INTERNET FUNDAMENTALS

LECTURE-26

Introduction to Network Security

OUTLINE

- Security Vulnerabilities
- DoS and D-DoS
- Firewalls
- Intrusion Detection Systems

SECURITY VULNERABILITIES

- Security Problems in the TCP/IP Protocol Suite – Steve Bellovin - 89
- Attacks on Different Layers
  - IP Attacks
  - ICMP Attacks
  - Routing Attacks
  - TCP Attacks
  - Application Layer Attacks

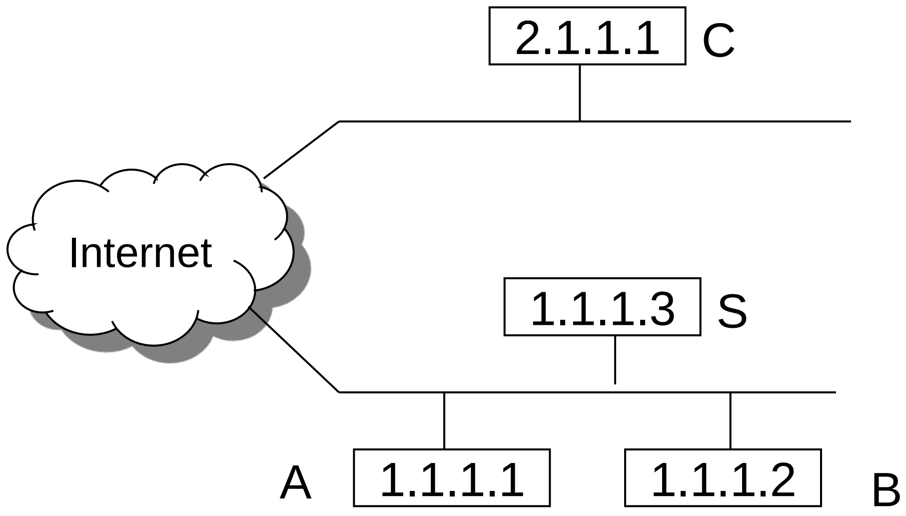
WHY?

- TCP/IP was designed for connectivity
  - Assumed to have lots of trust

- Host implementation vulnerabilities
  - Software “had/have/will have” bugs
  - Some elements in the specification were left to the implementers

SECURITY FLAWS IN IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, rhosts etc..)



•Can A claim it is B to the server S?

•ARP Spoofing

•Can C claim it is B to the server S?

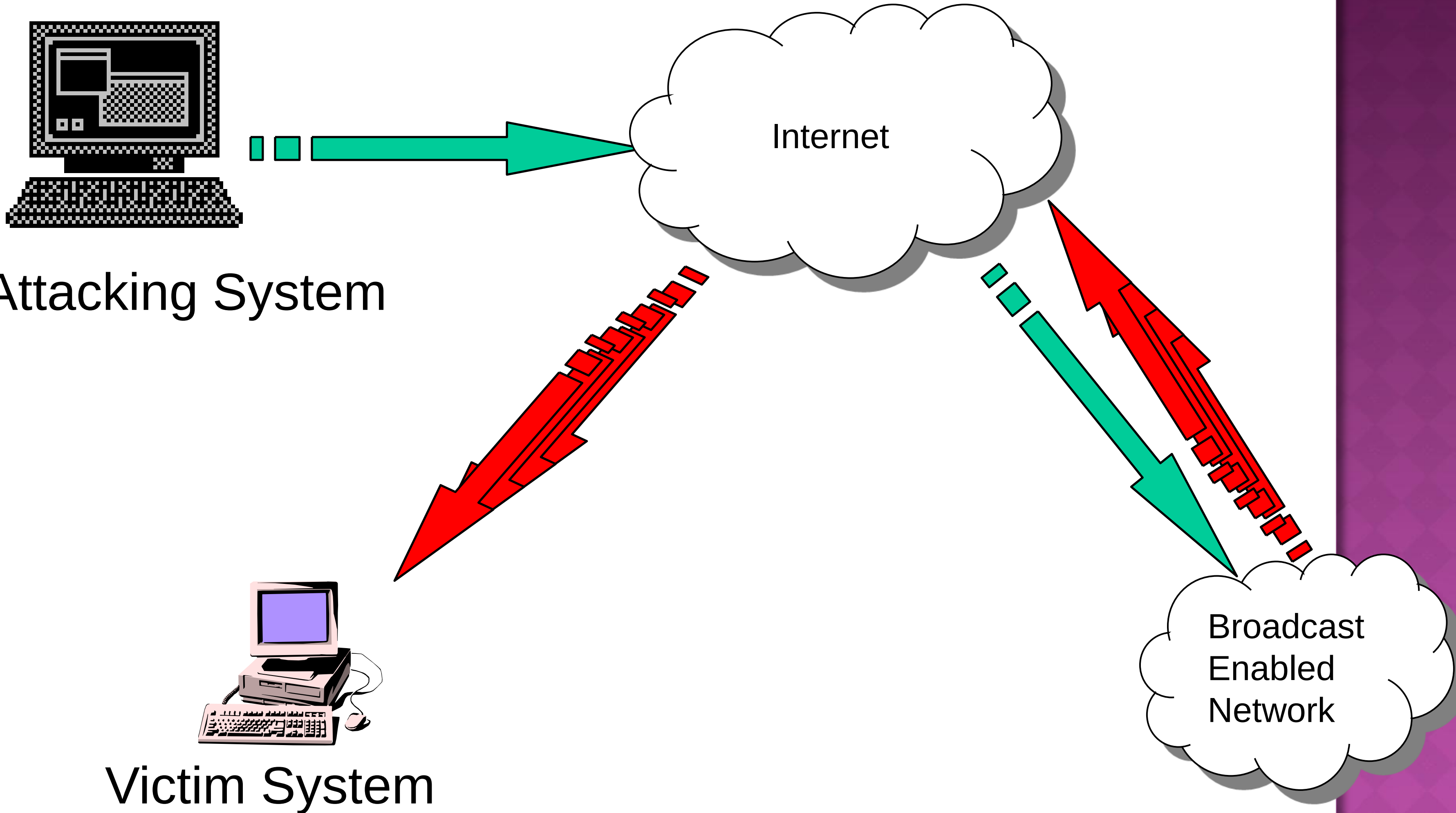
•Source Routing

SECURITY FLAWS IN IP

- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive

- Traffic amplification attack
  - IP allows broadcast destination
  - Problems?

PING FLOOD


Internet
Attacking System
Victim System
Broadcast
Enabled
Network

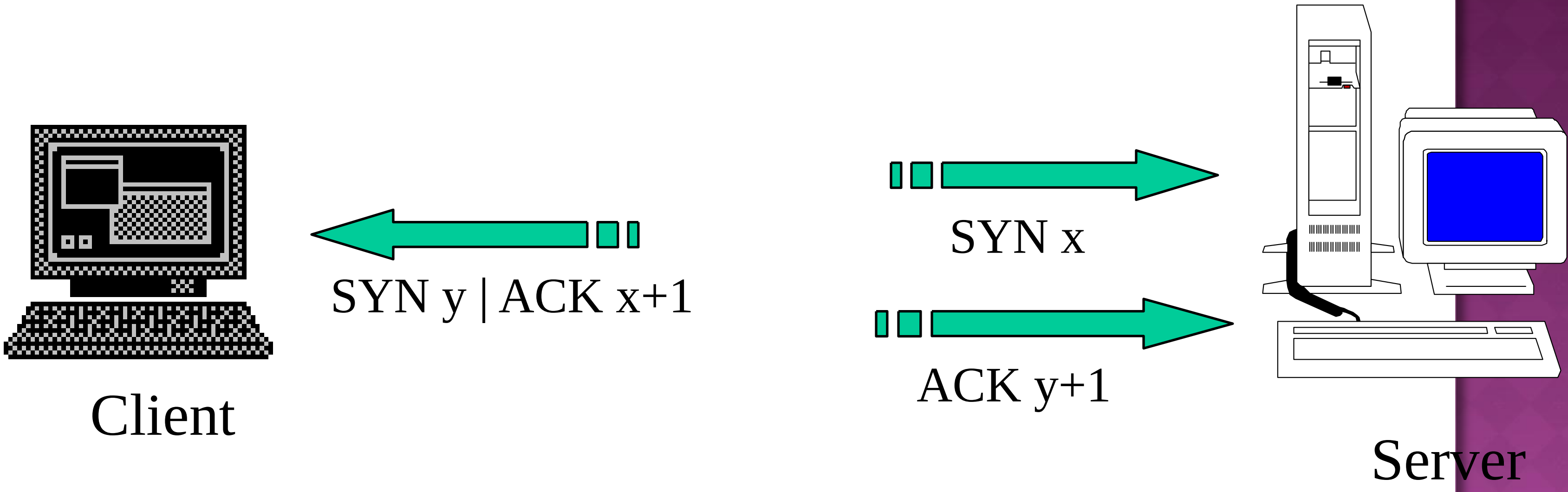
ICMP ATTACKS

- No authentication
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - Man in the middle attack, sniffing
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
- Many more…
  - http://www.sans.org/rr/whitepapers/threats/477.php

ROUTING ATTACKS

- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP
  - ASes can announce arbitrary prefix
  - ASes can alter path

TCP Attacks



Issues?

- Server needs to keep waiting for ACK y+1
- Server recognizes Client based on IP address/port and y+1

TCP LAYER ATTACKS

- TCP SYN Flooding
  - Exploit state allocated at server after initial SYN packet
  - Send a SYN and don’t reply with ACK
  - Server will wait for 511 seconds for ACK
  - Finite queue size for incomplete connections (1024)
  - Once the queue is full it doesn’t accept requests

TCP Layer Attacks

- TCP Session Hijack
  - When is a TCP packet valid?
    - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it
      - Many earlier systems had predictable ISN
  - Inject arbitrary data to the connection

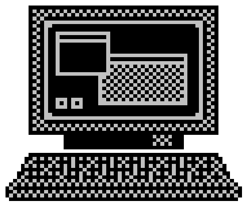
TCP LAYER ATTACKS

- TCP Session Poisoning
  - Send RST packet
    - Will tear down connection
  - Do you have to guess the exact sequence number?
    - Anywhere in window is fine
    - For 64k window it takes 64k packets to reset
    - About 15 seconds for a T1

APPLICATION LAYER ATTACKS

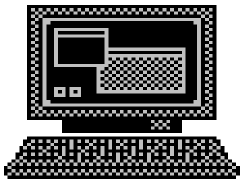
- Applications don’t authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

AN EXAMPLE



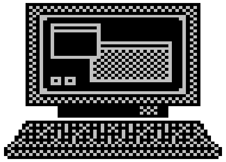
Shimomura (S)

Finger
Showmount -e
SYN



Trusted (T)

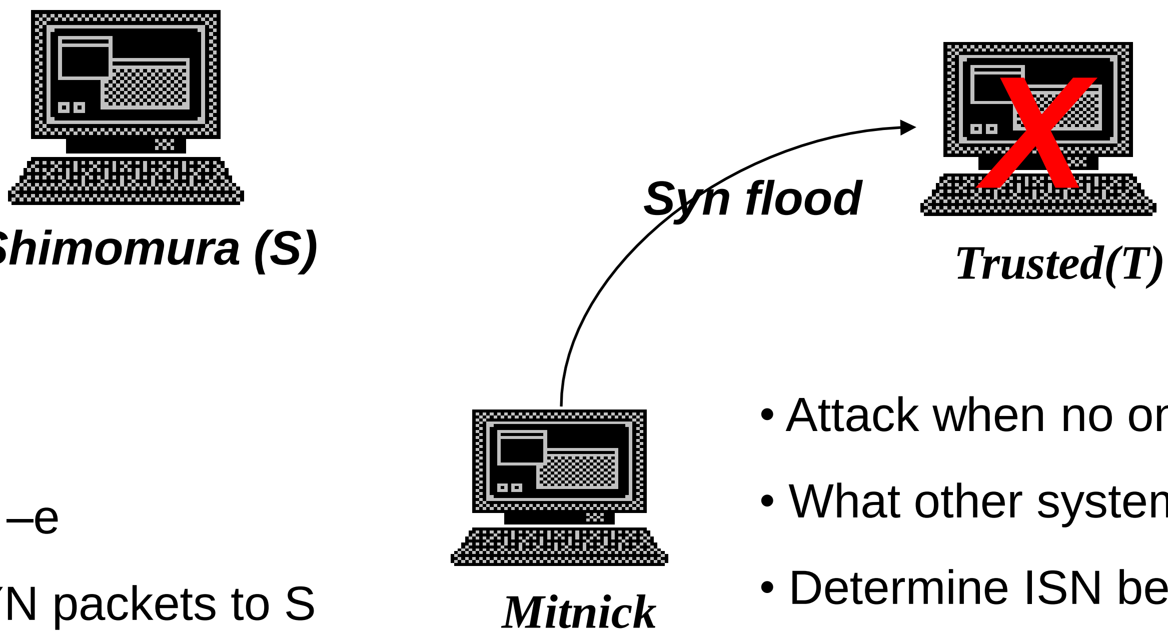
- Finger @S
- showmount –e
- Send 20 SYN packets to S



Mitnick

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior

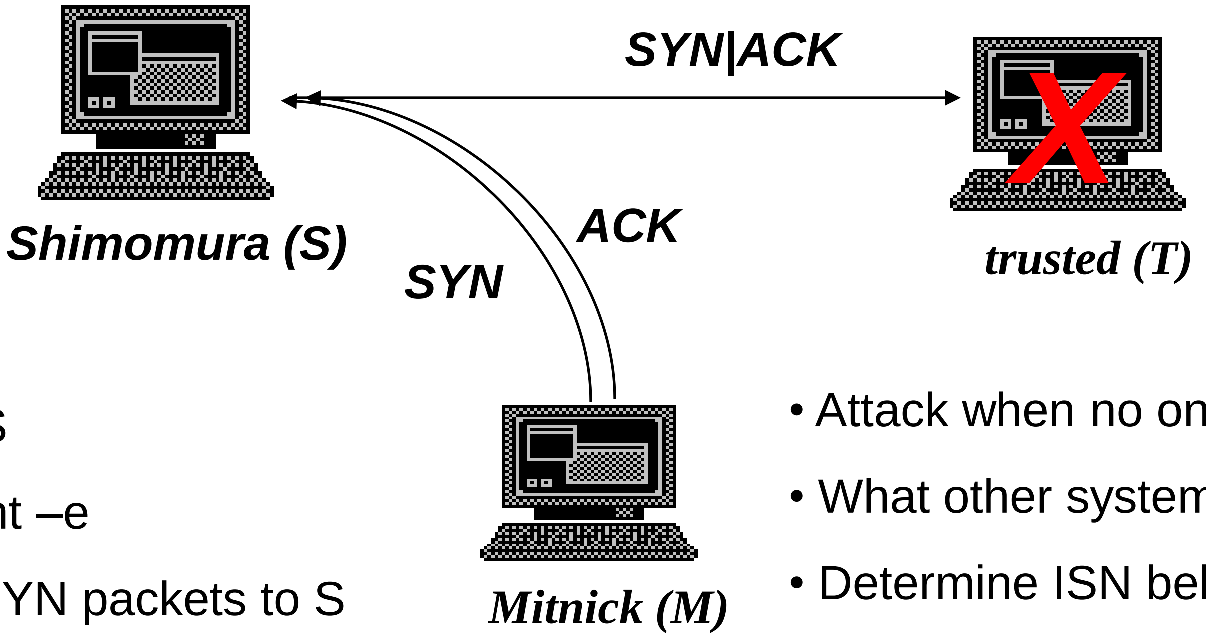
AN EXAMPLE



- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won’t respond to packets

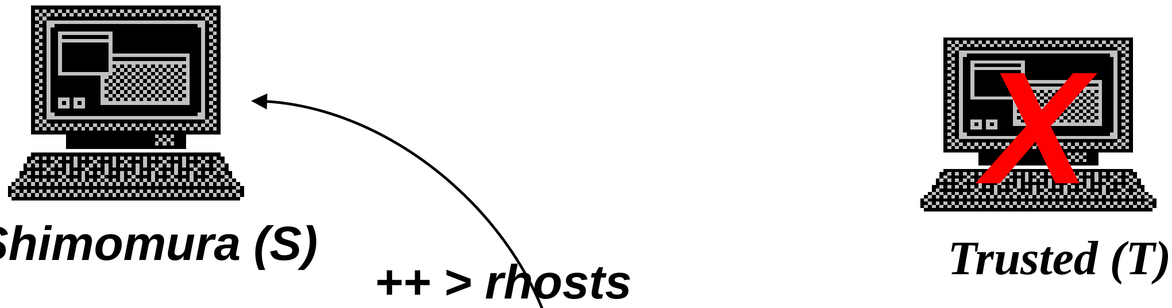
AN EXAMPLE



- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T
- Send SYN to S spoofing as T
- Send ACK to S with a guessed number

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won't respond to packets
- S assumes that it has a session with T

AN EXAMPLE



- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T
- Send SYN to S spoofing as T
- Send ACK to S with a guessed number
- Send “echo + + > ~/.rhosts”

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won’t respond to packets
- S assumes that it has a session with T
- Give permission to anyone from anywhere

OUTLINE

- Security Vulnerabilities
- DoS and D-DoS
- Firewalls
- Intrusion Detection Systems

You are here

DENIAL OF SERVICE

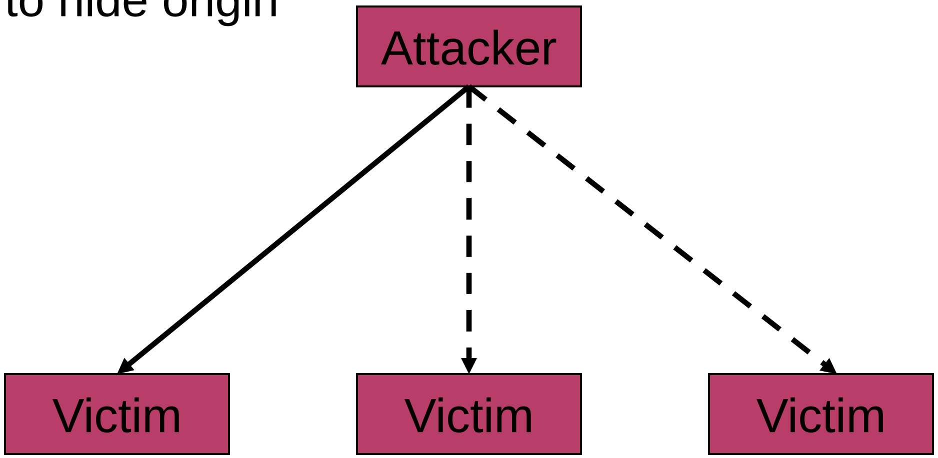
- Objective → make a service unusable, usually by overloading the server or network
- Consume host resources
  - TCP SYN floods
  - ICMP ECHO (ping) floods
- Consume bandwidth
  - UDP floods
  - ICMP floods

Denial of Service

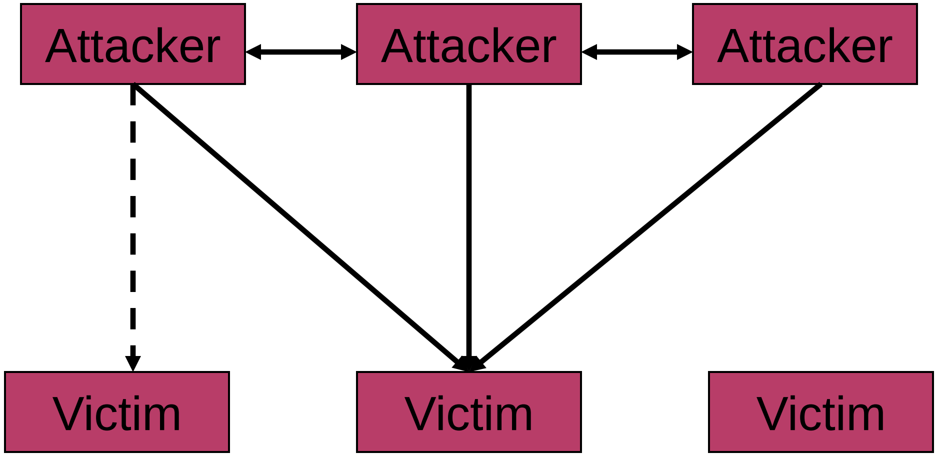
- Crashing the victim
  - Ping-of-Death
  - TCP options (unused, or used incorrectly)
- Forcing more computation
  - Taking long path in processing of packets

SIMPLE DOS

- The Attacker usually spoofed source address to hide origin
- Easy to block

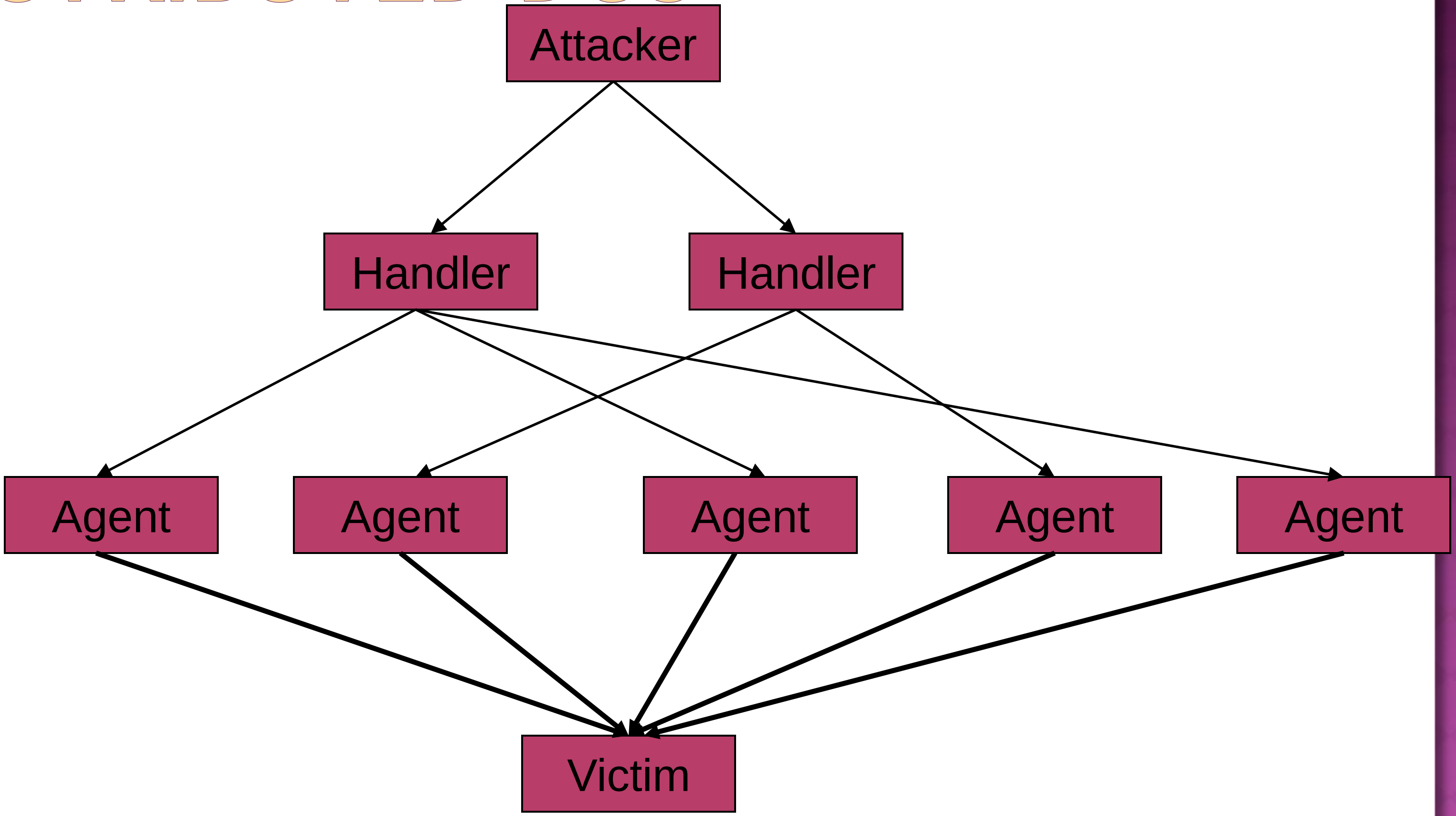


COORDINATED DOS



- The first attacker attacks a different victim to cover up the real attack
- The Attacker usually spoofed source address to hide origin
- Harder to deal with

DISTRIBUTED DOS



DISTRIBUTED DOS

- The handlers are usually very high volume servers
  - Easy to hide the attack packets
- The agents are usually home users with DSL/Cable
  - Already infected and the agent installed
- Very difficult to track down the attacker
- How to differentiate between DDoS and Flash Crowd?
  - Flash Crowd → Many clients using a service legimitaly
    - Slashdot Effect
    - Victoria Secret Webcast
  - Generally the flash crowd disappears when the network is flooded
  - Sources in flash crowd are clustered

OUTLINE

- Security Vulnerabilities
- DoS and D-DoS
- Firewalls
- Intrusion Detection Systems

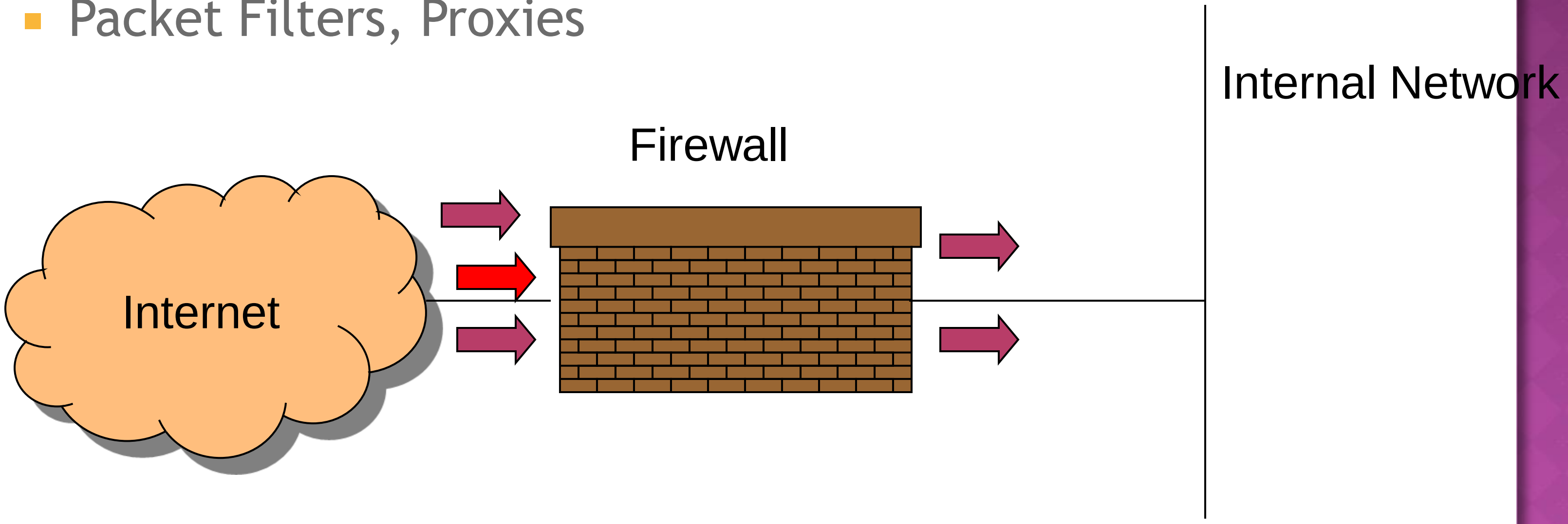
You are here

Firewalls

- Lots of vulnerabilities on hosts in network
- Users don't keep systems up to date
  - Lots of patches
  - Lots of exploits in wild (no patch for them)
- Solution?
  - Limit access to the network
  - Put firewalls across the perimeter of the network

FIREWALLS (CONTD…)

- Firewall inspects traffic through it
- Allows traffic specified in the policy
- Drops everything else
- Two Types
  - Packet Filters, Proxies



PACKET FILTERS

- Packet filter selectively passes packets from one network interface to another
- Usually done within a router between external and internal networks
  - screening router
- Can be done by a dedicated network element
  - packet filtering bridge
  - harder to detect and attack than screening routers

PACKET FILTERS CONTD.

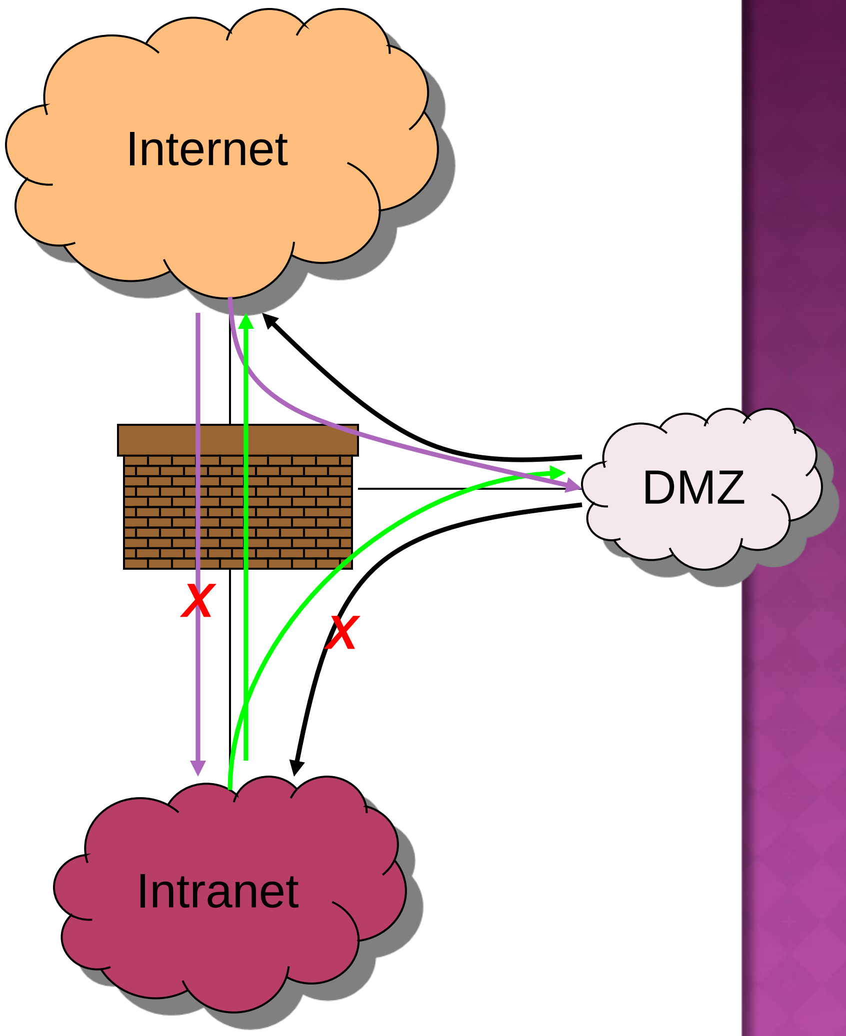
- **Data Available**
  - IP source and destination addresses
  - Transport protocol (TCP, UDP, or ICMP)
  - TCP/UDP source and destination ports
  - ICMP message type
  - Packet options (Fragment Size etc.)
- **Actions Available**
  - Allow the packet to go through
  - Drop the packet (Notify Sender/Drop Silently)
  - Alter the packet (NAT?)
  - Log information about the packet

PACKET FILTERS CONTD.

- Example filters
  - Block all packets from outside except for SMTP servers
  - Block all traffic to a list of domains
  - Block all connections from a specified domain

TYPICAL FIREWALL CONFIGURATION

- Internal hosts can access DMZ and Internet
- External hosts can access DMZ only, not Intranet
- DMZ hosts can access Internet only
- Advantages?
    - If a service gets compromised in DMZ it cannot affect internal hosts

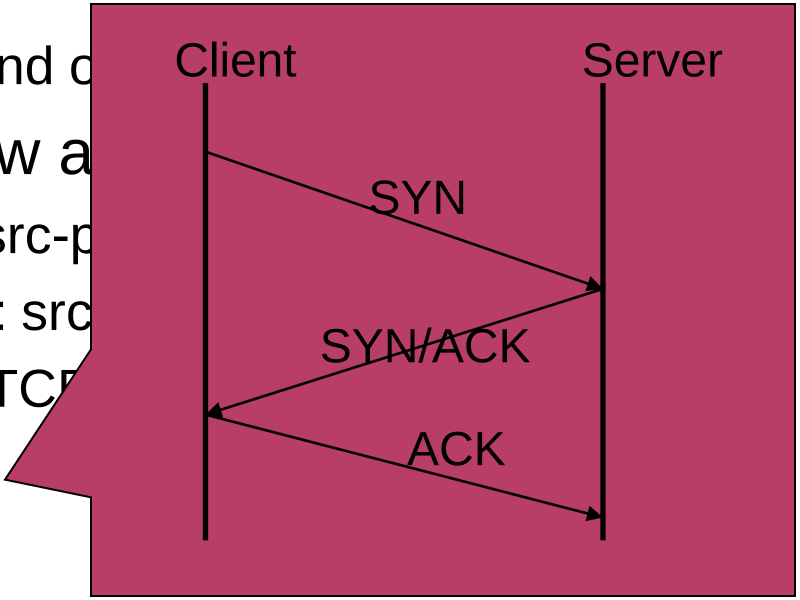


EXAMPLE FIREWALL RULES

- Stateless packet filtering firewall
- Rule → (Condition, Action)
- Rules are processed in top-down order
  - If a condition satisfied – action is taken

Sample Firewall Rule

- Allow SSH from external hosts to internal hosts
  - Two rules
    - Inbound and o
  - How to know a
    - Inbound: src-p
    - Outbound: src
    - Protocol=TCP
  - Ack Set?
  - Problems?



Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
SSH-1	In	Ext	> 1023	Int	22	TCP	Any	Allow
SSH-2	Out	Int	22	Ext	> 1023	TCP	Yes	Alow

DEFAULT FIREWALL RULES

- Egress Filtering
  - Outbound traffic from external address → Drop
  - Benefits?
- Ingress Filtering
  - Inbound Traffic from internal address → Drop
  - Benefits?
- Default Deny
  - Why?

Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
Egress	Out	Ext	Any	Ext	Any	Any	Any	Deny
Ingress	In	Int	Any	Int	Any	Any	Any	Deny
Default	Any	Any	Any	Any	Any	Any	Any	Deny

PACKET FILTERS

- Advantages
  - Transparent to application/user
  - Simple packet filters can be efficient
- Disadvantages
  - Usually fail open
  - Very hard to configure the rules
  - Doesn't have enough information to take actions
    - Does port 22 always mean SSH?
    - Who is the user accessing the SSH?

ALTERNATIVES

- Stateful packet filters
  - Keep the connection states
  - Easier to specify rules
  - More popular
  - Problems?
    - State explosion
    - State for UDP/ICMP?

Alternatives

- Proxy Firewalls
  - Two connections instead of one
  - Either at transport level
    - SOCKS proxy
  - Or at application level
    - HTTP proxy
- Requires applications (or dynamically linked libraries) to be modified to use the proxy

PROXY FIREWALL

- Data Available
  - Application level information
  - User information
- Advantages?
  - Better policy enforcement
  - Better logging
  - Fail closed
- Disadvantages?
  - Doesn’t perform as well
  - One proxy for each application
  - Client modification

OUTLINE

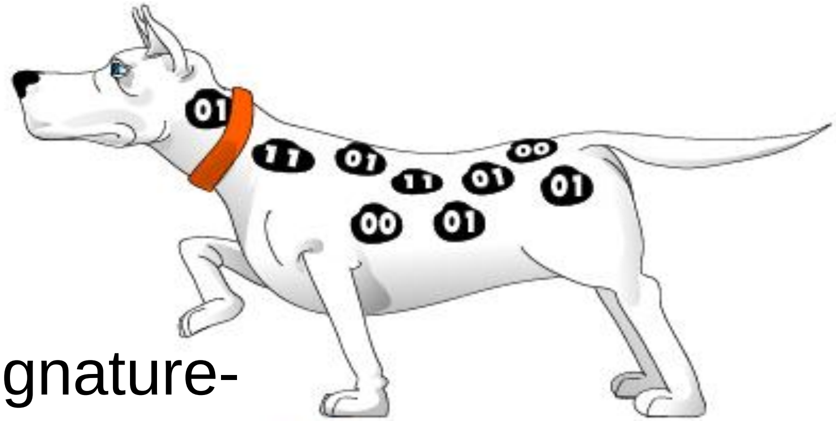
- Security Vulnerabilities
- DoS and DDoS
- Firewalls
- Intrusion Detection Systems

You are here

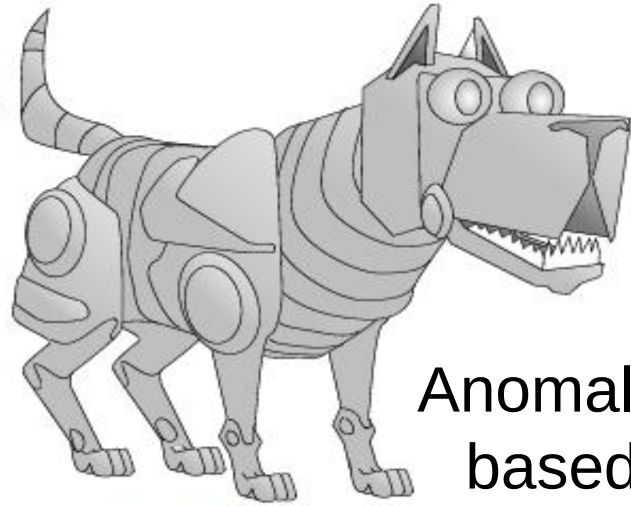
INTRUSION DETECTION SYSTEMS

- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks
  - CodeReds on IIS
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

TYPES OF IDS



Signature-based



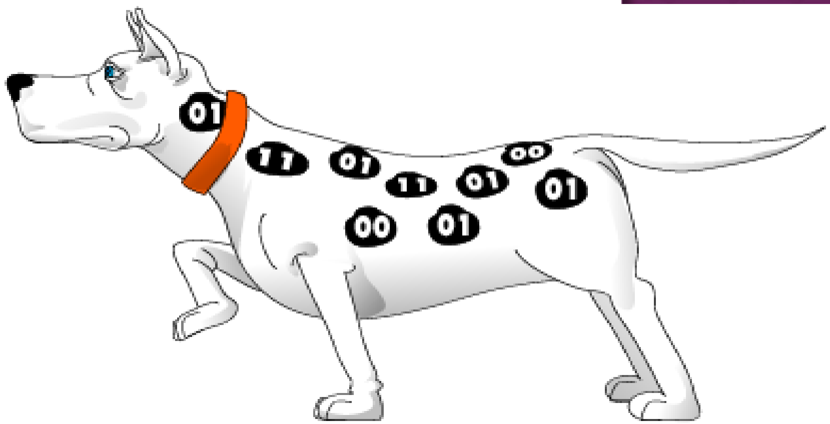
Anomaly-based

Host-based

Network-based

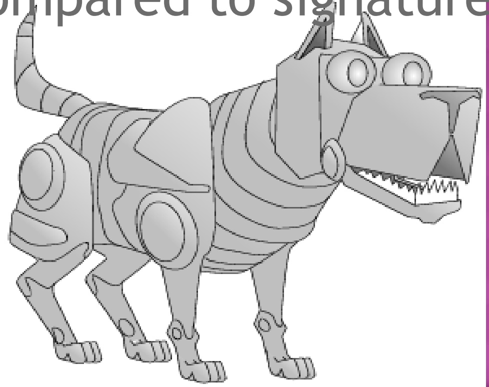
SIGNATURE-BASED IDS

- Characteristics
  - Uses known pattern matching to signify attack
- Advantages?
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- Disadvantages?
  - Cannot detect attacks for which it has no signature



ANOMALY-BASED IDS

- Characteristics
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- Advantages?
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- Disadvantages?
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts

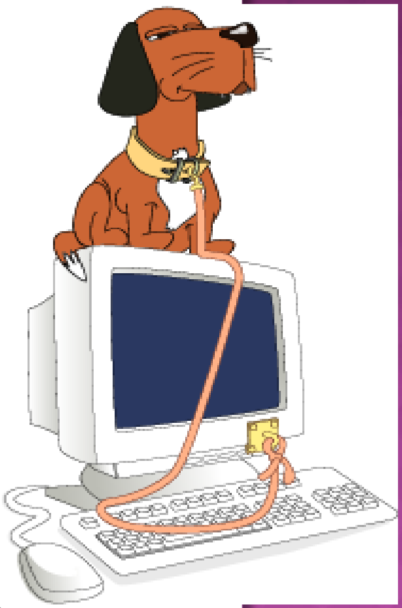


NETWORK-BASED IDS

- Characteristics
  - NIDS examine raw packets in the network passively and triggers alerts
- Advantages?
  - Easy deployment
  - Unobtrusive
  - Difficult to evade if done at low level of network operation
- Disadvantages?
  - Fail Open
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior

HOST-BASED IDS

- Characteristics
  - Runs on single host
  - Can analyze audit-trails, logs, integrity of files and directories, etc.
- Advantages
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- Disadvantages
  - Deployment is expensive
  - What happens when host get compromised?



SUMMARY

- TCP/IP security vulnerabilities
  - Spoofing
  - Flooding attacks
  - TCP session poisoning
- DOS and D-DOS
- Firewalls
  - Packet Filters
  - Proxy
- IDS
  - Signature and Anomaly IDS
  - NIDS and HIDS