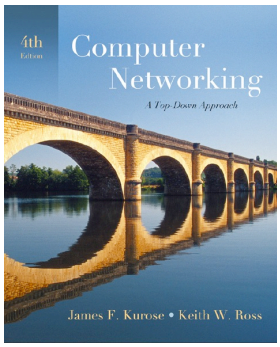
Overview of Network Security

from →



Computer Networking: A Top Down Approach, 4th edition. Jim Kurose, Keith Ross Addison-Wesley.

8-1

1

Roadmap:

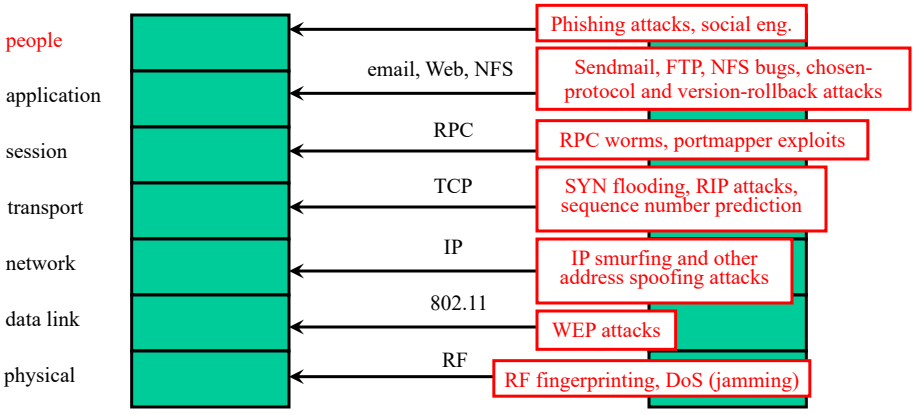
What is network security?

- Principles of cryptography
- Message integrity
- End-point authentication
- Securing e-mail
- Securing TCP connections: SSL/TLS
- Network layer security: IPsec
- Securing wireless LANs
- Operational security: firewalls and IDS

8-2

2

Sample Attacks: Network Stack

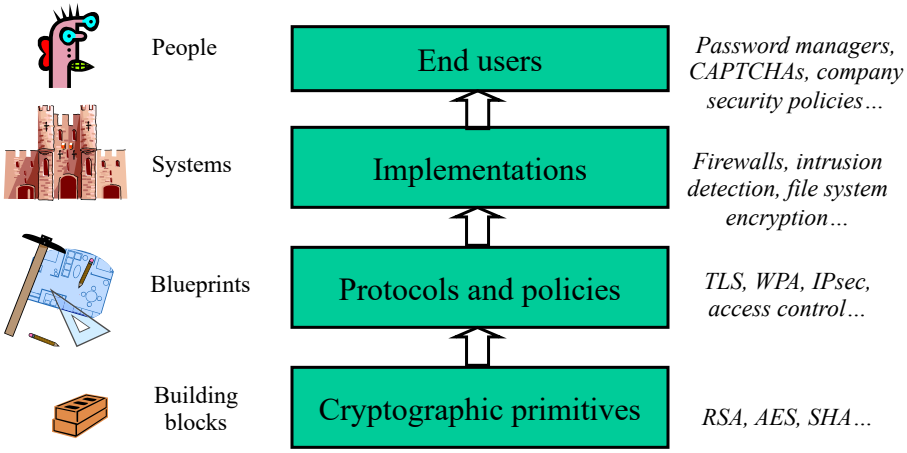


Only as secure as the single weakest layer…
… or interconnection between the layers

3

3

Network Defenses



… all of these defense mechanisms must work correctly and securely

4

4

What is network security?

Confidentiality: only sender & intended receiver should "see" message contents
- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm each other's identity

Message integrity: sender, receiver want to ensure that message not altered (in transit, or afterwards) without detection

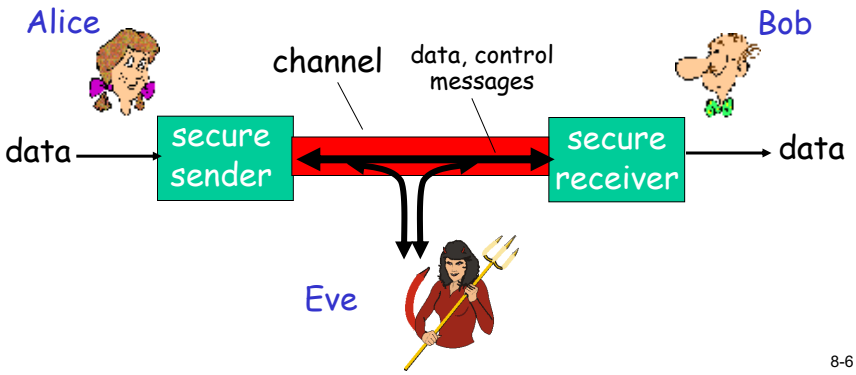
Access and availability: services/resources must be accessible and available to legitimate users

8-5

5

The Cast of Characters: Alice, Bob, Eve

- well-known in security world
- Bob and Alice (good guys) want to communicate "securely"
- Eve (adversary) may intercept, delete, modify, add messages



8-6

6

Who might Bob & Alice be?

- Real-life human users
- Web browser/server for electronic transactions (e.g., on-line purchases)
- On-line banking client/server
- DNS clients & DNS servers
- Routers exchanging routing table updates
- Game players
- P2P content peers
- Wireless client/AP
- other examples?

8-7

7

There are bad guys out there!

Q: What can Eve do?

A: a lot!

- *eavesdropping:* intercept messages
- *insertion:* introduce fake messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting itself in place
- *denial-of-service*: prevent service from being used by others (e.g., DoS by overloading resources)

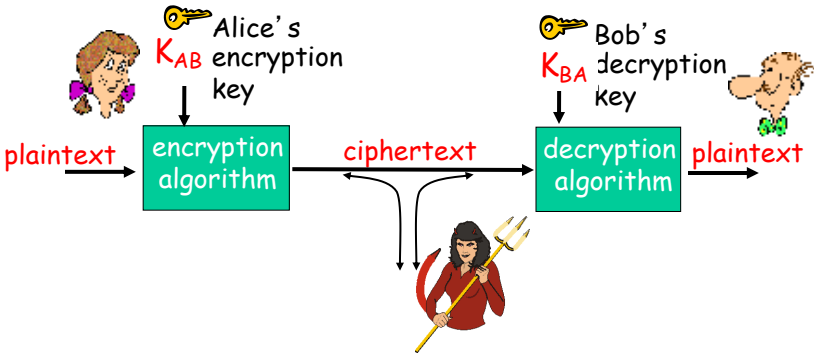
more on this later ……

8-8

8

Crypto

The language of cryptography



- Symmetric crypto: sender, receiver keys are **the same:**

$$K_{AB} = K_{BA}$$

- Public key crypto: encryption key is **public**, decryption key is **secret** (private) and **unique to each user:**

$$K_{AB} <> K_{BA}$$

Symmetric key cryptography

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
             |                       |
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

E.g.: `Plaintext: bob. i love you. alice`
`ciphertext: nkn. s gktc wky. mgsbc`

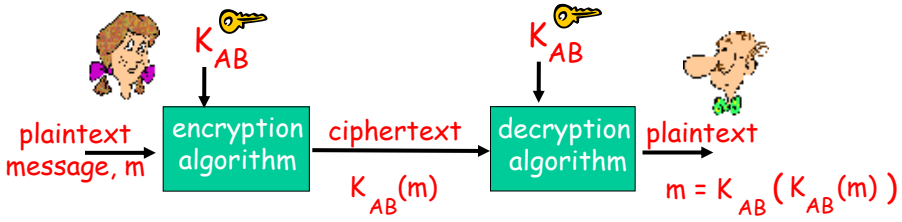
Q: How hard to break this simple cipher?:

- brute force (how hard?)
- other?

8-11

11

Symmetric key cryptography



symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{AB}

- e.g., key is the permutation in the mono-alphabetic cipher
- Q: how do Bob and Alice agree on the key?

8-12

12

Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
  - no known "backdoor" decryption approach
- making DES more secure:
  - use three keys sequentially (3-DES) on each nblock
  - use cipher-block chaining (hides patterns, prevents block rearrangement/deletion attacks)

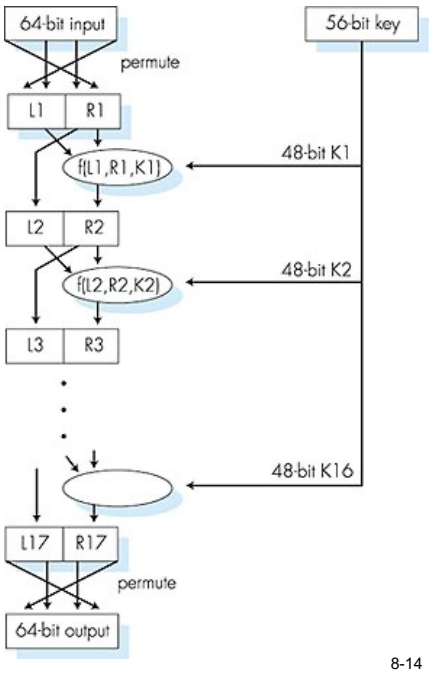
8-13

13

Symmetric key crypto: DES

DES operation

- initial permutation
- 16 identical "rounds" of function application, each using different 48 bits of key
- final permutation



8-14

14

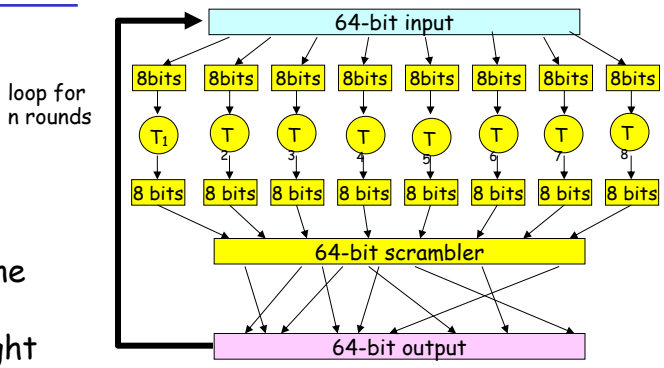
AES: Advanced Encryption Standard

- newer (2001) symmetric-key NIST standard, replacing DES
- processes data in 128-, 192- or 256-bit blocks
- supports 128-, 192-, or 256-bit keys
- brute force decryption (trying each key) taking 1 sec on DES, takes 149 trillion years for AES

8-15

15

Block Cipher



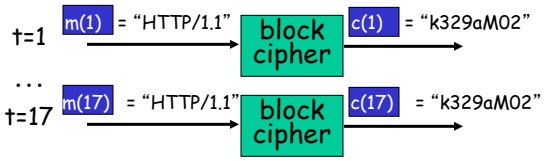
- one pass through: one input bit affects eight output bits
- multiple passes: each input bit afects all output bits
- block ciphers: DES, 3DES, AES

8-16

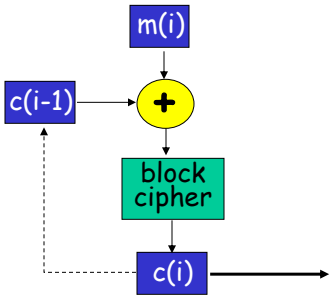
16

Cipher Block Chaining

- ECB: electronic code-book: if input block repeated, will produce same cipher text:



- CBC: cipher block chaining: XOR i-th input block, m(i), with previous block of cipher text, c(i-1)
  - c(0) = IV transmitted to receiver in clear
  - what happens in "HTTP/1.1" scenario from above?



8-17

17

Public key cryptography

symmetric key crypto

- requires sender, receiver to have the same (shared) secret key
- Q: how to agree on key in the first place (particularly, if they never "met" before)?

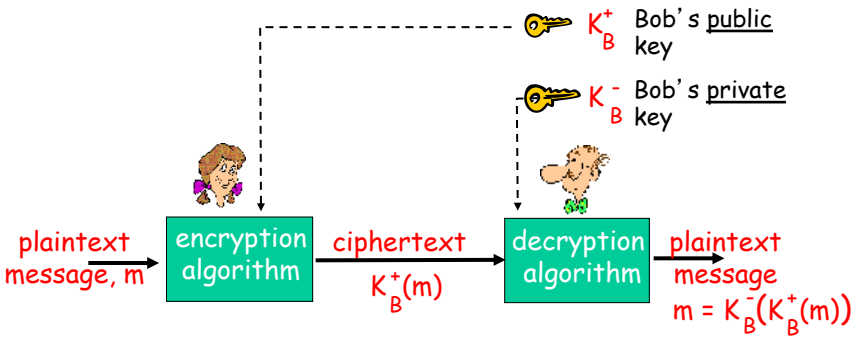
public key crypto

- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* pre-share secret key a priori
- *public* encryption key known to *all*
- *private* decryption key known only to receiver (owner)

8-18

18

Public key cryptography



8-19

19

Public key encryption algorithms

Requirements:

1. need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that
$$K_B^-(K_B^+(m)) = m$$

2. given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adleman algorithm

8-20

20

RSA: Choosing keys

1. Choose two large prime numbers p, q. (e.g., 2048 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) that has no common factors with z. (e, z are "relatively prime").
4. Choose d such that $(ed-1)$ is divisible by z. (in other words: ed mod $z = 1$).
5. *Public* key is $\underbrace{(n,e)}_{K_B^+}$. *Private* key is $\underbrace{(n,d)}_{K_B^-}$.

8-21

21

RSA: Encryption, decryption

0. Given (n,e) and (n,d) as computed above
1. To encrypt "message" m compute
   $c = m^e \bmod n$ (i.e., remainder when m^e is divided by n)
2. To decrypt ciphertext c compute
   $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n)

Magic happens! $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

8-22

22

RSA example:

Bob chooses *p=5, q=7*. Then *n=35, z=24*.
e=5 (so *e and z* are relatively prime).
d=29 (so (*e*d-1*) os divisible by z)

encrypt:

letter	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

decrypt:

c	c^d	$m = c^d \bmod n$	letter
17	48196857210675091509141182522307169 7	12	l

8-23

23

RSA: Why it works?

Useful number theory result: If *p,q* prime and *n = pq,* then:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(using number theory result above)

$$= m^1 \bmod n$$

(since we chose *ed* to be divisible by *(p-1)(q-1)* with remainder 1)

$$= m$$

8-24

24

RSA: another important property

The following property will be *very* useful later:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

Result is the same!

8-25

25

Data Integrity

8-26

26

Message Integrity + Origin Auth-n

Bob receives msg from Alice, wants to ensure:

- message originally came from Alice
- message not changed since sent by Alice

Cryptographic Hash:

- Take any-size input m, (quickly) compute a fixed-length value H(m)
- Must be computationally infeasible to:
  - Given z, find x such that H(x)=z.
  - Given x, find y<>x such that H(x)=H(Y)
  - Find any two messages, x<>y such that H(x) = H(y)

8-27

27

Internet checksum: poor crypto hash function

Internet checksum has some properties of hash function:

- ✓ produces fixed length digest (16-bit sum) of message
- ✓ is many-to-one

But given message with given hash value, it is easy to find another message with same hash value:

message	ASCII format
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 4F 42
	B2 C1 D2 AC

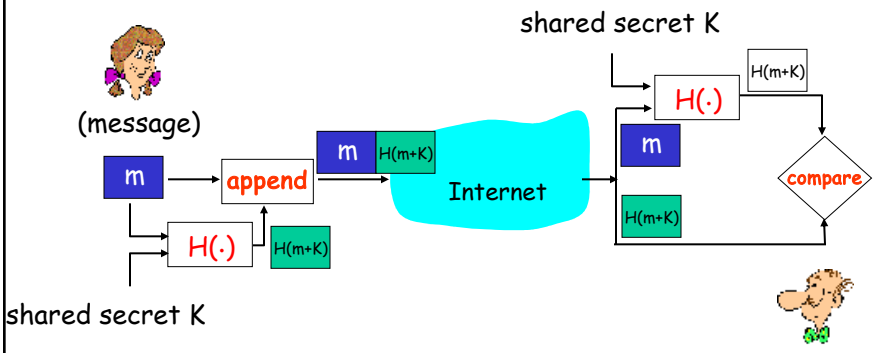
message	ASCII format
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 4F 42
	B2 C1 D2 AC

different messages but identical checksums!

8-28

28

Message Authentication Code



Real-world MAC example:

HMAC = H (K xor OPAD, H (K xor IPAD, m))

8-29

29

HASH functions in practice

- MD5 hash function was widely used 'till about 2009 (RFC 1321)
  - computes 128-bit MAC in 4-step process.
  - arbitrary 128-bit string x, appears difficult to construct msg m whose MD5 hash is equal to x
    - attacks on MD5
- SHA-2 and SHA-3 are used today
- SHA-2:
  - US standard: FIPS PUB 180-1/180-2
  - 160, 224, 256, 384, 512-bit output
  - 512, 1024 input block size
- SHA-3:
  - US standard: FIPS PUB 202
  - 224, 256, 384, 512-bit output
  - 1152, 1088, 832, 576 input block size

8-30

30

Digital Signatures

cryptographic techniques (somewhat) analogous to hand-written signatures

- signer (Bob) digitally signs document, establishing that he is the document's owner/creator
- Verifiable & nonforgeable: verifier (Alice) can prove to someone (also herself) that Bob, and no one else (including Alice), must have signed document

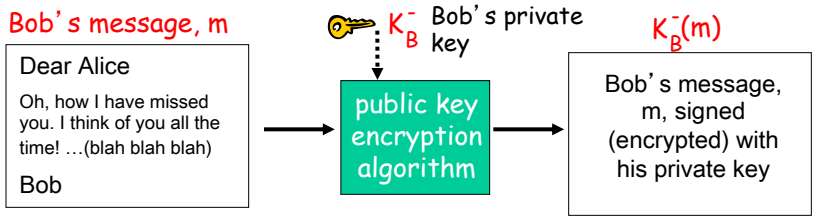
8-31

31

Digital Signatures

simple digital signature for message m:

- Bob signs m by "encrypting" m with his private key K_B^-, creating "signed" message, $K_B^-(m)$



8-32

32

Digital Signatures (more)

- suppose Alice receives msg m, digital signature $K_B^-(m)$
- Alice verifies that m is signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$. then checks $K_B^+(K_B^-(m)) = m$.
- if $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

- ✓ Bob signed m and no one else could've signed m
- ✓ Bob signed m and not m'

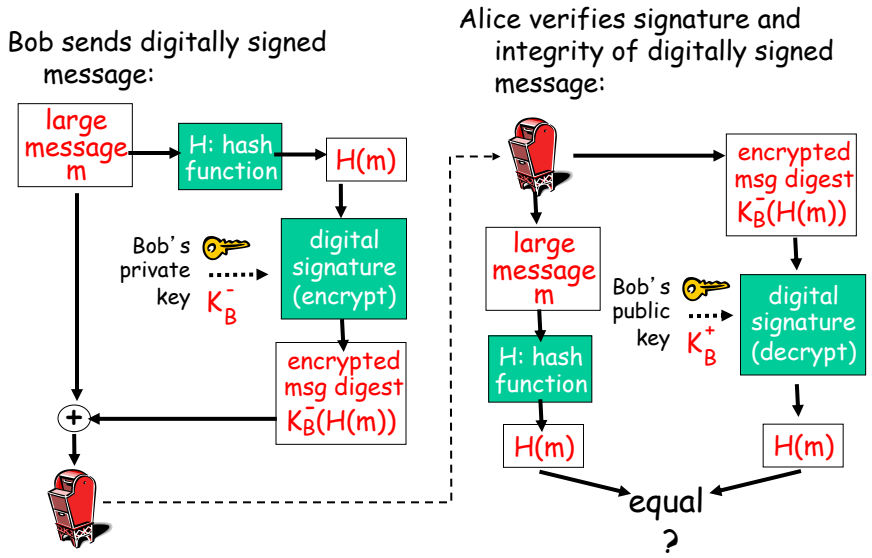
non-repudiation:

- ✓ Alice can take K_B^+, m, and signature $K_B(m)$ to a 3rd party (or court) and prove that Bob signed m

8-33

33

Digital signature = signed HASH



8-34

34

Public Key Certification

public key problem:

- When Alice obtains Bob's public key (from web site, e-mail, USB stick), how does she *know* it is actually Bob's public key, and not Eve's?

solution:

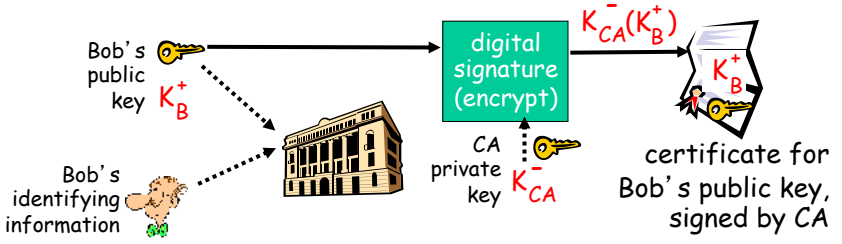
- trusted certification authority (CA)

8-35

35

Certification Authorities

- Certification Authority (CA): binds public key to particular entity, E.
- E registers its public key with CA.
  - E provides (perhaps off-line) a "proof of identity" to CA.
  - CA creates a **certificate** binding E to its public key.
  - certificate containing E's public key digitally signed by CA: CA says: "This is E's public key."

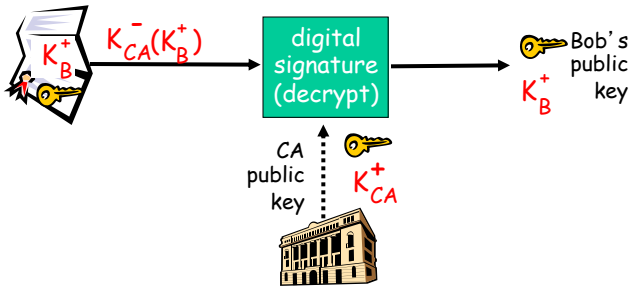


8-36

36

Certification Authorities

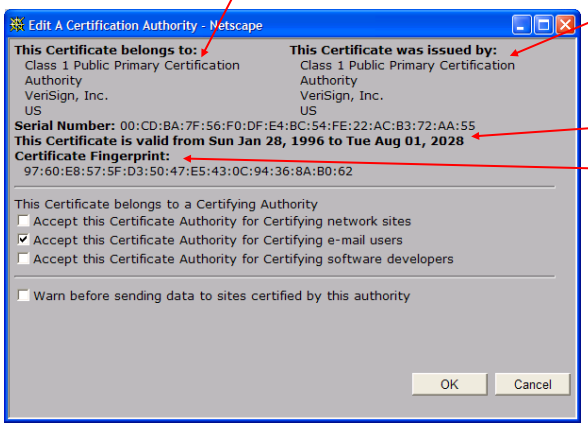
- when Alice wants Bob's public key (assume Bob knows CA's public key):
  - gets Bob's certificate (from Bob or elsewhere/anywhere)
  - checks for expiration
  - uses CA's public key to verify Bob's certificate
  - checks for revocation
  - extracts Bob's public key from Bob's certificate



37

A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)



- info about certificate issuer
- valid dates
- digital signature by issuer

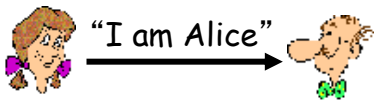
38

Authentication

Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"

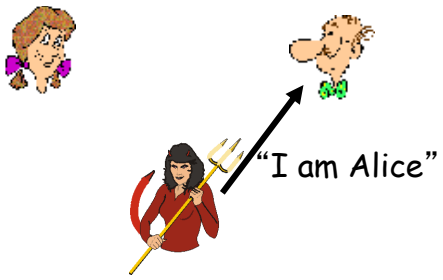


Failure scenario??

Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"



in a network, Bob can not "see" Alice, so Eve simply declares herself to be Alice

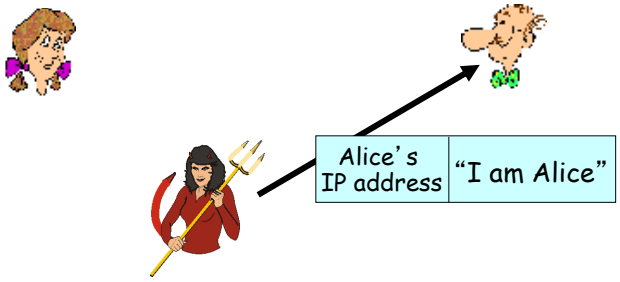
Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address

Failure scenario??

Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



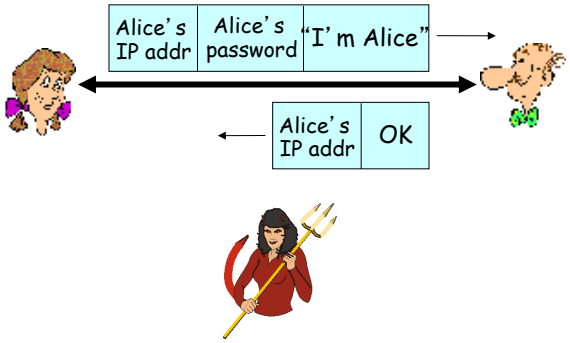
Eve can create a packet "spoofing" Alice's address

8-43

43

Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



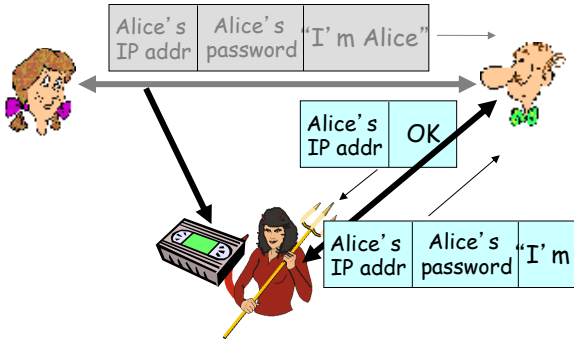
Failure scenario??

8-44

44

Authentication: another try

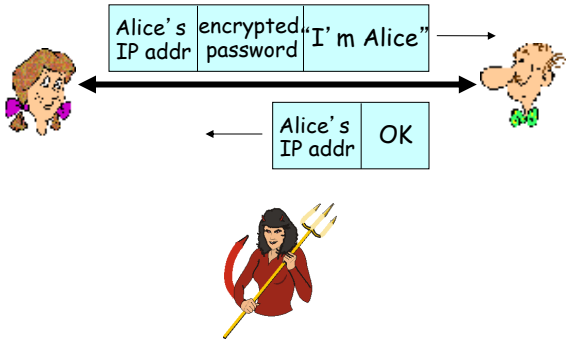
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



playback attack: Eve records Alice's packet and later plays it back to Bob

Authentication: yet another try

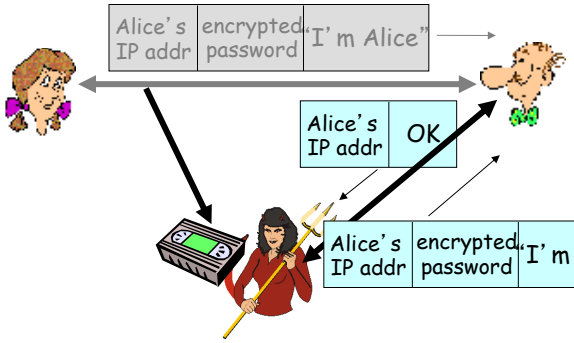
Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



Failure scenario??

Authentication: another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



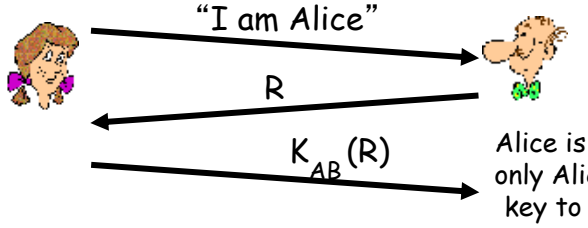
record and playback still works!

Authentication: yet another try

Goal: avoid playback attack

Nonce: number (R) used only *once*

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



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

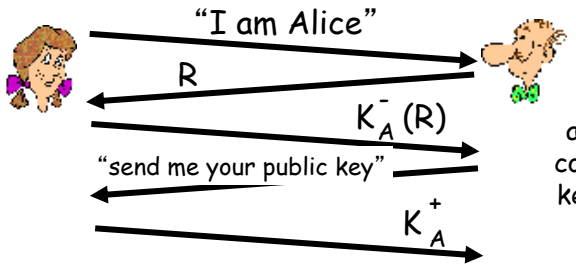
Failures, drawbacks?

Authentication: ap5.0

ap4.0 requires shared symmetric key

- can we authenticate using public key techniques?

ap5.0: use nonce, public key cryptography



Bob computes $K_A^+(K_A^-(R)) = R$ and knows only Alice could have the private key, that encrypted R such that $K_A^+(K_A^-(R)) = R$

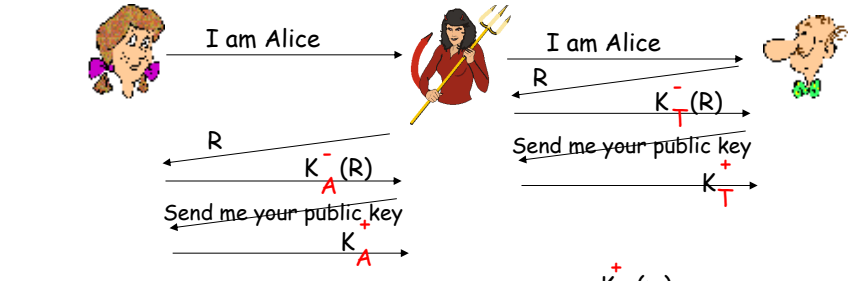
8-49

49

ap5.0: security hole

Man-in-the-Middle attack (MitM):

Eve poses as Alice (to Bob) and as Bob (to Alice)



8-50

50

ap5.0: security hole

Man-in-the-Middle attack (MitM):

Eve poses as Alice (to Bob) and as Bob (to Alice)

Difficult to detect:

- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation)
- problem is that Eve receives all messages as well!

8-51

51

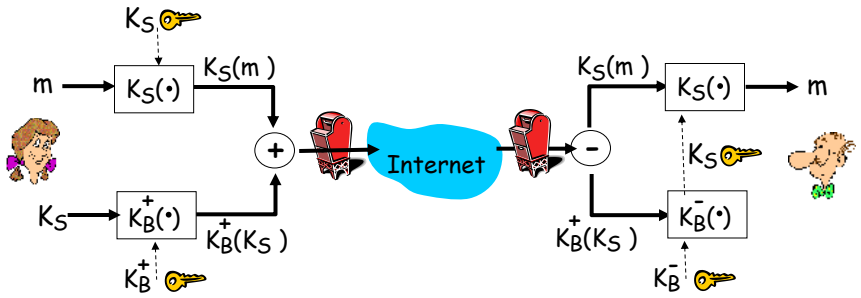
Apps: Email

8-52

52

Secure e-mail

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



Alice:

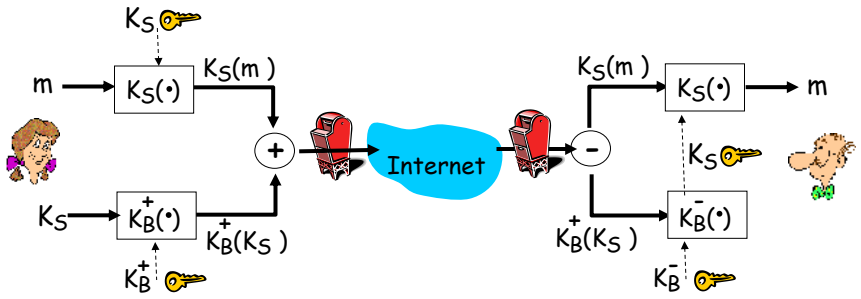
- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob

8-53

53

Secure e-mail

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



Bob:

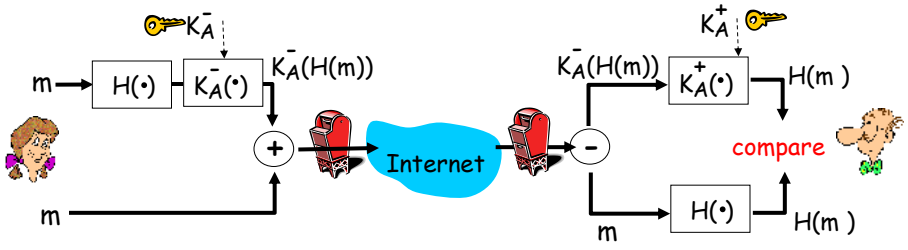
- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

8-54

54

Secure e-mail (continued)

• Alice wants to provide sender authentication message integrity.

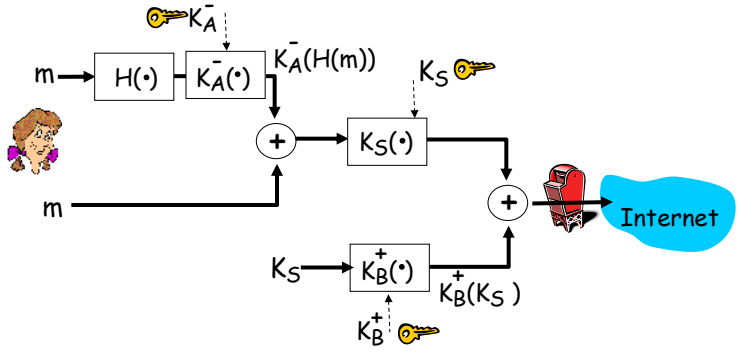


• Alice digitally signs message
• sends both message (in the clear) and digital signature

55

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

56

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 a 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+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

www.openpgp.org

8-57

57

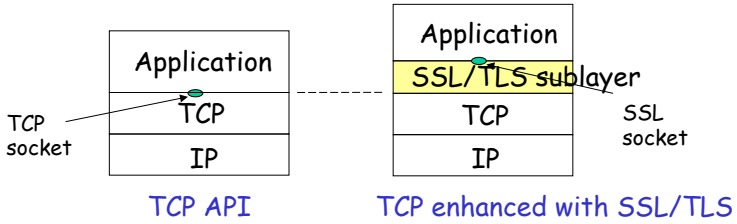
Apps: SSL/TLS

8-58

58

Siblings: Secure Sockets Layer (SSL) and Transaction Layer Security (TLS)

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



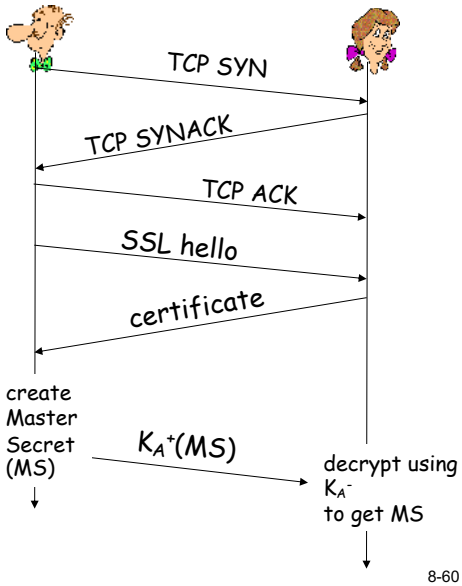
8-59

59

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



8-60

60

SSL: three phases

2. Key Derivation:

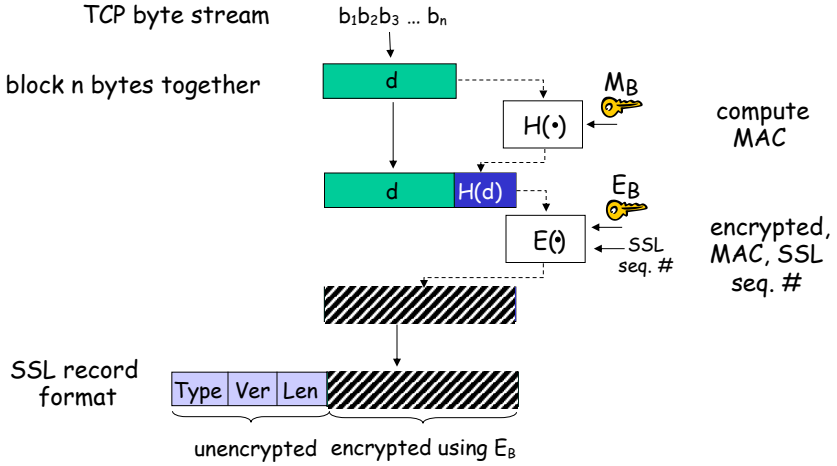
- Alice, Bob use shared secret (MS) to generate 4 keys:
  - E_B: Bob->Alice data encryption key
  - E_A: Alice->Bob data encryption key
  - M_B: Bob->Alice MAC key
  - M_A: Alice->Bob MAC key
- encryption and MAC algorithms negotiable between Bob, Alice
- why 4 keys?

8-61

61

SSL: three phases

3. Data transfer



8-62

62

Apps: IPSec

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:

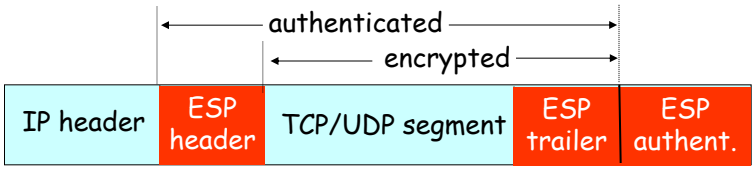
- connection identifier
- authentication data: source- signed message digest calculated over original IP datagram.
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)

8-65

65

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.



8-66

66

Wireless Security

IEEE 802.11 security

- *war-driving:* drive around your favorite business or residential neighborhood… see what 802.11 networks available?
  - 1,000s accessible from public roadways/walkways
  - 10-20% use no encryption/authentication
  - packet-sniffing and various attacks easy!
    - Especially, **traffic analysis**
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - more recent attempt: 802.11i

Wired Equivalent Privacy (WEP):

- authentication as in protocol *ap4.0*
  - host requests authentication from access point
  - access point sends a 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

8-69

69

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 ith byte, d_i, in frame:

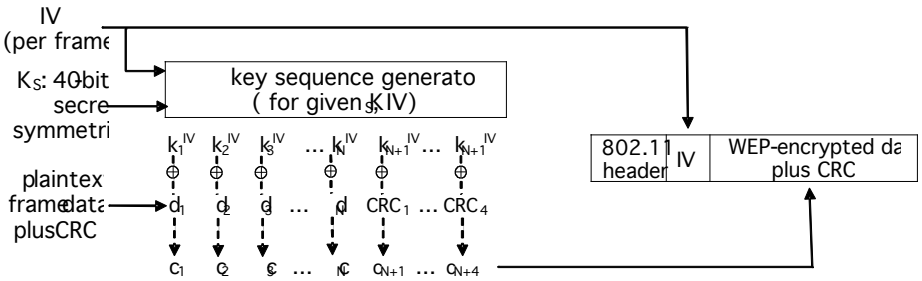
$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

8-70

70

802.11 WEP encryption



Sender-side WEP encryption

8-71

71

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:
  - Eve causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
  - Eve sees: $c_i = d_i$ XOR k_i^{IV}
  - Eve knows c_i d_i, so can compute k_i^{IV}
  - Eve knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time IV is used, Eve can decrypt!

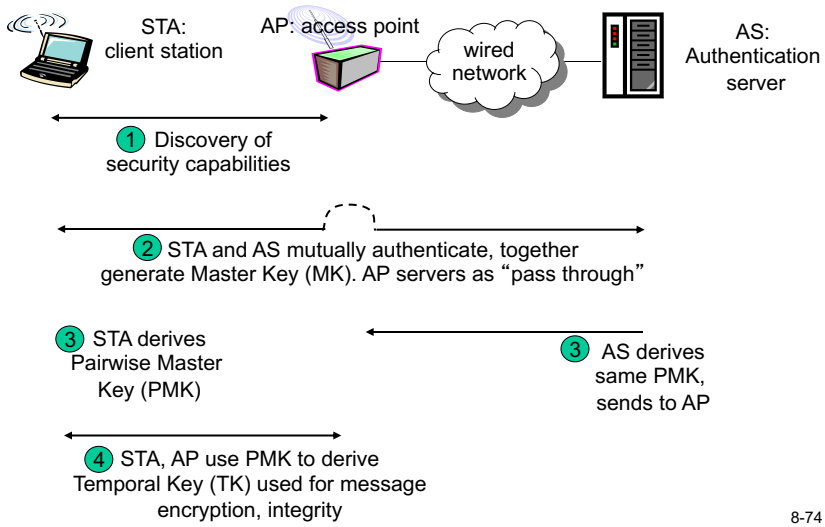
8-72

72

802.11i: improved security

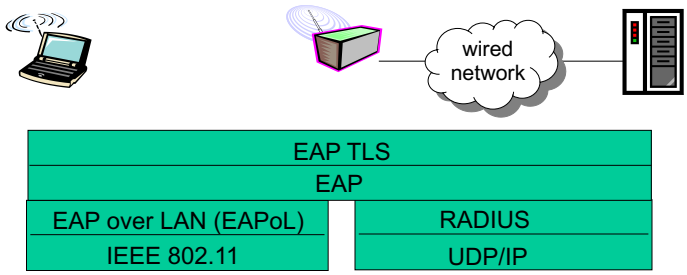
- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

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)



8-75

75

Firewalls, IDS-s

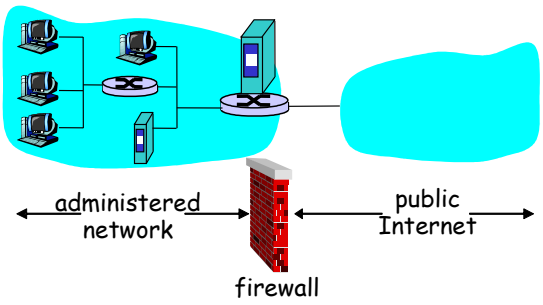
8-76

76

Firewalls

firewall

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



8-77

77

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)

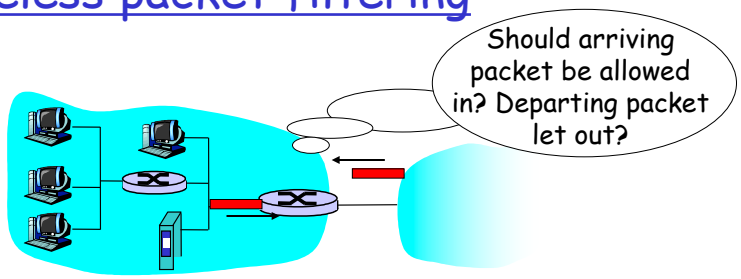
three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

8-78

78

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

8-79

79

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.

8-80

80

Stateless packet filtering: more examples

Policy	Firewall Setting
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

8-81

81

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

8-82

82

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

8-83

83

Stateful packet filtering

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

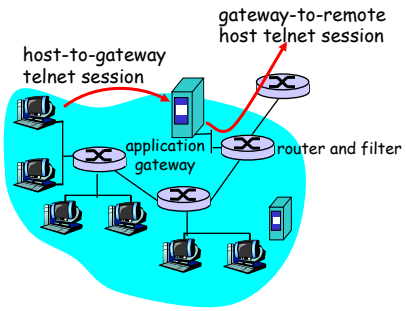
action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	>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

8-84

84

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 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

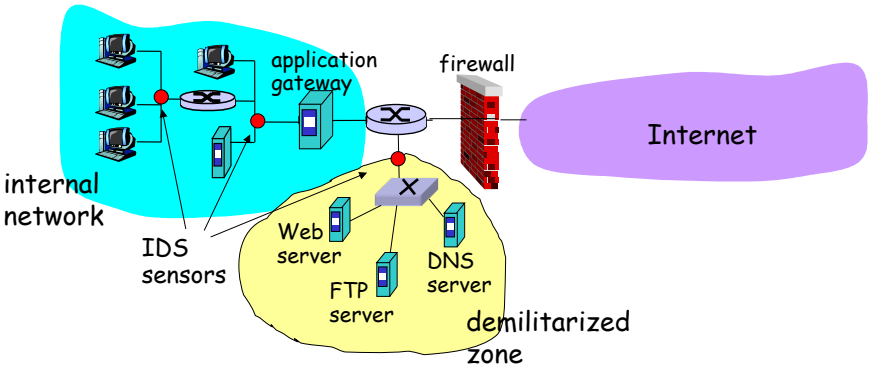
- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among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

8-87

87

Intrusion detection systems

- multiple IDSs: different types of checking at different locations



8-88

88

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/TLS)
- IP sec
- 802.11

Operational Security: firewalls and IDS

8-89