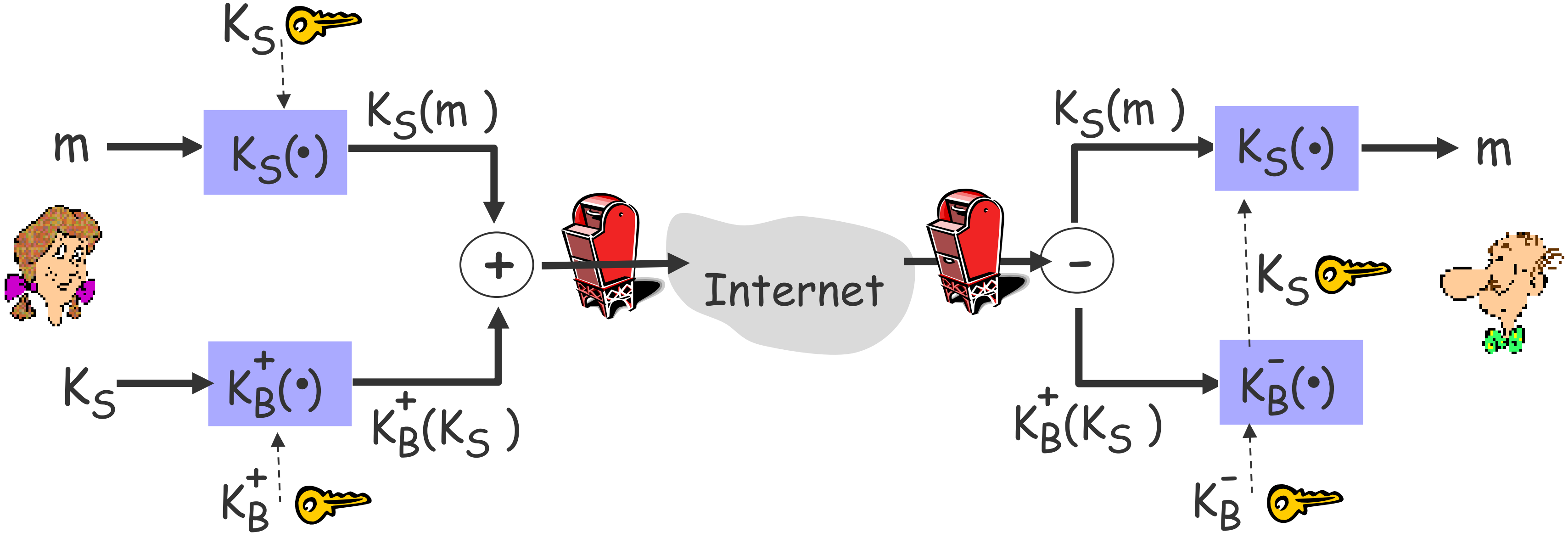
Network Security (Part 2)

Andy Carpenter

(Andy.Carpenter@manchester.ac.uk)

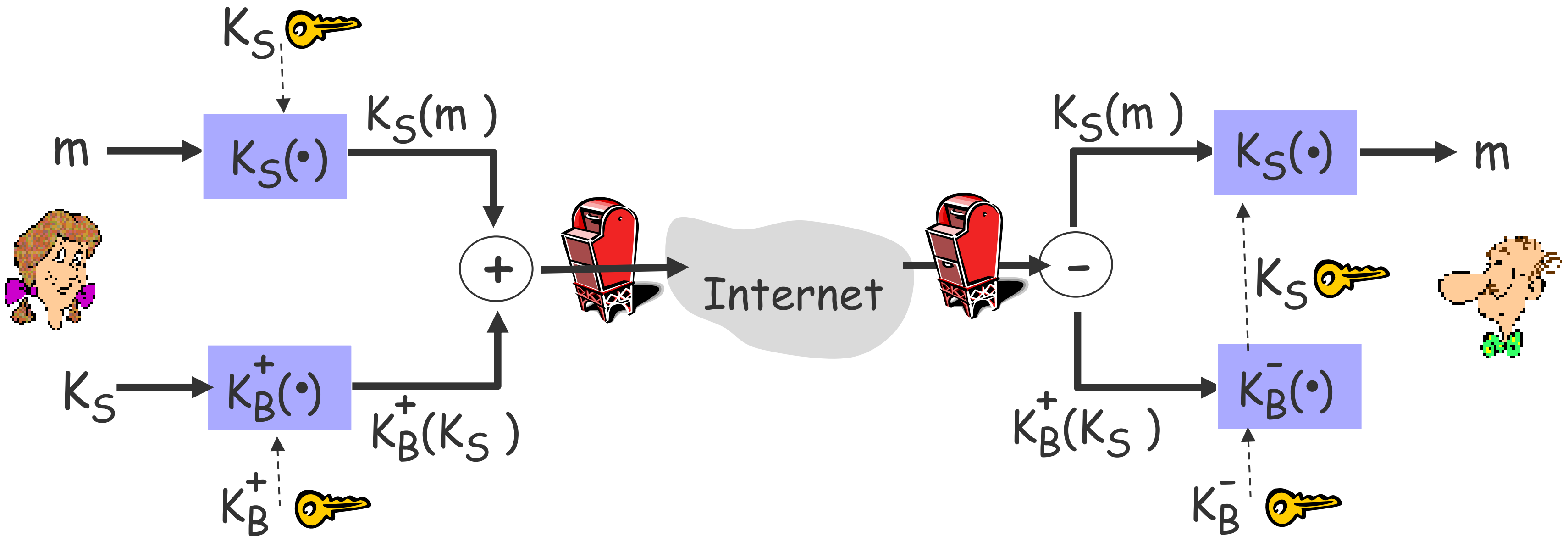
Elements these slides come from Kurose and Ross, authors of "Computer Networking: A Top-down Approach", and are copyright Kurose and Ross

Confidentiality: Secure Email



- 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

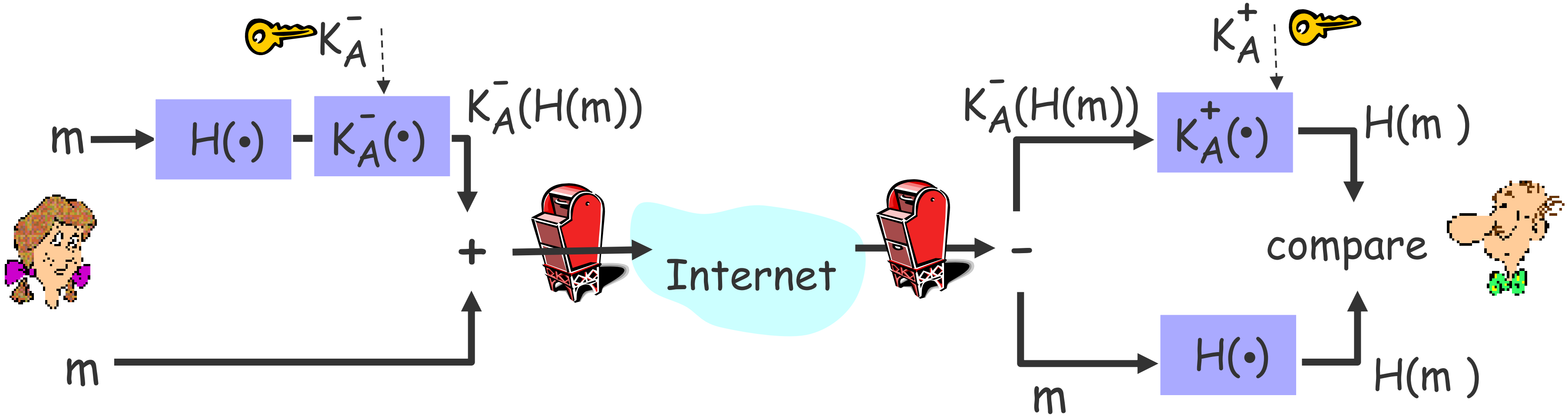
Confidentiality: Secure Email



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

No check that meaningful

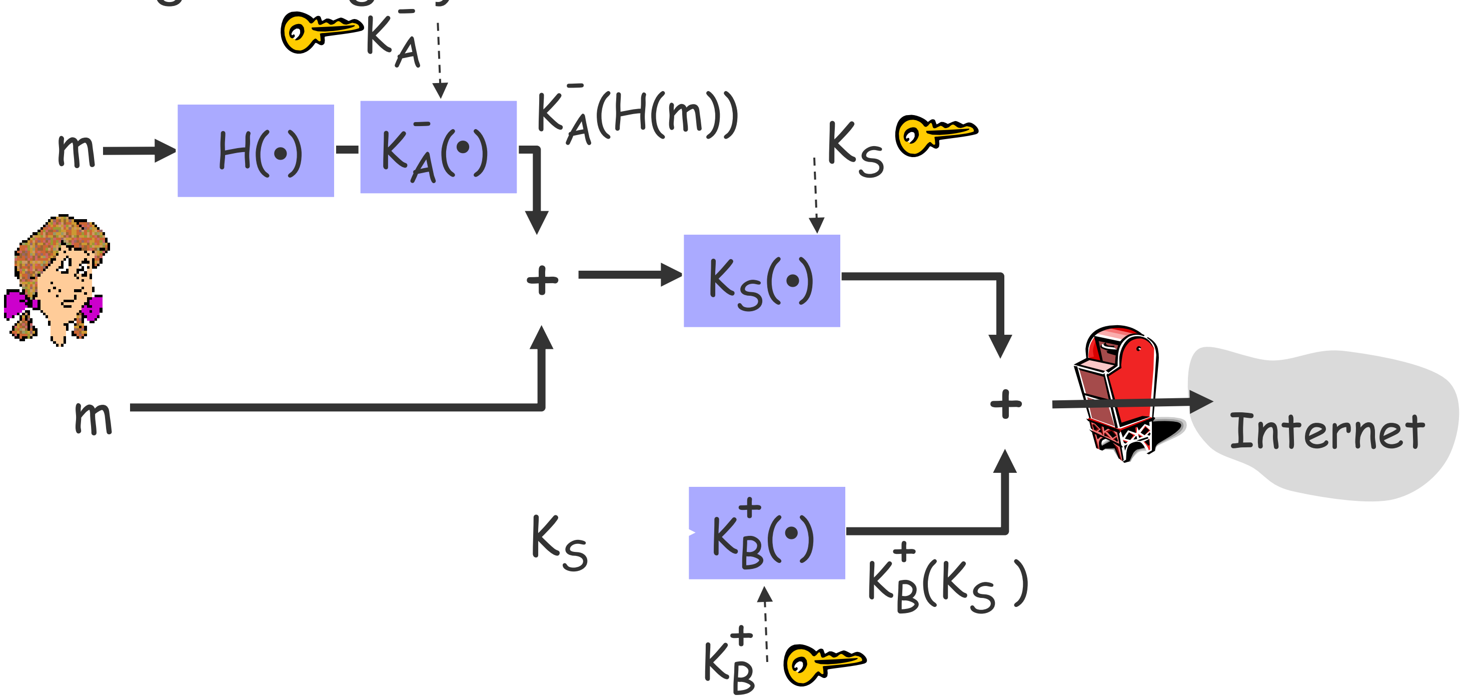
Sender Authentication: Secure Email



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

Sender Authentication: Secure Email

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



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

P&D: 8.2.3

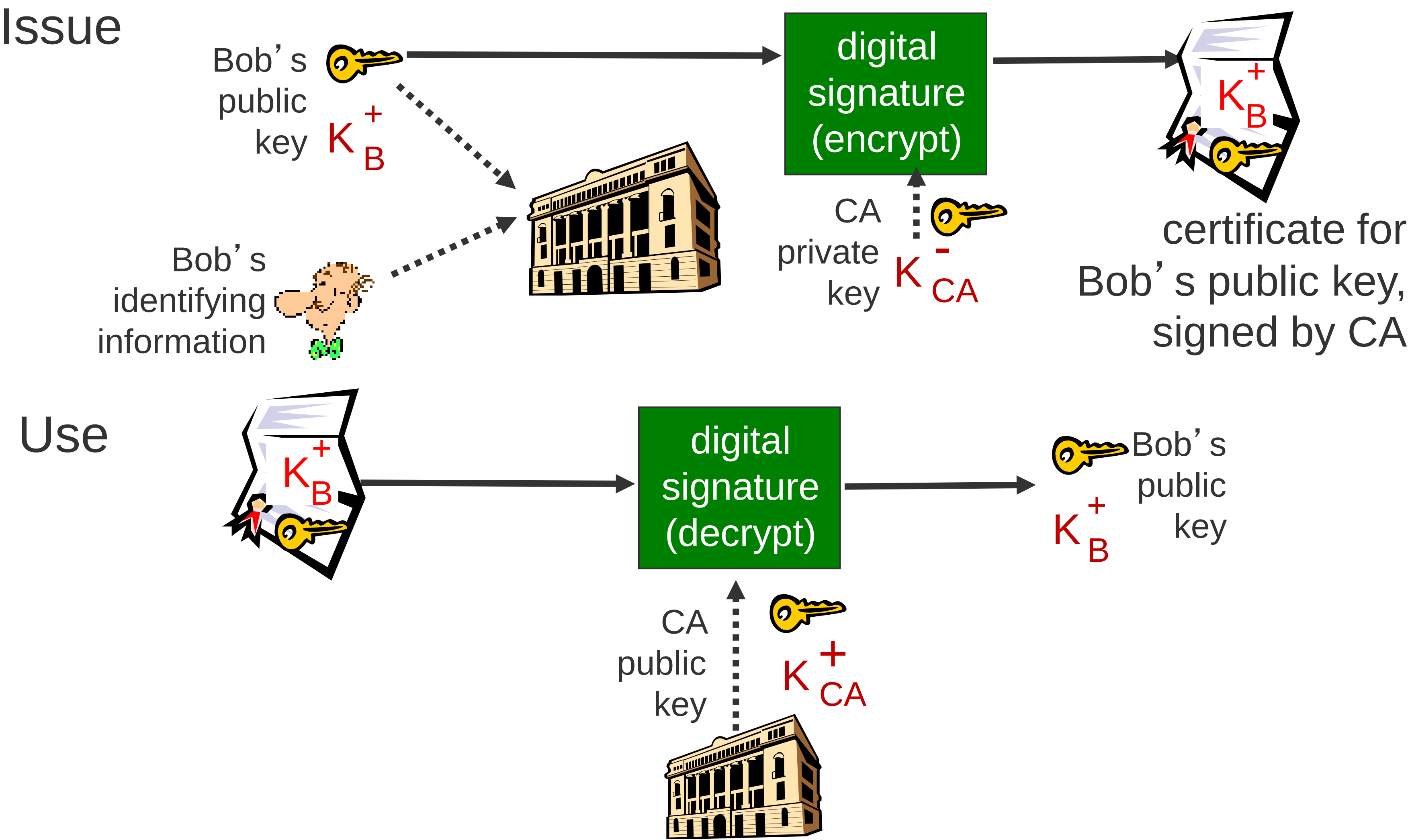
Public Key Distribution

Remember man-in-the-middle

Trudy can read everything

- Cryptography depends on knowing public keys
- Sending keys without protection means no confirmation of owner
- But, modification protection requires a key …
- Use digital certificates; aspects:
  - – using digital certificates to verify public keys
  - – building “chains of trust” using certificates
  - – how certificates are cancelled (revoked)

Digital Certificates



Issue

Bob’s public key K_B^+

Bob’s identifying information

digital signature (encrypt)

CA private key K_{CA}^-

K_B^+

certificate for Bob’s public key, signed by CA

Use

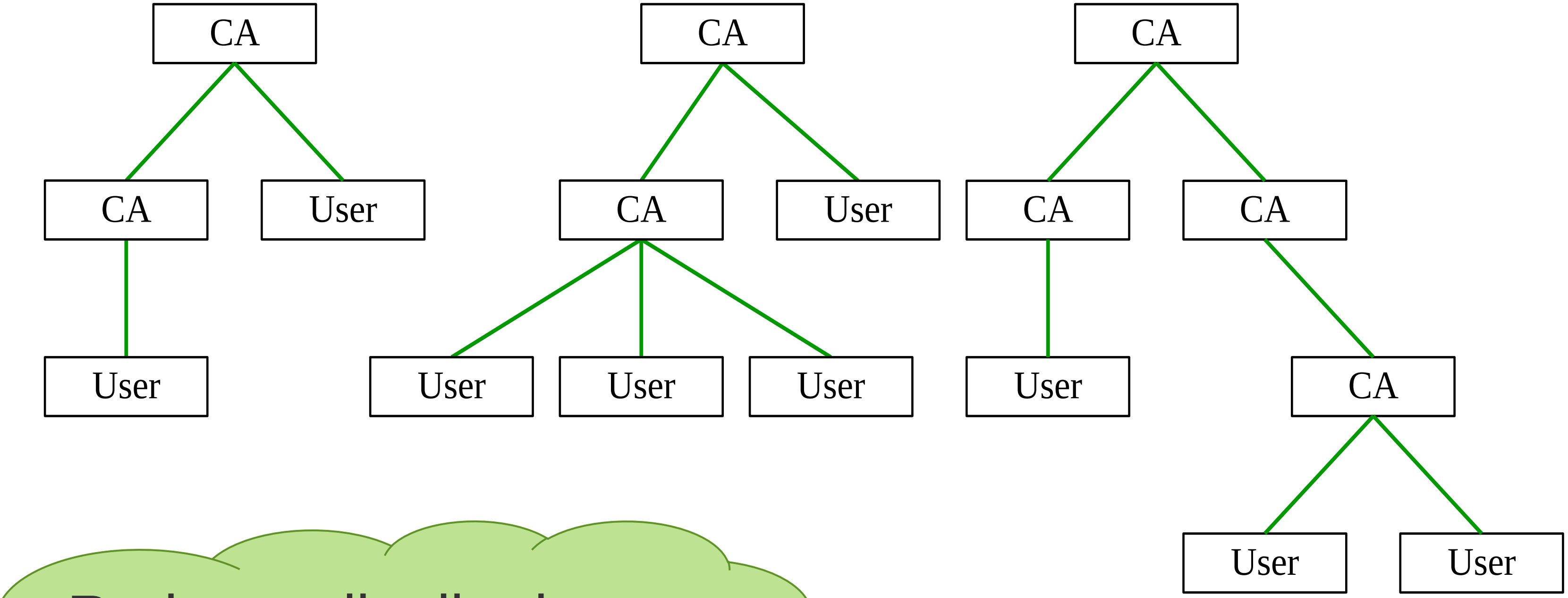
K_B^+

digital signature (decrypt)

Bob’s public key K_B^+

CA public key K_{CA}^+

Certificates: Chains of Trust



Reduces distribution problem but does not solve it

In practice, board and flat

P&D: 8.2.3

Digital Certificates: Revocation

- Necessary if, for example, private key becomes known
- This permits impersonation; so, must invalidate:
  - all certificates associated with compromised key
- Basic mechanism is CAs publish, at known location:
  - signed certificate revocation lists (CRLs)
- When receiver is validating a certificate:
  - consults CAs CRL to check certificate is not revoked
- One reason for lifetime of certificates,
  - means can eventually be removed from CRLs

Certificates: Example x509 Certificate

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=UK, L=Manchester, O=University of Manchester, …
        Validity
            Not Before: Apr 16 13:28:56 2003 GMT
            Not After : Apr 13 13:28:56 2013 GMT
        Subject: …, CN=Andy.Carpenter@cs.man.ac.uk
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b9:d8:c6:d0:19:d6:e8:3a:00:9c:74:6b:75:45:
                    …
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        27:de:40:31:54:ce:55:29:1f:26:29:42:e7:bd:9e:a0:8a:92:
```

Issuer/CA

Certificate lifetime

Entity being certified

Key algorithm and parameters

Key

Signature algorithm

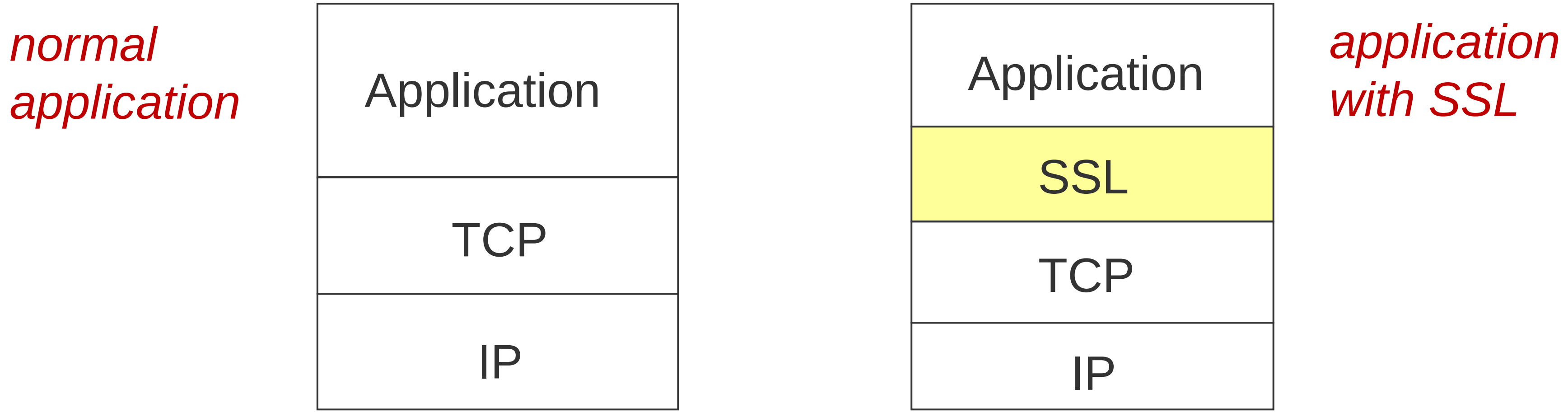
Signature

P&D: 8.3

Implementing Network Security

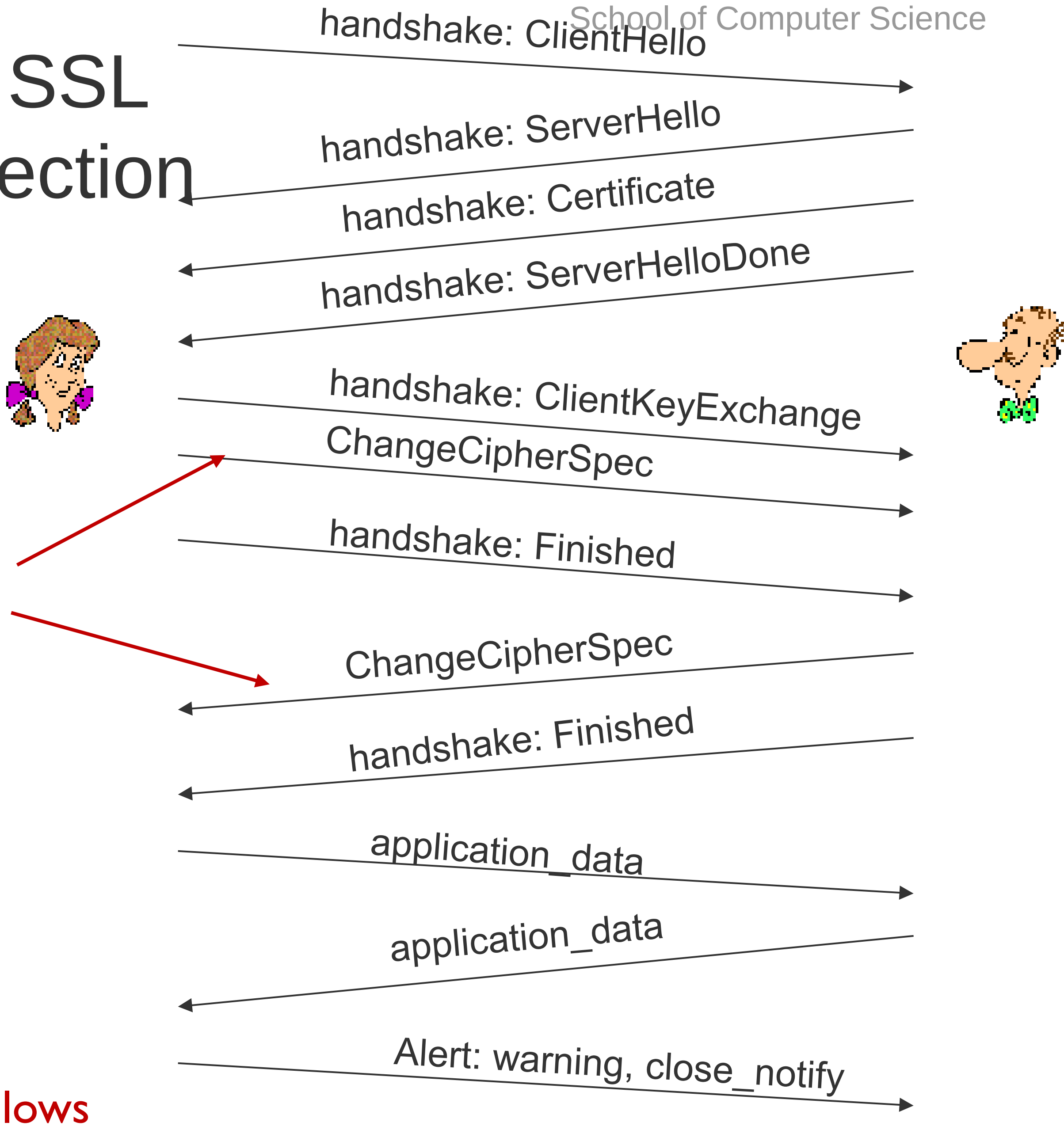
- Implemented various levels of network
- Application, e.g. PGP, SSH
  - provides application-to-application security
  - each application must implement its own security
- Transport, e.g. TLS/SSL
  - provides application-to-application security
  - single implementation for all applications
- Network, e.g. IPSEC
  - used to build complete secure networks

Transport Layer Security (TLS)/SSL



- Transport protocol with built-in security mechanisms
- Provides security to any TCP-based application
  - e.g., e-commerce via web (https)
- Security services:
  - server authentication, data encryption
  - client authentication (optional)

Real SSL connection



handshake: ClientHello

handshake: ServerHello

handshake: Certificate

handshake: ServerHelloDone

handshake: ClientKeyExchange

ChangeCipherSpec

handshake: Finished

ChangeCipherSpec

handshake: Finished

application_data

application_data

Alert: warning, close_notify

everything henceforth is encrypted

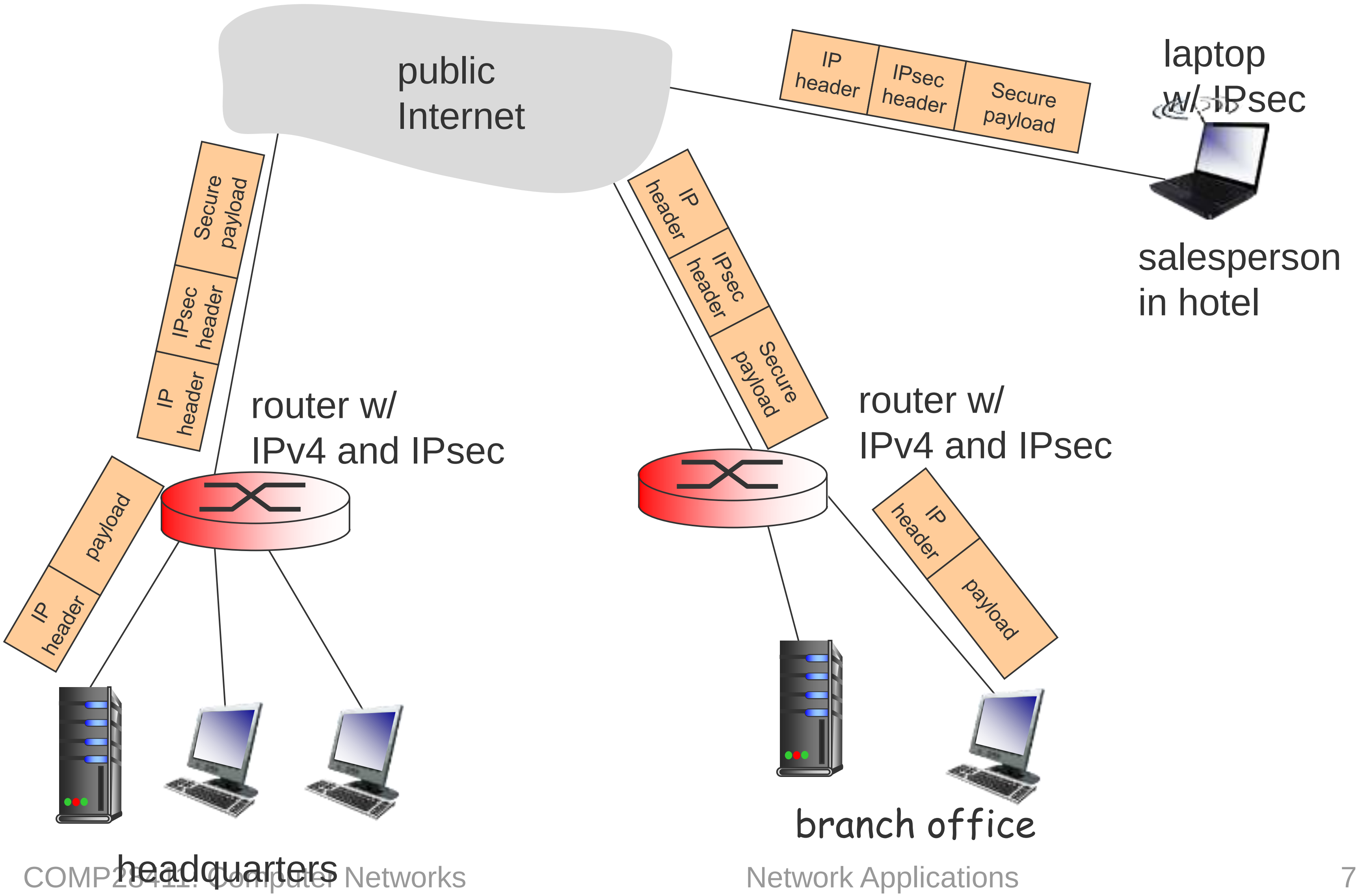
TCP FIN follows

P&D: 8.3.4

IPSEC

- Framework providing security services including
  - access control, integrity, authentication
  - protection against replay, confidentiality
- Modula
- Allows section of security services used
- Granularity secured, e.g. single TCP connection, all comms

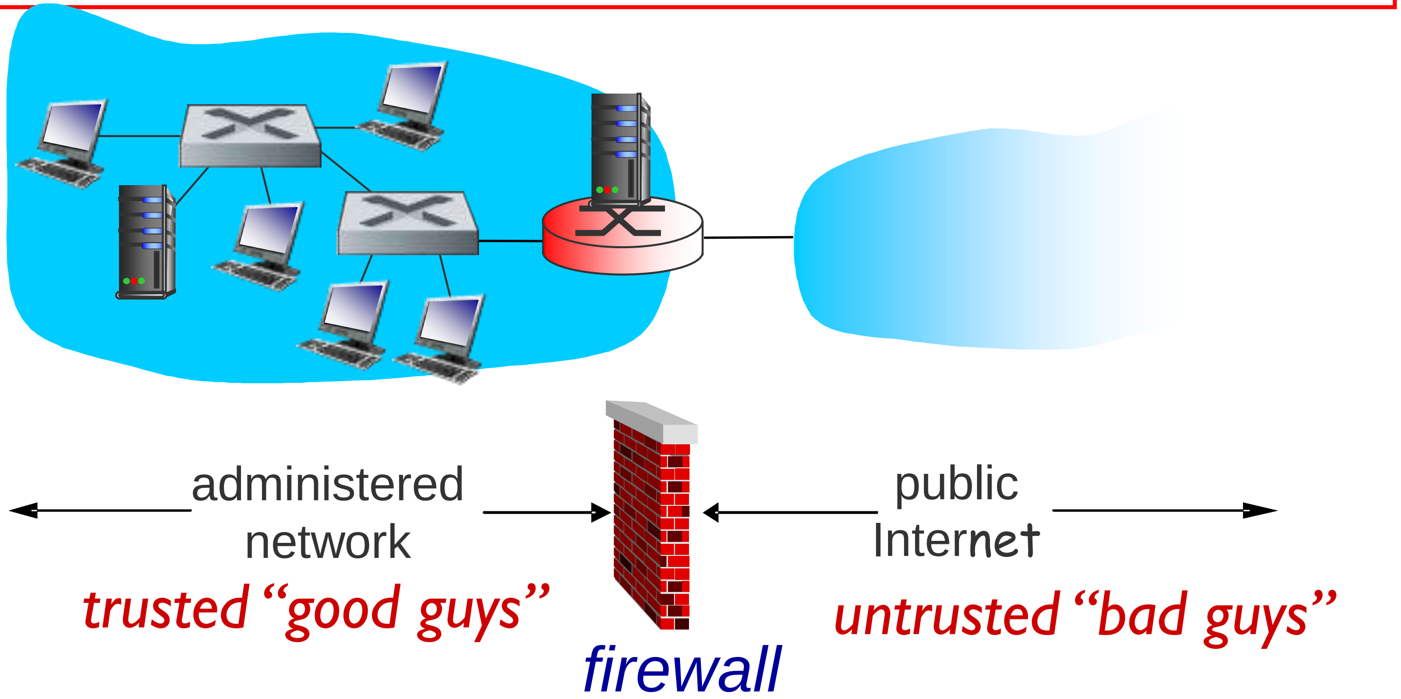
Virtual Private Networks (VPNs)



Firewalls

firewall

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



administered network

trusted "good guys"

firewall

public Internet

untrusted "bad guys"

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.

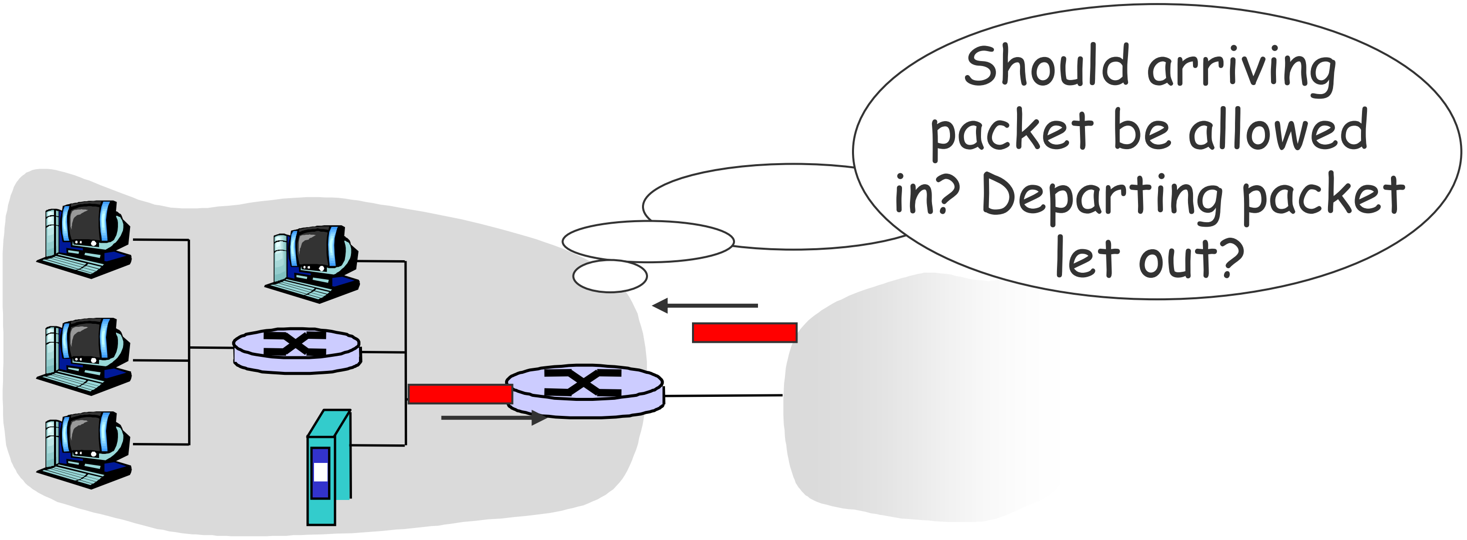
- e.g., attacker replaces CIA’s homepage with something else

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


Should arriving packet be allowed in? Departing packet let out?

- 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

Stateful packet filtering

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

- stateless packet filter: heavy handed tool
  - admits packets that “make no sense,”
- stateful packet filter: track status of TCP connections
  - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets “makes sense”
  - timeout inactive connections at firewall: no longer admit packets

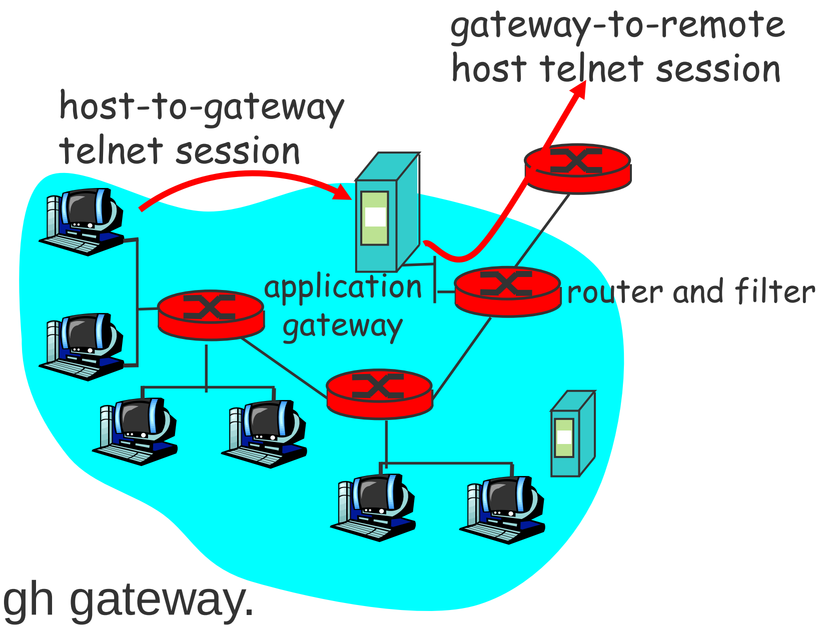
Stateful packet filtering

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	

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

Application gateways

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

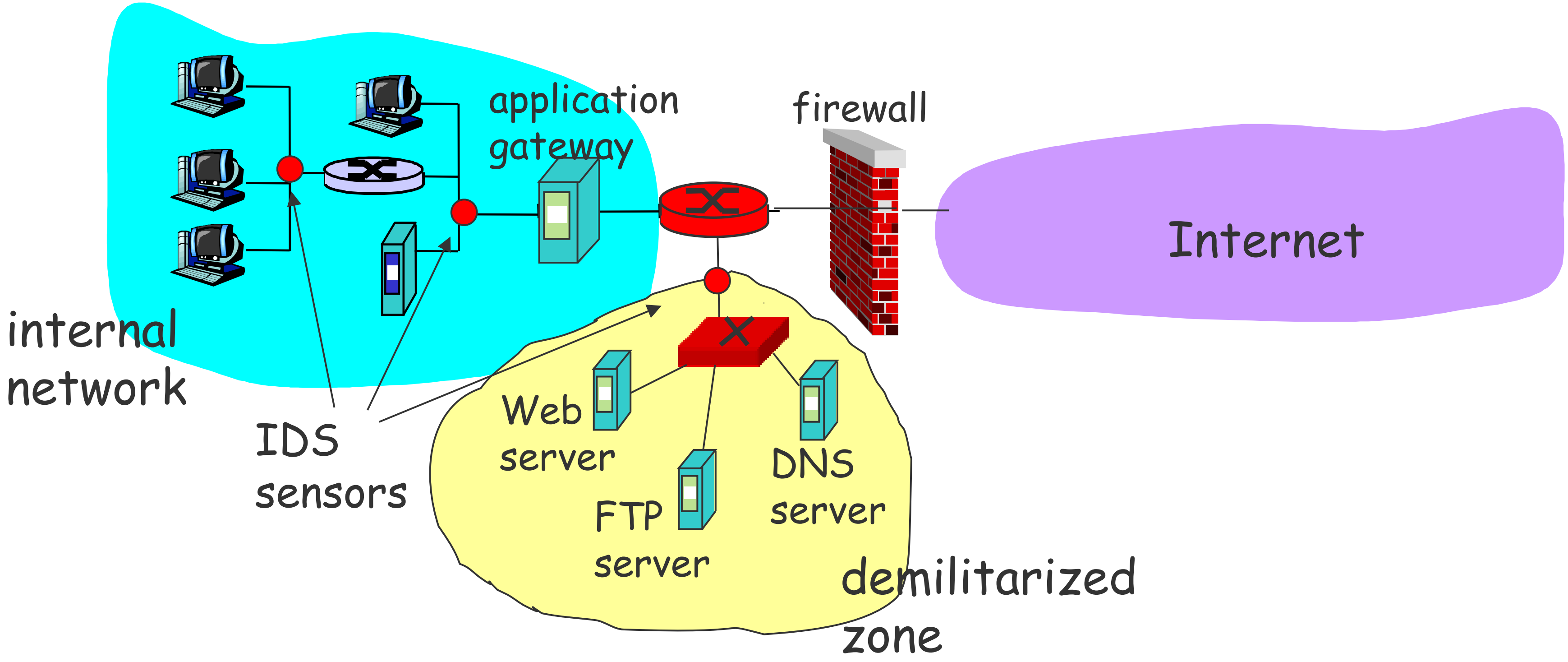

gateway-to-remote host telnet session
host-to-gateway telnet session
application gateway
router and filter

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.

Typical Enterprise Environments



Summary

- Keystone of security is encryption
- For authentication public-key algorithms are used
- Once authorised, participants use shared (session) key
- Session keys are used to implement privacy
- Core is mechanism used to distribute public keys
- Elements now used to build secure Internet applications
- Can implement at application, transport or network level
- Until networks fully secure:
  - firewalls provide protection from external threats