Contents
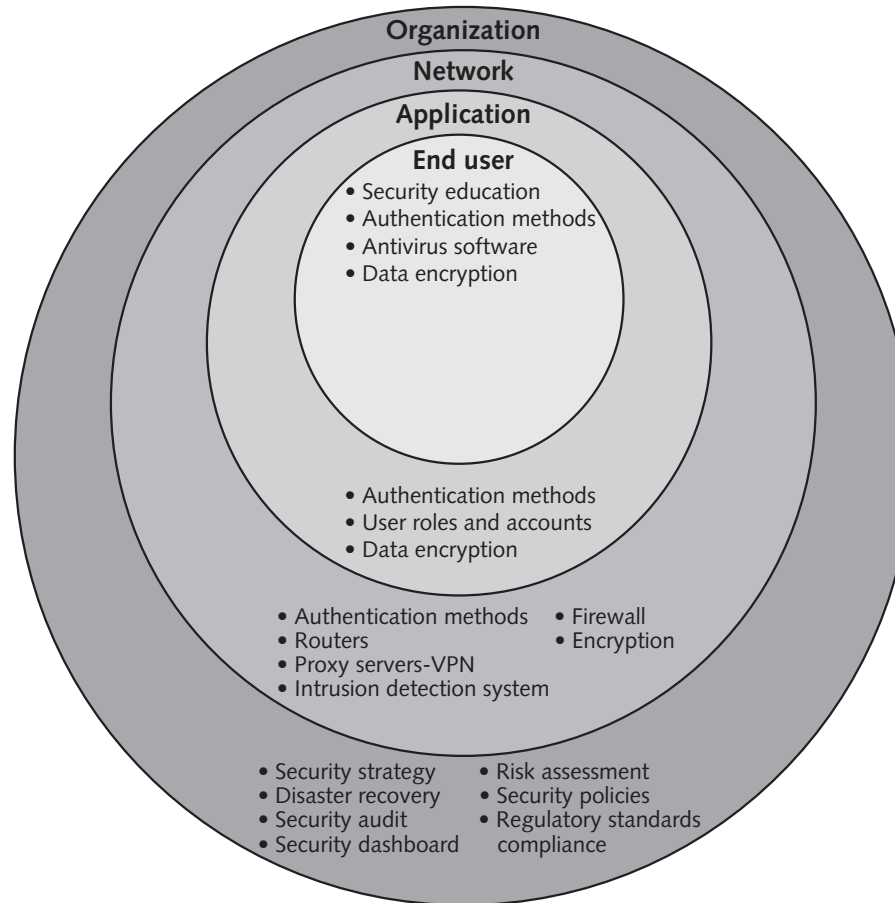
➢Implementing Trustworthy Computing

◇ CIA Security Triad

◇ Implementing CIA at the Organization Level

✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard

◇ Implementing CIA at the Network Level

✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS

◇ Implementing CIA at the Application Level

✦ User Roles and Accounts, Data Encryption

◇ Implementing CIA at the End-User Level

✦ Security Education, Authentication Methods, Antivirus Software

◇ Response to CyberAttack

Implementing CIA Security at the Organization, Network, Application, and End-user Levels

Organization

Network

Application

End user
- Security education
- Authentication methods
- Antivirus software
- Data encryption

- Authentication methods
- User roles and accounts
- Data encryption

- Authentication methods
- Routers
- Proxy servers-VPN
- Intrusion detection system
- Firewall
- Encryption

- Security strategy
- Disaster recovery
- Security audit
- Security dashboard
- Risk assessment
- Security policies
- Regulatory standards compliance

Main Goals in Network Security

- Unauthorized network access by a hacker or resentful employee can result in compromised sensitive data and severely degrade services, with a resulting negative impact on productivity and operational capability.

- Organizations must carefully manage the security of their networks and implement strong measures to ensure that sensitive data are not accessible to anyone who is not authorized to see it.

28

1. Authentication Methods

- Organization must authenticate users attempting to access the network by requiring them:

    - Enter a username and password, Inserting a smart card and entering the associated PIN, Providing a fingerprint, Voice pattern sample, or Retina scan.
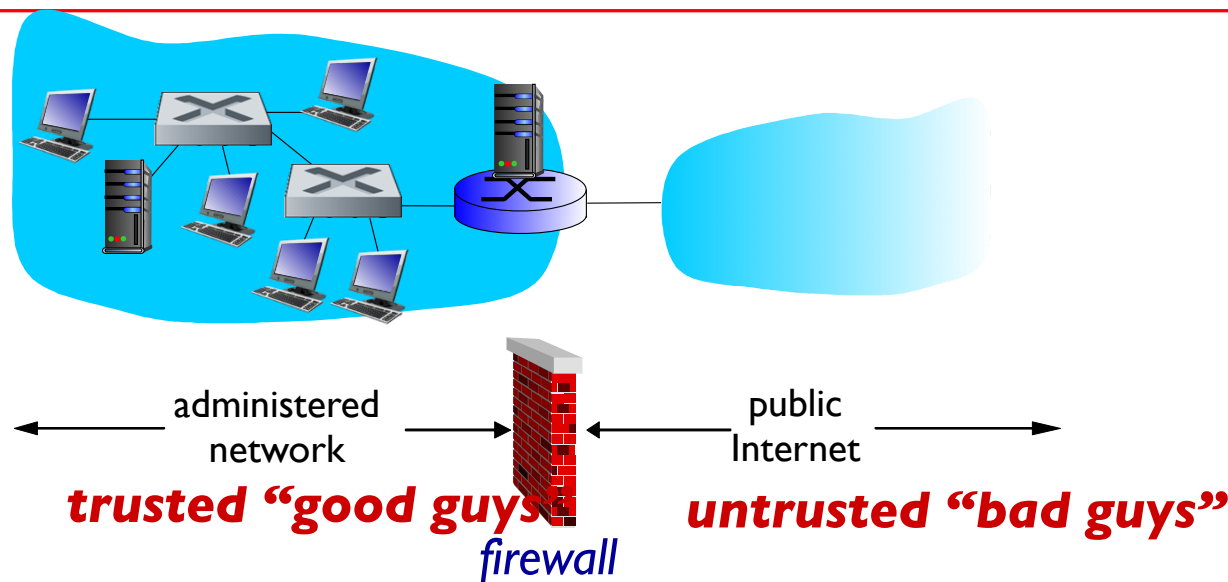
Biometric Authentication: Case Study

- MasterCard ID Checks
- Apple Pay Authentication Service

2. Firewalls

firewall

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

administered
network

public
Internet

trusted "good guys"   **untrusted "bad guys"**

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

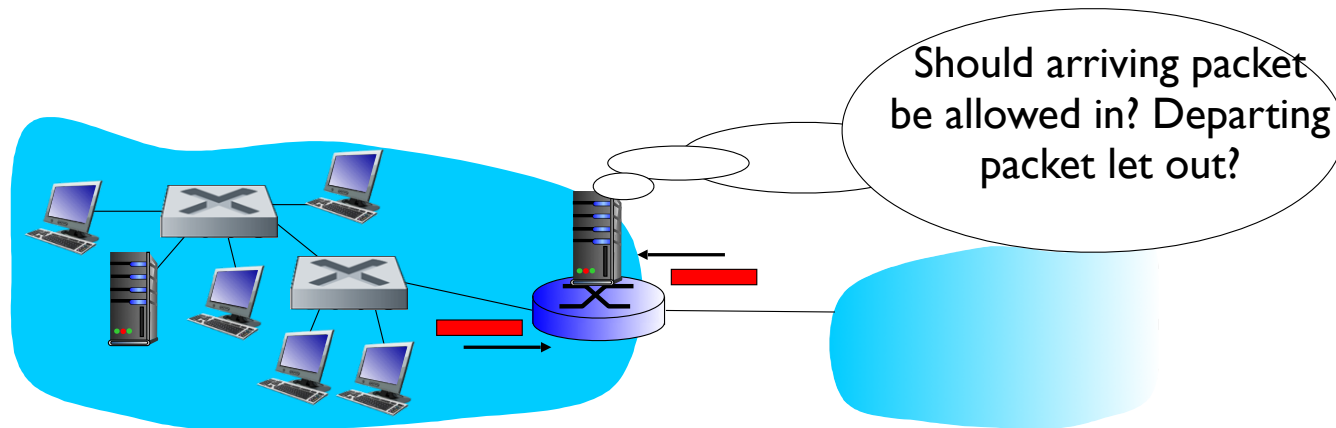- ❖ e.g., attacker replaces CIA's homepage with something else

Allow only authorized access to inside network

- ❖ set of authenticated users/hosts

Three types of firewalls:

1. Stateless packet filters
2. Stateful packet filters
3. 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

Stateless packet filtering: example

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

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 (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists (ACL)

❖ *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): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets
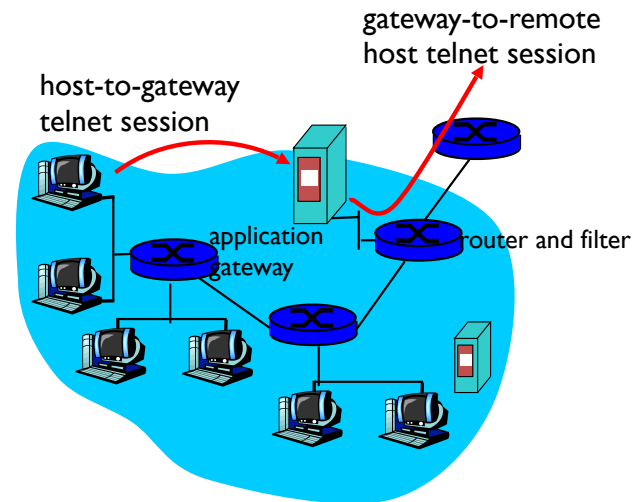
37

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 select internal users to telnet outside.**

host-to-gateway telnet session

gateway-to-remote host 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, 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