by following parameters:

- Server and client random: Byte sequences that are chosen by the server and client for each connection.
- Server write MAC secret: The secret key used in MAC operations on data sent by the server.
- Client write MAC secret: The secret key used in MAC operations on data sent by the client.
- Server write key: The secret encryption key for data encrypted by the server and decrypted by the client.

- Client write key: The symmetric encryption key for data encrypted by the client and decrypted by the server.
- Initialization vectors: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter, the final ciphertext block from each record is preserved for use as the IV with the following record.
- Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed 264 - 1

SSL Record Protocol Services

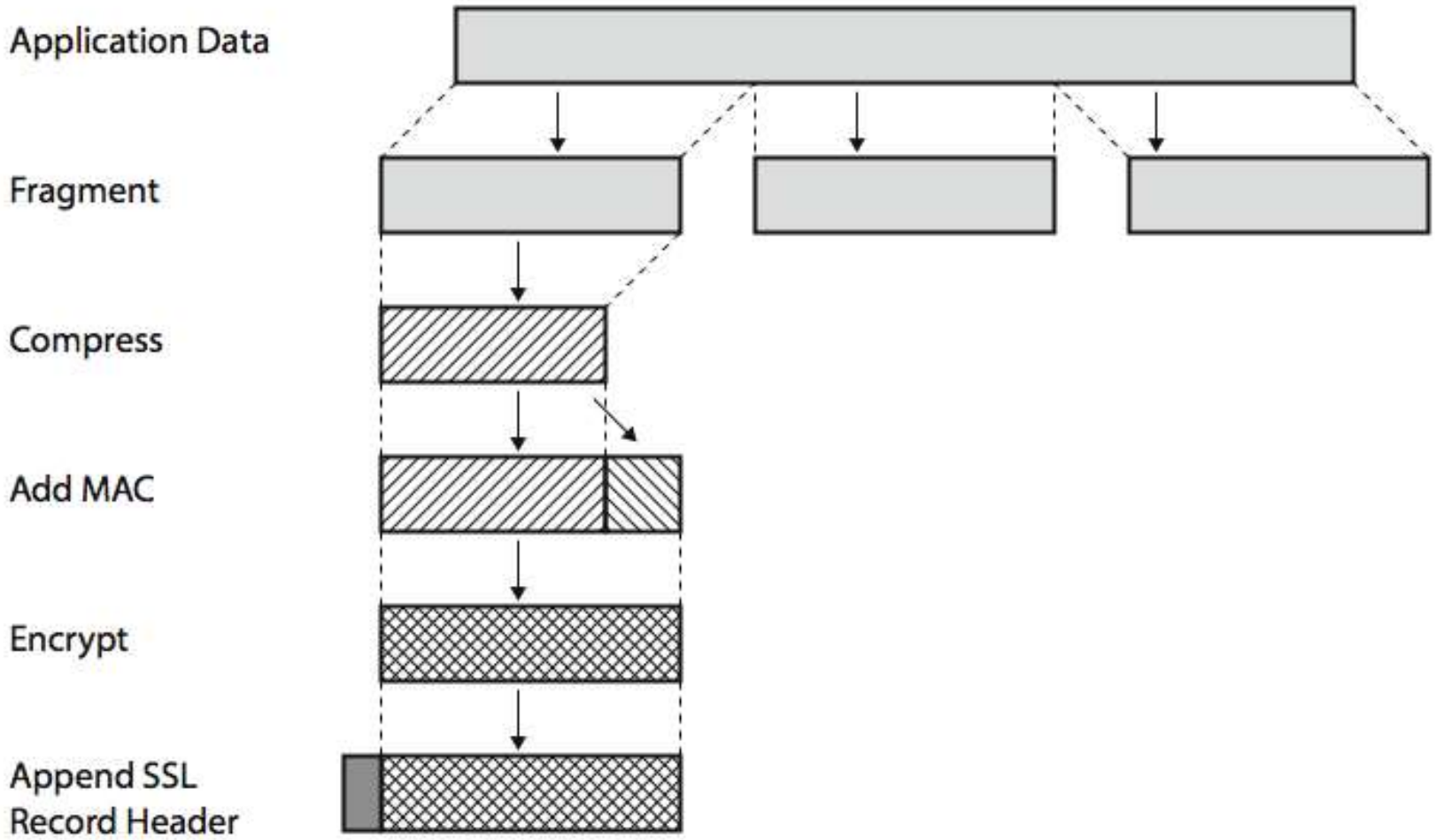
1. confidentiality

- using symmetric encryption with a shared secret key defined by Handshake Protocol
- AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
- message is compressed before encryption

2. message integrity

1. using a MAC with shared secret key
2. similar to HMAC but with different padding

SSL Record Protocol Operation



SSL Record Protocol Operation

1. **Fragmentation**: Each upper-layer message is fragmented into blocks of 214 bytes (16384 bytes) or less.
2. **Compression**: Compression must be lossless and may not increase the content length by more than 1024 bytes.
3. **MAC:** compute a message authentication code over the compressed data. For this purpose, a shared secret key is used.

   The calculation is defined as:

   hash(MAC_write_secret || pad_2 || hash(MAC_write_secret || pad_1 }

   seq_num || SSLCompressed.type || SSLCompressed.length ||

   SSLCompressed.fragment))

4. **Encryption**: compressed message plus the MAC are encrypted using symmetric encryption.(AES, IDEA,RC2,DES,3DES,Fortezza)

SSL Record Protocol Operation

|| = concatenation

MAC_write_secret = shared secret key

Hash = cryptographic hash algorithm; either MD5 or SHA-1

pad_1 = the byte 0x36 (0011 0110) repeated 48 times

pad_2 = the byte 0x5C (0101 1100) repeated 48 times

seq_num = the sequence number for this message

SSLCompressed.type = the higher-level protocol used to process this fragment

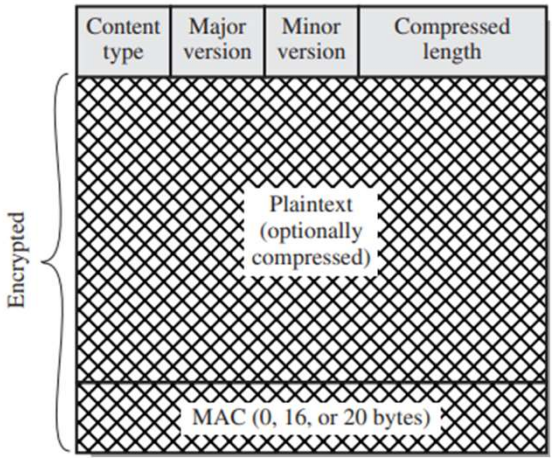
SSLCompressed.length = the length of the compressed fragment

SSLCompressed.fragment = the compressed fragment (if compression is not used, this is the plaintext fragment)

SSL Record Protocol Operation

The final step is to prepare the header with following fields:

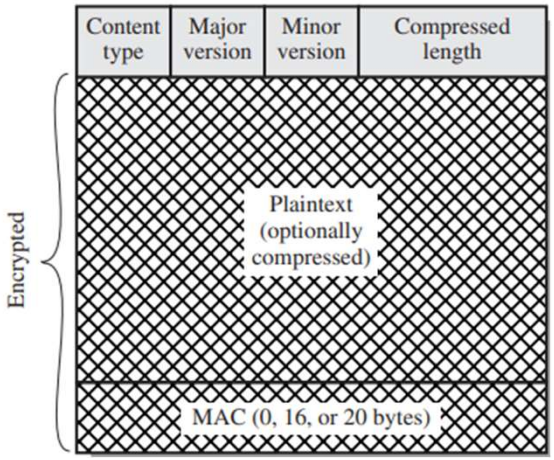
- **Content Type (8 bits):** The higher-layer protocol used to process the enclosed fragment.
- **Major Version (8 bits):** Indicates major version of SSL in use. For SSLv3, the value is 3.
- **Minor Version (8 bits):** Indicates minor version in use. For SSLv3, the value is 0.
- **Compressed Length (16 bits):** The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is 214 + 2048.



SSL Record Protocol Operation

The final step is to prepare the header with following fields:

- **Content Type (8 bits):** The content types that have been defined are:
  - change_cipher_spec
  - alert, handshake
  - application_data.

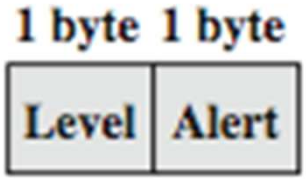


SSL Change Cipher Spec Protocol

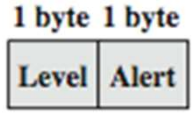
- The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the just-negotiated CipherSpec and keys.
- It exists to update the cipher suite to be used in the connection.
- It permits a change in the SSL session occur without having to renegotiate the connection.
- The message consists of a single byte of value 1.
- The change cipher spec message is normally sent at the end of the SSL handshake.

SSL Alert Protocol

- conveys SSL-related alerts to peer entity
- severity
  - warning or fatal
- specific alert
  - fatal: unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data



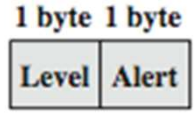
(b) Alert Protocol



(b) Alert Protocol

SSL Alert Protocol

- Each message in this protocol consists of two bytes.
- The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
- If the level is fatal, SSL immediately terminates the connection.
- Other connections on the same session may continue, but no new connections on this session may be established.
- The second byte contains a code that indicates the specific alert.

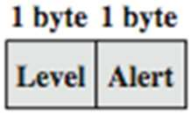


(b) Alert Protocol

SSL Alert Protocol

Fatal Errors:

- unexpected_message: An inappropriate message was received.
- bad_record_mac: An incorrect MAC was received.
- decompression_failure: The decompression function received improper input (e.g., unable to decompress or decompress to greater than maximum allowable length).
- handshake_failure: Sender was unable to negotiate an acceptable set of security parameters given the options available.
- illegal_parameter: A field in a handshake message was out of range or inconsistent with other fields.



(b) Alert Protocol

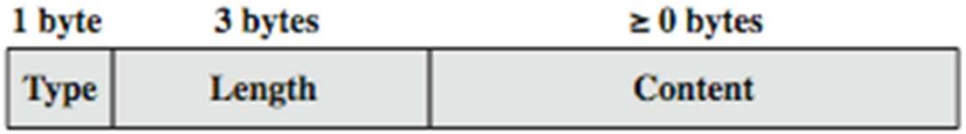
SSL Alert Protocol

Other type of Errors:

- close_notify: Notifies the recipient that the sender will not send any more messages on this connection.
- no_certificate: May be sent in response to a certificate request if no appropriate certificate is available.
- bad_certificate: A received certificate was corrupt (e.g., contained a
- signature that did not verify).
- unsupported_certificate: The type of the received certificate is not supported.
- certificate_revoked: A certificate has been revoked by its signer.
- certificate_expired: A certificate has expired.
- certificate_unknown: Some other unspecified issue arose in processing the certificate, rendering it unacceptable.

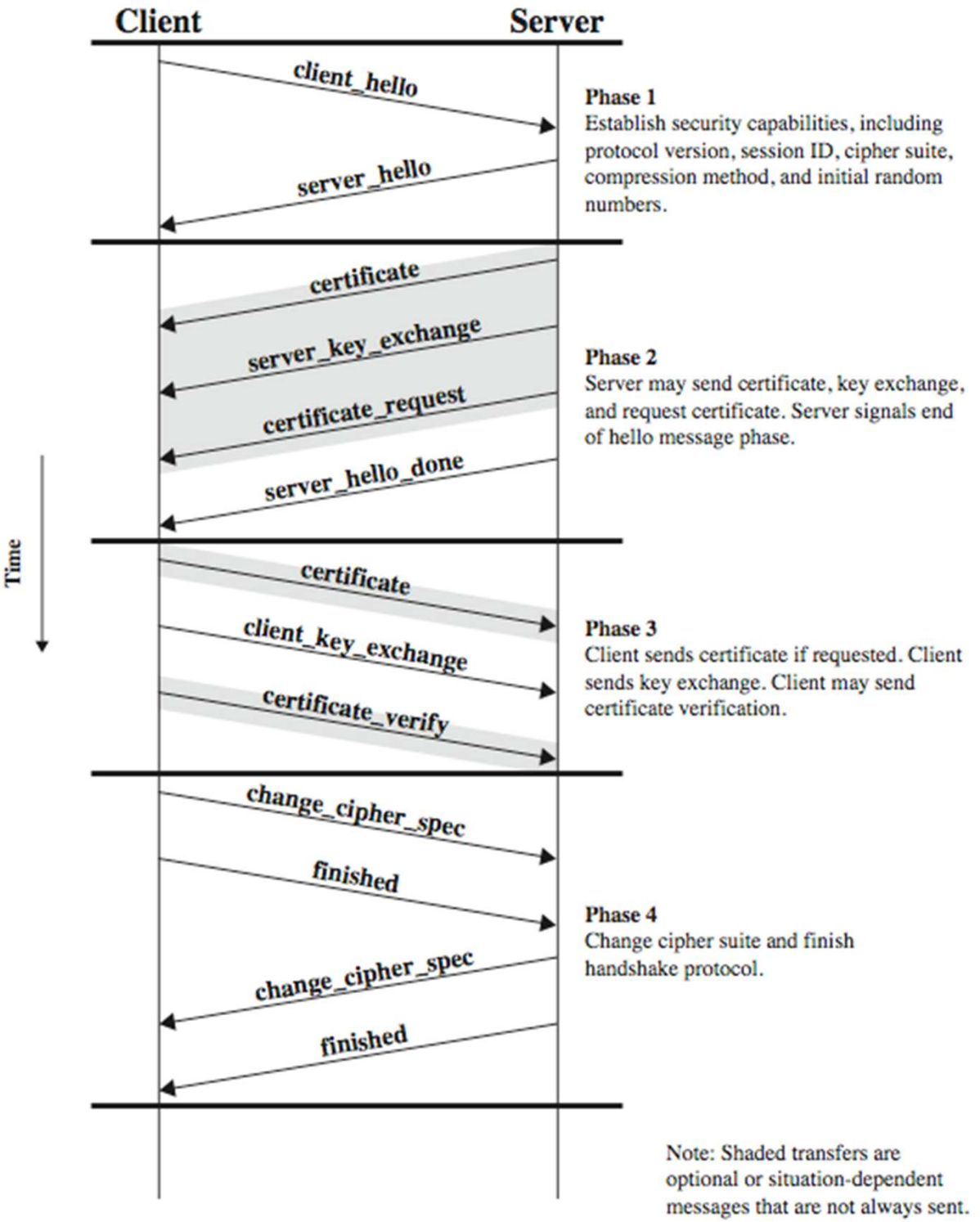
SSL Handshake Protocol

- allows server & client to:
  i. authenticate each other
  ii. to negotiate encryption & MAC algorithms
  iii. to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  i. Establish Security Capabilities
  ii. Server Authentication and Key Exchange
  iii. Client Authentication and Key Exchange
  iv. Finish



(c) Handshake Protocol

SSL Handshake Protocol



TLS (Transport Layer Security)

- Transport Layer Security (TLS) is the most widely used protocol for implementing cryptography on the web.
- TLS uses a combination of cryptographic processes to provide secure communication over a network.
- TLS provides a secure enhancement to the standard TCP/IP sockets protocol used for Internet communications.
- The application most commonly used with TLS is Hypertext Transfer Protocol (HTTP), the protocol for Internet web pages.
- Other applications - Net News Transfer Protocol (NNTP), Telnet, Lightweight Directory Access Protocol (LDAP), Interactive Message Access Protocol (IMAP), and File Transfer Protocol (FTP), can be used with TLS as well.

How TLS Works

- One of the reasons that TLS is effective is that it uses several different cryptographic processes.
- TLS uses public-key cryptography to provide authentication, and secret-key cryptography with hash functions to provide for privacy and data integrity.

Cryptographic Processes

HTTPS

- HTTPS (HTTP over SSL)
  i. combination of HTTP & SSL/TLS to secure communications between browser & server
     i. documented in RFC2818
     ii. no fundamental change using either SSL or TLS
- use https:// URL rather than http://
  i. and port 443 rather than 80
- encrypts
  i. URL, document contents, form data, cookies, HTTP headers

HTTPS Use

- connection initiation
  - TLS handshake then HTTP request(s)
- connection closure
  - have “Connection: close” in HTTP record
  - TLS level exchange close_notify alerts
  - can then close TCP connection
  - must handle TCP close before alert exchange sent or completed

Wireless Security, Mobile Device Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:

✓ Channel

- Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
- Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

✓ Mobility

- Wireless devices are far more portable and mobile, thus resulting in a number of risks

✓ Resources

- Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

✓ Accessibility

- Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks

802.11 Wireless LAN Security

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - Set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - Final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program

IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

The Wi-Fi Alliance

- 802.11b
  - First 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
  - Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
  - Later renamed the Wi-Fi Alliance
- Term used for certified 802.11b products is *Wi-Fi*
  - Has been extended to 802.11g products
- Wi-Fi Protected Access (WPA)
  - Wi-Fi Alliance certification procedures for IEEE802.11 security standards
  - WPA2 incorporates all of the features of the IEEE802.11i WLAN security specification

IEEE 802 Protocol Architecture

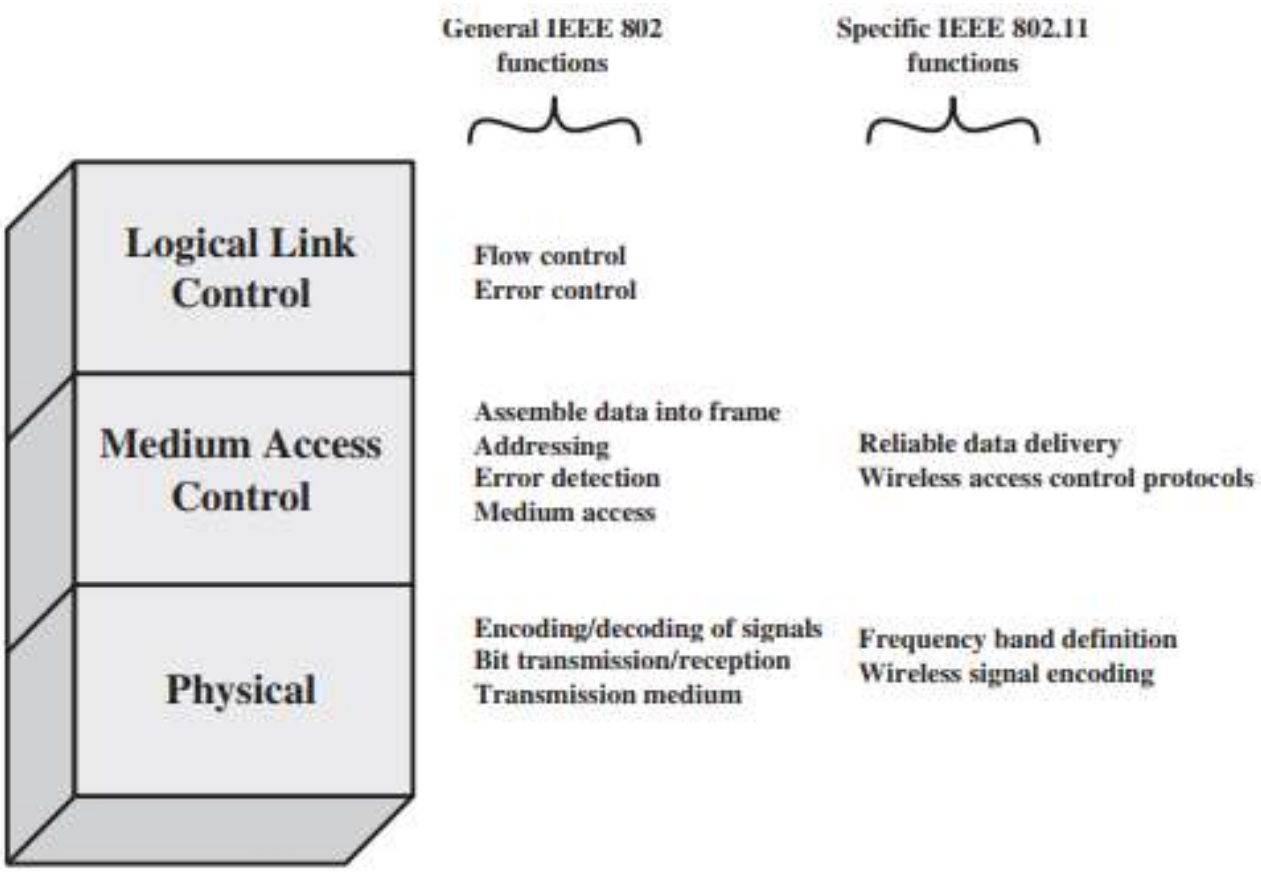


Figure 18.3 IEEE 802.11 Protocol Stack

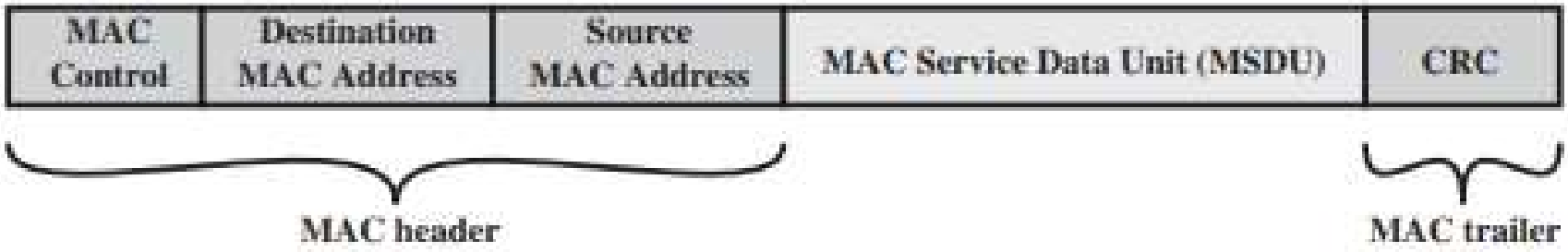


Figure 18.4 General IEEE 802 MPDU Format

IEEE 802.11 Network Components and Architectural Model

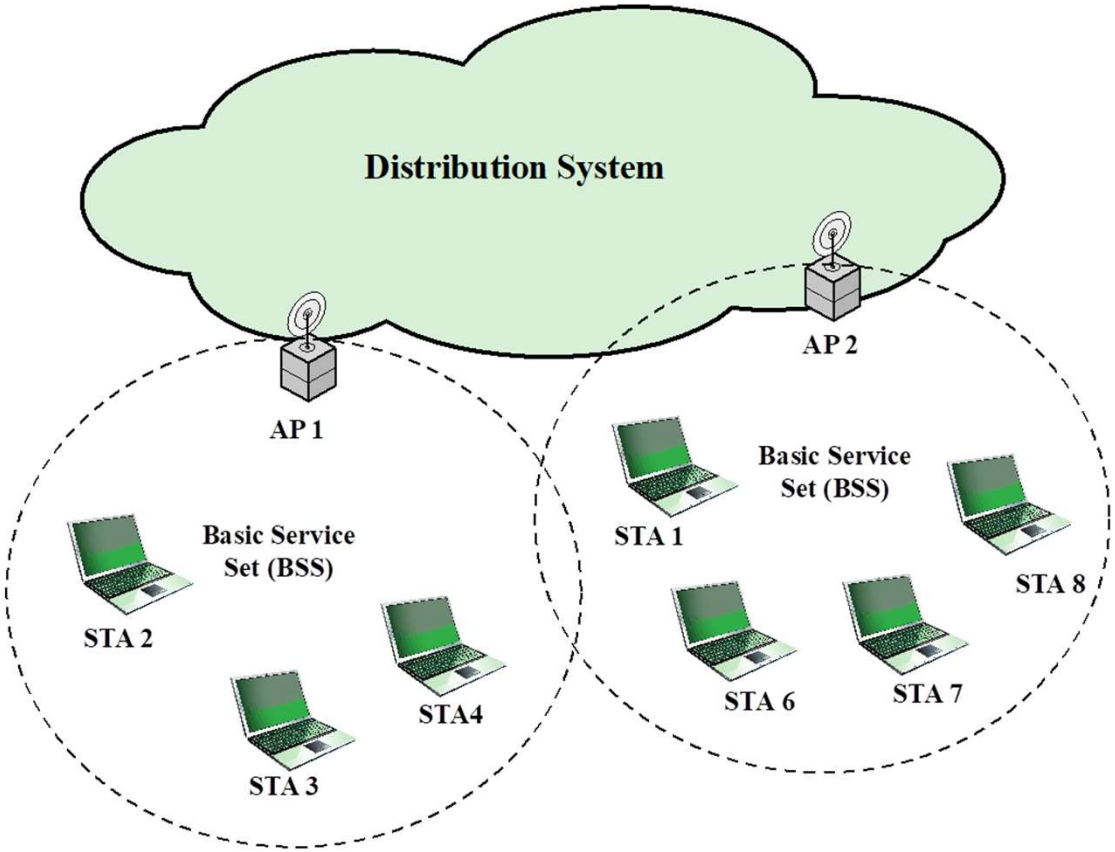


Figure 24.5 IEEE 802.11 Extended Service Set

IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

Distribution of Messages Within a DS

- The two services involved with the distribution of messages within a DS are:
  - Distribution
  - Integration

Distribution

- The primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS

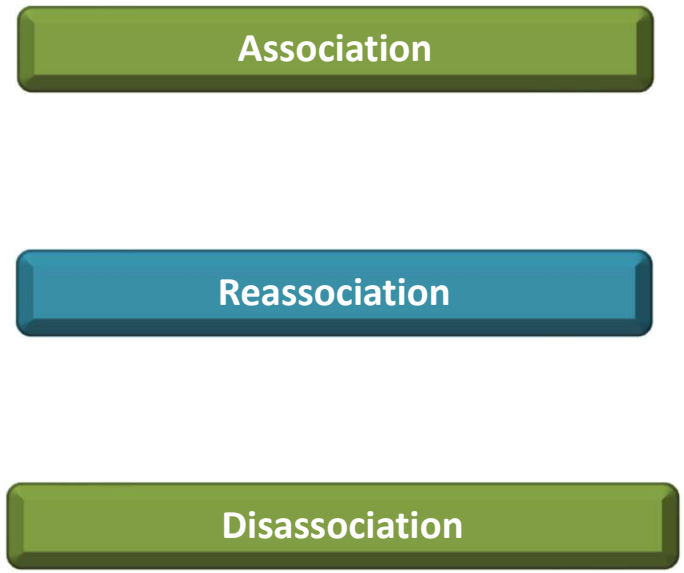
Integration

- Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802x LAN
- Service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN

Association-Related Services

- Transition types, based on mobility:
  - No transition
    - A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS
  - BSS transition
    - Station movement from one BSS to another BSS within the same ESS; delivery of data to the station requires that the addressing capability be able to recognize the new location of the station
  - ESS transition
    - Station movement from a BSS in one ESS to a BSS within another ESS; maintenance of upper-layer connections supported by 802.11 cannot be guaranteed

Services

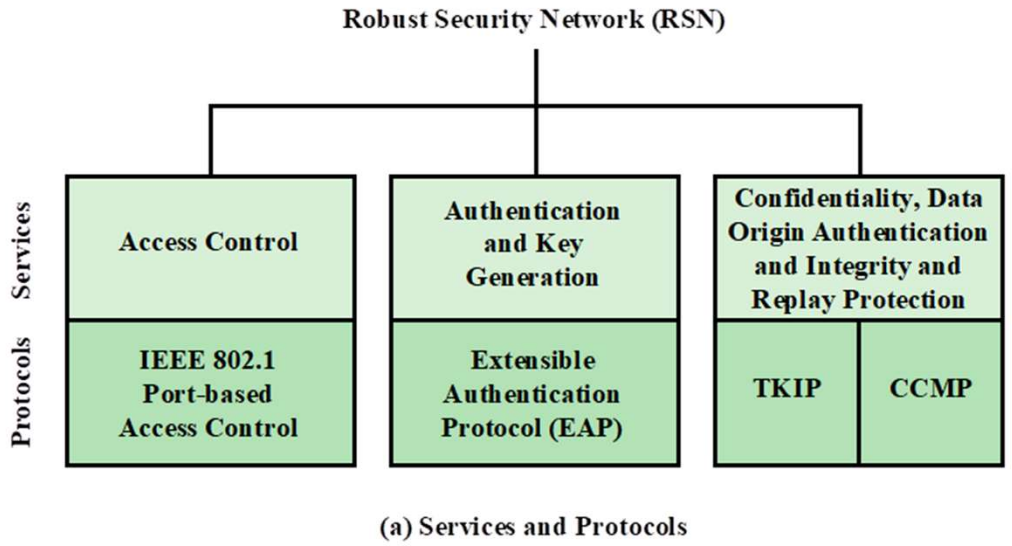


- **Establishes an initial association between a station and an AP**
- **Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another**
  - **A notification from either a station or an AP that an existing association is terminated**

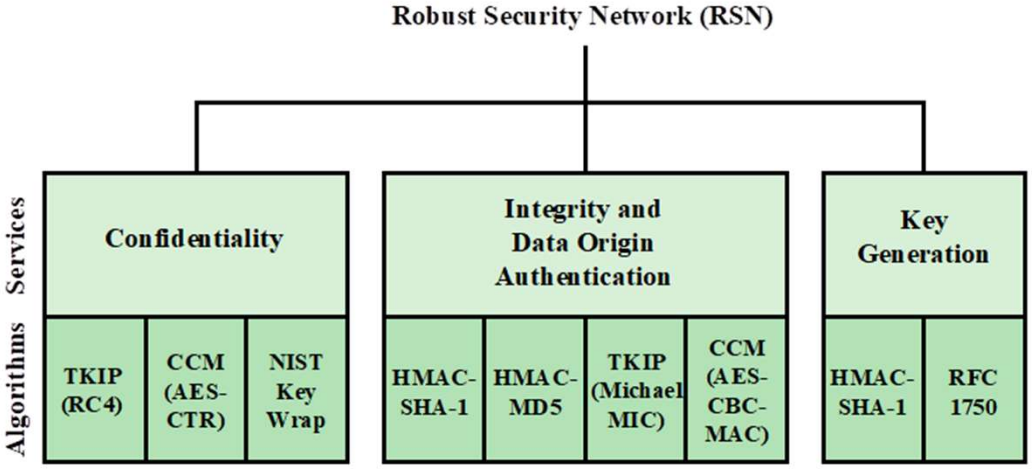
Wireless LAN Security

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - Set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - Final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program

Elements of IEEE 802.11i



(a) Services and Protocols

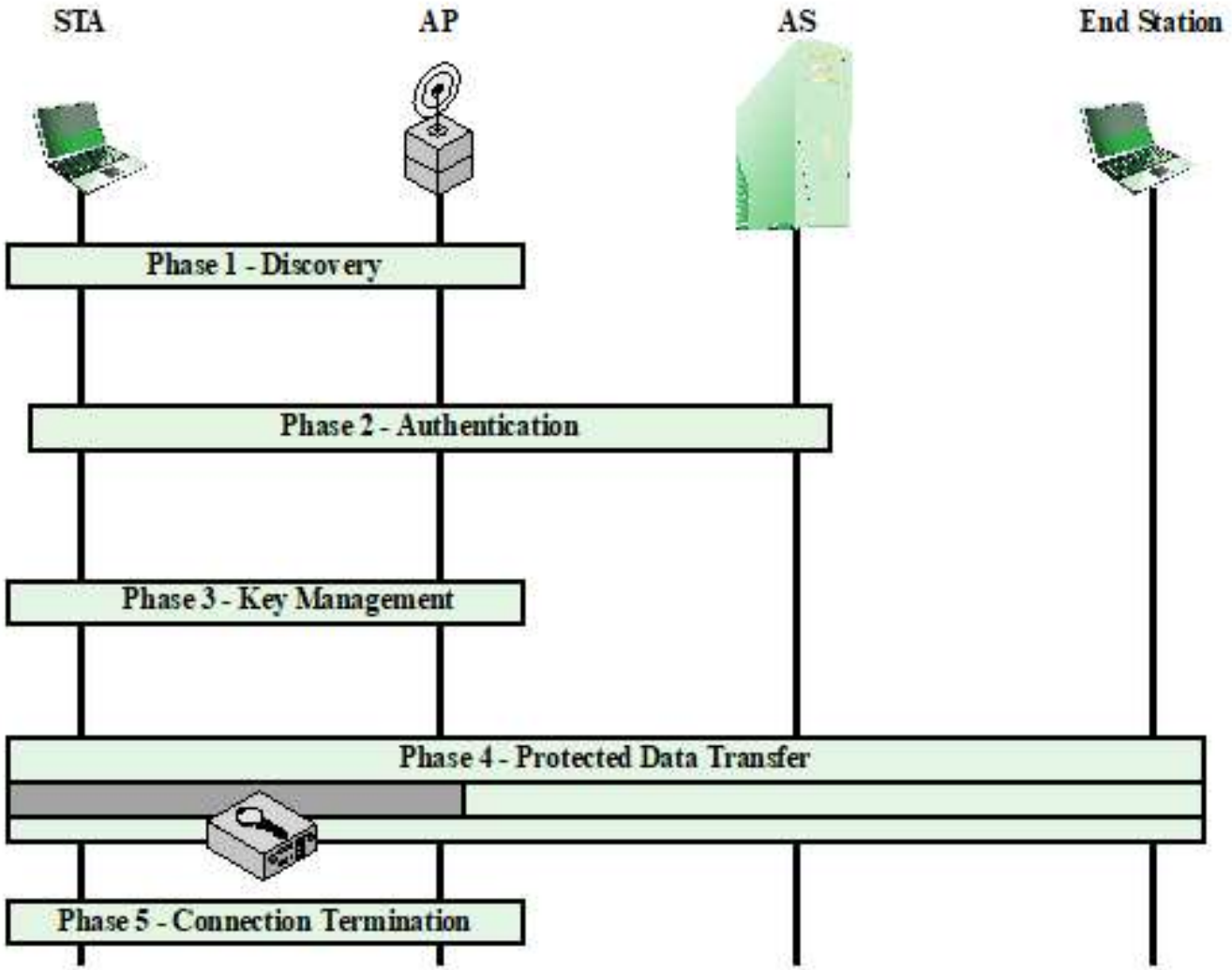


(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 24.6 Elements of IEEE 802.11i

Phases of operation



IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association