Computer Networks - Exercise 12

Stephan Sigg

Georg-August-University Goettingen, Computer Networks

29.01.2015

12.1

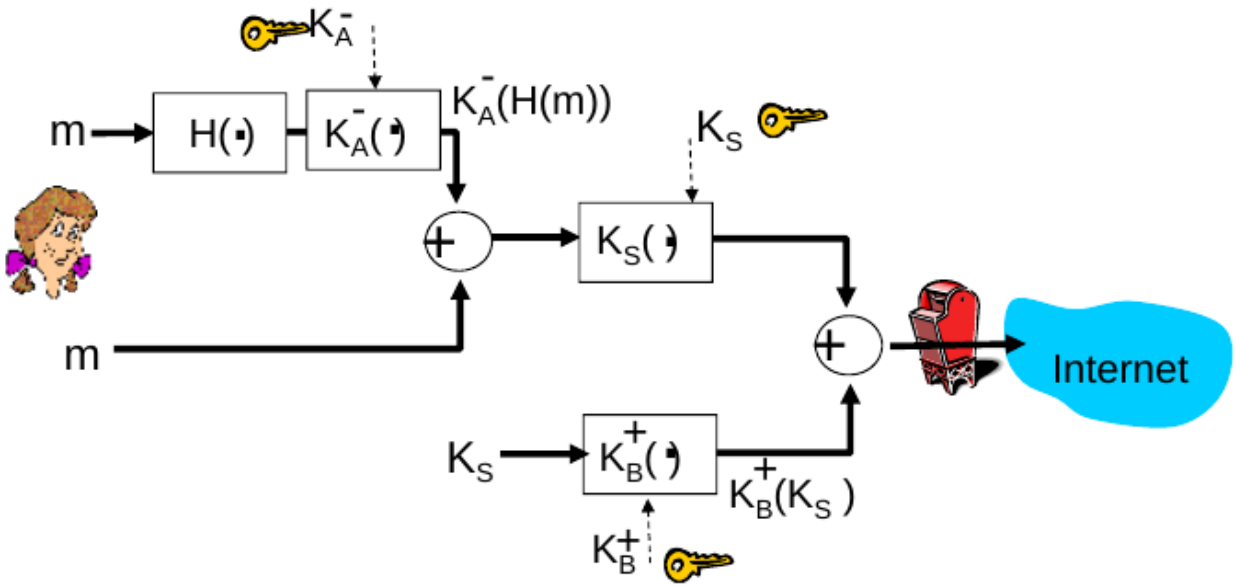
Q12.1 In the lecture it was discussed how an email can be sent providing secrecy, sender authentication and message integrity. Sketch how the receiver side will decrypt and authenticate the message.

12.1

Sketch how the receiver side will decrypt and authenticate the message.

Secure e-mail (continued)

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



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

12.1

Sketch how the receiver side will decrypt and authenticate the message.

- Here: Design and draw receiver side

12.2

Q12.2 What is PGP? Discuss the concepts and implementation.

12.2

What is PGP? Discuss the concepts and implementation

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

12.2

What is PGP? Discuss the concepts and implementation

TOdO Add further details here?

12.3

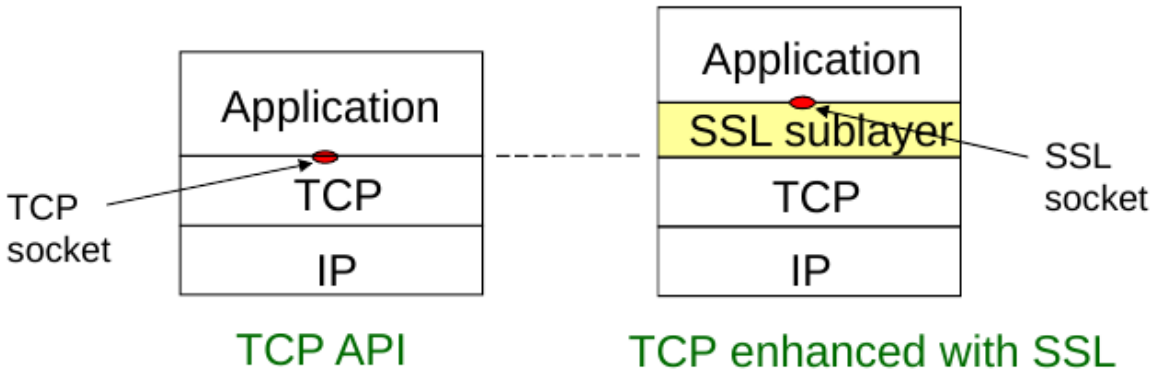
Q12.3 Explain how SSL works.

12.3 – Symmetric encryption

Explain how SSL works

Secure sockets layer (SSL)

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

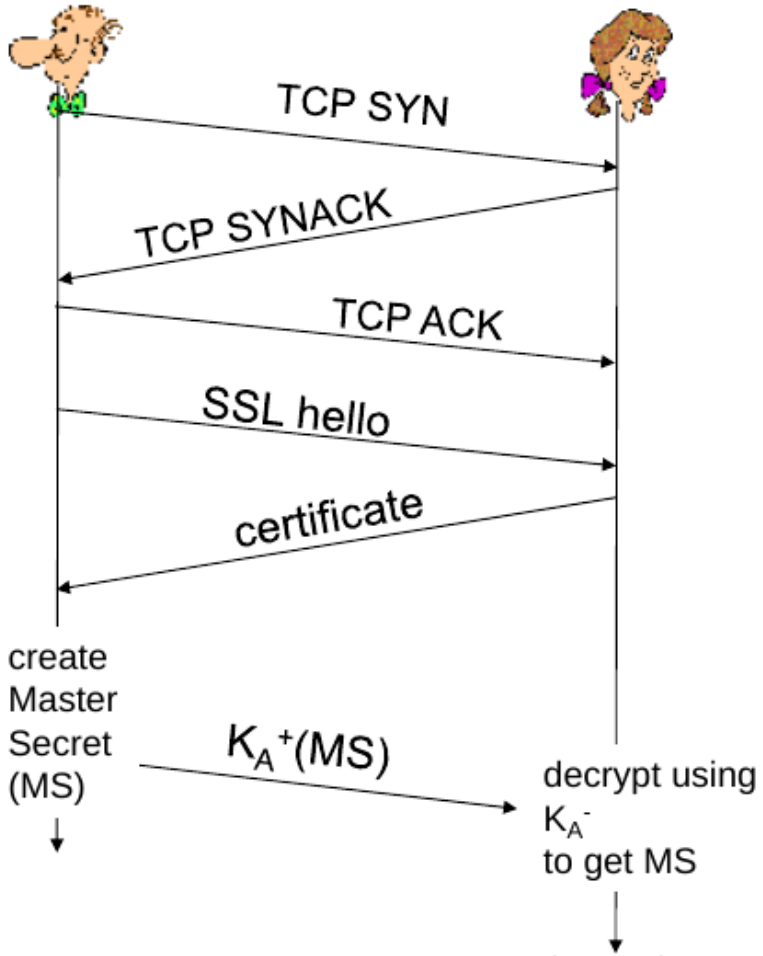


12.3 – Symmetric encryption

Explain how SSL works

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



12.3 – Symmetric encryption

Explain how SSL works

SSL: three phases

2. Key Derivation:

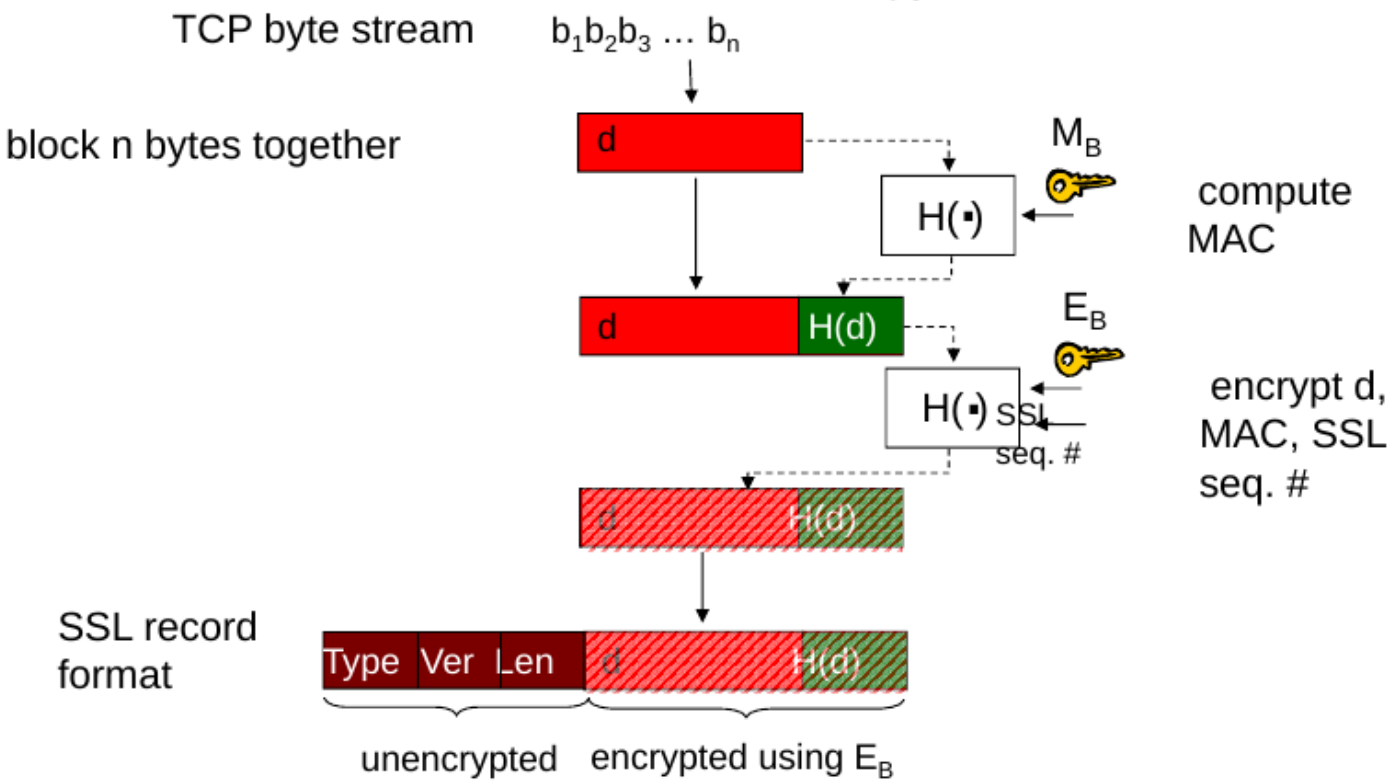
- Alice, Bob use shared secret (MS) to generate 4 keys:
  - E_B: Bob->Alice data encryption key
  - E_A: Alice->Bob data encryption key
  - M_B: Bob->Alice MAC key
  - M_A: Alice->Bob MAC key
- encryption and MAC algorithms negotiable between Bob, Alice
- why 4 keys?

12.3 – Symmetric encryption

Explain how SSL works

SSL: three phases

3. Data transfer



12.4

Q12.4 Discuss the Authentication header and the Encapsulation Security Payload protocol utilised in IPsec

12.4

Discuss the Authentication header and the Encapsulation Security Payload protocol utilised in 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

12.4

Discuss the Authentication header and the Encapsulation Security Payload protocol utilised in IPsec

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:

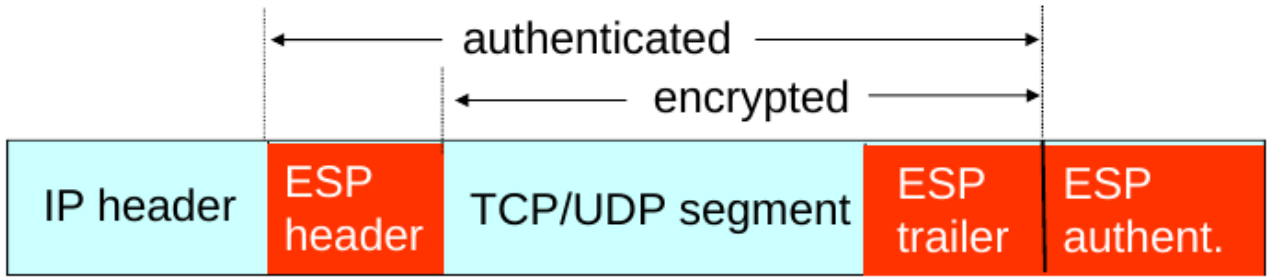
- connection identifier
- authentication data: source-signed message digest calculated over original IP datagram.
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)

12.4

Discuss the Authentication header and the Encapsulation Security Payload protocol utilised in IPsec

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.



12.5

Q12.5 Explain the encryption scheme used for WEP. What is the weakness in WEP that was used to break it?

12.5

Explain the encryption scheme used for WEP

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

12.5

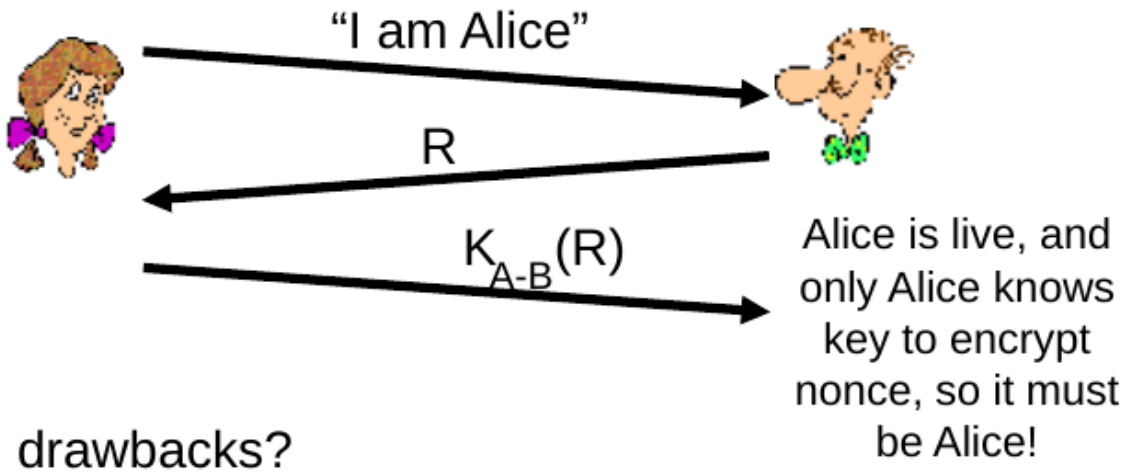
Explain the encryption scheme used for WEP

Authentication: yet another try

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



Failures, drawbacks?

12.5

Explain the encryption scheme used for WEP

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:

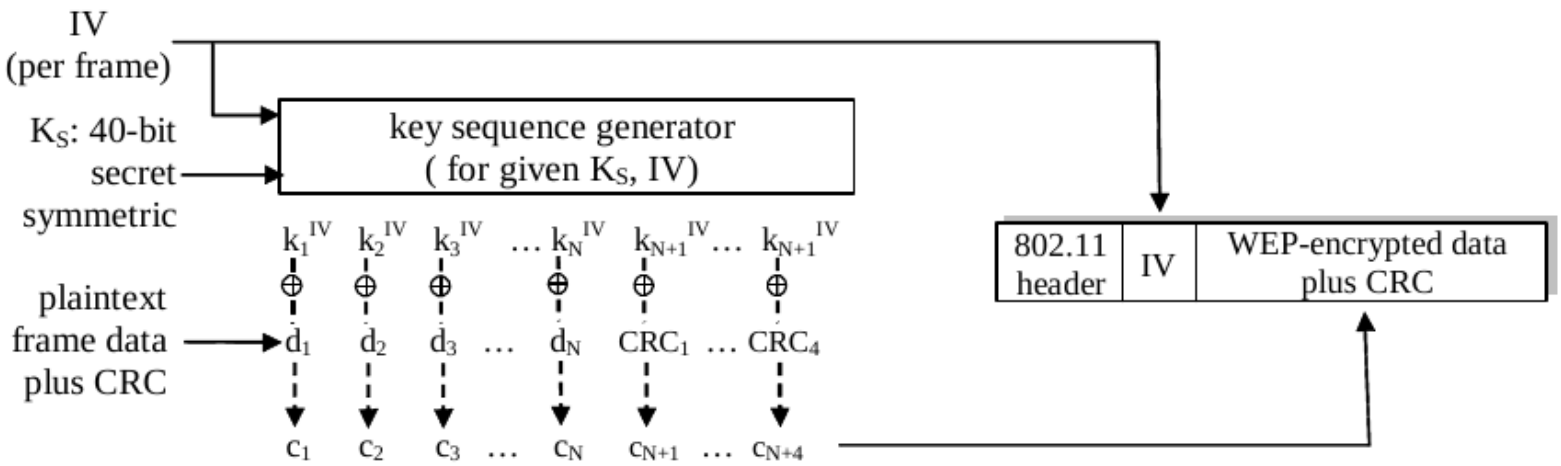
$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

12.5

Explain the encryption scheme used for WEP

802.11 WEP encryption



Sender-side WEP encryption

12.5

What is the weakness in WEP that was used to break it?

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 $d_1\ d_2\ d_3\ d_4\ \ldots$
  - Trudy sees: $c_i = d_i$ XOR k_i^{IV}
  - Trudy knows $c_i\ d_i$, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence $k_1^{IV}\ k_2^{IV}\ k_3^{IV}\ \ldots$
  - Next time IV is used, Trudy can decrypt!

12.6

Q12.6 Which are possible use cases for a firewall?

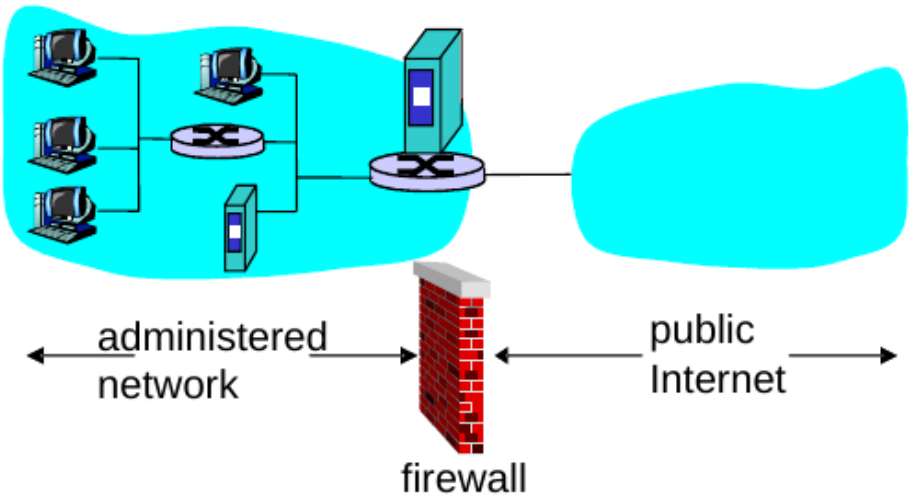
12.6

Which are possible use cases for a firewall?

Firewalls

firewall

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



12.6

Which are possible use cases for a firewall?

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)

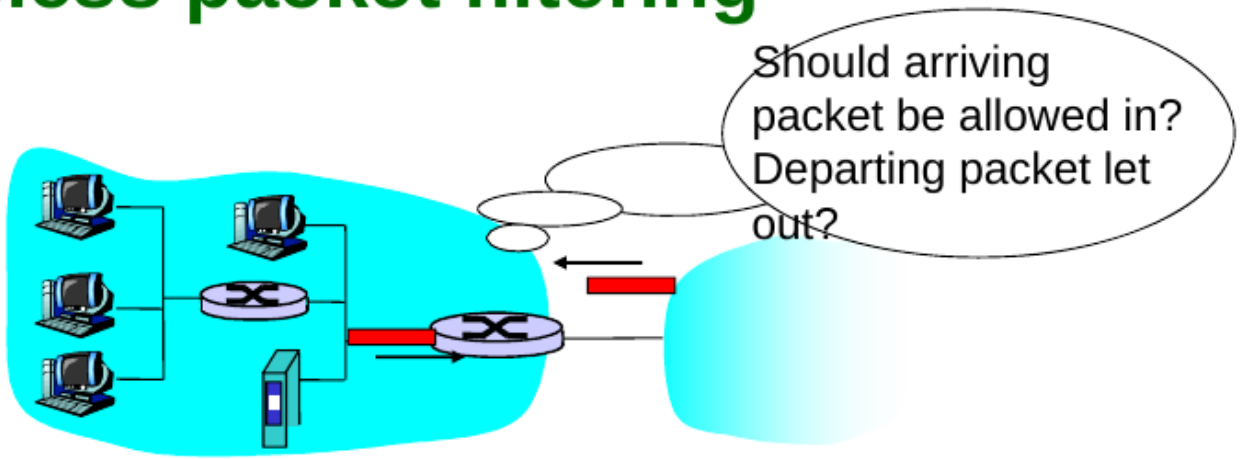
three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

12.6

Which are possible use cases for a firewall?

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

12.6

Which are possible use cases for a firewall?

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.

12.6

Which are possible use cases for a firewall?

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

12.6

Which are possible use cases for a firewall?

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

12.6

Which are possible use cases for a firewall?

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

12.6

Which are possible use cases for a firewall?

Stateful packet filtering

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

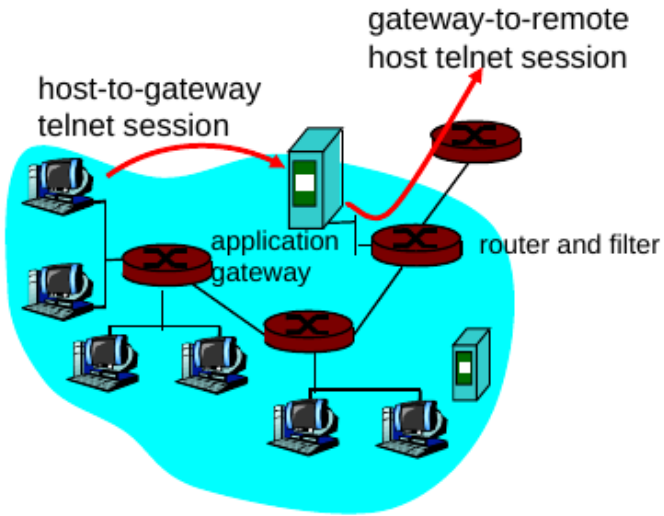
action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	>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

12.6

Which are possible use cases for a firewall?

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.

12.6

Which are possible use cases for a firewall?

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.

12.7

Q12.7 7. What are intrusion detection systems?

12.7

What are intrusion detection systems?

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

12.7

What are intrusion detection systems?

Intrusion detection systems

- multiple IDSs: different types of checking at different locations