Last time

- Message Integrity
- Authentication
- Key distribution and certification

This time

- Firewalls
- Attacks and countermeasures
- Security in many layers

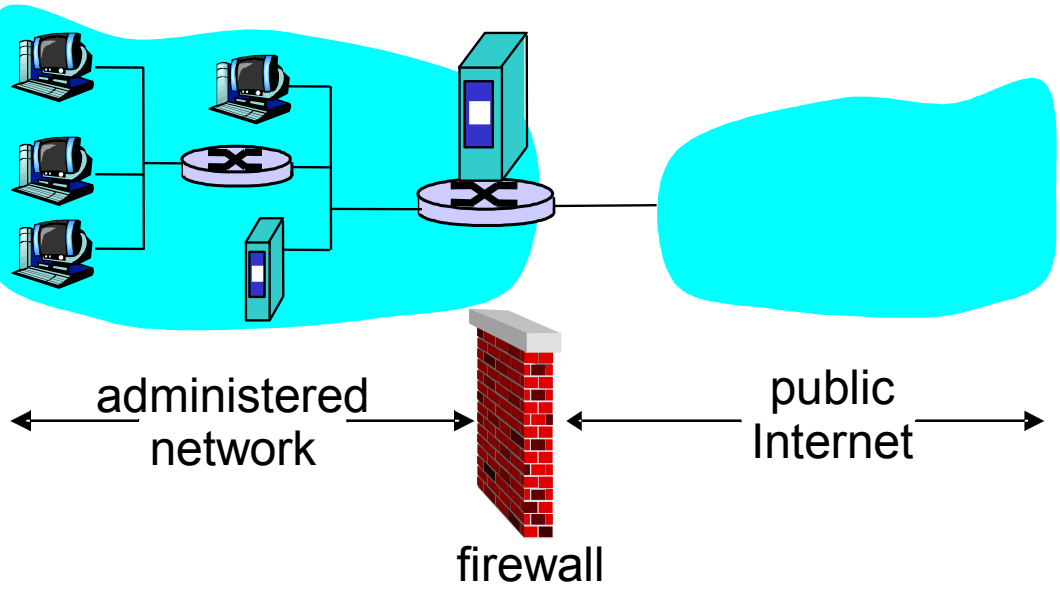
Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Authentication
8.4 Integrity
8.5 Key Distribution and certification
8.6 Access control: firewalls
8.7 Attacks and counter measures
8.8 Security in many layers

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.

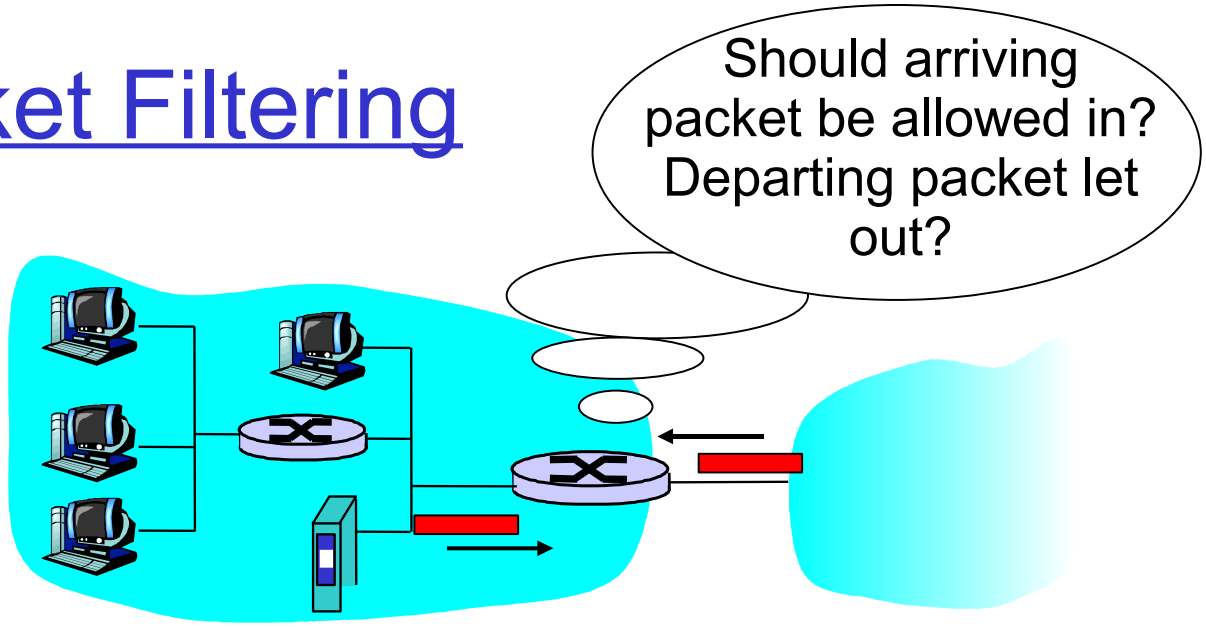
- e.g., attacker replaces CIA’s homepage with something else

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

Two types of firewalls:

- application-level
- packet-filtering

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

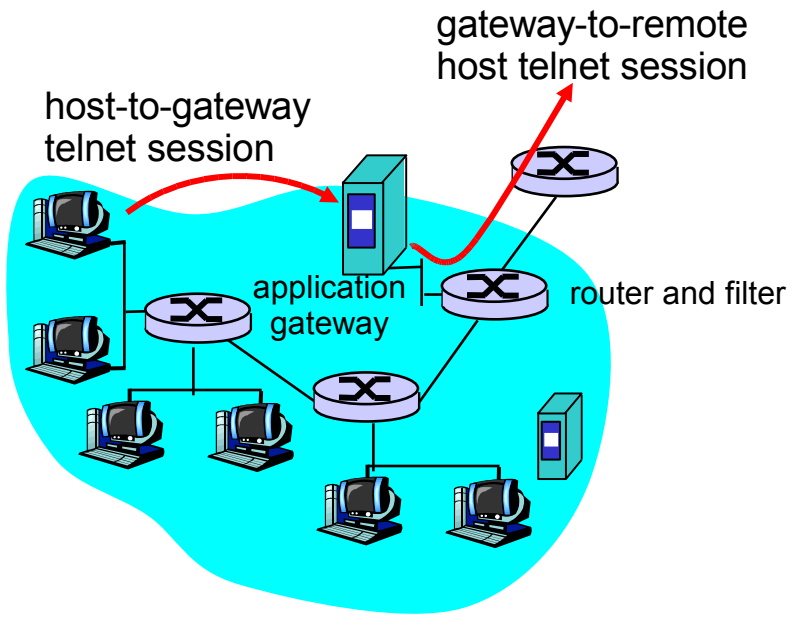
Packet Filtering

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 or with either source or dest port = 23.
  - All incoming and outgoing UDP flows, as well as 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.

Application gateways

- Filters packets on application data as well as on IP/TCP/UDP fields.
- Example: allow select 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 applications 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.

Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Authentication
8.4 Integrity
8.5 Key Distribution and certification
8.6 Access control: firewalls
8.7 Attacks and counter measures
8.8 Security in many layers

Internet security threats

Mapping:

- before attacking: “case the joint” – find out what services are implemented on network
- Use `ping` to determine what hosts have addresses on network
- Port-scanning: try to establish TCP connection to each port in sequence (see what happens)
- nmap (http://www.insecure.org/nmap/) mapper: “network exploration and security auditing”

Countermeasures?

Internet security threats

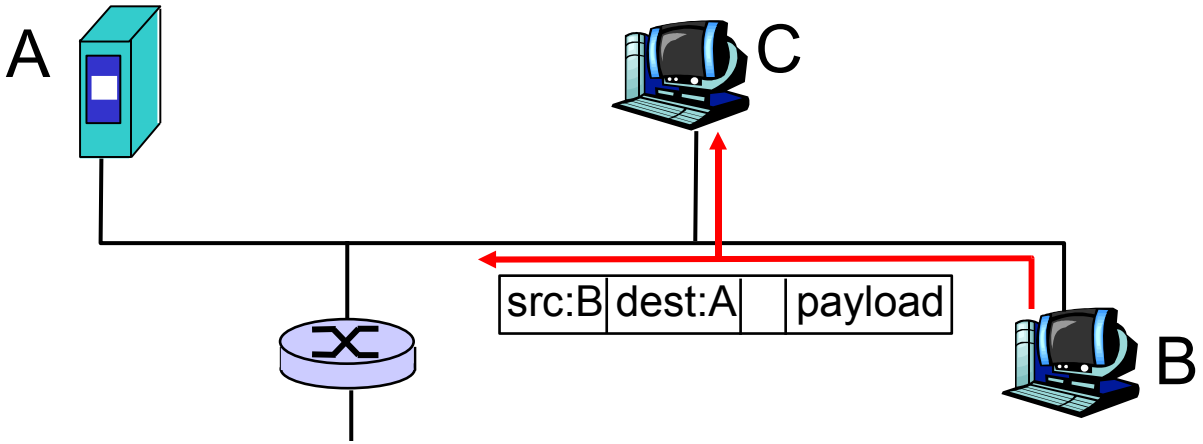
Mapping: countermeasures

- record traffic entering network
- look for suspicious activity (IP addresses, ports being scanned sequentially)

Internet security threats

Packet sniffing:

- broadcast media
- promiscuous NIC reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B's packets

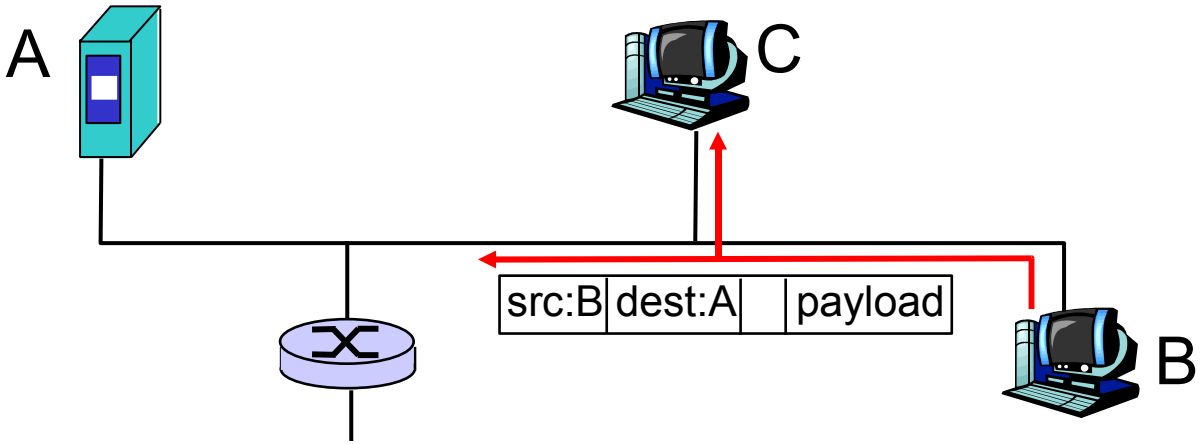


Countermeasures?

Internet security threats

Packet sniffing: countermeasures

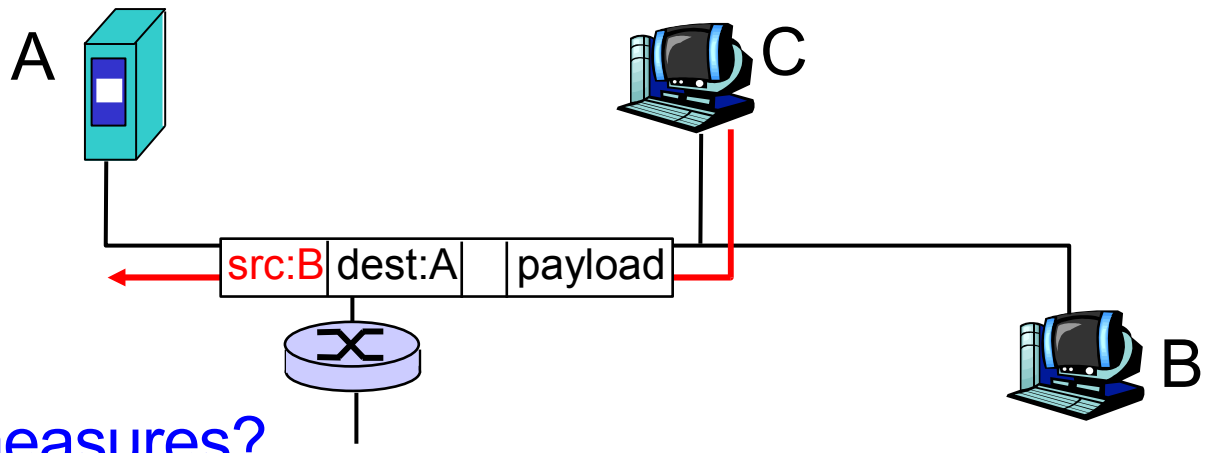
- all hosts in organization run software that checks periodically if host interface in promiscuous mode (or try to remotely detect this)
- one host per segment of broadcast media (switched Ethernet at hub)



Internet security threats

IP Spoofing:

- can generate “raw” IP packets directly from application, putting any value into IP source address field
- receiver can’t tell if source is spoofed
- e.g.: C pretends to be B

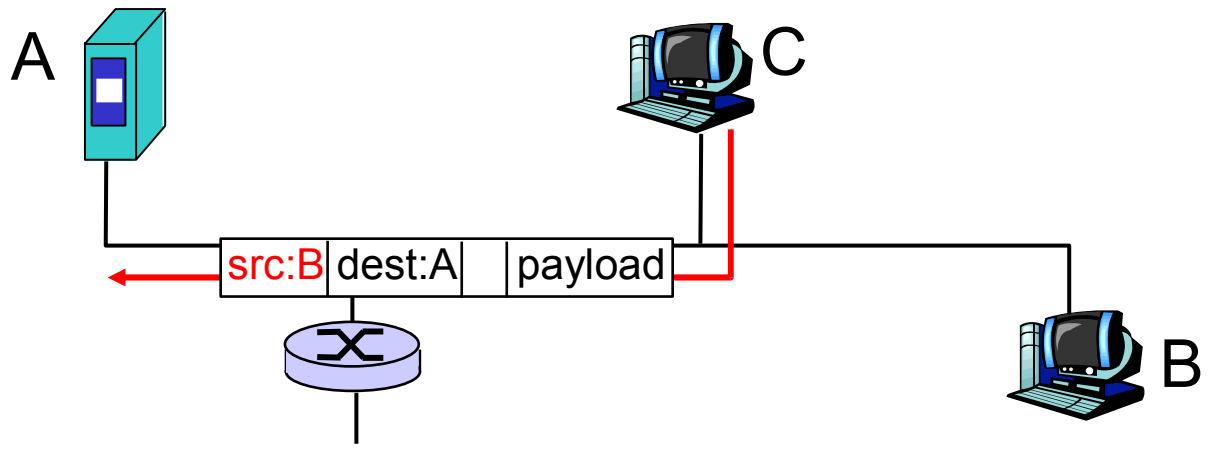


Countermeasures?

Internet security threats

IP Spoofing: ingress filtering

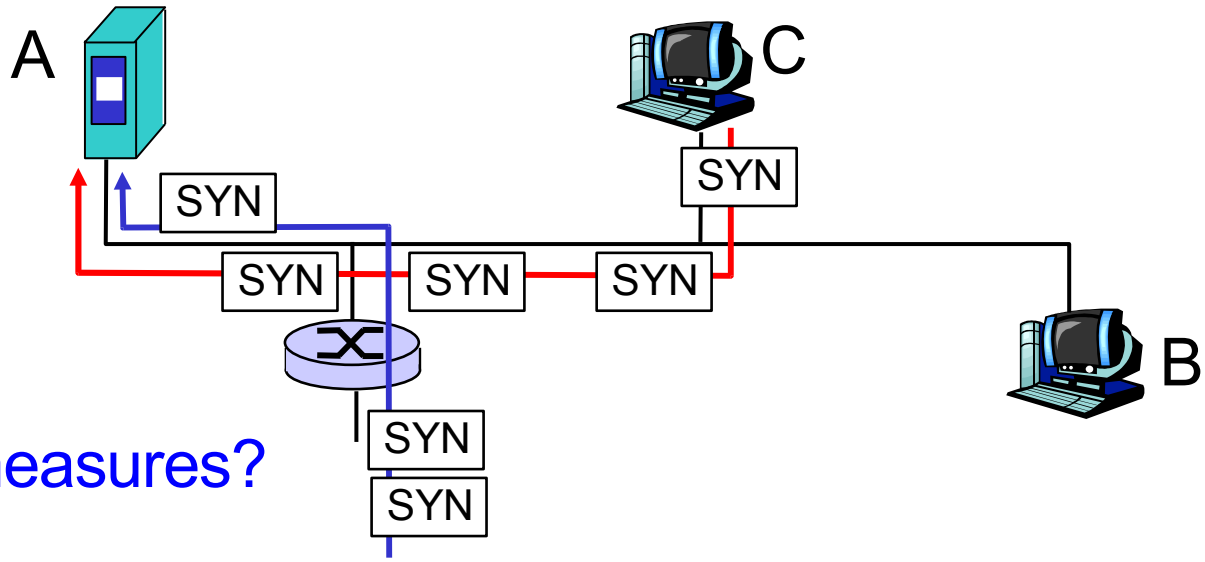
- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router's network)
- great, but ingress filtering can not be mandated for all networks



Internet security threats

Denial of service (DoS):

- flood of maliciously generated packets “swamp” receiver
- Distributed DOS (DDoS): multiple coordinated sources swamp receiver
- e.g., C and remote host SYN-attack A

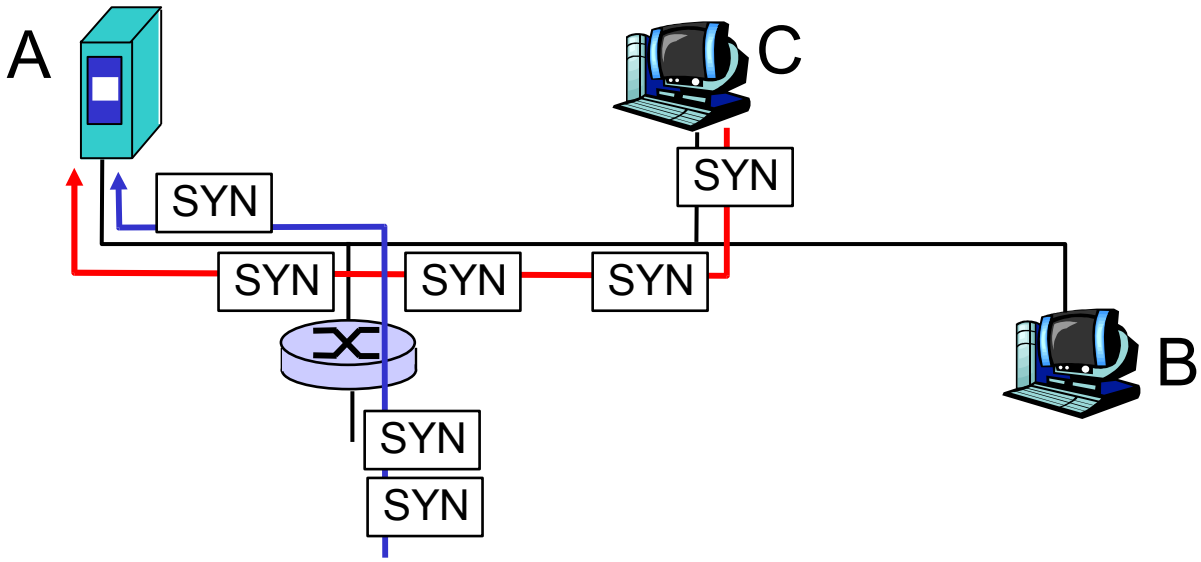


Countermeasures?

Internet security threats

Denial of service (DoS): countermeasures

- filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad
- traceback to source of floods (most likely an innocent, compromised machine)

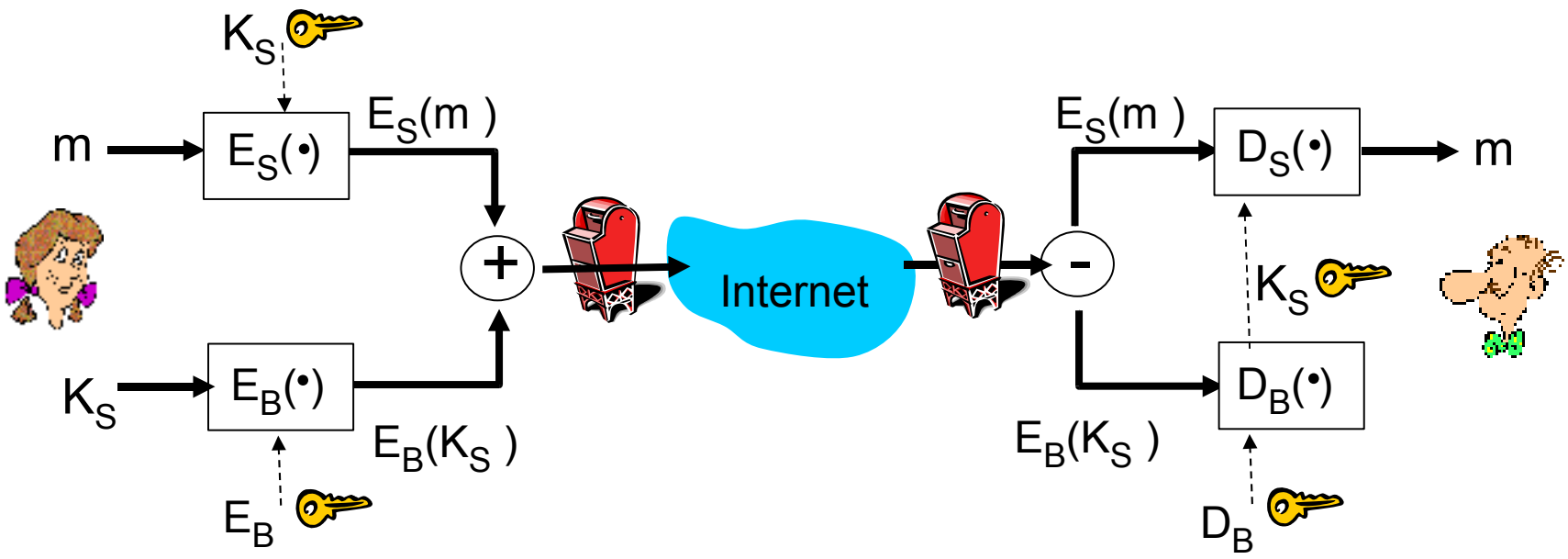


Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Authentication
8.4 Integrity
8.5 Key Distribution and certification
8.6 Access control: firewalls
8.7 Attacks and counter measures
8.8 Security in many layers
- 8.8.1. Secure email
- 8.8.2. Secure sockets
- 8.8.3. IPsec
- 8.8.4. Security in 802.11
- Bonus: Secure Instant Messaging

Secure e-mail

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

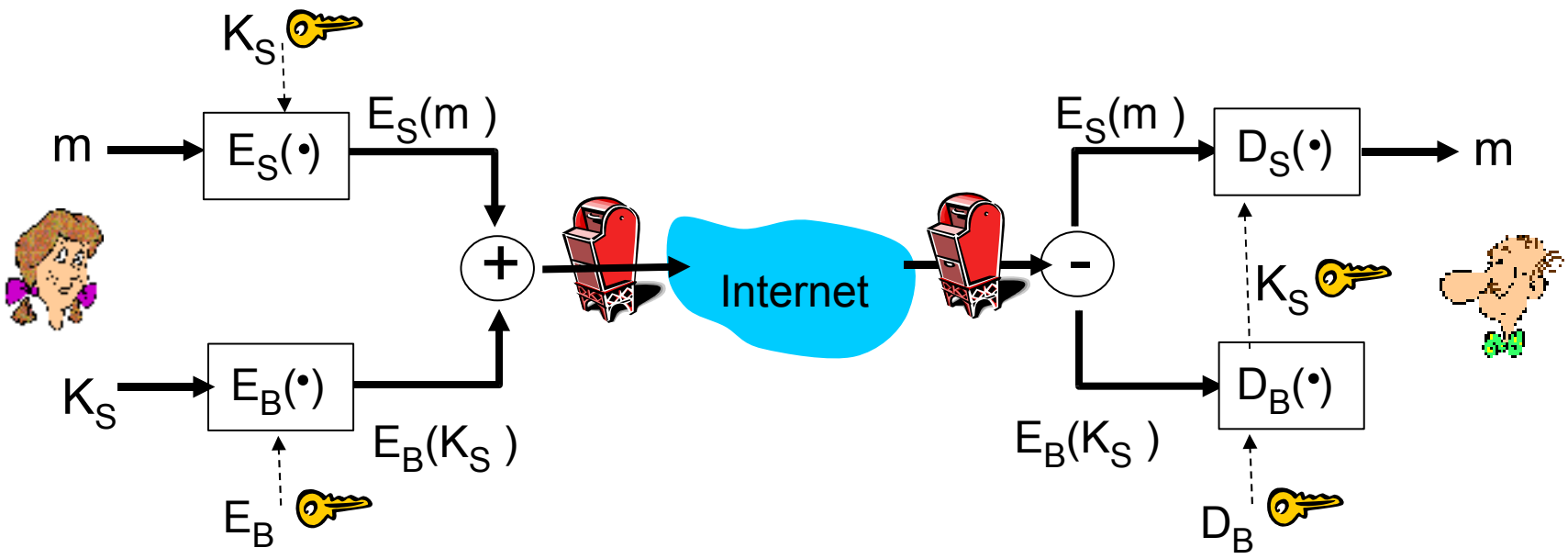


Alice:

- Generates random *symmetric* private key, K_S.
- Encrypts message with K_S (for efficiency and size reasons)
- Also encrypts K_S with Bob's public key.
- Sends both $E_S(m)$ and $E_B(K_S)$ to Bob.

Secure e-mail

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

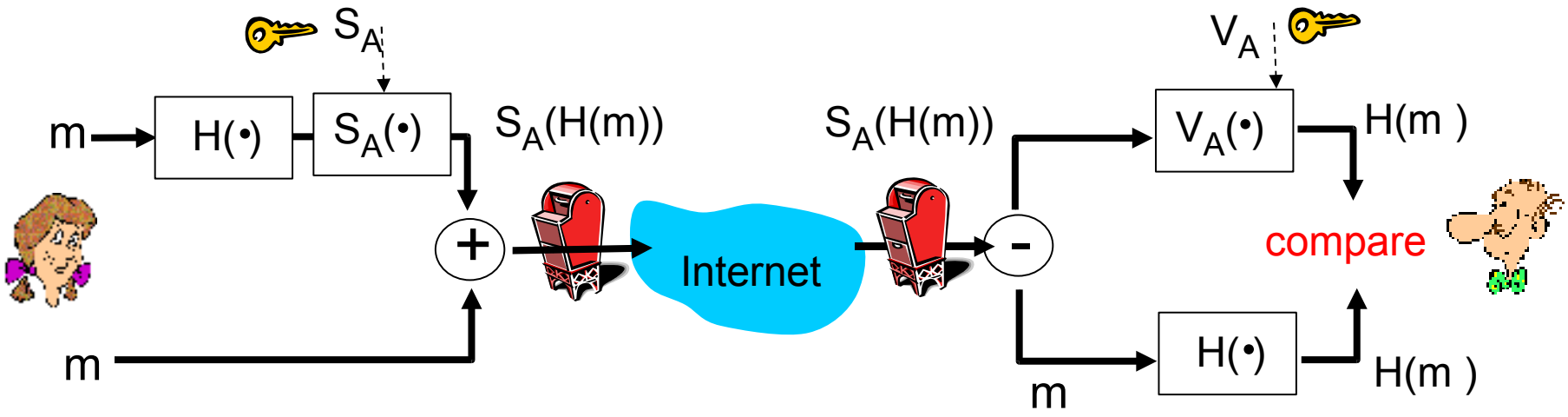


Bob:

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

Secure e-mail (continued)

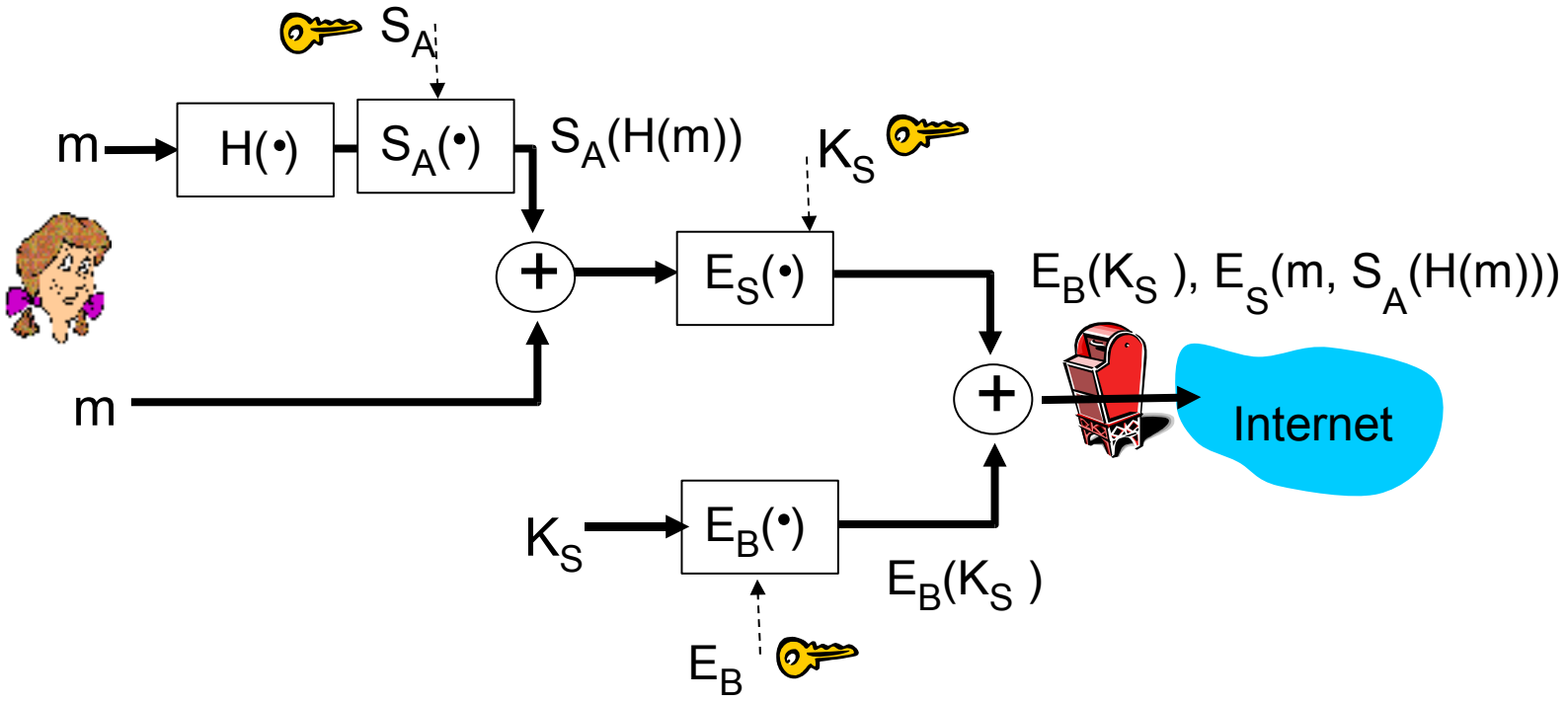
- Alice wants to provide sender authentication and message integrity.



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

Secure e-mail (continued)

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



Alice uses three keys: her private signing key, Bob's public encryption 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+lo8gE4vB3mqJh
   FEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Secure sockets layer (SSL)

- Transport layer security to any TCP-based app using SSL services.
- Used between Web browsers, servers for e-commerce (https).
- Security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- Server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Server presents a certificate signed by a CA.
  - Browser uses CA's public key to verify server's public key.
- Check your browser's security menu to see its trusted CAs.

SSL (continued)

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
  - All data sent into TCP socket (by client or server) encrypted with session key.

- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

IPsec: Network Layer Security

- Network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments, ICMP messages, etc.
- 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

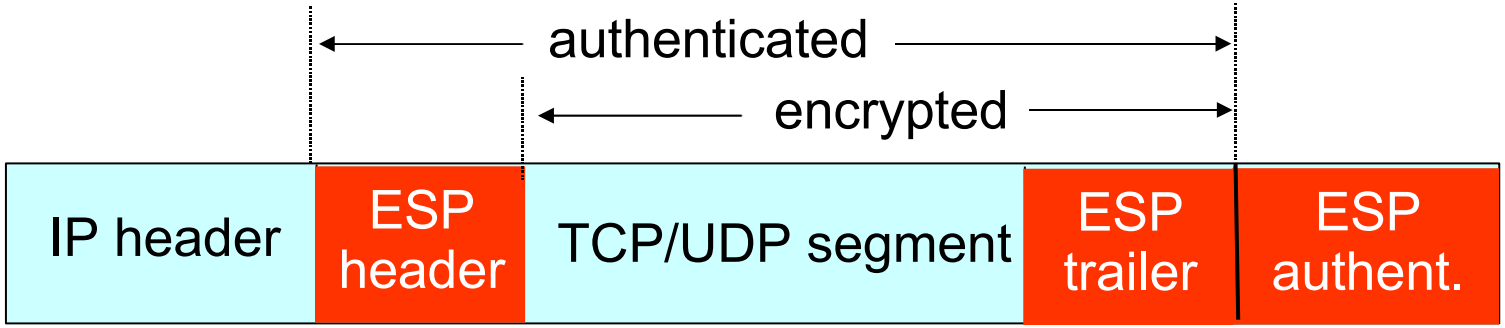
- Provides source authentication, data integrity, no confidentiality
- AH header inserted between IP header, data field.
- IP header protocol field: 51
- Intermediate routers process datagrams as usual

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)

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.



Recap

- Firewalls
- Attacks and countermeasures
- Security in many layers
  - PGP
  - SSL
  - IPSec

Next time

- Security in many layers
  - WEP
  - OTR
- Final review