Computer and Network Security

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

Protocol Vulnerabilities and Firewalls (Pfleeger Ch. 9, KPS Ch. 12)

1 Network Protocol Vulnerabilities

1.1 ARP

1.1.1

- Spoofing
- Poisoning cache

1.2 IP

1.2.1

- loose source routing option - force inverse use
- trace route option
- ARC

1.3 ICMP

1.3.1 Attacks

- Redirection
- Destination unreachable
- Echo request - reconnaissance
- Echo request - smurf

1.4 RIP

1.4.1 Engineering

- Distance Vector algorithm
- no authentication

1.4.2 attacks

- False DV
- misinformation propagation

1.5 OSPF

1.5.1

- Weak or no authentication
- Link State (Link Update) algorithm

1.6 UDP

1.6.1 Design

- No sequence numbers
- Checksum optional

1.6.2 Attacks

- Source Spoofing
- Replay
- Content modification

1.7 TCP

1.7.1 Design

- 3-way Handshake
- RTT estimation
- Slow start

1.7.2 Attacks

- Sequence Number Attack
- Session hijacking
- Syn Attack

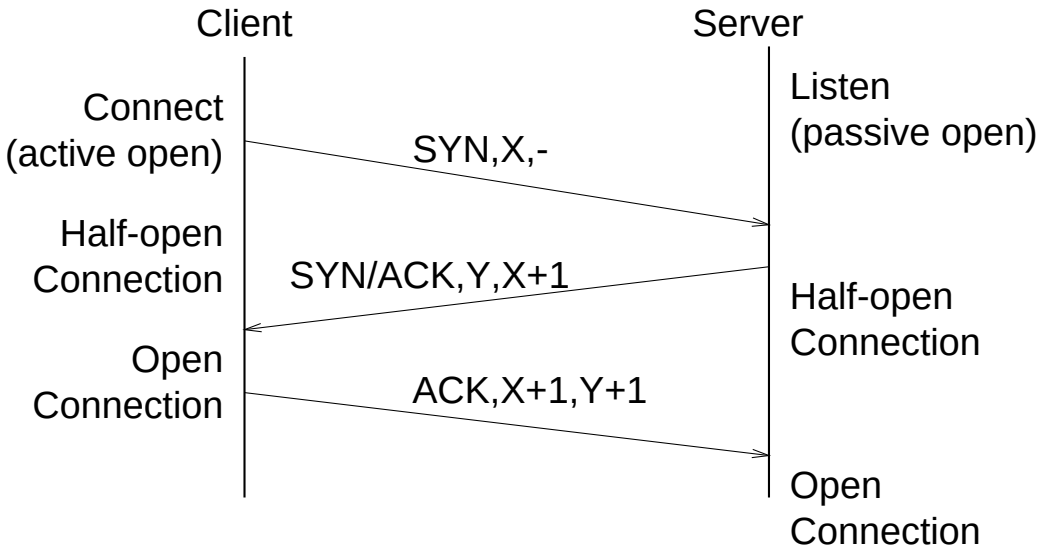

Figure 1: TCP Three-way Handshake

1.8 IGMP

1.8.1

- No ACKs
- No join authorization
- Firewall bypass via tunnel

1.9 DNS

1.9.1 Design

- Tree Structured Namespace
- Host name-to-IP address tree
- IP address-to-Host name tree (inverse queries)
- No enforce relationships between trees

1.9.2 Attacks

- Forged DNS entries
- Inverse tree entries - r commands
- Contamination of DNS cache
- Flood DNS server
- Common components in non-FQDN - trailer completion

1.10 SMTP

1.10.1

- From field not authenticated
- sendmail - run as root
- MIME executables
- MIME interpreted documents
- MIME buffer overflow

1.11 telnet

1.11.1

- password exposed in transit
- trojan horse telnet server

1.12 NTP

1.12.1

- Resetting time

1.13 finger

1.13.1

- finger attack (reconnaissance)
- finger buffer overflow

1.14 RPC and portmapper

1.14.1

- Null authentication for anonymous services
- "Authentication" consists of giving host-name, numeric UID, GID
- indirect calls

1.15 NIS

Yellow Pages service

- /etc/passwd file access
- host address table
- public & private key databases for secure RPC
- redirect to fraudulent backup NIS server
- bogus replies

1.16 NFS

1.16.1

- File handle = capability
- revocation impossible

1.17 TFTP

- misconfigured - anonymous overwrite of /etc/passwd, etc.
- misconfigured - anonymous read of /etc/passwd, etc.
- boot via broadcast TFTP - reconfigure

1.18 FTP

- run as root
- drop box
- misconfigured - file overwrite
- misconfigured - file read
- misconfigured - file permissions change

1.19 WWW

- Applets, code downloads without MIC or MAC
- Pointers with embedded file names (server threat)
- Anonymous FTP space shared with WWW - drop & run
- CGI scripts run as server, with powerful interpreters....

1.20 X11

- User host a server
- cookies

2 Firewalls

Barrier at internal/external network interface

- always invoked
- only authorized traffic may pass1
- tamper-proof

2.1 Policies

- All that is not expressly permitted is forbidden (German)
- All that is not expressly forbidden is permitted (French)
- Order counts in the rules

2.2 Techniques

1. Service control
2. Direction control
3. User control
4. Behavior control

2.3 Types of Firewalls

2.3.1 Packet Filters

- IP source, destination
- Protocol
- source, destination port (service)
- packet length
- packet flags
- priority
- fragmentation
- header options

2.3.2 Proxies

- application layer (or just below - SOCKS)
- interpret content

2.3.3 Guards

- Complex proxy
- history/state-based
- user ID
- user history
- traffic state
- traffic properties
- encrypting gateway

2.4 Caveats

- Minimal configuration
- Disable write access
- Rule order
- Only access to N/W

2.5 Firewall Configurations

- Filtering Router
- Filtering Router with Bastion Host
- Filtering Router/Bastion Host with Separate LAN
- Sacrificial lamb on LAN
- Dual Firewall/Bastion Host with DMZ

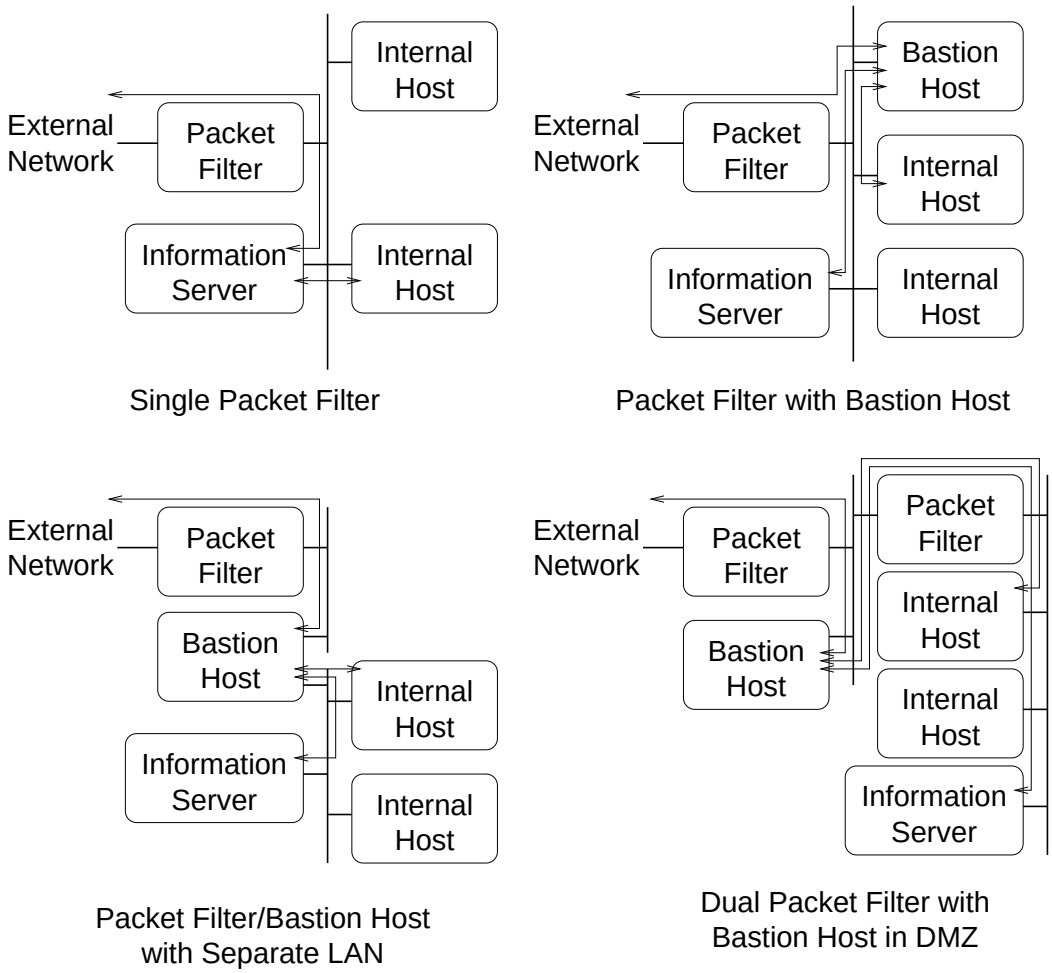

Figure 2: Firewall Configurations

2.6 Gemini Trusted Guard Base (GTGB)

- Gemsos A1 Operating System
- Dual mode (run and administer)
- Category label per subnet
- Cryptographic seal per subnet
- Cryptographic seal per VPN pair
- Source/dest IP/port filtering
- "Invisible" in topology

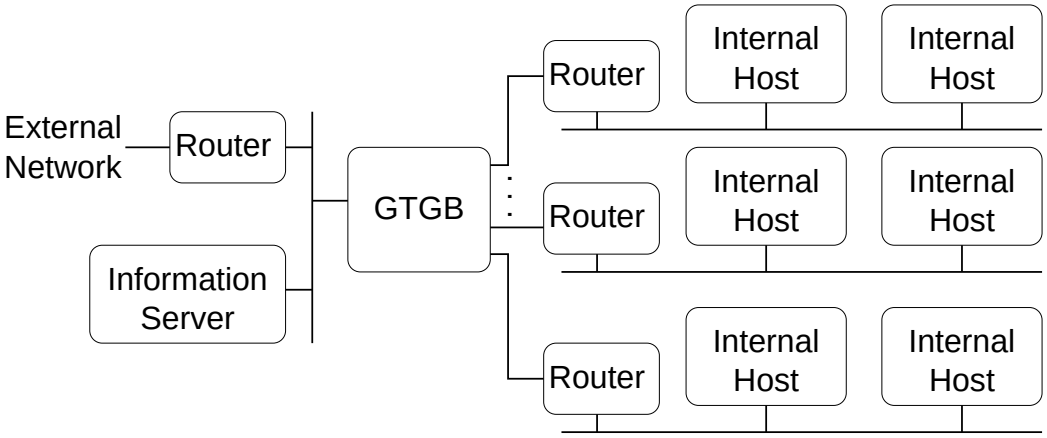

Figure 3: GTGB firewall

2.7 Firewall Capabilities

- Single choke point
- Simplifies security administration
- Part of defense in depth
- Audit/alarms
- Convenient for NAT, SNMP
- IPsec platform
- VPN
- Can prevent source addr spoofing
- Can prevent source routing attacks
- Can prevent smurf attack
- Can prevent tiny fragment attack

2.8 Firewall Limitations

- Can't protect if whole perimeter not firewalled
- Can't protect data outside perimeter
- Can't prevent some DoS attacks
- Can't prevent internal attacks
- Can't prevent tunnelling
- Can't prevent viruses
- likely target