CS321: Computer Networks

Securing E-mail, WLAN
SSL, IPsec

Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Jodhpur
E-mail: manaskhatua@iitj.ac.in

Application Layer Security: Securing E-mail

Security in Internet protocol stack

- It is possible to provide security services in any of the top four layers of the Internet protocol stack.

- Why security functionality is being provided at more than one layer in the Internet?

  - First, although security at the network layer can offer "blanket coverage" by encrypting all the data in the datagrams (that is, all the transport-layer segments) and by authenticating all the source IP addresses, it can't provide user-level security.

  - For example, a commerce site cannot rely on IP-layer security to authenticate a customer who is purchasing goods at the commerce site.

  - Second, it is generally easier to deploy new Internet services, including security services, at the higher layers of the protocol stack.

  - So, many application developers introduce security functionality into their favorite applications

Secure E-mail System

- Which security features would be most desirable for e-mail system.
  - *Confidentiality:* Neither Alice nor Bob wants Trudy to read Alice's e-mail message.
  - *Sender authentication*: Bob would naturally want to be sure that the message came from Alice and not from Trudy.
  - *Message integrity*: assurance that the message Alice sends is not modified while en-route to Bob.
  - *Receiver authentication*: Alice wants to make sure that she is indeed sending the letter to Bob and not to someone else (for example, Trudy) who is impersonating Bob.

Confidentiality (in E-mail)

- Information needs to be hidden from unauthorized access
- Solution: Symmetric key cryptography

- Problem: Secure Key distribution among Alice and Bob
- Solution: Public key cryptography + PKI

- Problem: Inefficient for long message and long key (as RSA needs exponentiation)
- Solution: Public key + Session key + PKI

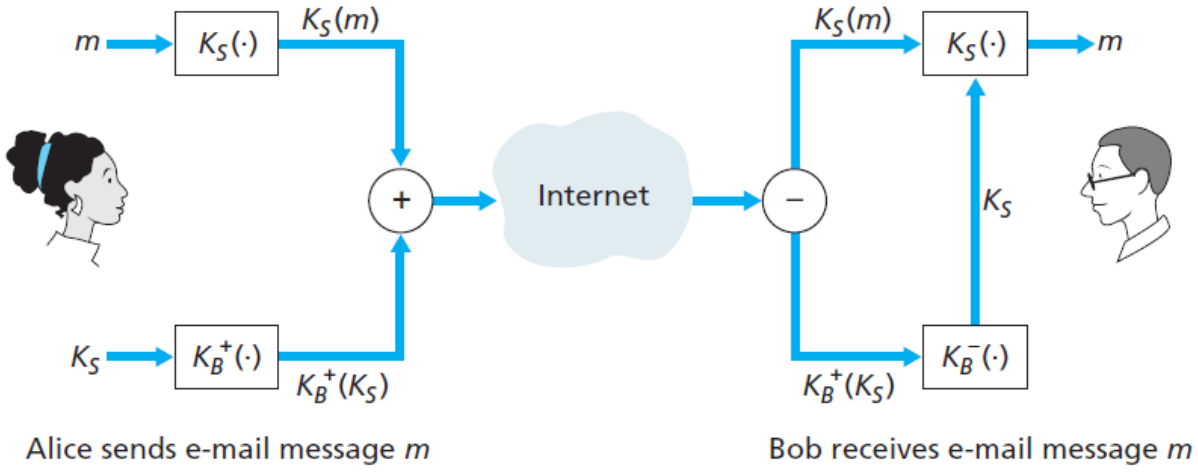


Figure 8.19 ♦ Alice used a symmetric session key, K_S, to send a secret e-mail to Bob

Sender Authentication, Message Integrity (in E-mail)

- We use digital signatures and message digests

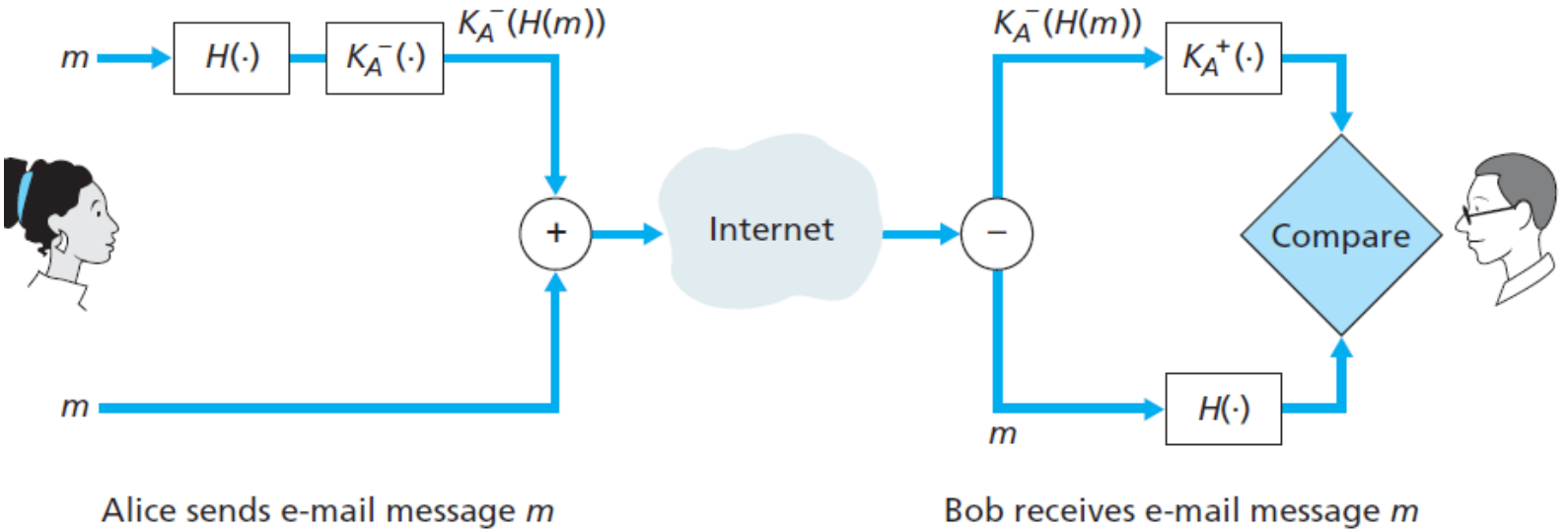


Figure 8.20 ♦ Using hash functions and digital signatures to provide sender authentication and message integrity

Secure E-mail System

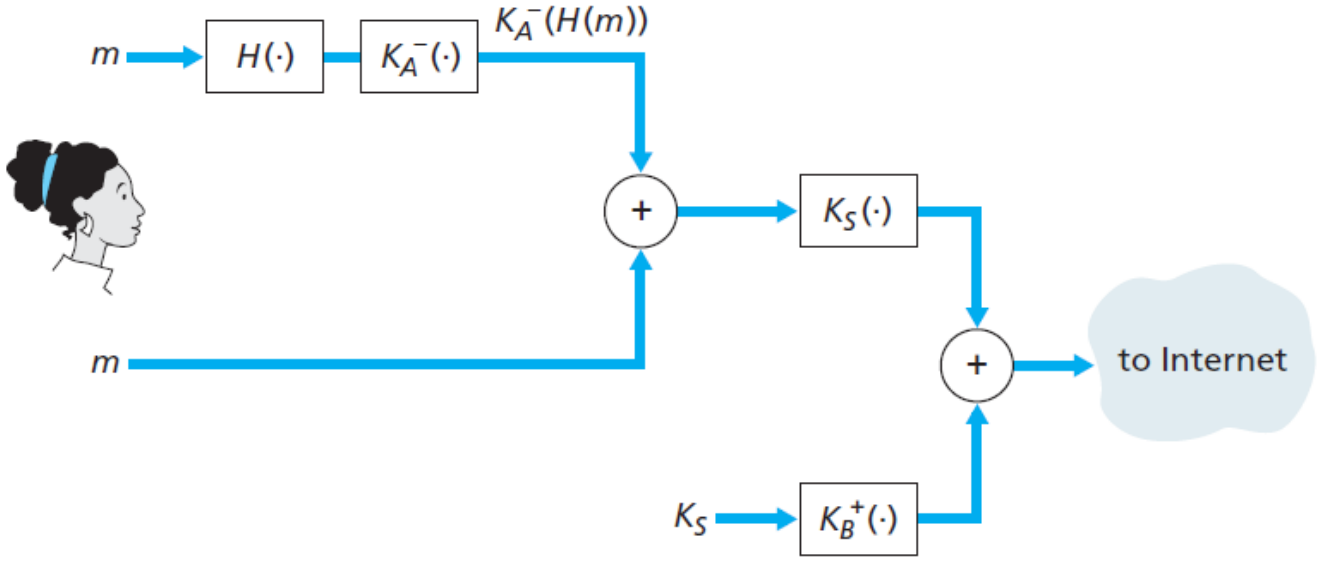


Figure 8.21 ♦ Alice uses symmetric key cyptography, public key cryptography, a hash function, and a digital signature to provide secrecy, sender authentication, and message integrity

- Note that, in this scheme, Alice uses public key cryptography twice:
  - once with her own private key and
  - once with Bob's public key.
- Public key distribution is done using CA
- Hash function is known by both Alice and Bob

Pretty Good Privacy (PGP)

- Pretty Good Privacy (PGP) is an e-mail encryption scheme that has become a de facto standard.
- The PGP design is, in essence, the same as the design shown in Figure 8.21.
- Depending on the version, the PGP software uses
  - MD5 or SHA for calculating the message digest;
  - CAST, triple-DES, or IDEA for symmetric key encryption;
  - RSA for the public key encryption.

- When PGP is installed, the software creates a public key pair for the user.
- The public key can be posted on the user's Web site or placed in a public key server.
- The private key is protected by the use of a password.
- The password has to be entered every time the user accesses the private key.

Securing TCP

Securing TCP Connections: SSL

- The secured version of TCP is commonly known as **Secure Sockets Layer (SSL)**.
- A slightly modified version of SSL version 3, called **Transport Layer Security (TLS)**
- SSL is supported by all popular Web browsers and Web servers
- SSL is used by essentially all Internet commerce sites (including Amazon, eBay, Yahoo!, MSN, and so on).
- Why SSL?
  - Bob is surfing the Web and arrives at the Alice Incorporated site, which is selling perfume.
  - Bob orders a perfume and paid for it.
  - Bob is waiting to receive the product using home delivery.
  - Let, no security measures are taken.
  - What will happen then?

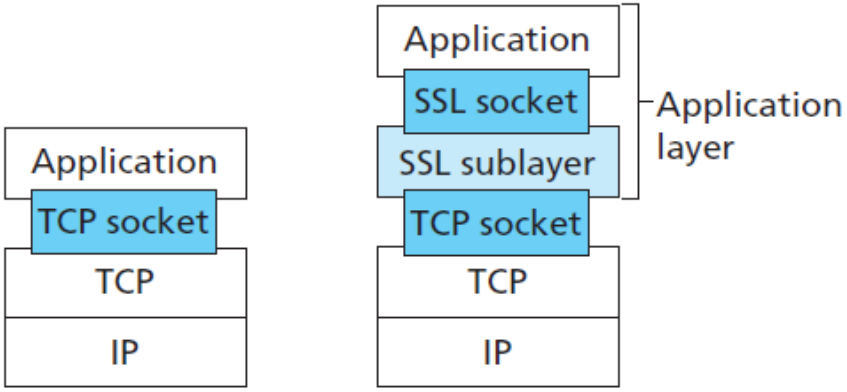
Cont…

- If no confidentiality (encryption) is used, an intruder could intercept Bob's order and obtain his payment card information.
- If no data integrity is used, an intruder could modify Bob's order.
- If no server authentication is used, a server could display Alice Incorporated's famous logo when in actuality the site maintained by Trudy, who is masquerading as Alice Incorporated.
- SSL addresses these issues by enhancing TCP with
  - confidentiality,
  - data integrity,
  - server authentication, and
  - client authentication.

Basics of SSL

- SSL is often used to provide security to transactions that take place over HTTP.

- SSL provides a simple Application Programmer Interface (API) with sockets, which is similar and analogous to TCP's API.



- Although SSL technically resides in the application layer, from the developer's perspective it is a transport-layer protocol

How SSL works?

- SSL has three phases:
  - *handshake*,
  - *key derivation*, and
  - *data transfer*.

- Handshake
  - Bob needs to establish a TCP connection with Alice;
  - needs to verify that Alice is *really* Alice; and
  - sends Alice an *encrypted master secret (MS)*, which will be used by both Alice and Bob to generate all the *symmetric session keys* they need for the SSL session.

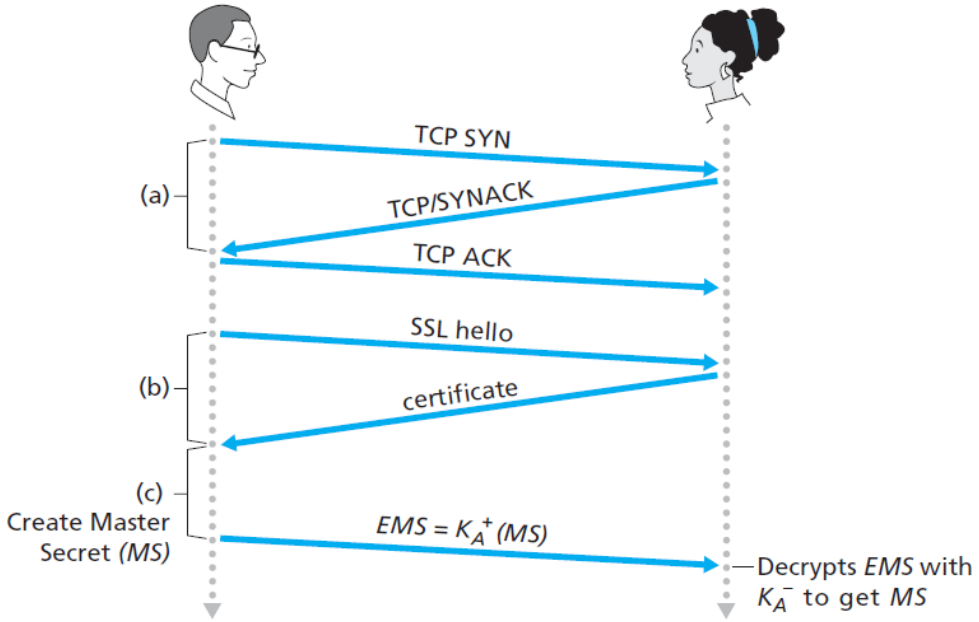


Figure 8.25 ♦ The almost-SSL handshake, beginning with a TCP connection

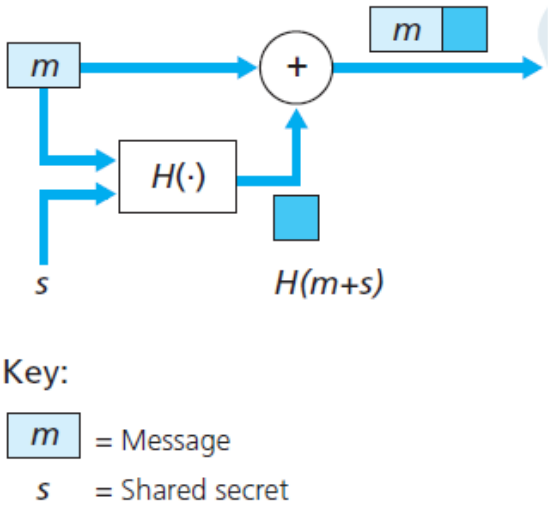
Cont…

- Key Derivation
  - the shared MS could be used to generate the symmetric session key for all subsequent encryption and data integrity checking.
  - Both Alice and Bob generate four keys
    - E_B = session encryption key for data sent from Bob to Alice
    - M_B = session authentication/MAC key for data sent from Bob to Alice
    - E_A = session encryption key for data sent from Alice to Bob
    - M_A = session authentication/MAC key for data sent from Alice to Bob

Cont…

- Data Transfer
  - Since TCP is a byte-stream protocol, where would we put the MAC for the integrity check?
  - Solution: SSL breaks the data stream into records, appends a MAC to each record for integrity checking, and then encrypts the *record+MAC*.

- To create the MAC, Bob inputs the record data along with the key M_B into a hash function (as shown below in Figure)
- To encrypt the package (record+MAC), Bob uses his session encryption key E_B.



- This encrypted package is then passed to TCP for transport over the Internet.
- It still isn't bullet-proof !
- Trudy could capture two segments sent by Bob, reverse the order of the segments, adjust the TCP sequence numbers (which are not encrypted), and then send.

Cont…

- Solution: add sequence number for each record
  - Bob doesn't actually include a sequence number in the record. It includes in MAC calculation.
  - MAC = hash (data + MAC key M_B + *current sequence number)*
  - Alice tracks Bob's sequence numbers, allowing her to verify the data integrity of a record by including the appropriate sequence number in the MAC calculation.

- SSL Record / Message Format

Figure 8.26 ♦ Record format for SSL

Type field : indicates whether the record is a handshake message or a message that contains application data.
Note that the first three fields are not encrypted.

Network Layer Security: IPsec

IPsec

- IP security protocol (IPsec) provides security at the network layer.
- Many institutions use IPsec to create virtual private networks (VPNs) that run over the public Internet.
- Network layer security services between a pair of network entities
  - Confidentiality
    - the sending entity encrypts the payloads of all the datagrams it sends
    - the encrypted payload could be a TCP segment, a UDP segment, an ICMP message, and so on
    - all data sent from one entity to the other would be hidden from any third party that might be sniffing the network
    - network-layer security is said to provide “blanket coverage”
  - Source authentication
    - the receiving entity can verify the source of the secured datagram
  - Data integrity
    - the receiving entity can check for any tampering of the datagram that may have occurred while the datagram was in transit.
  - Replay-attack prevention
    - the receiving entity could detect any duplicate datagrams that an attacker might insert

VPN

- An institution often desires its own IP network even if the institution is spread across in multiple geographical regions

- Private network:
  - It is a stand-alone physical network of an Institution
  - It includes routers, links, and a DNS infrastructure
  - it is completely separate from the public Internet

- VPN: With a VPN, the institution's inter-office traffic is sent over the public Internet rather than over a physically independent network.

- A leased line is not a dedicated cable; it is a reserved circuit between two points. The leased line is always active and available.

- Leased line maintain a single open circuit at all times, as opposed to traditional telephone services that reuse the same line for many different conversations through a process called switching.

How VPN Works?

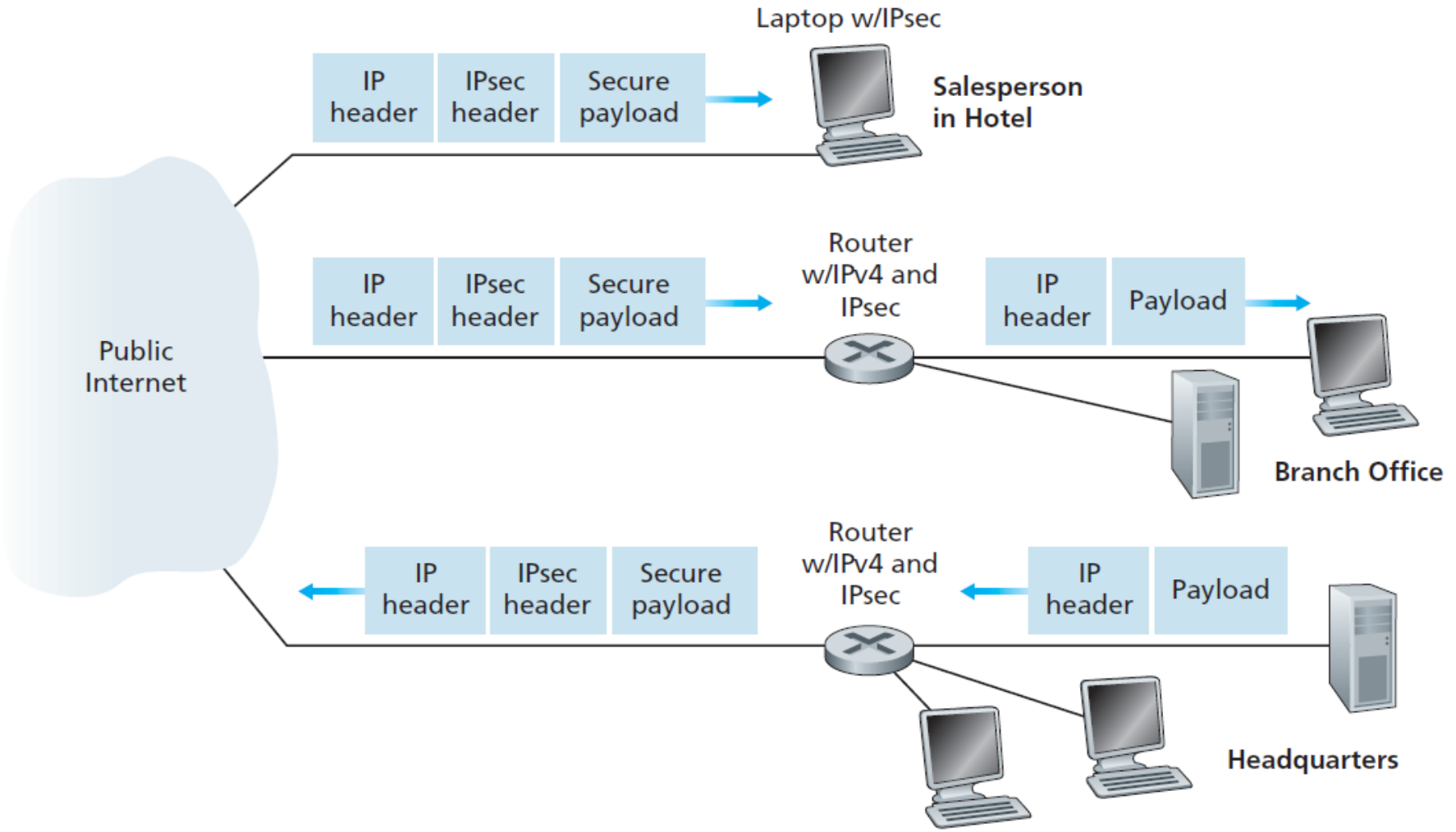


Figure 8.27 ♦ Virtual Private Network (VPN)

IPSec Protocol Suite

- In the IPsec protocol suite, there are two principal protocols:
  - Authentication Header (AH) protocol
  - Encapsulation Security Payload (ESP) protocol
- The AH protocol provides source authentication and data integrity but *does not* provide confidentiality.
- The ESP protocol provides source authentication, data integrity, *and* confidentiality.
- The ESP protocol is much more widely used than the AH protocol.

Security Association (SA)

- Before sending IPsec datagrams from source entity to destination entity, the source and destination entities create a network-layer logical connection.
- This logical connection is called a security association (SA).
- An SA is a simplex logical connection
- If both entities want to send secure datagrams to each other, then two SAs (that is, two logical connections) need to be established, one in each direction.

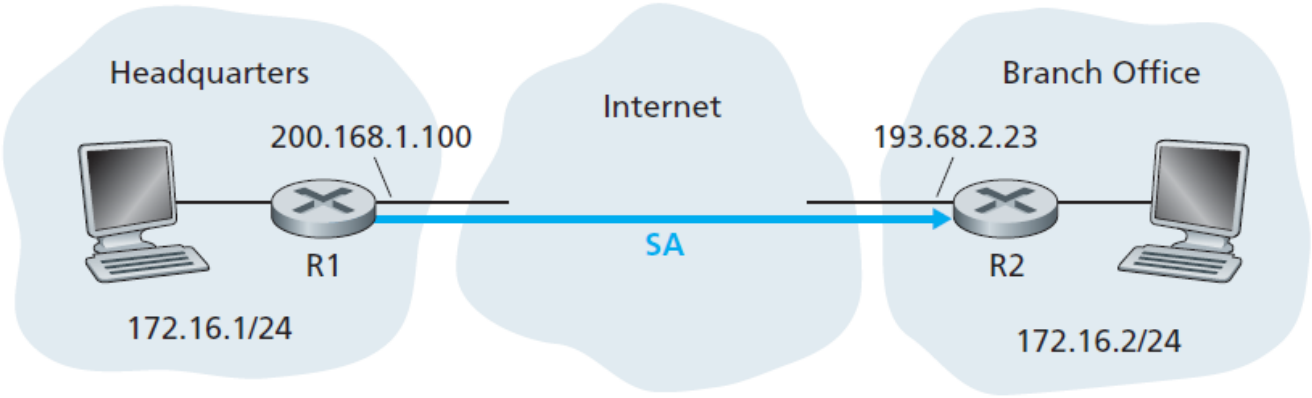


Figure 8.28 ♦ Security Association (SA) from R1 to R2

Cont…

- Router R1 will maintain state information about this SA, which will include:
  - A 32-bit identifier for the SA, called the Security Parameter Index (SPI)
  - The origin interface of the SA (in this case 200.168.1.100) and the destination interface of the SA (in this case 193.68.2.23)
  - The type of encryption to be used (e.g., 3DES with CBC)
  - The encryption key
  - The type of integrity check (e.g., HMAC with MD5)
  - The authentication key

- Whenever router R1 needs to construct an IPsec datagram for forwarding over this SA, it accesses this state information to determine how it should authenticate and encrypt the datagram.

- Router R2 will maintain the same state information for this SA and will use this information to authenticate and decrypt any IPsec datagram that arrives from the SA.

- An IPsec entity (router or host) often maintains state information for many SAs.
- It stores the state information for all of its SAs in its Security Association Database (SAD)

The IPsec Datagram

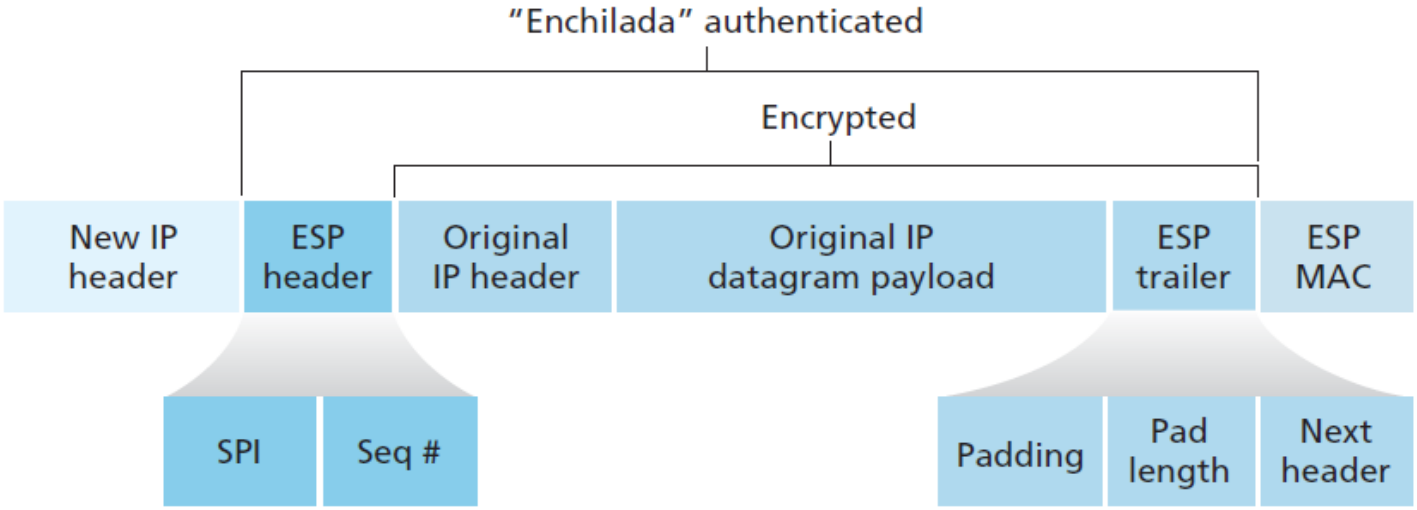


Figure 8.29 ♦ IPsec datagram format

- IPsec has two different packet forms
  - tunnel mode,
  - transport mode.
- The tunnel mode is more appropriate for VPNs, and thus, widely deployed

Cont…

- Router R1 uses the following recipe to convert this “original IPv4 datagram” into an IPsec datagram:
  - Appends to the back of the original IPv4 datagram (which includes the original header fields!) an “ESP trailer” field
  - Encrypts the result using the algorithm and key specified by the SA
  - Appends to the front of this encrypted quantity a field called “ESP header”; the resulting package is called the “enchilada”
  - Creates an authentication MAC over the whole enchilada using the algorithm and key specified in the SA
  - Appends the MAC to the back of the enchilada forming the payload
  - Finally, creates a brand new IP header with all the classic IPv4 header fields (together normally 20 bytes long), which it appends before the payload

Brand New IP Header

- The original IP datagram has 172.16.1.17 for the source IP address and 172.16.2.48 for the destination IP address.
- What about the source and destination IP addresses that are in the new IP header?
  - they are set to the source and destination router interfaces at the two ends of the tunnels, namely, 200.168.1.100 and 193.68.2.23.
  - Also, the protocol number in this new IPv4 header field is not set to that of TCP, UDP, or SMTP, but instead to 50, designating that this is an IPsec datagram using the ESP protocol.
- After R1 sends the IPsec datagram into the public Internet, it will pass through many routers before reaching R2.
- All intermediate routers will process the datagram as if it were an ordinary datagram—they are completely oblivious to the fact that the datagram is carrying IPsec-encrypted data.

At the R2

- When R2 receives the IPsec datagram,
  - As the protocol field is 50, R2 sees that it should apply IPsec ESP processing
  - First, R2 uses the SPI to determine to which SA the datagram belongs.
  - Second, it calculates the MAC of the enchilada and verifies that the MAC is consistent with the value in the ESP MAC field.
  - Third, it checks the sequence-number field to verify that the datagram is fresh (and not a replayed datagram).
  - Fourth, it decrypts the encrypted unit using the decryption algorithm and key associated with the SA.
  - Fifth, it removes padding and extracts the original, vanilla IP datagram.
  - And finally, sixth, it forwards the original datagram into the branch office network towards its ultimate destination.

Security Summary of IPsec

- Confidentiality: Trudy cannot see the original datagram. If fact, not only is the data in the original datagram hidden from Trudy, but s is the protocol number, the source IP address, and the destination IP address.

- Data Integrity: Suppose Trudy tries to tamper with a datagram in the SA by flipping some of its bits. When this tampered datagram arrives at R2, it will fail the integrity check (using the MAC), thwarting Trudy's vicious attempts once again.

- Source Authentication: Suppose Trudy tries to masquerade as R1, creating a IPsec datagram with source 200.168.1.100 and destination 193.68.2.23. Trudy's attack will be futile, as this datagram will again fail the integrity check at R2.

- Replay Attack: Because IPsec includes sequence numbers, Trudy will not be able create a successful replay attack.

Securing Wireless LAN

Securing Wireless LAN

- Security is a particularly important concern in wireless networks
- Standardized security mechanisms:
  - Wired Equivalent Privacy (WEP); designed in 1999
    - provide authentication and data encryption between a host and a wireless AP using a symmetric shared key approach.
    - does not specify any key management algorithm,
    - host and wireless AP have somehow agreed on the key via an out-of-band method
  - IEEE 802.11i or WiFi Protected Access (WPA); designed in 2004
    - provides much stronger forms of encryption,
    - provides an extensible set of authentication mechanisms, and a key distribution mechanism.
    - In addition, 802.11i defines an authentication server with which the AP can communicate.
    - Separating the authentication server from the AP allows one authentication server to serve many APs

Wired Equivalent Privacy (WEP)

- Authentication is carried out as follows:
  1. A wireless host requests authentication by an access point.
  2. The access point responds to the authentication request with a 128-byte nonce value.
  3. The wireless host encrypts the nonce using the symmetric key that it shares with the access point.
  4. The access point decrypts the host-encrypted nonce.
  5. If the decrypted nonce matches the nonce value originally sent to the host, then the host is authenticated by the access point.

- Requirements:
  - Symmetric encryption key
  - Shared a priory between host and AP
  - Encryption algorithm
  - None generation algorithm

WEP Data Encryption

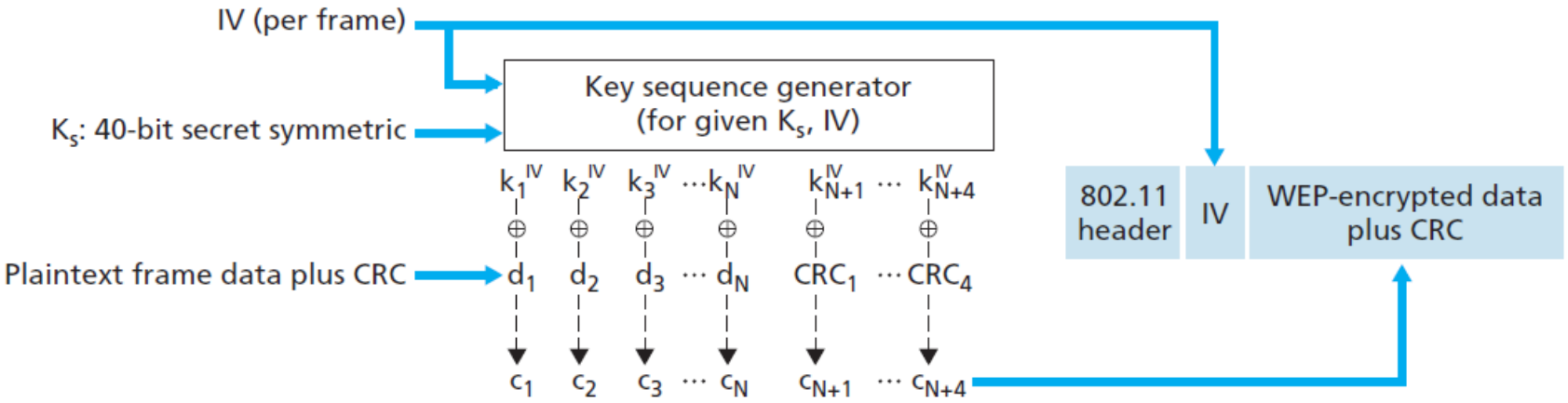


Figure 8.30 ♦ 802.11 WEP protocol

- A secret 40-bit symmetric key, K_S, is assumed to be known by both a host and the AP.
- A 24-bit Initialization Vector (IV) is appended to the 40-bit key to create a 64-bit key that will be used to encrypt a single frame.
- The IV will change from one frame to another; and is included *in plaintext* in the header of each WEP-encrypted 802.11 frame

- Encryption method:
  - A 4-byte CRC value is computed for the data payload
  - The payload and the four CRC bytes are then encrypted using the RC4 stream cipher.
  - RC4 algorithm produces a stream of key values that are used to encrypt the data and CRC value in a frame

Security Gap in WEP

- Proper use of the RC4 algorithm requires that the same 64-bit key value *never* be used more than once.

- So, for a given K_S, there are only 2^{24} unique keys
- If these keys are chosen randomly, the probability of having chosen the same IV value is more than 99% after only 12,000 frames!
- With 1 Kbyte frame sizes and a data transmission rate of 11 Mbps, only a few seconds are needed before 12,000 frames are transmitted.

- Furthermore, since the IV is transmitted in plaintext in the frame, an eavesdropper (Trudy) will know whenever a duplicate IV value is used.
- When Trudy sees the same value of IV being used, she will know the key sequence, and will thus be able to decrypt the encrypted message!

- Few More Gaps:
  1. a known weakness in RC4 when certain weak keys are chosen.
  2. an attacker can changes the encrypted payload, computes a CRC over the modified data, places the CRC into a WEP frame; that frame will be accepted by the receiver !

IEEE 802.11i

- It is improved version of WEP
- Separating the authentication server from the AP
- 802.11i operates in four phases

1. *Discovery*
2. *Mutual authentication, and Master Key (MK) generation*
3. *Pairwise Master Key (PMK) generation*
4. *Temporal Key (TK) generation*

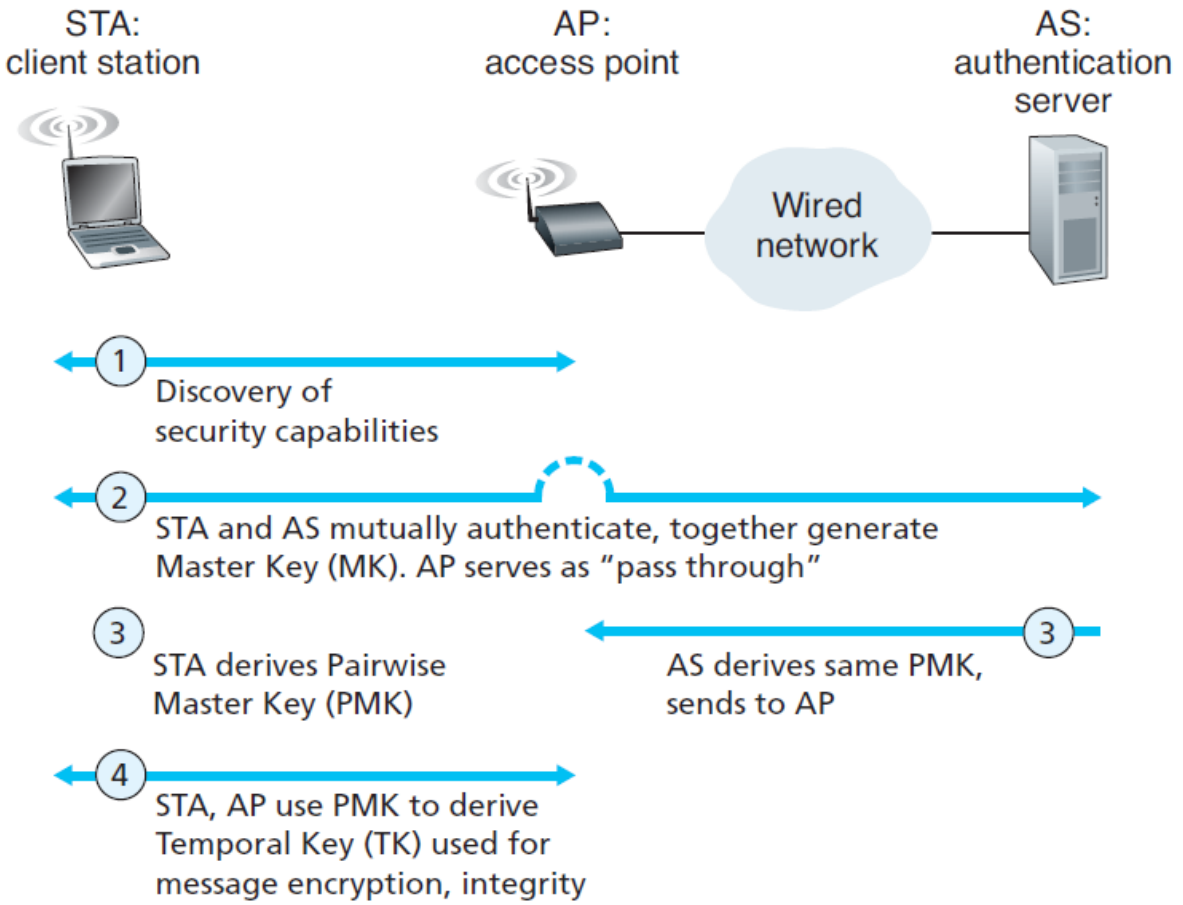


Figure 8.31 ♦ 802.11i: four phases of operation

IEEE 802.11i

- IEEE 802.11i operates in four phases
  1. Discovery:
     - the AP advertises its presence and the forms of authentication and encryption
     - client then requests the specific forms of authentication and encryption that it desires
  2. Mutual authentication and Master Key (MK) generation:
     - Authentication takes place between the STA and the authentication server
     - In this phase, the AP acts essentially as a relay
     - The Extensible Authentication Protocol (EAP) is used
     - Authentication server derives a Master Key (MK) that is shared to STA
  3. Pairwise Master Key (PMK) generation:
     - The MK is a shared secret which is used to generate the Pairwise Master Key (PMK)
     - STA and authentication server separately generates the same PMK
     - The authentication server the sends the PMK to the AP
  4. Temporal Key (TK) generation:
     - With the PMK, the wireless client and AP can now generate additional keys that will be used for communication.

Extensible Authentication Protocol (EAP)

- EAP uses a simple request/response mode of interaction between the client and authentication server.
- the EAP-TLS authentication scheme is often used.

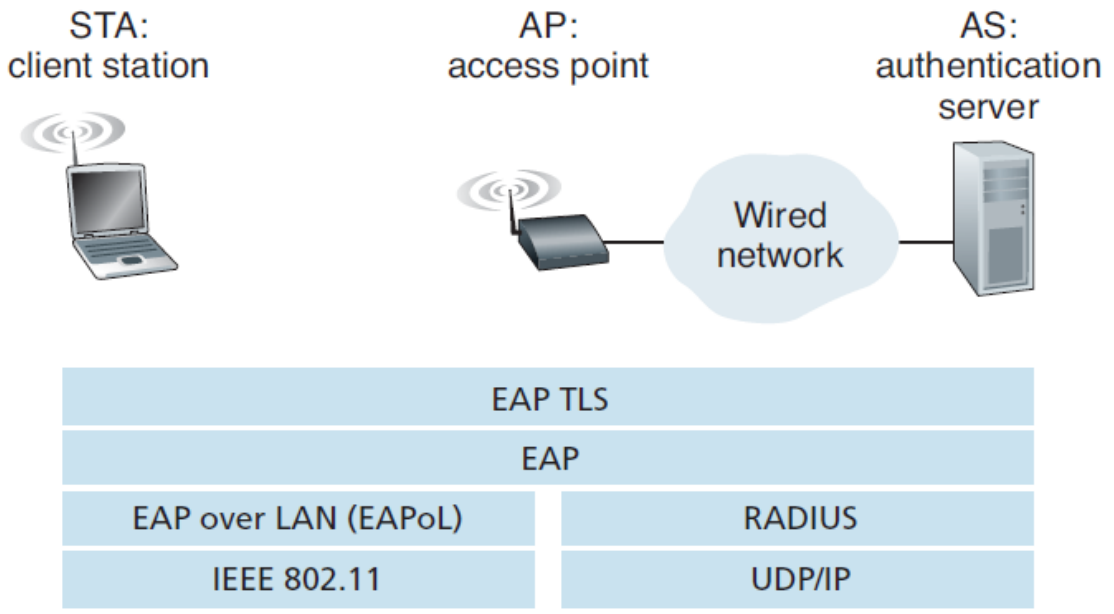


Figure 8.32 ♦ EAP is an end-to-end protocol. EAP messages are encapsulated using EAPoL over the wireless link between the client and the access point, and using RADIUS over UDP/IP between the access point and the authentication server

EAP-TLS uses public key techniques (including nonce encryption and message digests) to allow the client and authentication server to mutually authenticate each other, and to derive a Master Key (MK) that is known to both parties.

Thanks!