Introduction to Network Security

Part I

Outline

- Security Vulnerabilities
- DoS and D-DoS
- Firewalls

Security Vulnerabilities

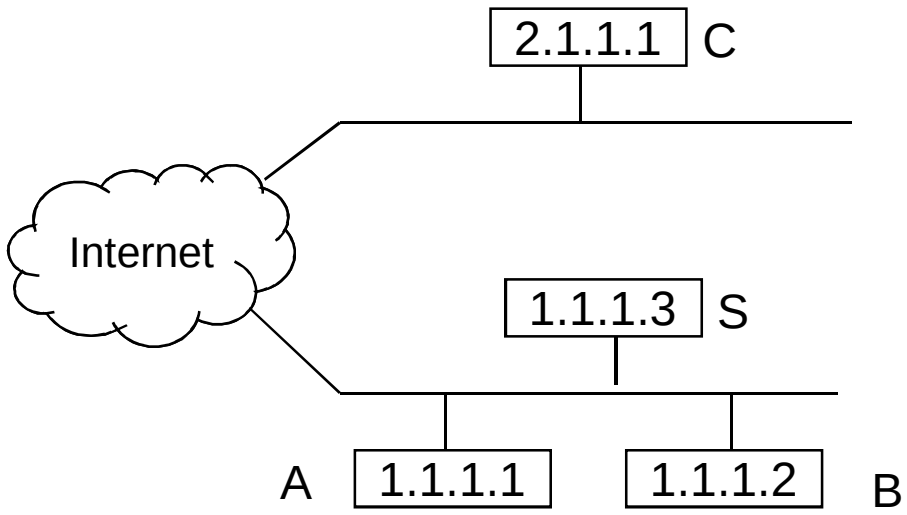
- Security Problems in the TCP/IP Protocol Suite
- Attacks on Different Layers
  - IP Attacks
  - ICMP Attacks
  - Routing Attacks
  - TCP Attacks
  - Application Layer Attacks

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?

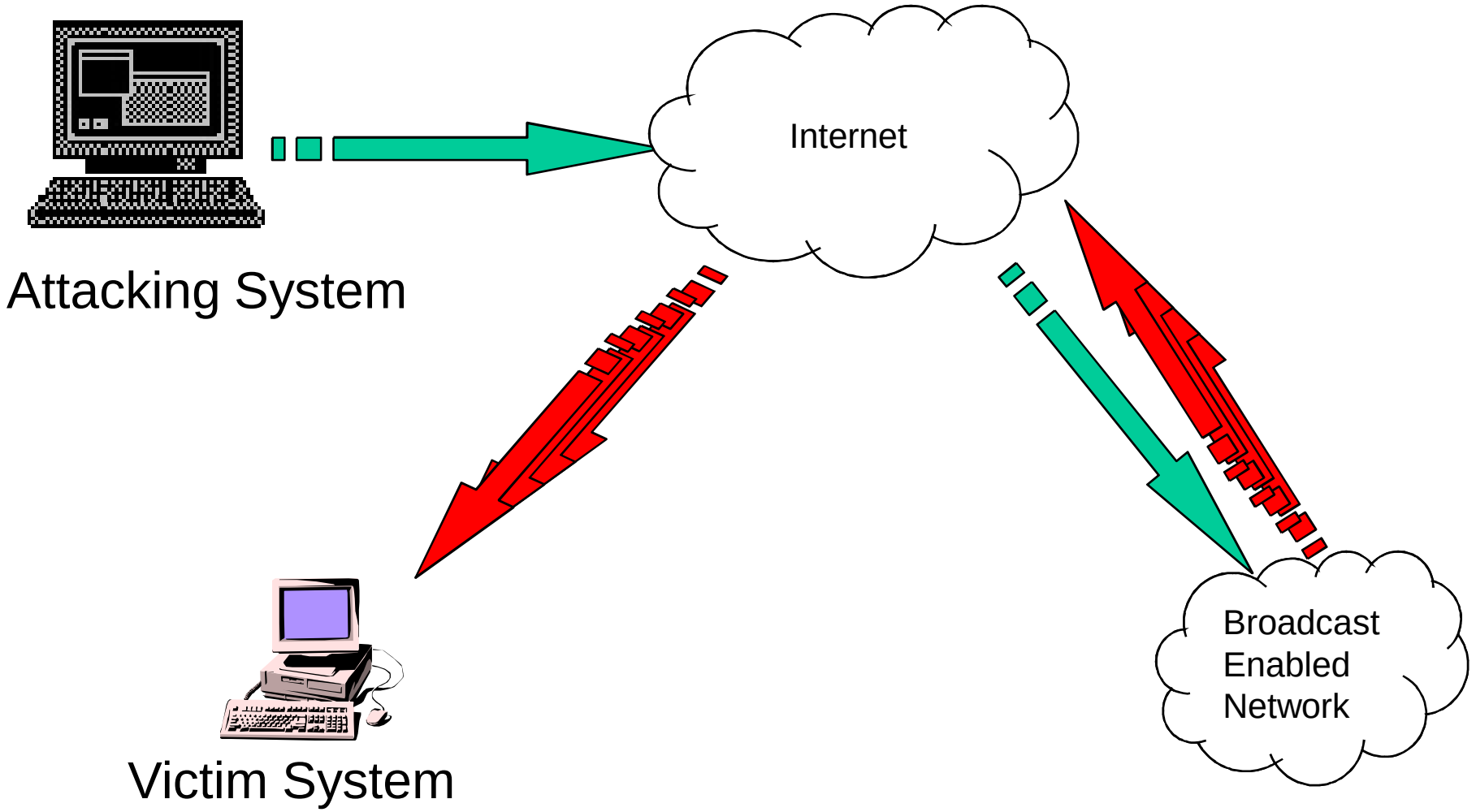
•Source Routing

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

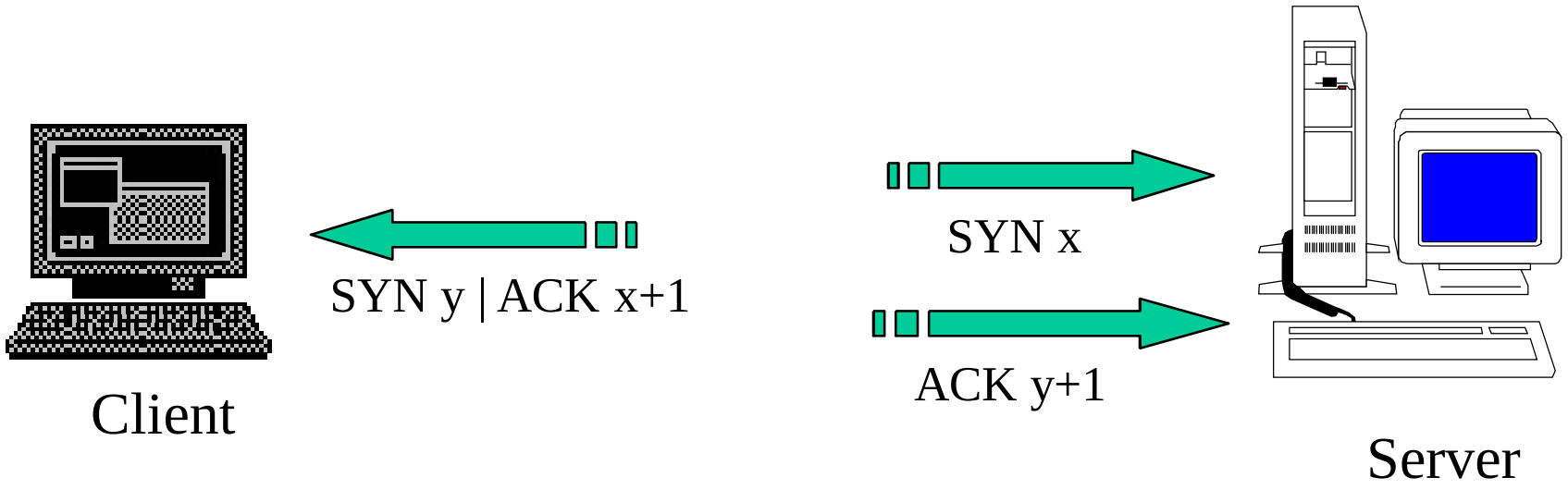
ICMP Attacks

- 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

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

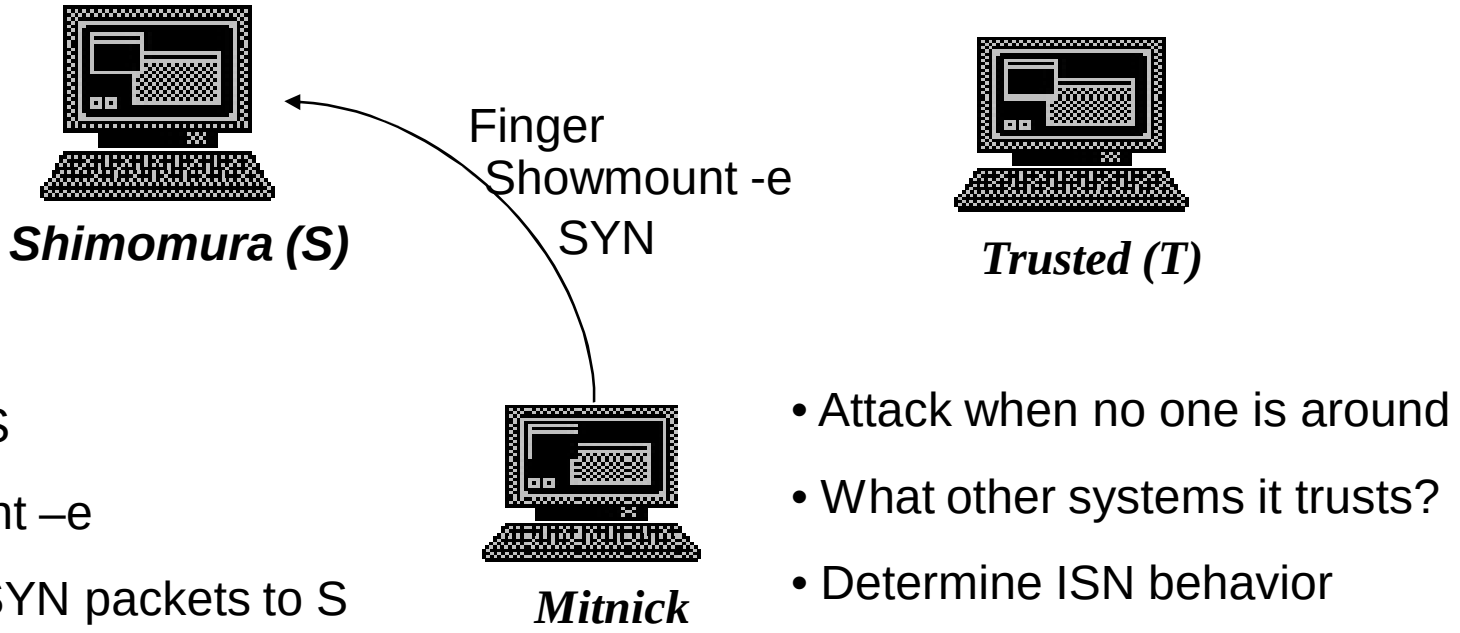
TCP Layer Attacks

- 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

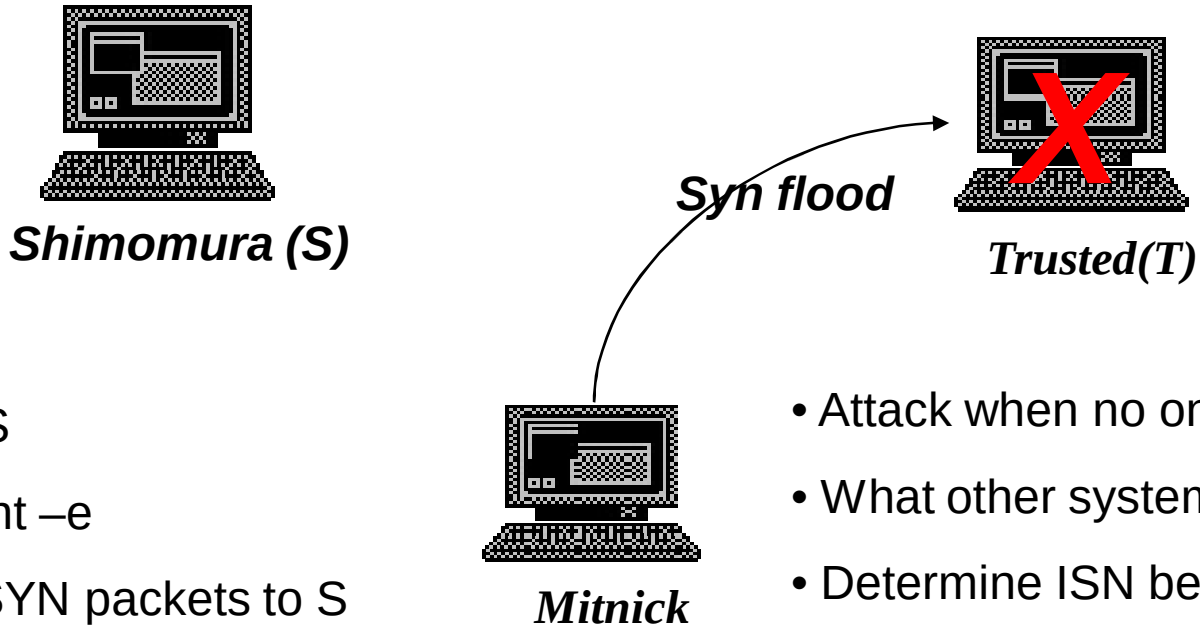
An Example



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

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

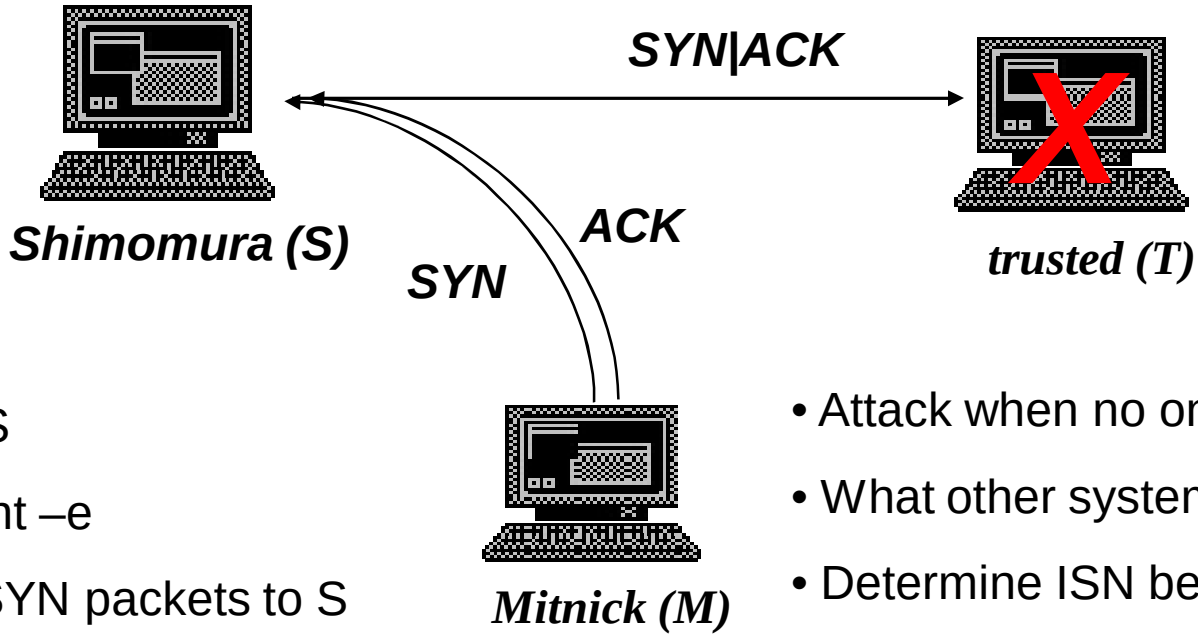
An Example



- 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

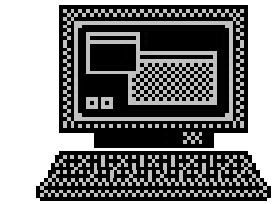
An Example



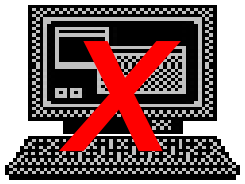
- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T
- Send SYN to S spoofing as T
- Send ACK to S with a guessed number

- 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

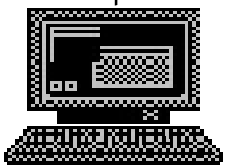


Shimomura (S)



Trusted (T)

++ > rhosts



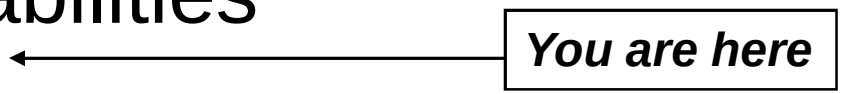
Mitnick

- 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



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

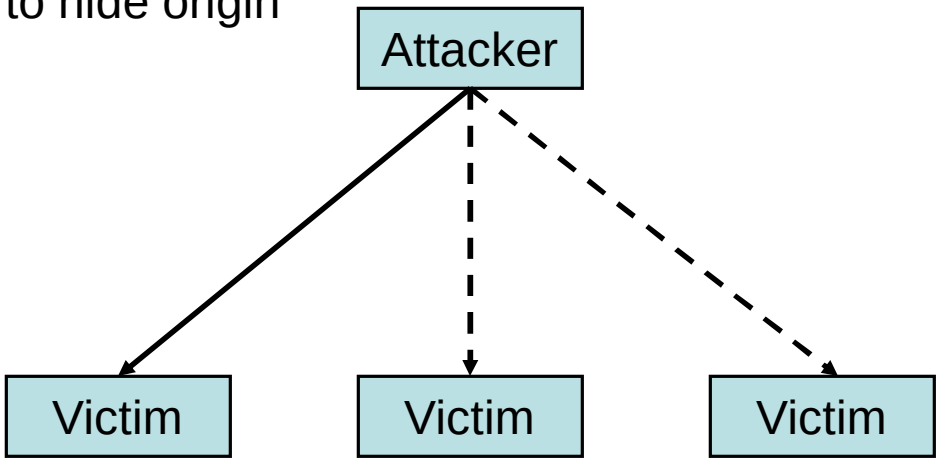
- Consume bandwidth
  - UDP floods
  - ICMP floods

Denial of Service

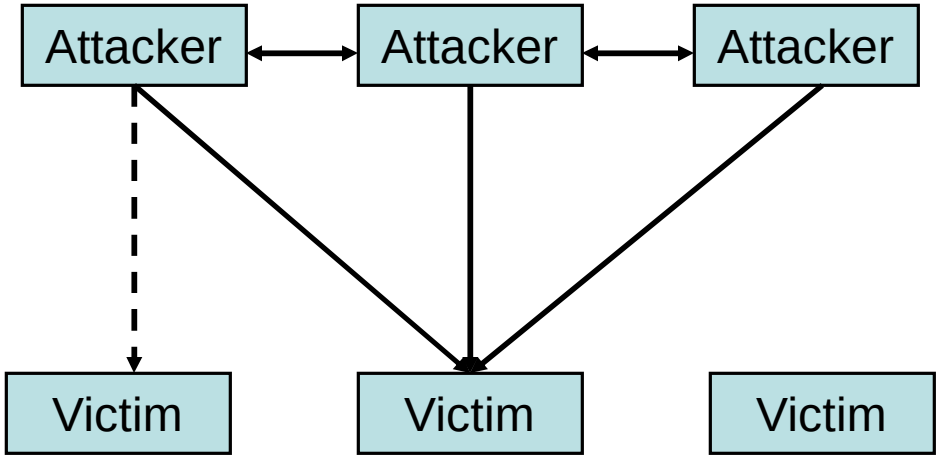
- Crashing the victim
  - Ping-of-Death
  - TCP options (unused, or used incorrectly)
- Forcing more computation
  - Taking long path in processing of packets

Simple DoS

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

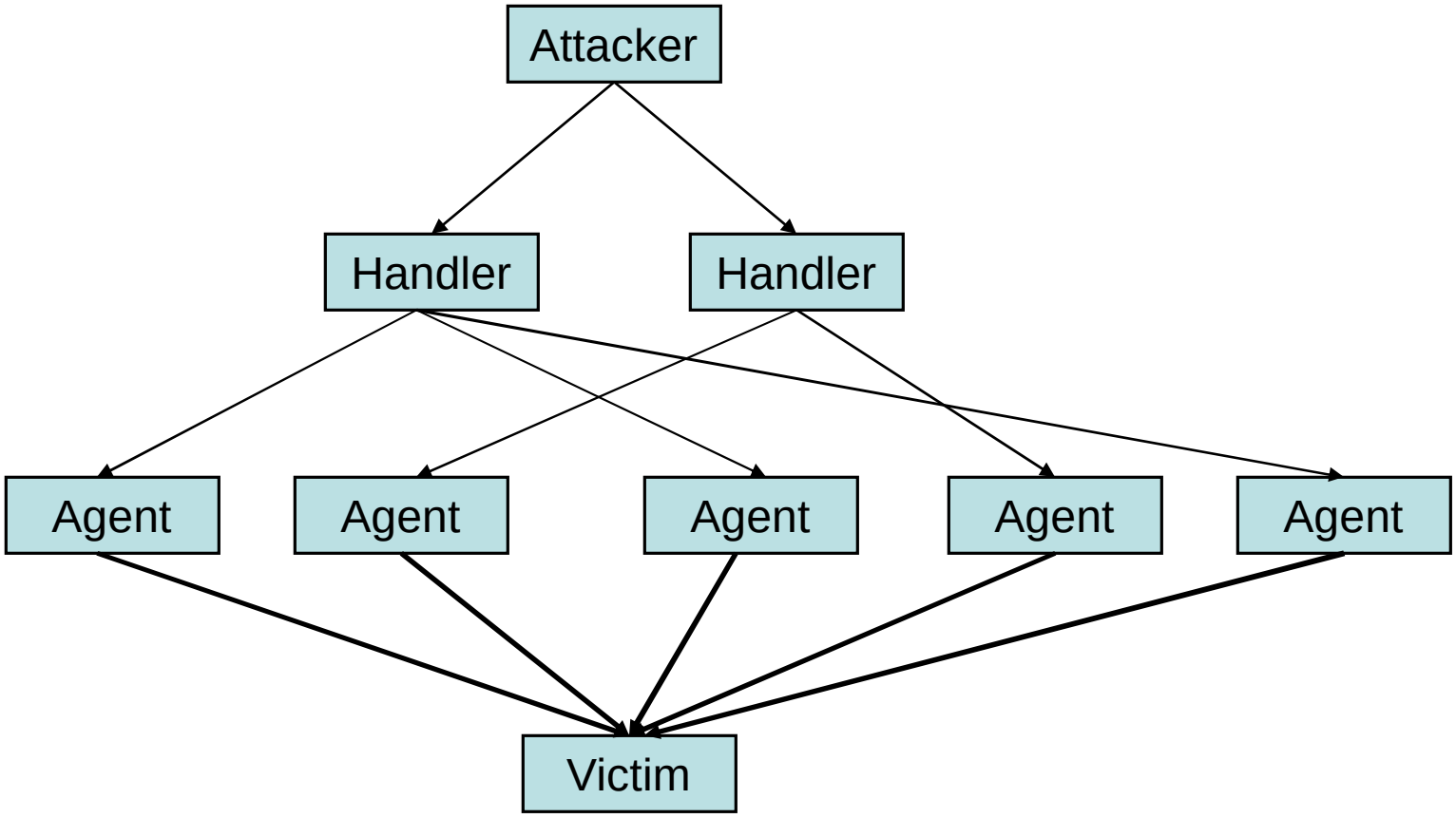


Coordinated DoS



- 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

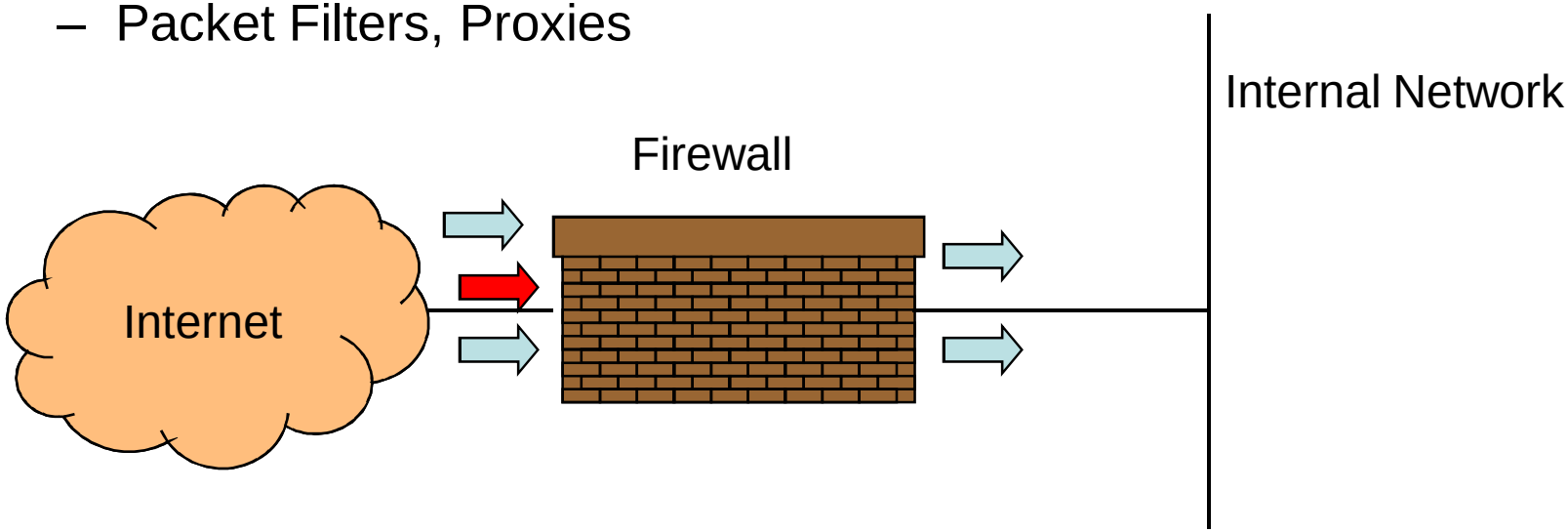
- The handlers are usually very high volume servers
  - Easy to hide the attack packets
- The agents are usually home users with DSL/Cable
  - Already infected and the agent installed
- Very difficult to track down the attacker

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.

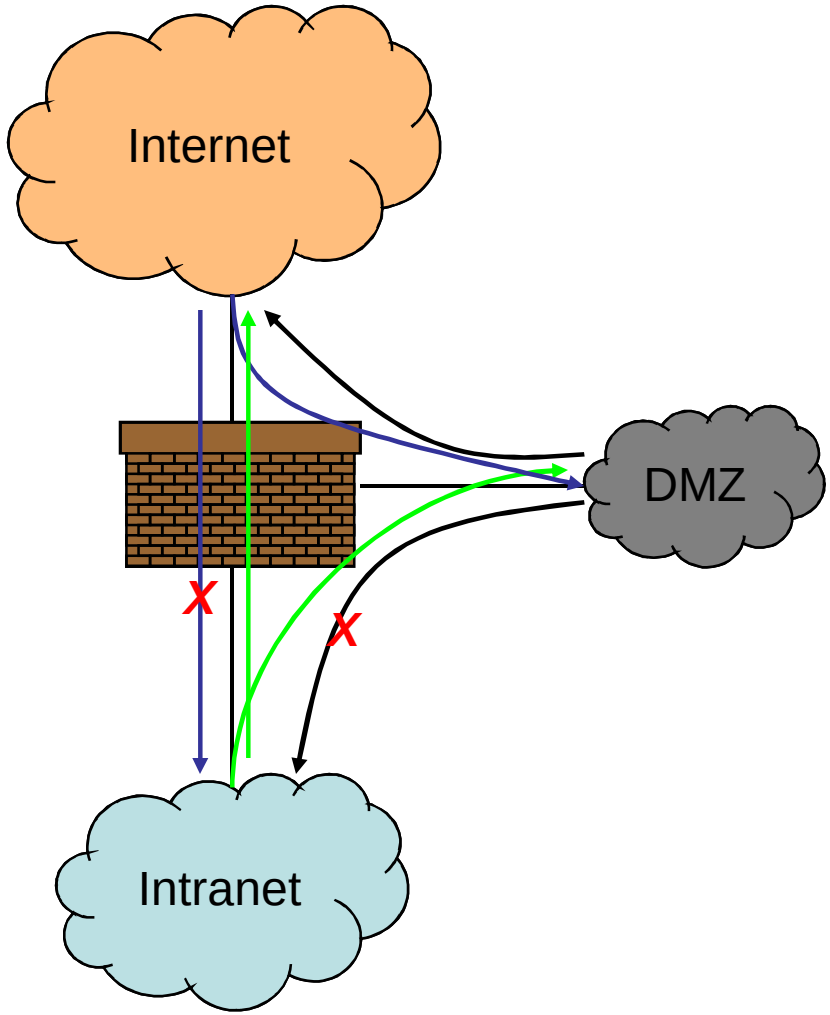
- **Data Available**
  - IP source and destination addresses
  - Transport protocol (TCP, UDP, or ICMP)
  - TCP/UDP source and destination ports
  - ICMP message type
  - Packet options (Fragment Size etc.)
- **Actions Available**
  - Allow the packet to go through
  - Drop the packet (Notify Sender/Drop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

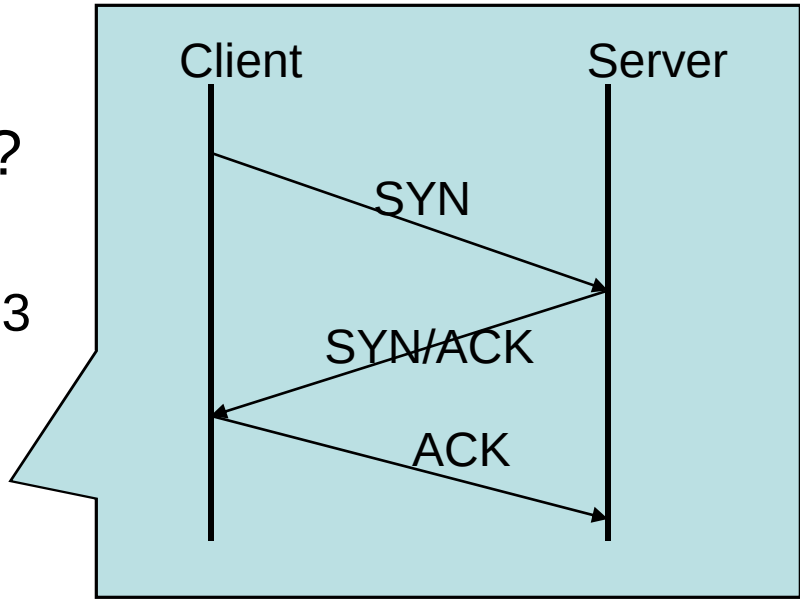


Example Firewall Rules

- 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 outbound
  - How to know a packet is for SSH?
    - Inbound: src-port>1023, dst-port=22
    - Outbound: src-port=22, dst-port>1023
    - 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	Allow

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

Introduction to Network Security

Part II

Outline

- What is Internet?
- What do we need to protect?
- Threat Motivation
- Attack Types
- Security Objectives

What is Internet?

- The Internet is a worldwide IP network, that links collection of different networks from various sources, governmental, educational and commercial.

What is Security?

Security means protecting any object, computer system, asset from unauthorized access.

Term in Information Security

- **Threat:** It is a potential that can cause harm
- **Vulnerability** is the weakness in the design
- **Attack:** A human who exploits a vulnerability in the computer system perpetrates an attack on the system

Terms cont…

- **Computer Security** - generic name for the collection of tools designed to protect data

- **Network Security** - measures to protect data during their transmission

- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Terms cont...

- Data Security
- Database Security
- OS Security
- Program Security

Protective Measures or Controls

- Control is an action, device, procedure or technique that reduces vulnerability.

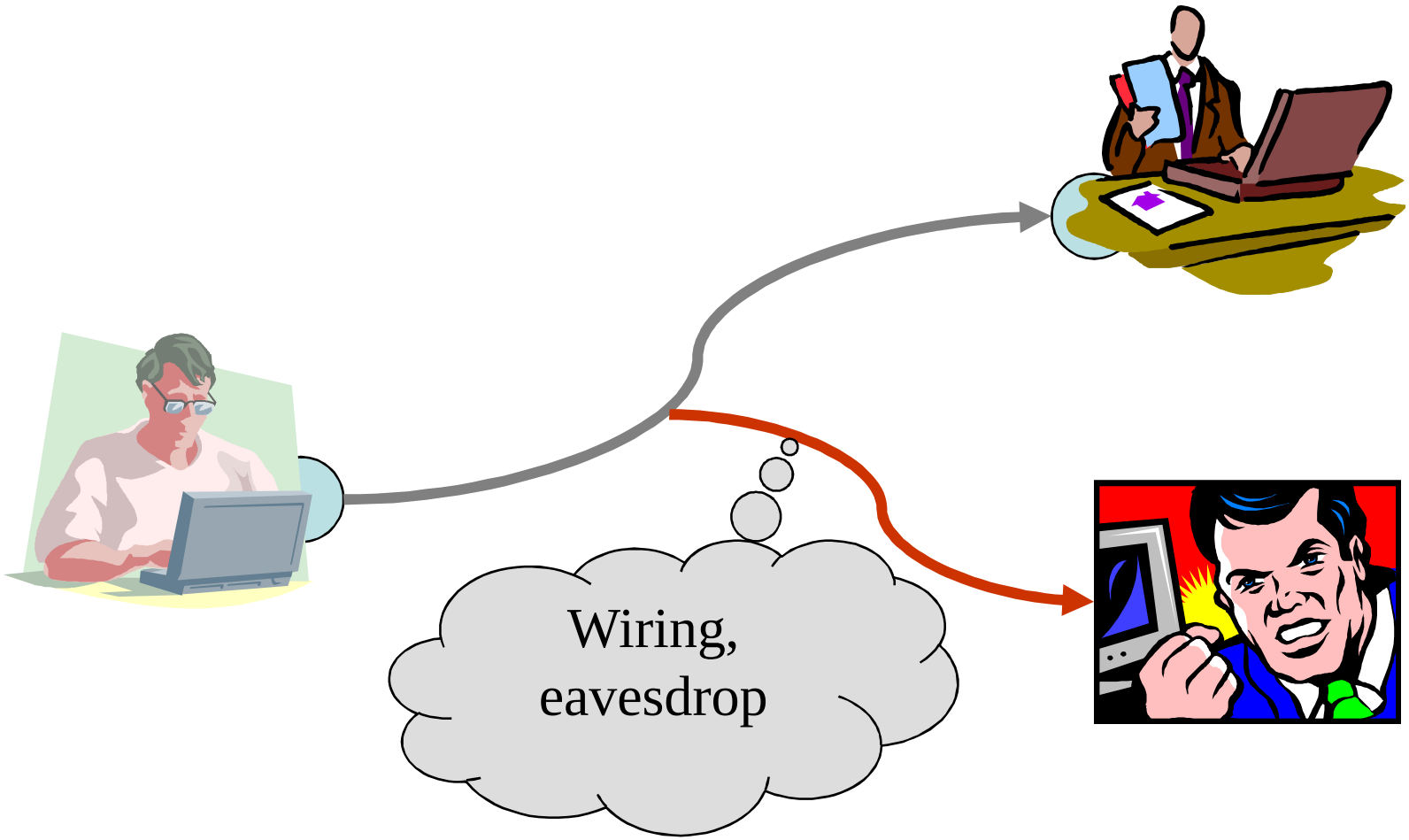
Kinds of Threats

- Interception
  - Release of message contents
  - Traffic analysis
- Interruption
- Modification
- Fabrication
  - To come with something different instead of something existing one.

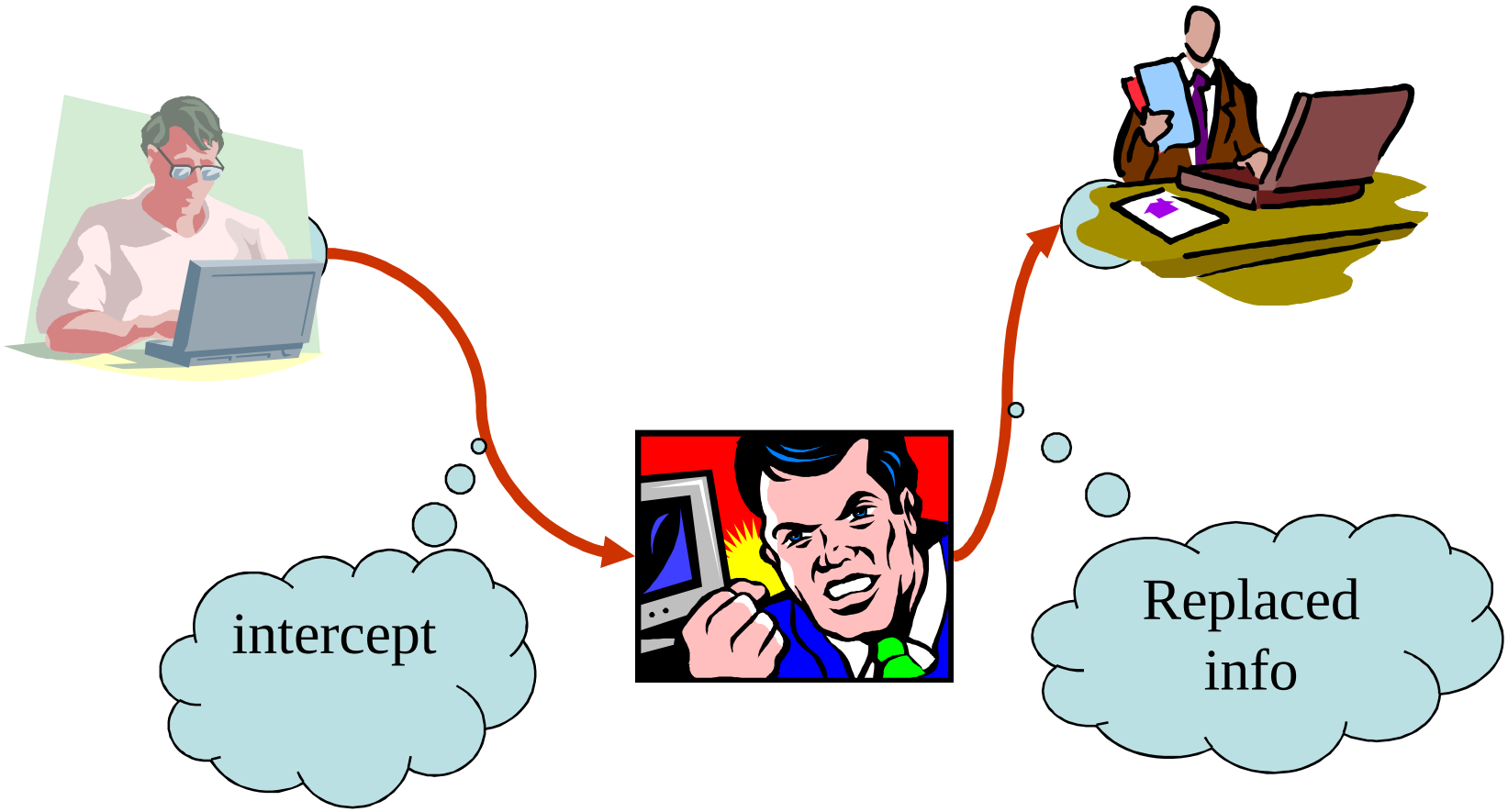
Interruption

Cut wire lines,
Jam wireless
signals,
Drop packets,

Interception



Modification



Fabrication

Also called impersonation

What do we need to protect

- Data
- Resources
- Reputation

Threat Motivation

- Spy
- Joyride
- Ignorance
- Score Keeper
- Revenge
- Greed
- Terrorist

Types of Attacks

- Passive
- Active
  - Denial of Services
  - Social Engineering

Security Objectives / Services

- Identification
- Authentication
- Authorization
- Access Control
- Data Integrity
- Confidentiality
- Non-repudiation

Identification

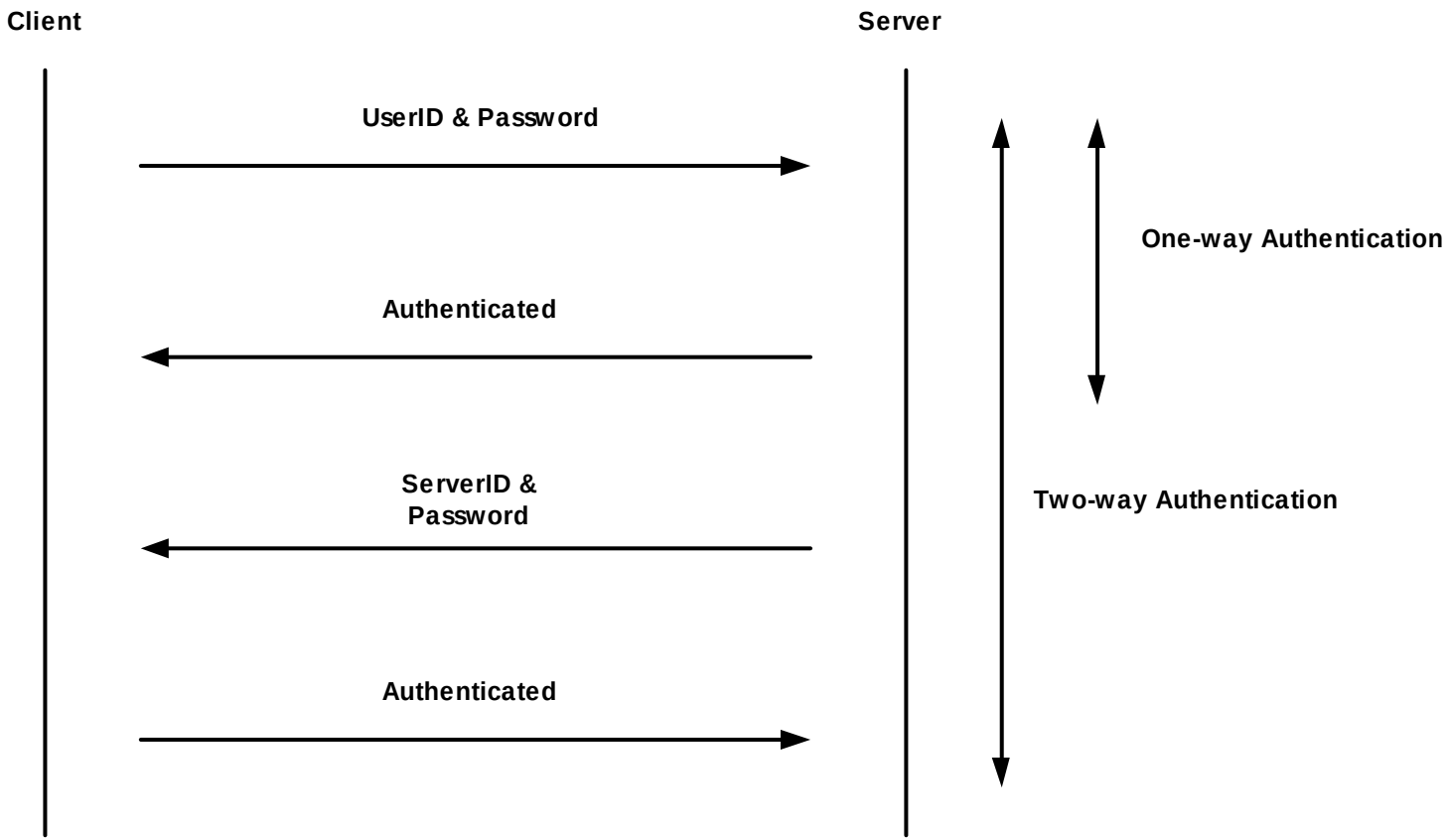
- Something which uniquely identifies a user and is called UserID.
- Sometime users can select their ID as long as it is given too another user.
- UserID can be one or combination of the following:
  - User Name
  - User Student Number
  - User SSN

Authentication

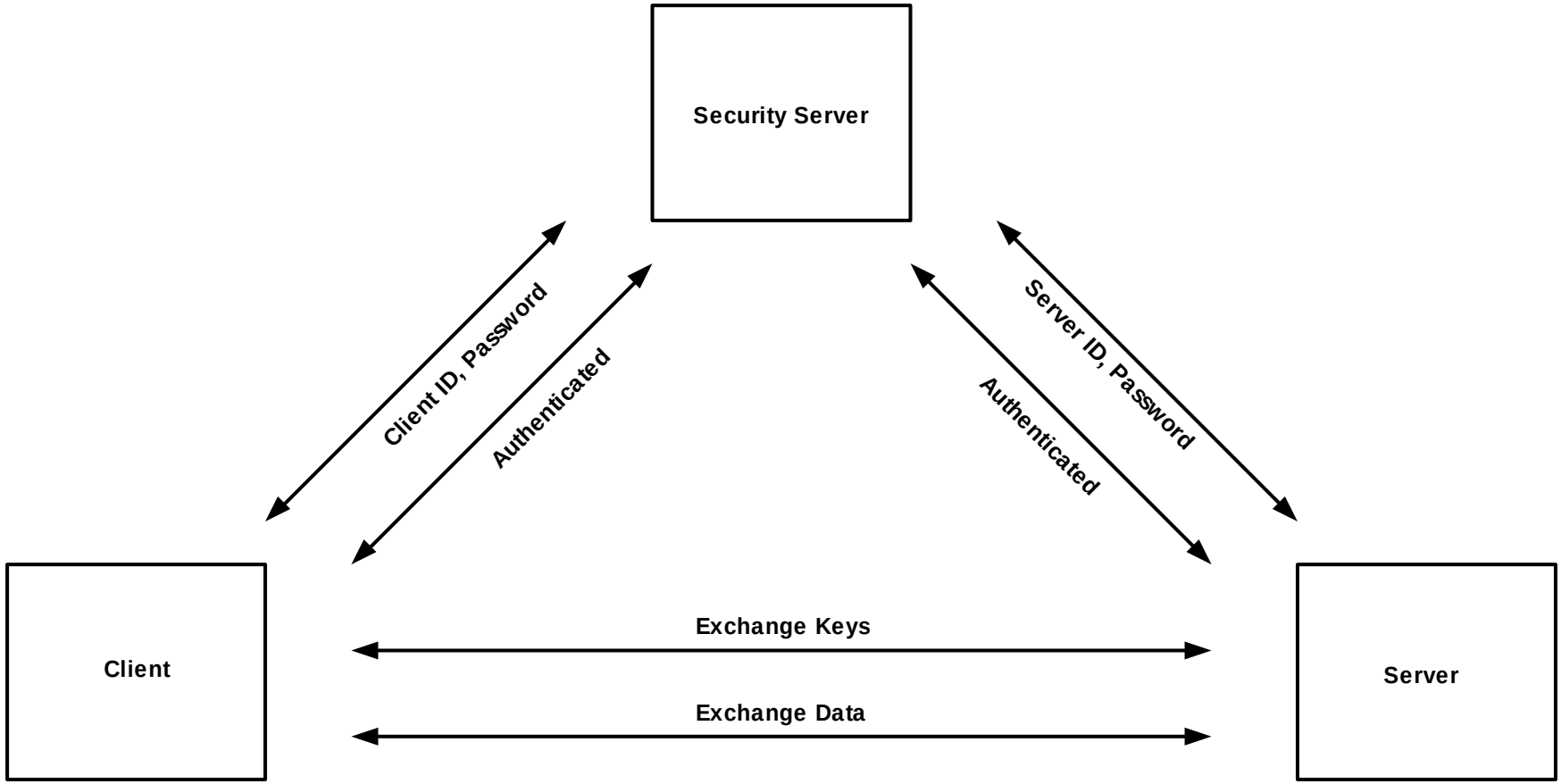
- The process of verifying the identity of a user
- Typically based on
  - Something user knows
    - Password
  - Something user have
    - Key, smart card, disk, or other device
  - Something user is
    - fingerprint, voice, or retinal scans

Authentication Cont.

- Authentication procedure
  - Two-Party Authentication
    - One-Way Authentication
    - Two-Way Authentication
  - Third-Party Authentication
    - Kerberos
    - X.509
  - Single Sign ON
    - User can access several network resources by logging on once to a security system.



Two-Party Authentications



Third-Party Authentications

Authorization

- The process of assigning access right to user

Access Control

- The process of enforcing access right
- and is based on following three entities
  - Subject
    - is entity that can access an object
  - Object
    - is entity to which access can be controlled
  - Access Right
    - defines the ways in which a subject can access an object.

Access Control Cont.

- Access Control is divided into two
  - Discretionary Access Control (DAC)
    - The owner of the object is responsible for setting the access right.
  - Mandatory Access Control (MAC)
    - The system defines access right based on how the subject and object are classified.

Data Integrity.

- Assurance that the data that arrives is the same as when it was sent.

Confidentiality

- Assurance that sensitive information is not visible to an eavesdropper. This is usually achieved using encryption.

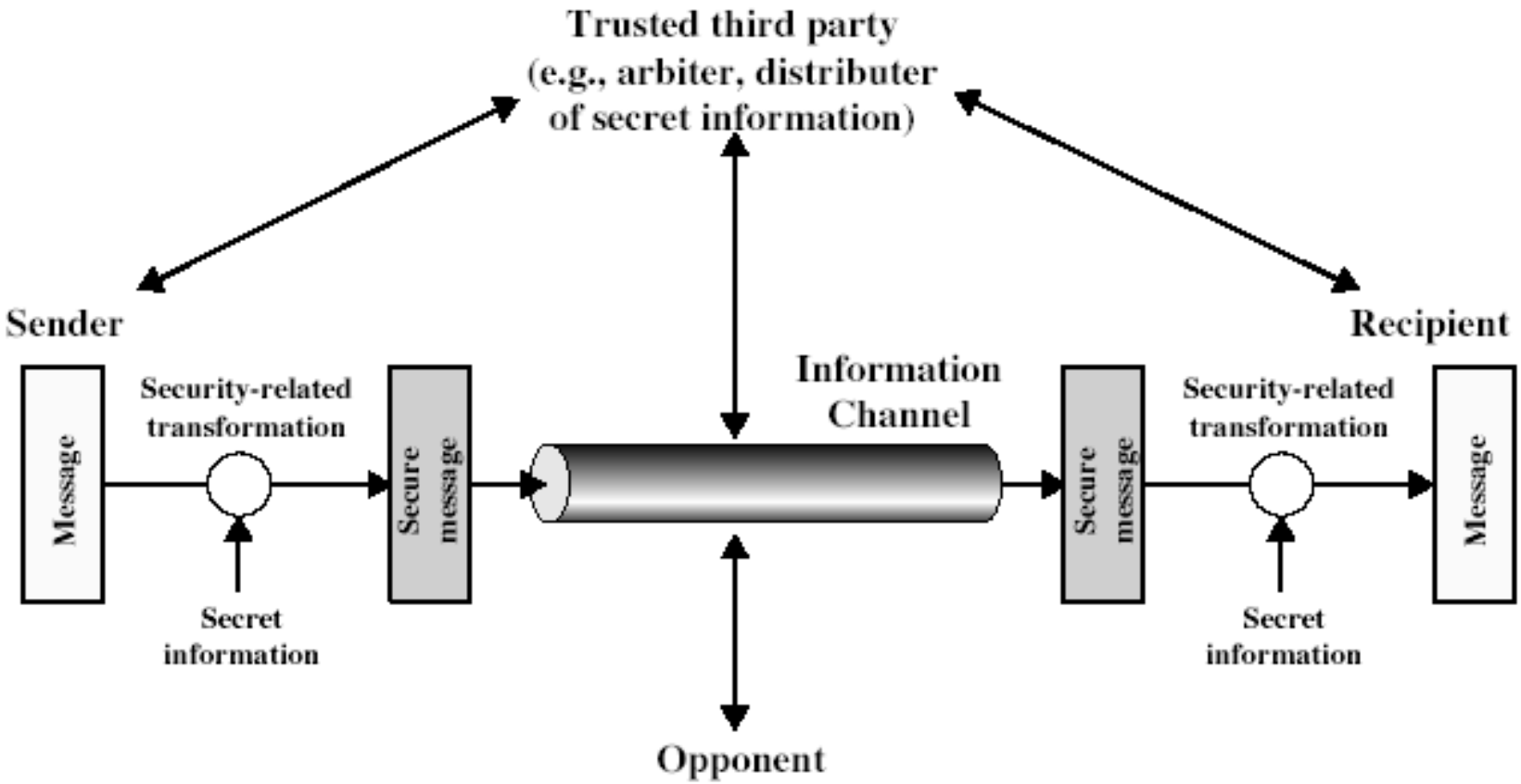
Non-repudiation

- Assurance that any transaction that takes place can subsequently be proved to have taken place. Both the sender and the receiver agree that the exchange took place.

Security Mechanism cont…

- **Encipherment**
- **Digital Signature**
- **Access Control**
  - **Proxy Server**
  - **Firewall**
- **Data Integrity**
- **Authentication Exchange**

Model for Network Security



Thank you….