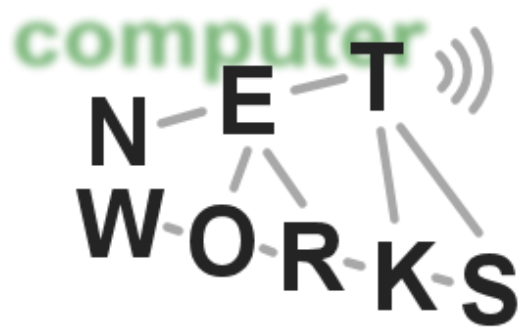


# Network Security – Part II

Computer Networks, Winter 2016/2017



# Chapter 7 roadmap

7.1 What is network security?

7.2 Principles of cryptography

7.3 Message integrity

7.4 End point authentication

7.5 Securing e-mail

7.6 Securing TCP connections: SSL

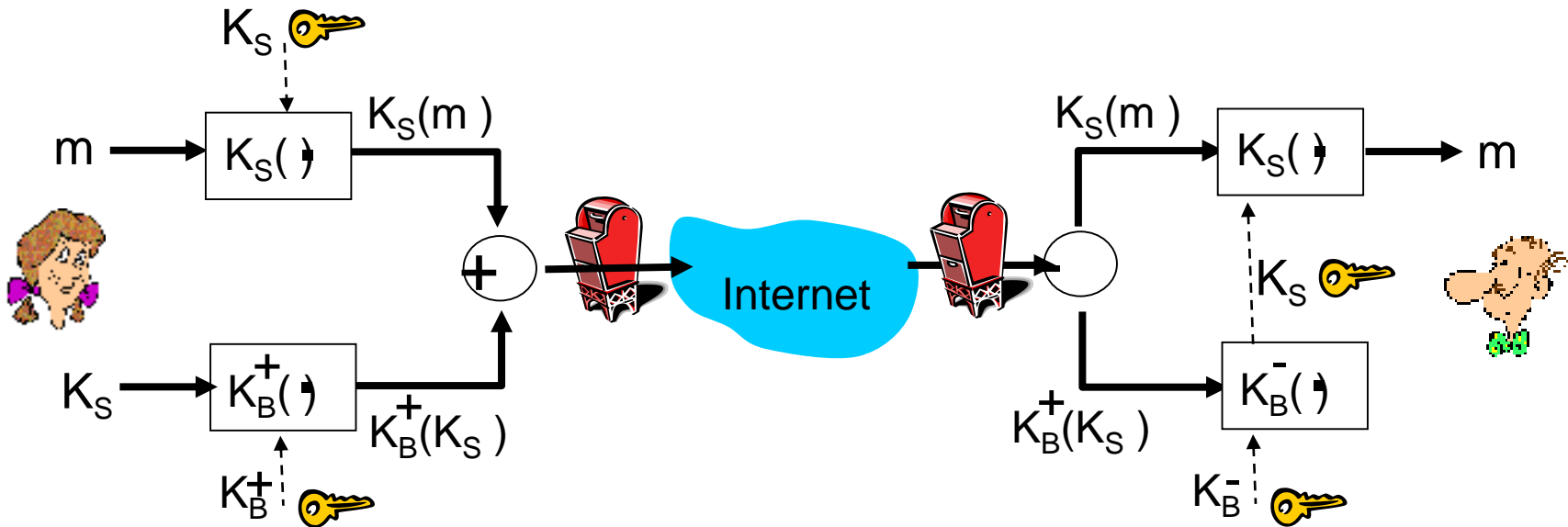
7.7 Network layer security: IPsec

7.8 Securing wireless LANs

7.9 Operational security: firewalls and IDS

# Secure e-mail

- Alice wants to send confidential e-mail,  $m$ , to Bob.

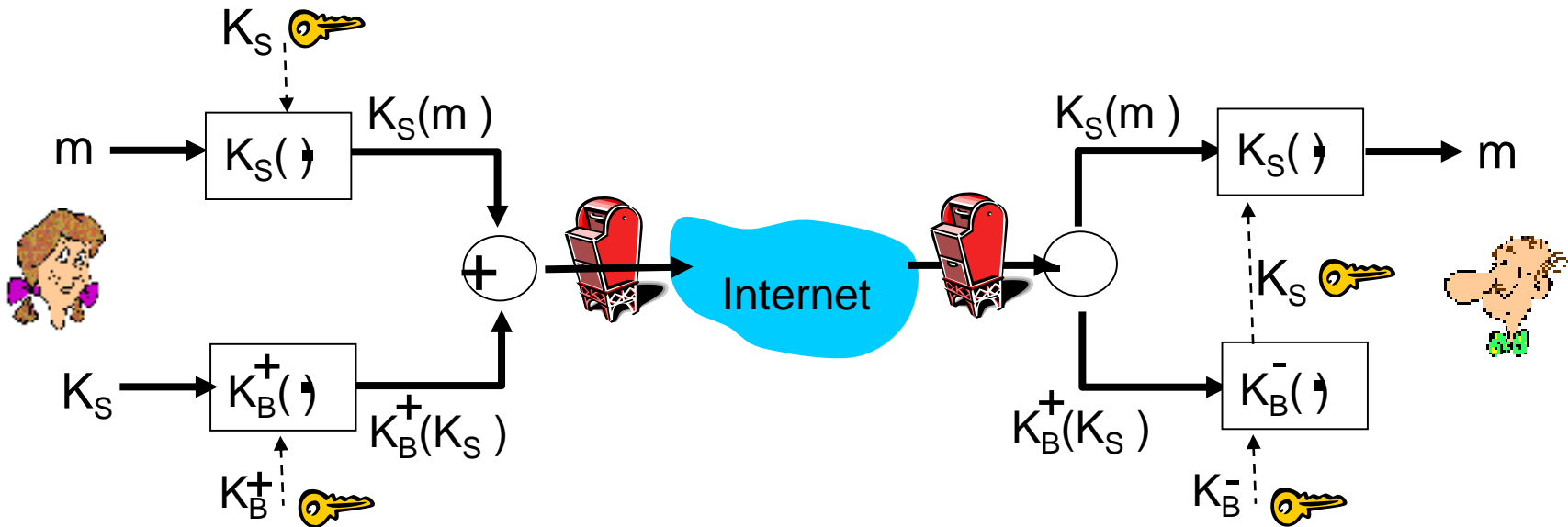


## Alice:

- generates random *symmetric* private key,  $K_S$ .
- encrypts message with  $K_S$  (for efficiency)
- also encrypts  $K_S$  with Bob's public key.
- sends both  $K_S(m)$  and  $K_B^+(K_S)$  to Bob.

# Secure e-mail

- Alice wants to send confidential e-mail,  $m$ , to Bob.

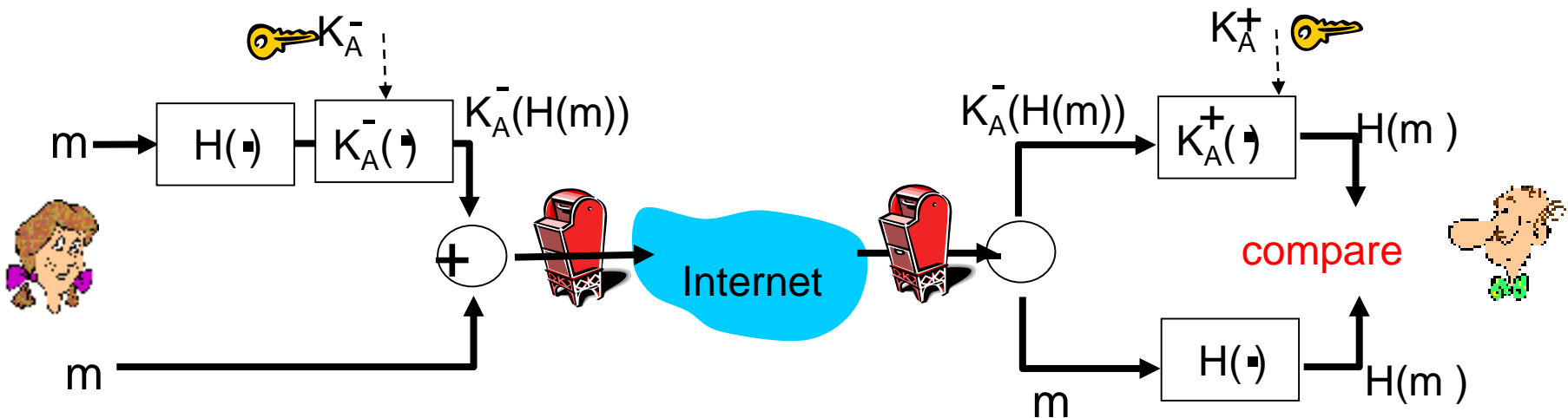


Bob:

- uses his private key to decrypt and recover  $K_S$
- uses  $K_S$  to decrypt  $K_S(m)$  to recover  $m$

# Secure e-mail (continued)

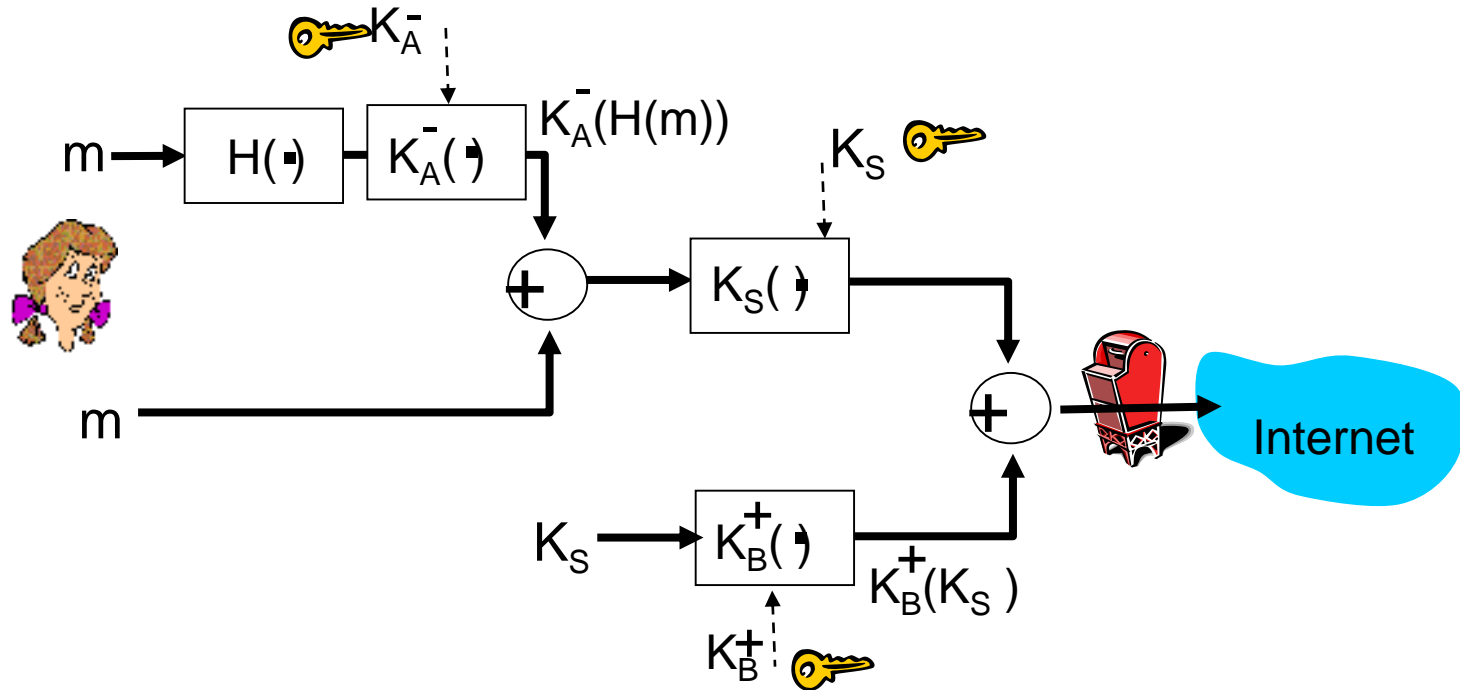
- Alice wants to provide sender authentication message integrity.



- Alice digitally signs message
- sends both message (in the clear) and digital signature.

# Secure e-mail (continued)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

# Pretty good privacy (PGP)

- Internet e-mail encryption scheme, de-facto standard.
- uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- provides secrecy, sender authentication, integrity.
- inventor, Phil Zimmerman, was target of 3-year federal investigation.

## A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob: My husband is out of town
    tonight.Passionately yours,
    Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+l08gE4vB3mqJ
    hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

# Chapter 7 roadmap

7.1 What is network security?

7.2 Principles of cryptography

7.3 Message integrity

7.4 End point authentication

7.5 Securing e-mail

7.6 Securing TCP connections: SSL

7.7 Network layer security: IPsec

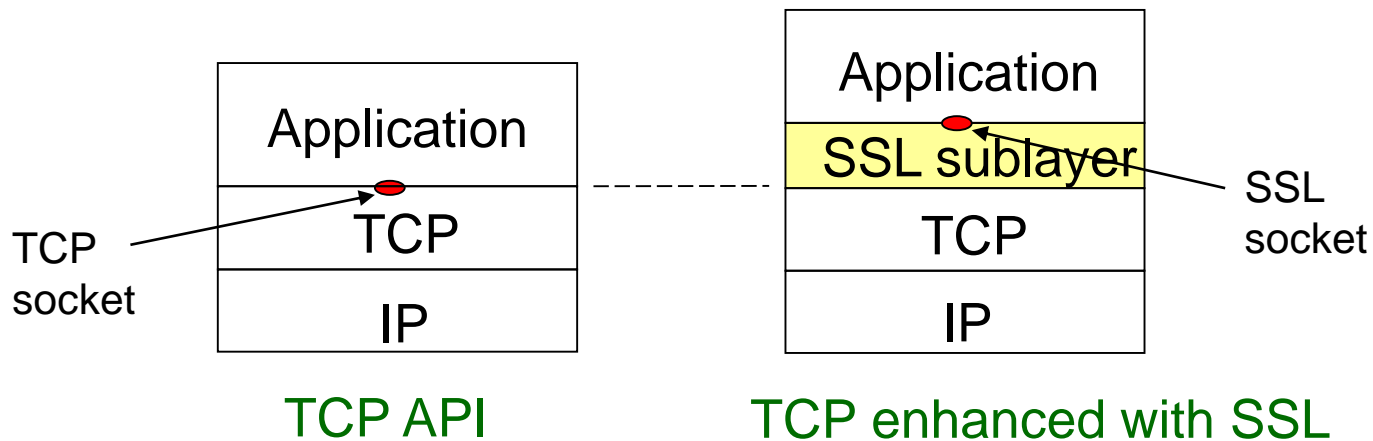
7.8 Securing wireless LANs

7.9 Operational security: firewalls and IDS



# Secure sockets layer (SSL, aka TLS)

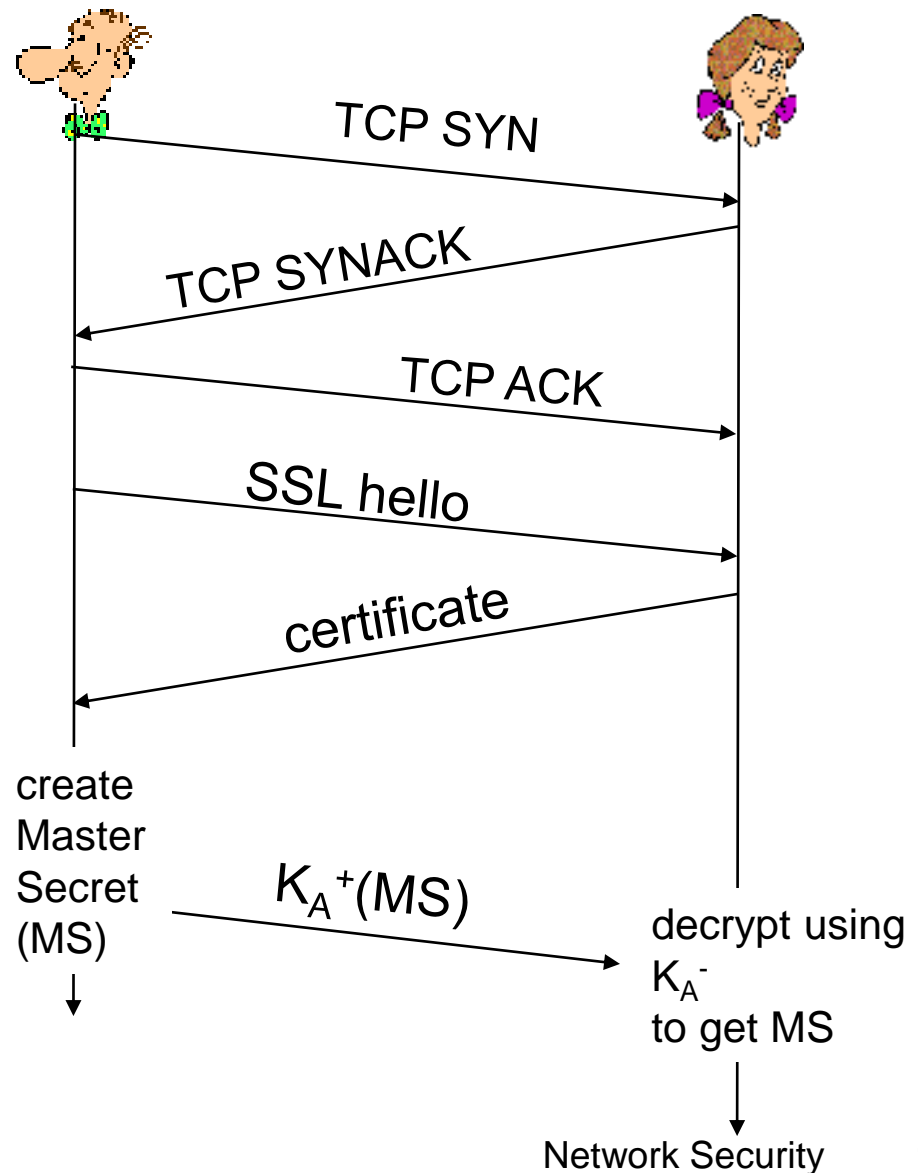
- provides transport layer security to any TCP-based application using SSL services.
  - e.g., between Web browsers, servers for e-commerce (https)
- security services:
  - server authentication, data encryption, client authentication (optional)



# SSL: three phases

## 1. Handshake:

- Bob establishes TCP connection to Alice
- authenticates Alice via CA signed certificate
- creates, encrypts (using Alice's public key), sends master secret key to Alice
  - nonce exchange not shown



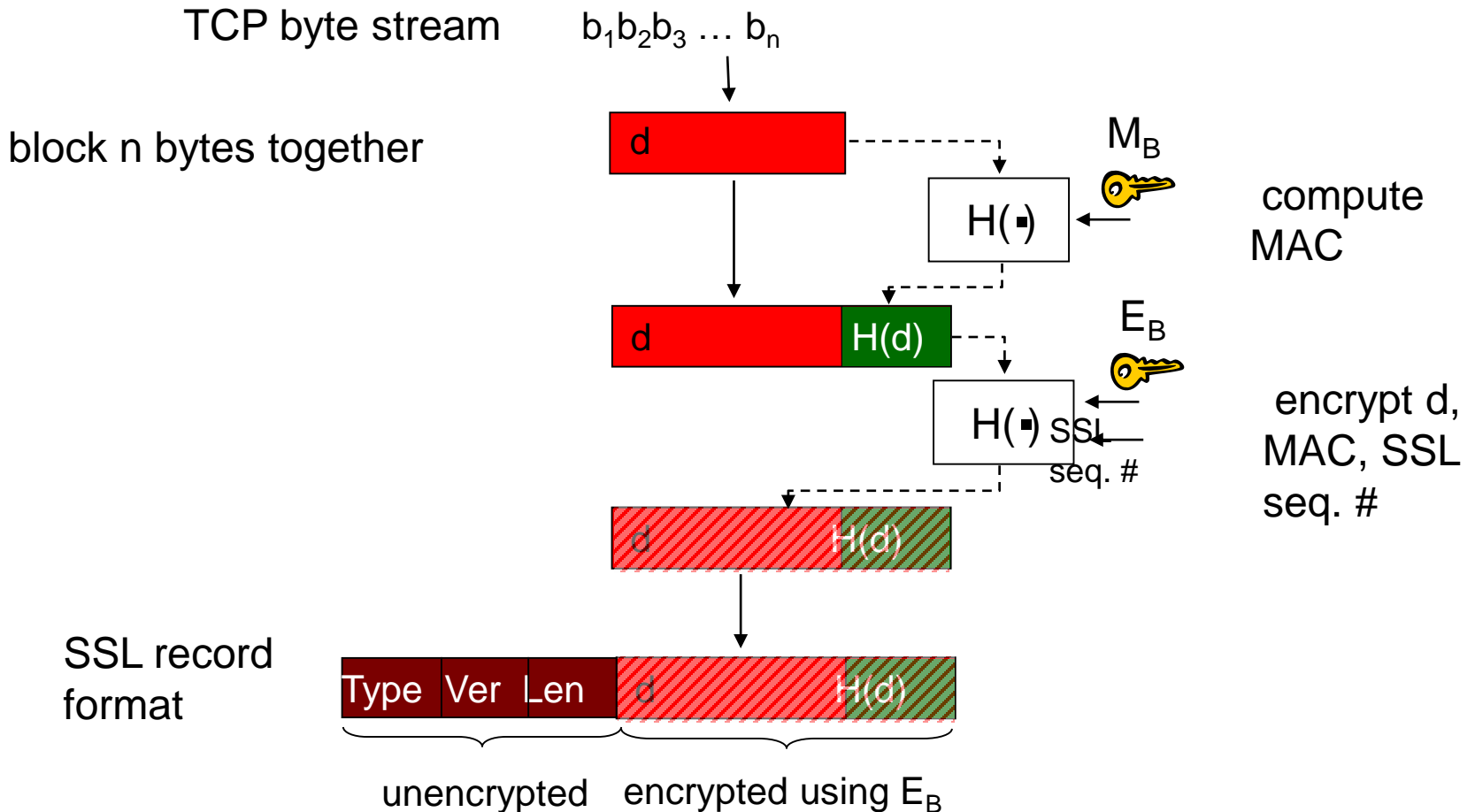
# SSL: three phases

## 2. Key Derivation:

- Alice, Bob use shared secret (MS) to generate 4 keys:
  - $E_B$ : Bob->Alice data encryption key
  - $E_A$ : Alice->Bob data encryption key
  - $M_B$ : Bob->Alice MAC key
  - $M_A$ : Alice->Bob MAC key
- encryption and MAC algorithms negotiable between Bob, Alice
- why 4 keys?

# SSL: three phases

## 3. Data transfer



# Chapter 7 roadmap

- 7.1 What is network security?
- 7.2 Principles of cryptography
- 7.3 Message integrity
- 7.4 End point authentication
- 7.5 Securing e-mail
- 7.6 Securing TCP connections: SSL
- 7.7 Network layer security: IPsec
- 7.8 Securing wireless LANs
- 7.9 Operational security: firewalls and IDS

# IPsec: Network Layer Security

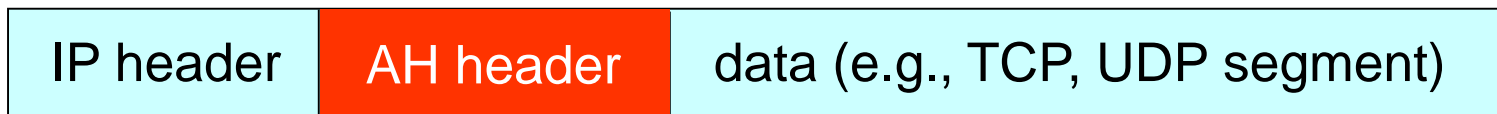
- network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages.
- network-layer authentication
  - destination host can authenticate source IP address
- two principal protocols:
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol
- for both AH and ESP, source, destination handshake:
  - create network-layer logical channel called a security association (SA)
- each SA unidirectional.
- uniquely determined by:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID

# Authentication Header (AH) Protocol

- provides source authentication, data integrity, no confidentiality
- AH header inserted between IP header, data field.
- protocol field: 51
- intermediate routers process datagrams as usual

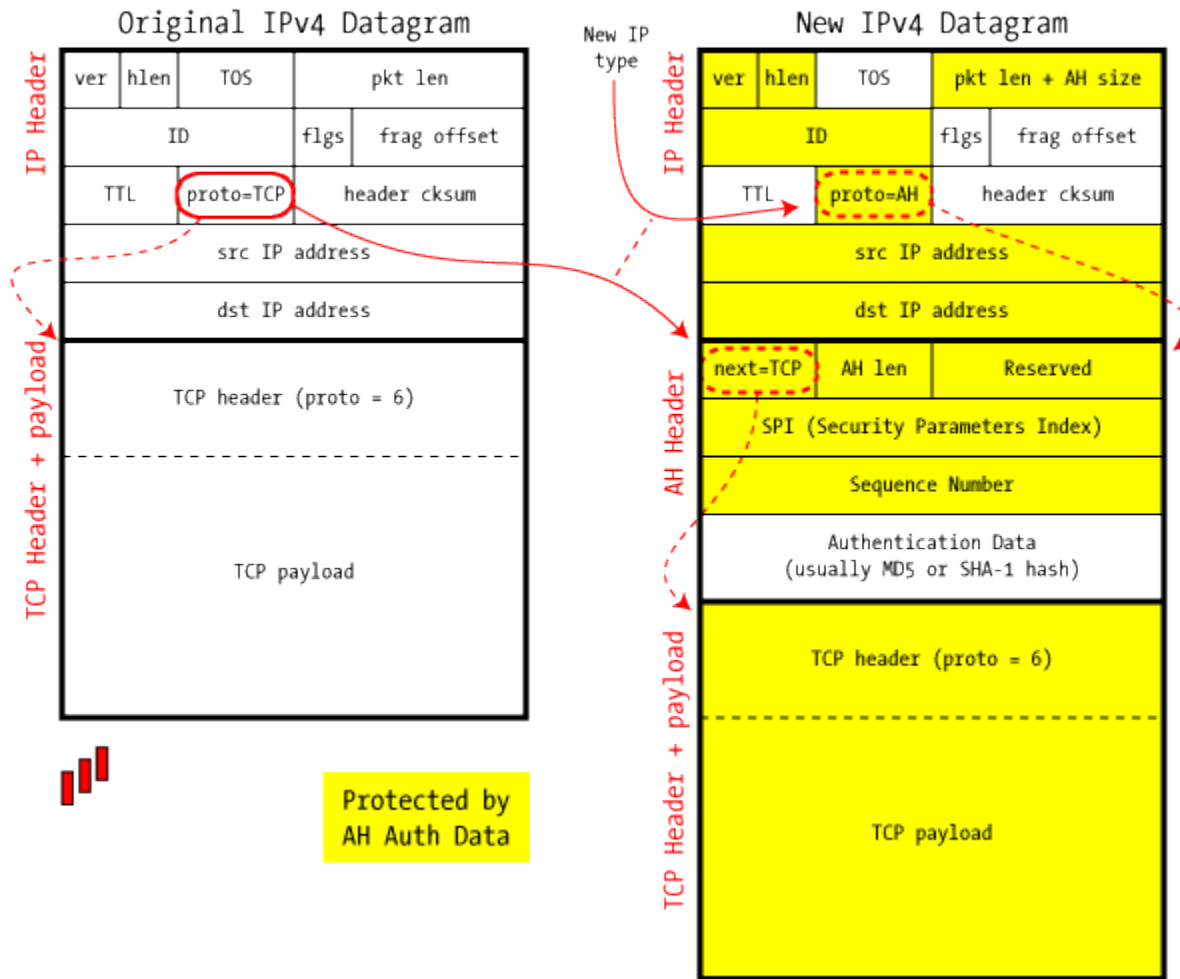
## AH header includes:

- connection identifier
- authentication data: source-signed message digest calculated over original IP datagram.
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)



# Authentication Header (AH) Protocol

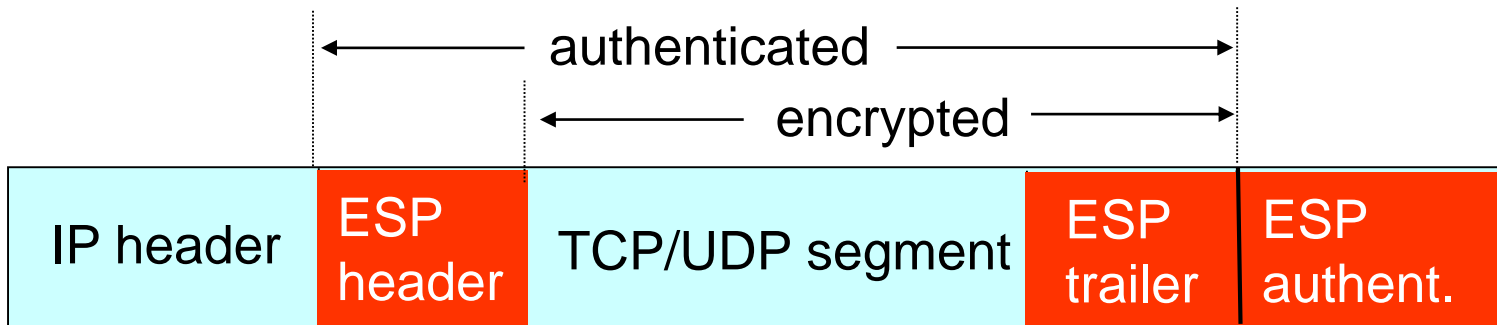
## IPSec in AH Transport Mode





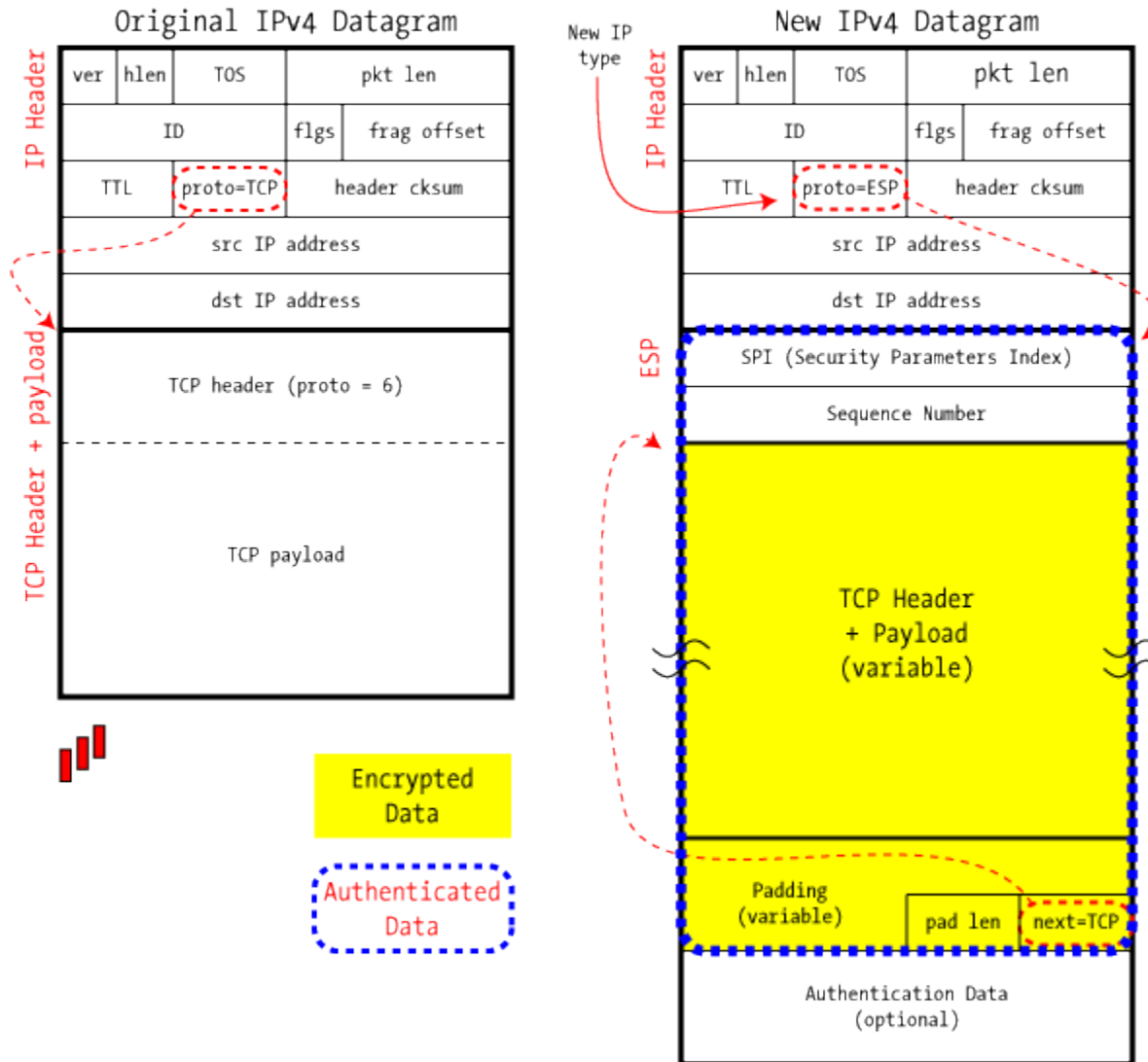
# ESP Protocol

- provides secrecy, host authentication, data integrity.
- data, ESP trailer encrypted.
- next header field is in ESP trailer.
- ESP authentication field is similar to AH authentication field.
- Protocol = 50.



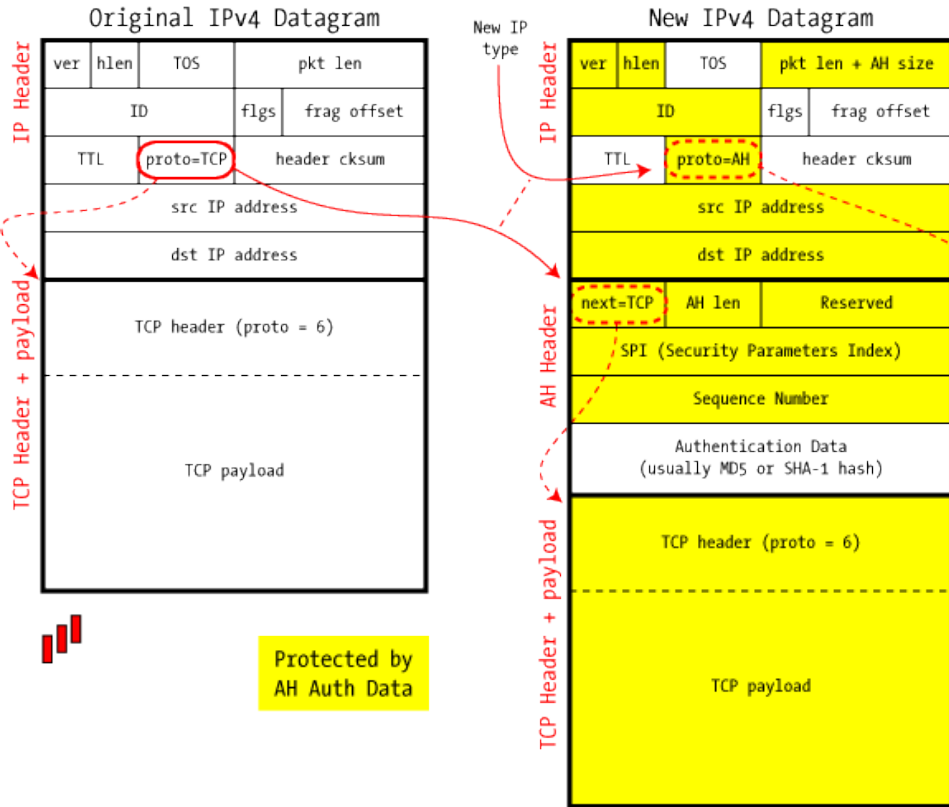
# ESP Protocol

## IPSec in ESP Transport Mode

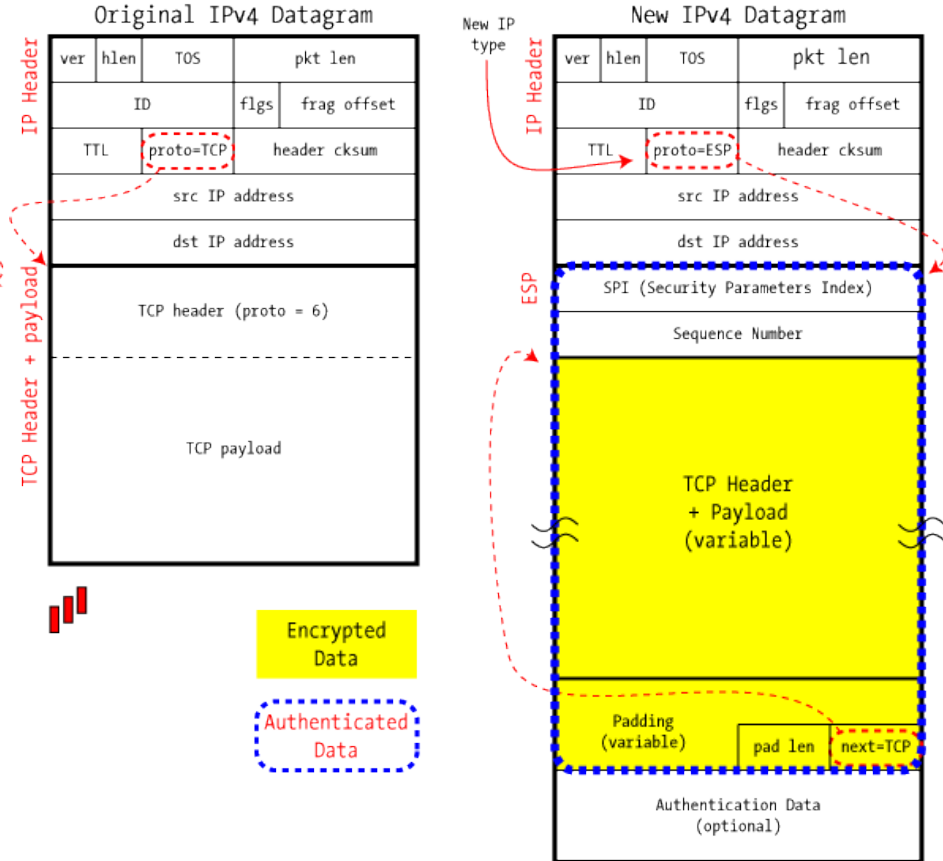


# NAT Traversal: AH vs ESP?

IPSec in AH Transport Mode



IPSec in ESP Transport Mode



# Chapter 7 roadmap

7.1 What is network security?

7.2 Principles of cryptography

7.3 Message integrity

7.4 End point authentication

7.5 Securing e-mail

7.6 Securing TCP connections: SSL

7.7 Network layer security: IPsec

7.8 Securing wireless LANs

7.9 Operational security: firewalls and IDS

# IEEE 802.11 security

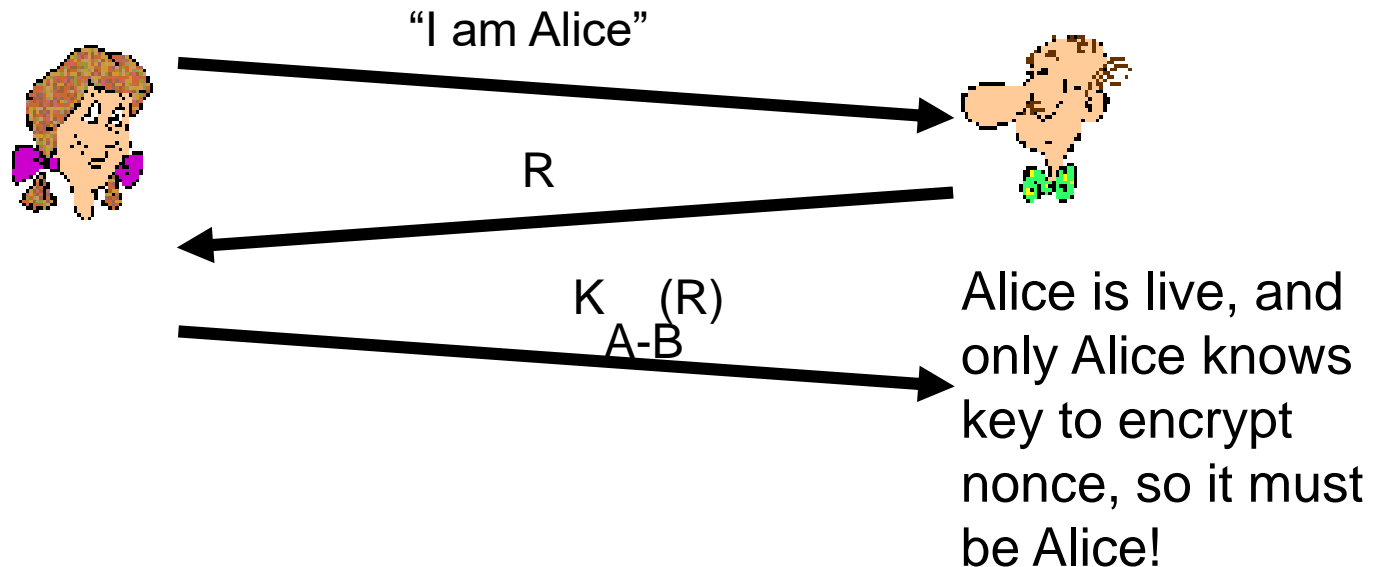
- **war-driving:** drive around Bay area, see what 802.11 networks available?
  - More than 9000 accessible from public roadways
  - 85% use no encryption/authentication
  - packet-sniffing and various attacks easy!
- **securing 802.11:**
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - current attempt: 802.11i (aka WPA/WPA2)

# Authentication: Recap

Goal: avoid playback attack

Nonce: number (R) used only *once* –*in-a-lifetime*

ap4.0: to prove Alice “live”, Bob sends Alice a nonce, R. Alice must return R, encrypted with shared secret key



# Wired Equivalent Privacy (WEP):

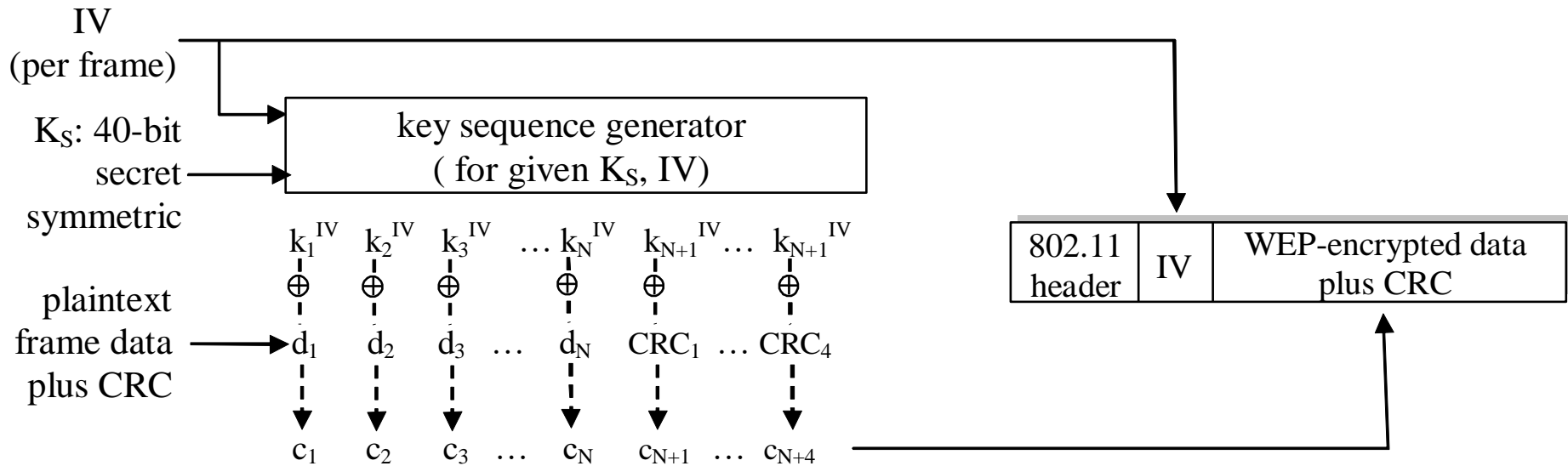
- authentication as in protocol *ap4.0*
  - host requests authentication from access point
  - access point sends 128 bit nonce
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- no key distribution mechanism
- authentication: knowing the shared key is enough

# WEP data encryption

- host/AP share 40 bit symmetric key (semi-permanent)
- host appends 24-bit initialization vector (IV) to create 64-bit key
- 64 bit key used to generate stream of keys,  $k_i^{IV}$
- $k_i^{IV}$  used to encrypt i-th byte,  $d_i$ , in frame:  
$$c_i = d_i \text{ XOR } k_i^{IV}$$
- IV and encrypted bytes,  $c_i$  sent in frame



# 802.11 WEP encryption



Sender-side WEP encryption

# Breaking 802.11 WEP encryption

## security hole:

- 24-bit IV, one IV per frame, -> IV's eventually reused
- IV transmitted in plaintext -> IV reuse detected
- **attack:**
  - Trudy causes Alice to encrypt known plaintext  $d_1 d_2 d_3 d_4 \dots$
  - Trudy sees:  $c_i = d_i \text{ XOR } k_i^{\text{IV}}$
  - Trudy knows  $c_i d_i$ , so can compute  $k_i^{\text{IV}}$
  - Trudy knows encrypting key sequence  $k_1^{\text{IV}} k_2^{\text{IV}} k_3^{\text{IV}} \dots$
  - Next time IV is used, Trudy can decrypt!

# Breaking 802.11 WEP encryption

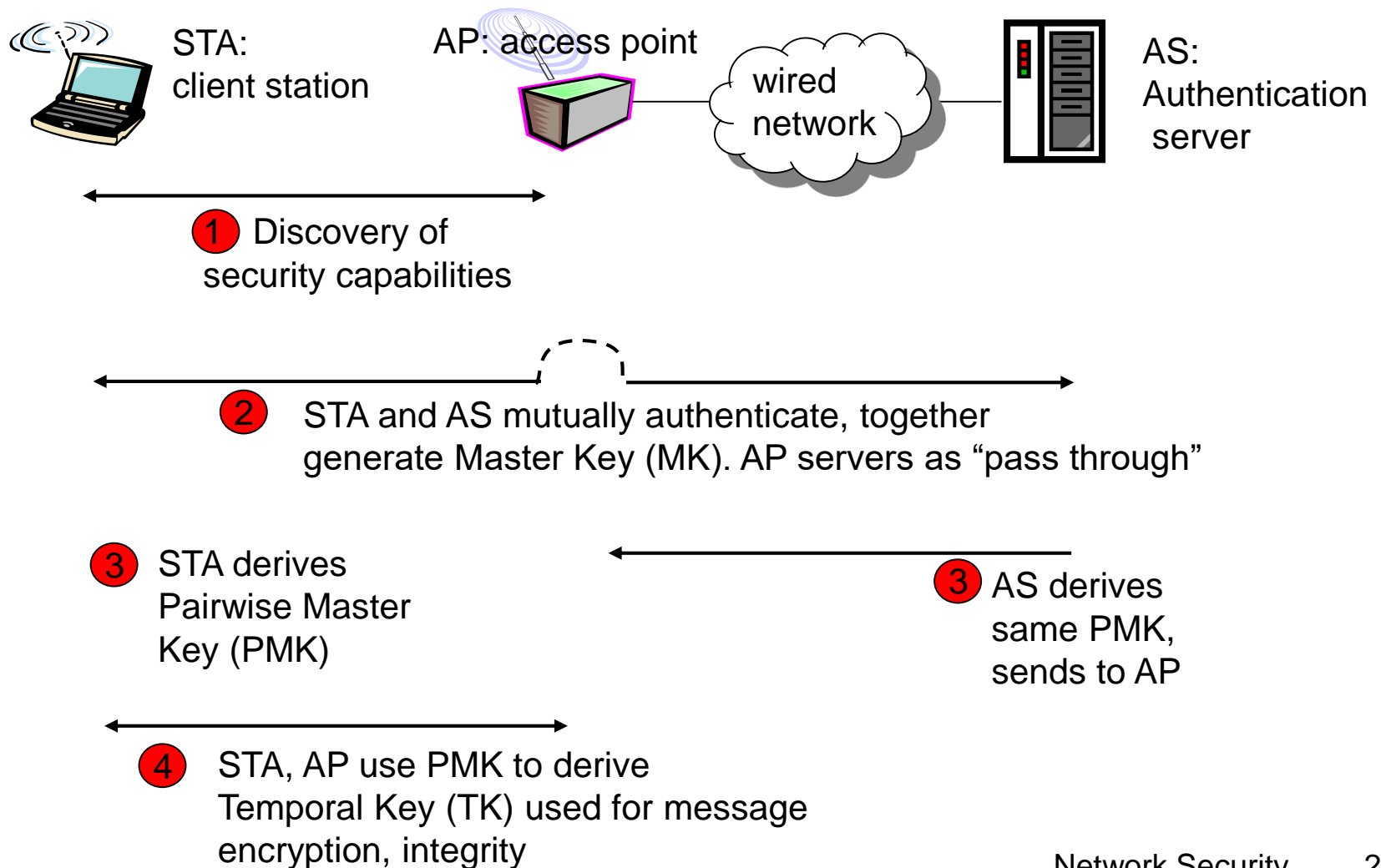
## Sample calculation:

- Probability to have a repeating IV: 99% after 12000 frames
- If frame size = 1KB, transfer rate = 11 Mbps: few seconds until repeat
  
- Many other issues (e.g., CRC unsuited as hash function)

# 802.11i (aka WPA): improved security

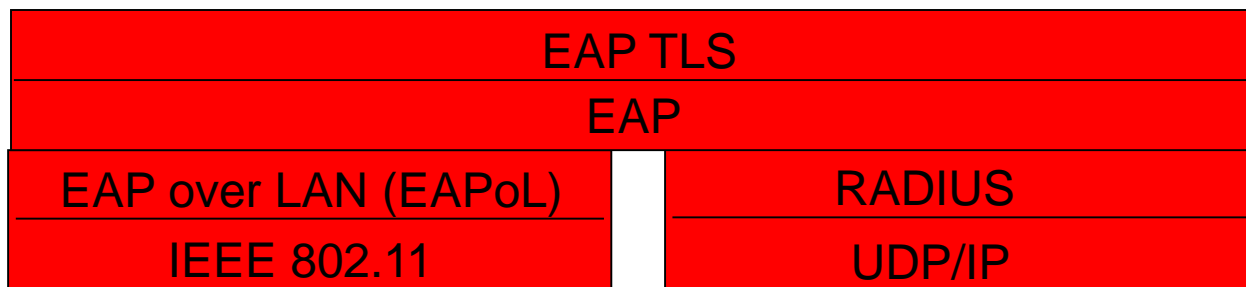
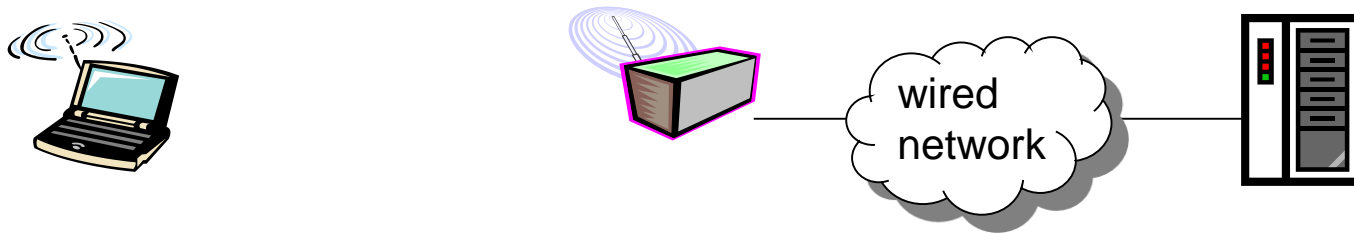
- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

# 802.11i: four phases of operation



# EAP: extensible authentication protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate “links”
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)



# EAP or Pre-Shared-Key (PSK)?

- EAP should be used for larger networks
  - Multiple access points, many devices
  - Auth server can reduce load on access points
- In home networks: PSK usage
  - Security depends on chosen PSK

# WPA or WPA2 – difference?

- WPA2 uses block cipher (AES) instead of stream cipher (RC4)
- Both are relatively safe
  - WPA: brute-force attacks on PSK shown in 2009
  - WPA 2 is recommended



# Chapter 7 roadmap

7.1 What is network security?

7.2 Principles of cryptography

7.3 Message integrity

7.4 End point authentication

7.5 Securing e-mail

7.6 Securing TCP connections: SSL

7.7 Network layer security: IPsec

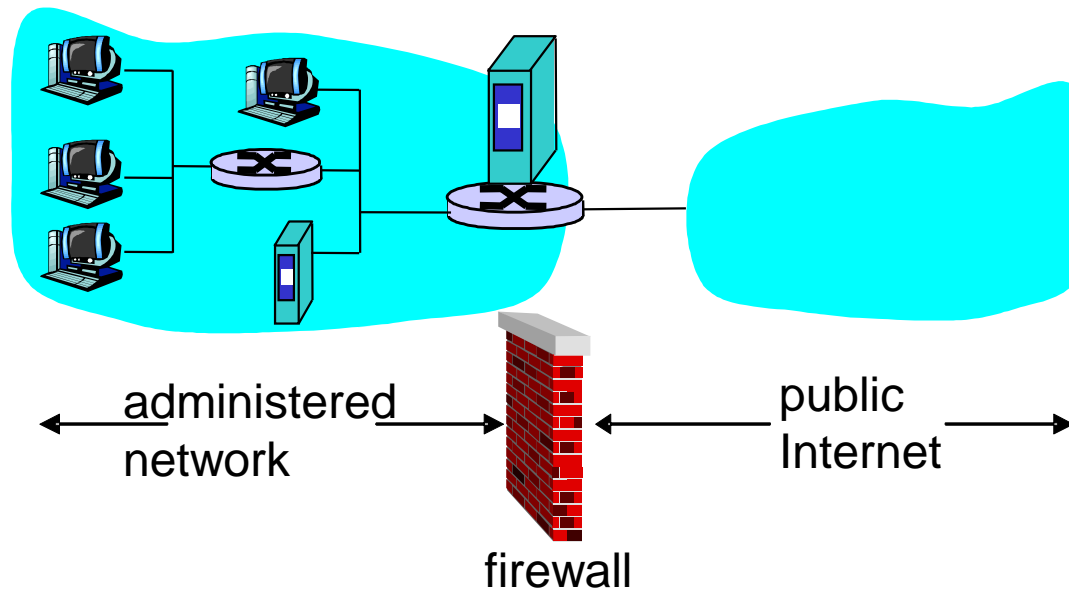
7.8 Securing wireless LANs

7.9 Operational security: firewalls and IDS

# Firewalls

## firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



# Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data.

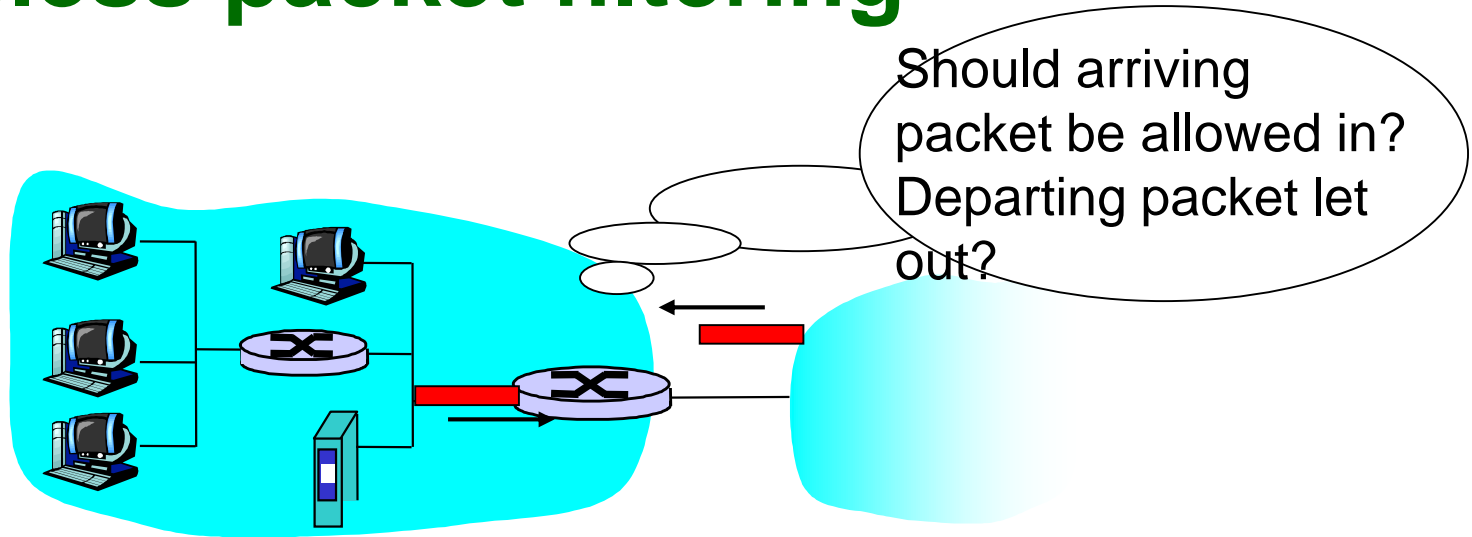
- e.g., attacker replaces CIA’s homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

# Stateless packet filtering



- internal network connected to Internet **via router firewall**
- router **filters packet-by-packet**, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

# Stateless packet filtering: example

- example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - all incoming, outgoing UDP flows and telnet connections are blocked.
- example 2: Block inbound TCP segments with ACK=0.
  - prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

# Stateless packet filtering: more examples

<u>Policy</u>	<u>Firewall Setting</u>
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

# Access Control Lists

**ACL:** table of rules, applied top to bottom to incoming packets: (action, condition) pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

# Stateful packet filtering

- stateless packet filter: heavy handed tool
  - admits packets that “make no sense,” e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter*: track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets “makes sense”
  - timeout inactive connections at firewall: no longer admit packets



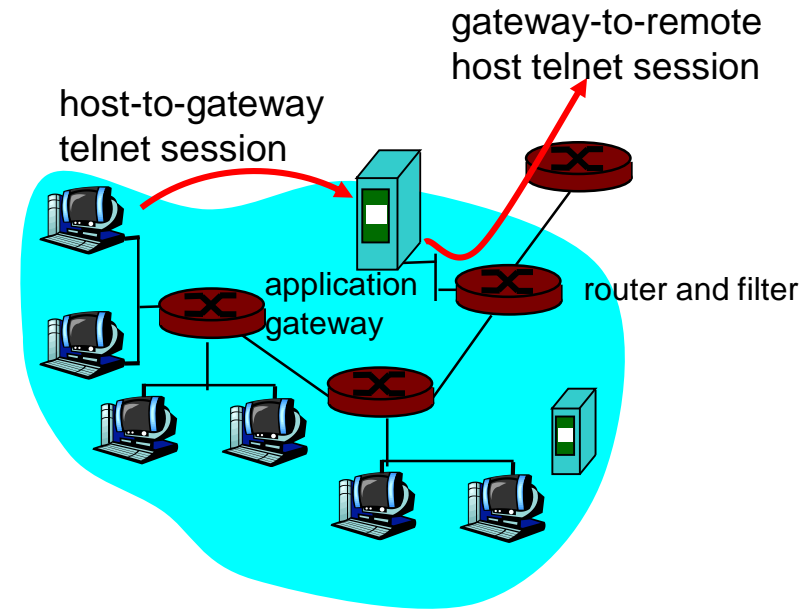
# Stateful packet filtering

ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

# Application gateways

- filters packets on application data as well as on IP/TCP/UDP fields.
- **example:** allow selected internal users to telnet outside.



1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

# Limitations of firewalls and gateways

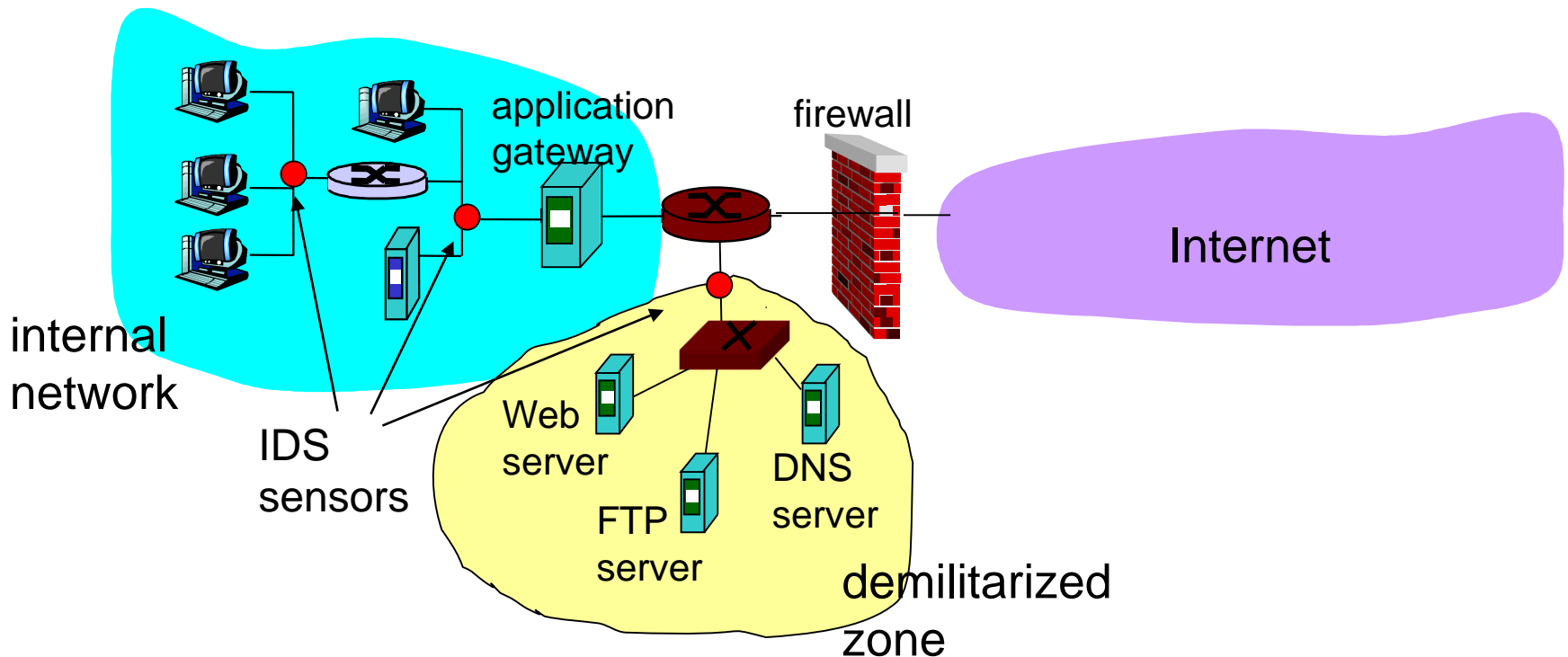
- **IP spoofing:** router can't know if data “really” comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: **degree of communication with outside world, level of security**
- many highly protected sites still suffer from attacks.

# Intrusion detection systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- **IDS: intrusion detection system**
  - *deep packet inspection*: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - **examine correlation** among multiple packets
    - port scanning
    - network mapping
    - DoS attack

# Intrusion detection systems

- multiple IDSs: different types of checking at different locations



# Network Security (summary)

## Basic techniques.....

- cryptography (symmetric and public)
- message integrity
- end-point authentication

## .... used in many different security scenarios

- secure email
- secure transport (SSL)
- IP sec
- 802.11

## Operational Security: firewalls and IDS

# Additional Evaluation Questions

“Frage 1”: The exercises help me learning to solve problems and think critically.

“Frage 2”: During the exercises, the teacher encourages students to speak up and be active in the class.

“Frage 3”: During the exercise, the teacher listens and understands students’ point of view; he may not agree, but students feel understood.