Network Security

Nauman Israr

Objectives

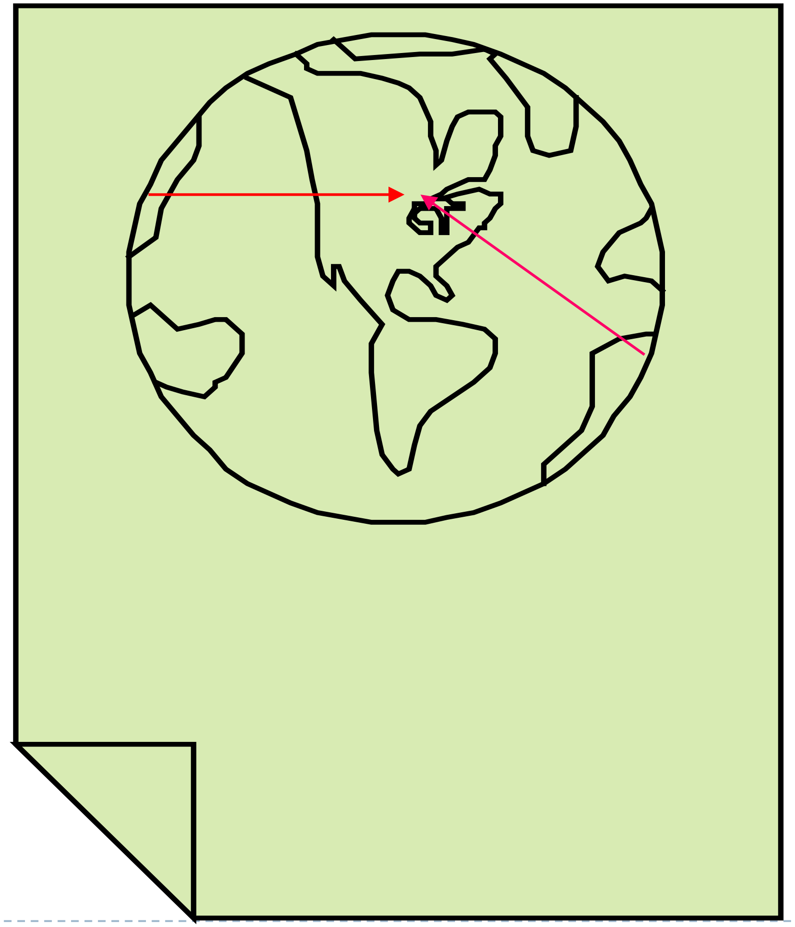
- Define attacks:
- Describe defenses
- Identify techniques

- Acknowledgements
  - *Slides adopted from Computer Networking: A Top Down Approach by* Jim Kurose, Keith Ross and Justin Weisz's tutorial, CISA review Manual and other Network Security sources

The Problem of Network Security

The Internet allows an attacker to attack from anywhere in the world from their home desk.

They just need to find one vulnerability: a security analyst need to close every vulnerability.



What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

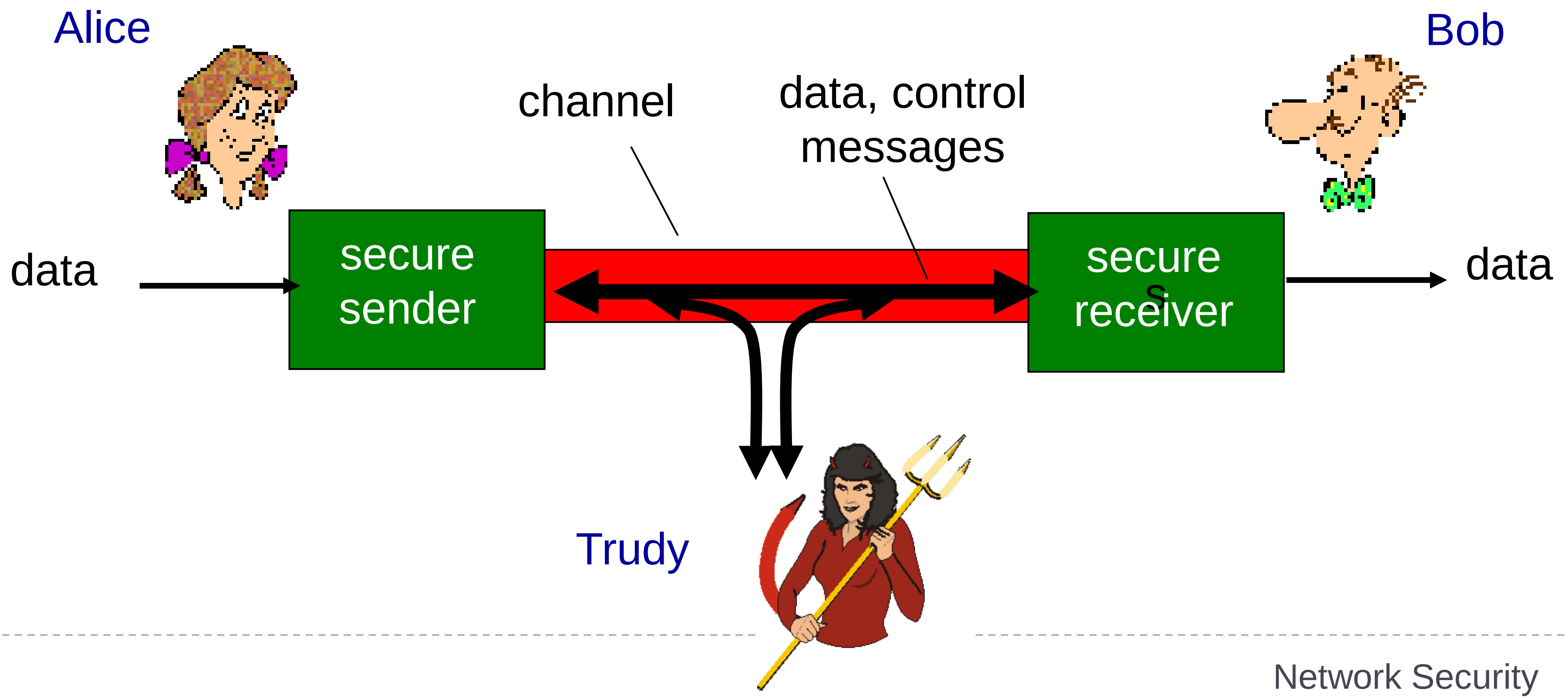
authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Alice

Bob

channel

data, control messages

data

secure sender

secure

s

receiver

data

Trudy

Who might Bob, Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: A lot!

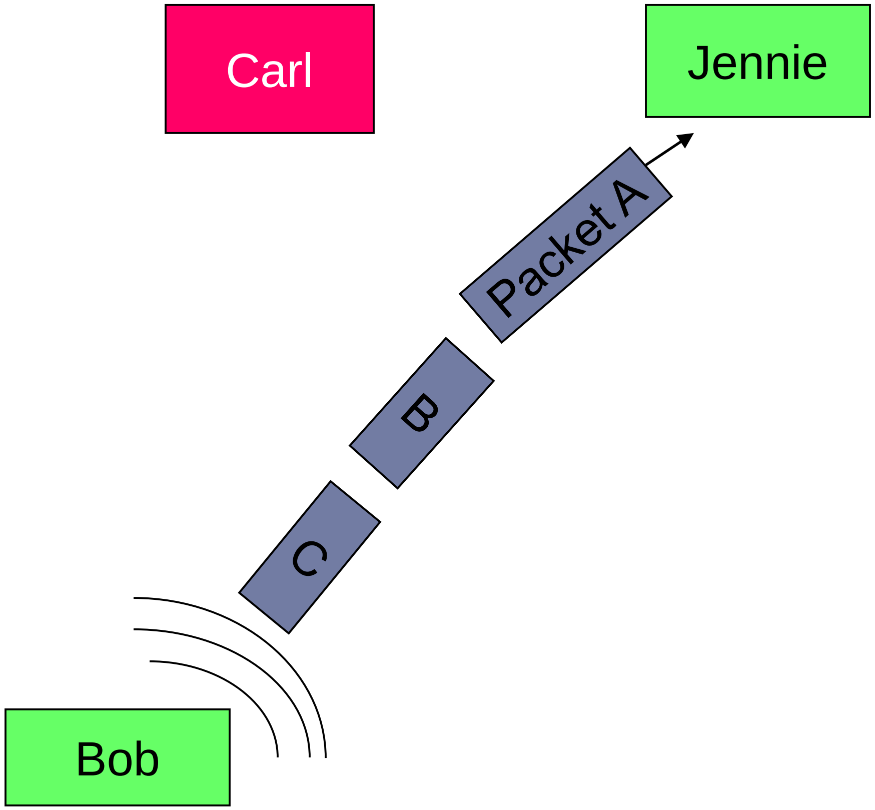
- *Eavesdrop:*
- *insert* messages
- *Impersonation:*
- *Hijacking:*
- *denial of service:*

Passive Attacks

Eavesdropping: Listen to packets from other parties = **Sniffing**

Traffic Analysis: Learn about network from observing traffic patterns

Footprinting: Test to determine software installed on system = **Network Mapping**



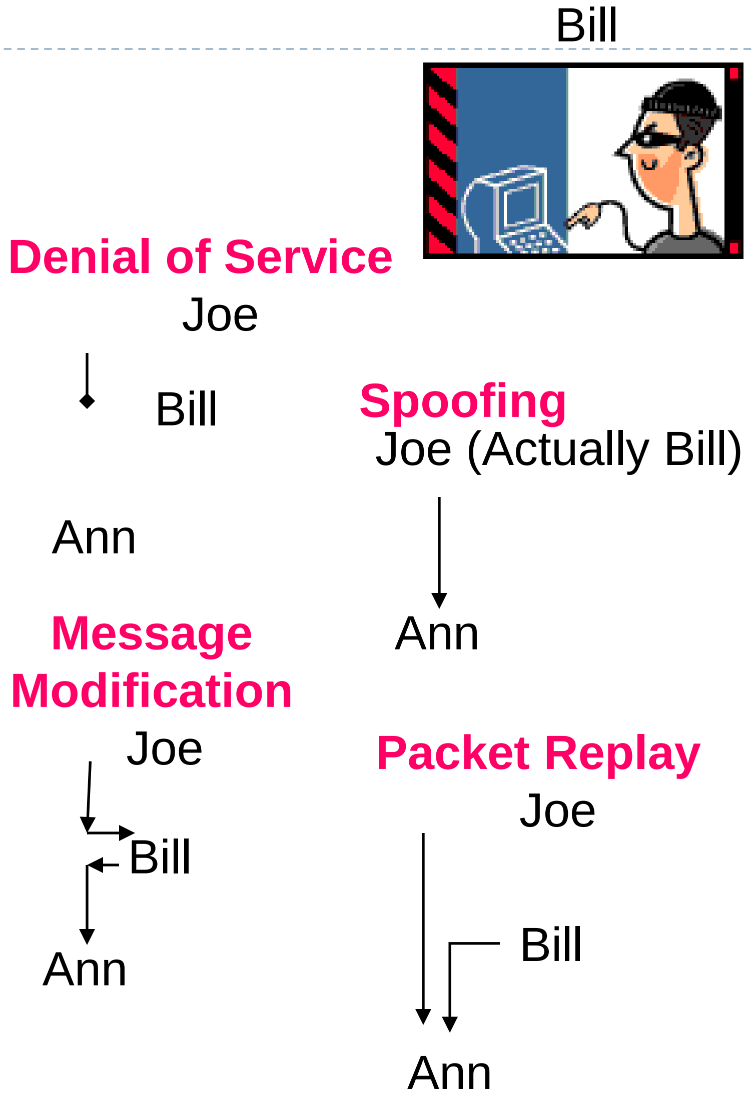
Some Active Attacks

Denial of Service: Message did not make it; or service could not run

Masquerading or Spoofing: The actual sender is not the claimed sender

Message Modification: The message was modified in transmission

Packet Replay: A past packet is transmitted again in order to gain access or otherwise cause damage



Bill

Denial of Service

Joe

Bill

Ann

Spoofing

Joe (Actually Bill)

Ann

Message Modification

Joe

Bill

Ann

Packet Replay

Joe

Bill

Ann

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

Firewalls

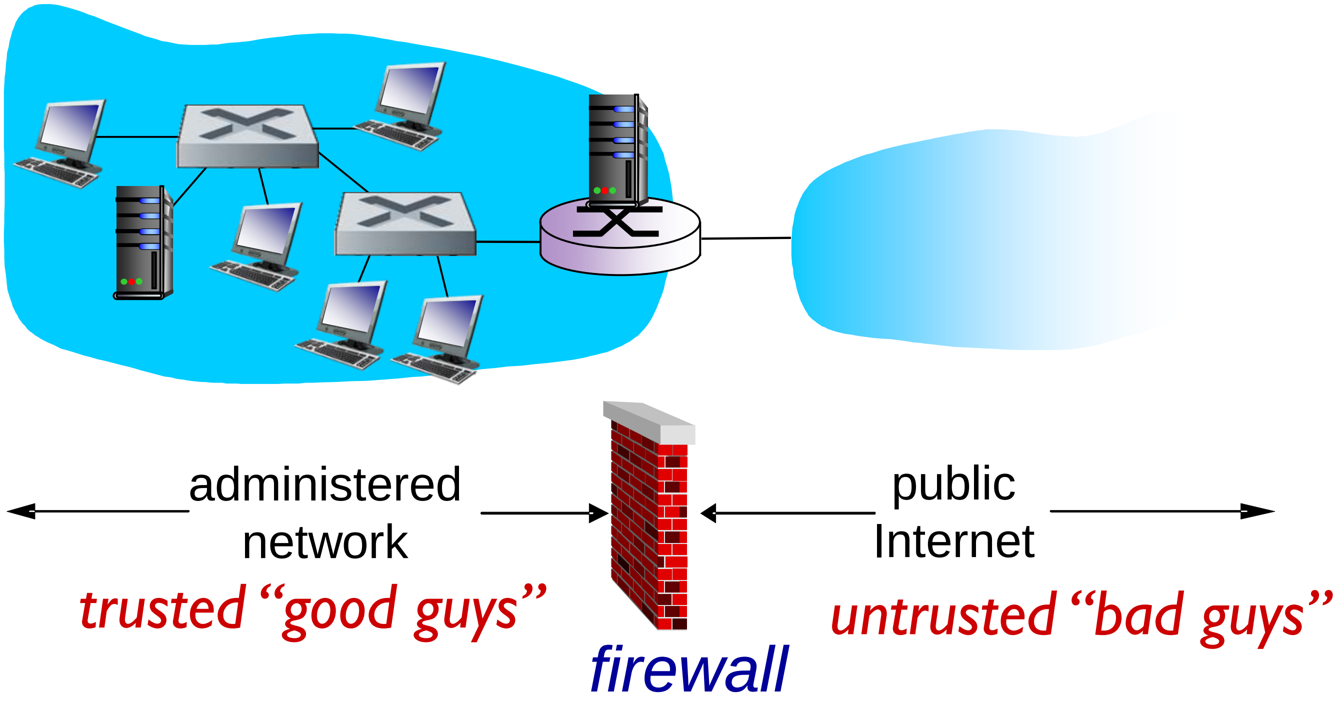
Basic problem – many network applications and protocols have security problems that are fixed over time

- Difficult for users to keep up with changes and keep host secure
- Solution
  - Administrators limit access to end hosts by using a firewall
  - Firewall is kept up-to-date by administrators

Firewalls

firewall

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



administered network

trusted "good guys"

firewall

public Internet

untrusted "bad guys"

Firewalls

A firewall is like a castle with a drawbridge

- Only one point of access into the network
- This can be good or bad

Can be hardware or software

- Ex. Some routers come with firewall functionality
- Windows XP and Mac OS X have built in firewalls

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:

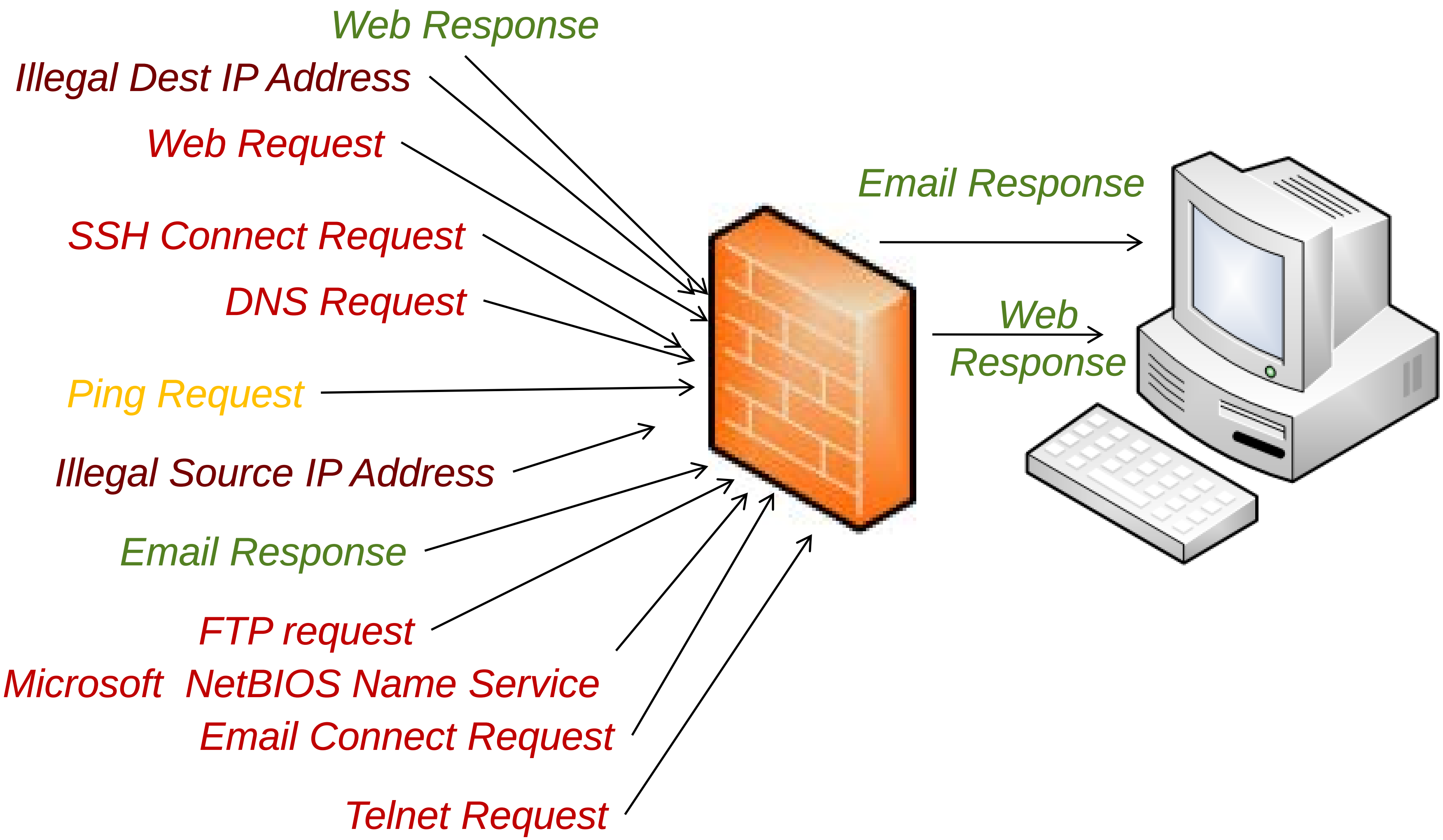
- stateless packet filters
- stateful packet filters
- application gateways

Firewalls

Used to filter packets based on a combination of features

- These are called packet filtering firewalls
  - There are other types too.
- Ex. Drop packets with destination port of 23 (Telnet)
- Can use any combination of IP/UDP/TCP header information

Packet Filter Firewall



Web Response

Illegal Dest IP Address

Web Request

SSH Connect Request

DNS Request

Ping Request

Illegal Source IP Address

Email Response

FTP request

Microsoft NetBIOS Name Service

Email Connect Request

Telnet Request

Email Response

Web Response

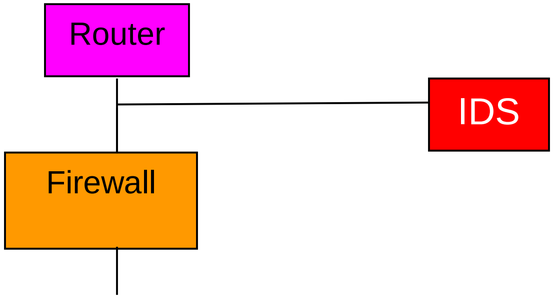
Intrusion detection systems

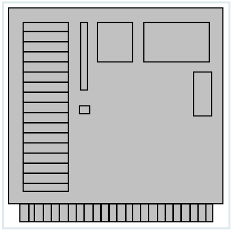
- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

Intrusion Detection

- Used to monitor for "suspicious activity" on a network
  - Can protect against known software exploits, like buffer overflows
- Open Source IDS: Snort, www.snort.org
- Uses "intrusion signatures"
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.

Intrusion Detection Systems (IDS)





Network IDS=NIDS

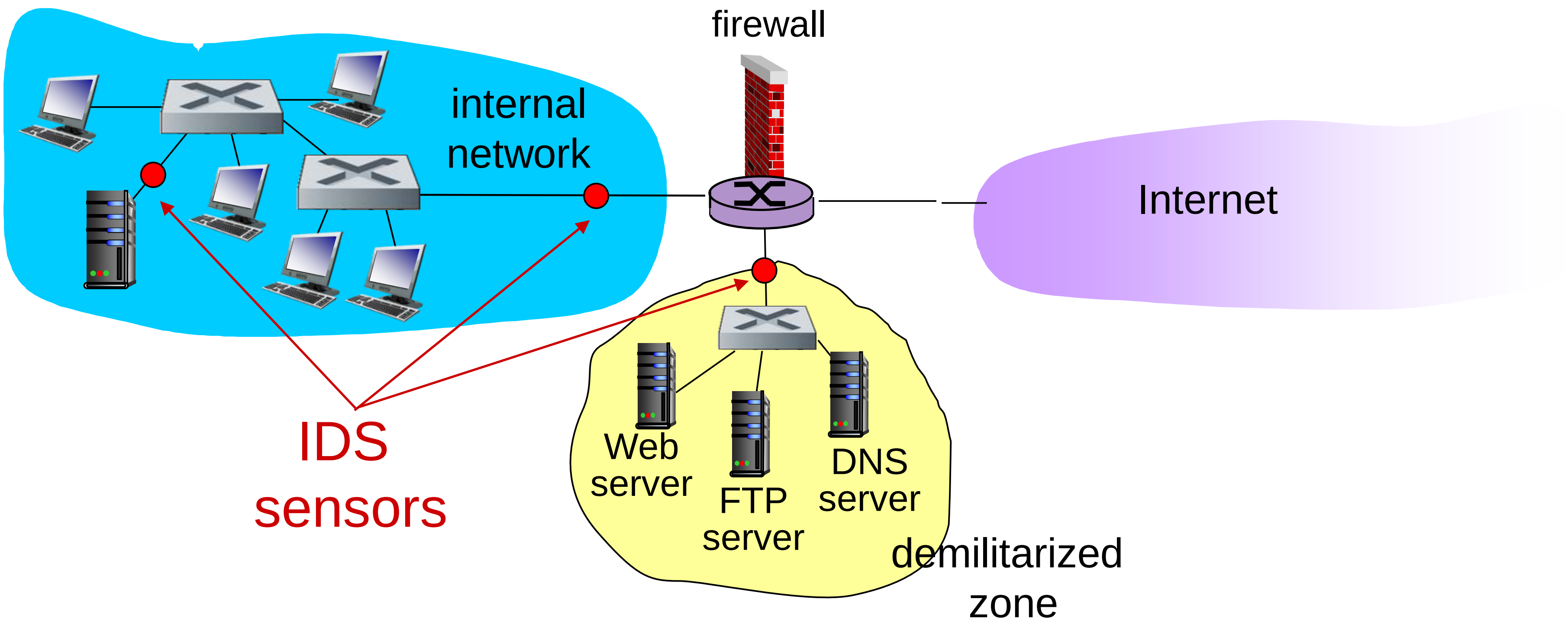
- Examines packets for attacks
- Can find worms, viruses, org-defined attacks
- Warns administrator of attack

Host IDS=HIDS

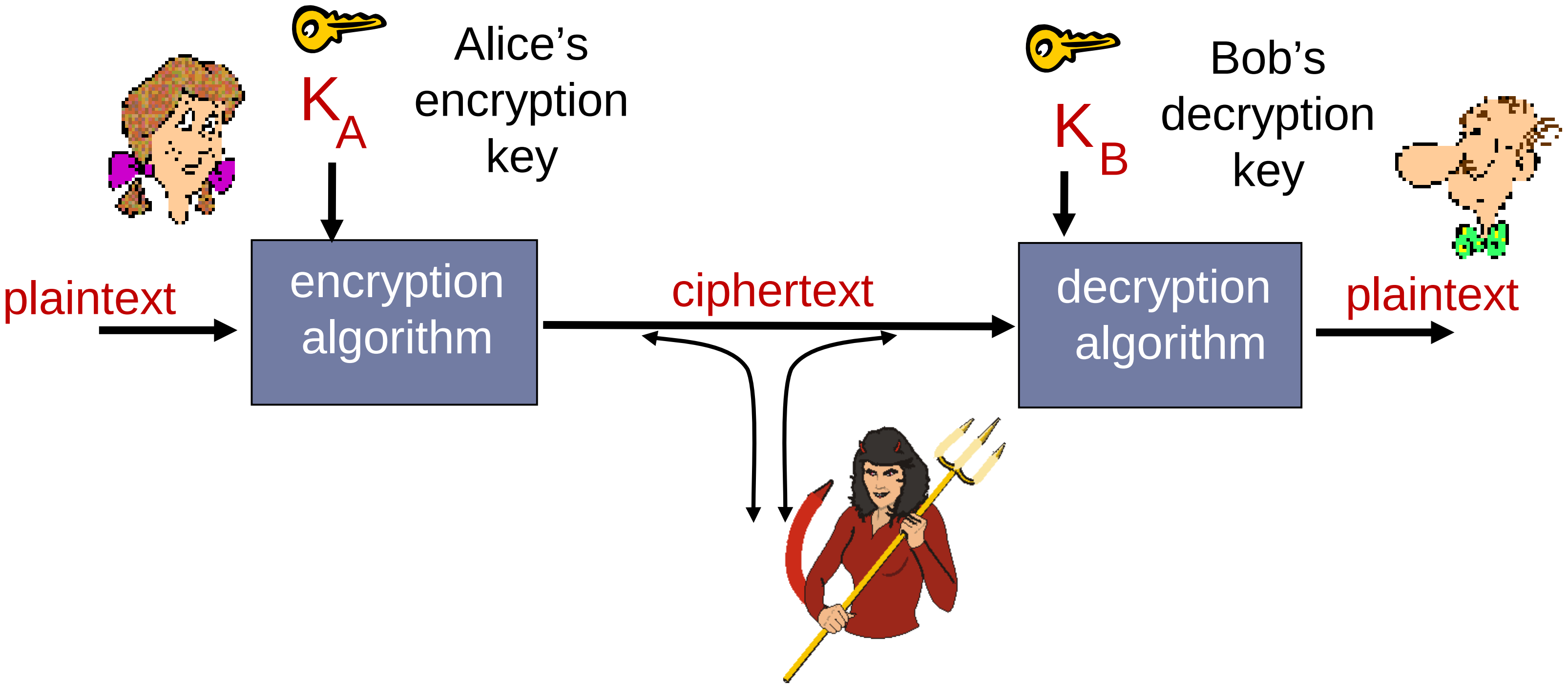
- Examines actions or resources for attacks
- Recognize unusual or inappropriate behavior
- E.g., Detect modification or deletion of special files

Intrusion detection systems

- multiple IDSs: different types of checking at different locations



The language of cryptography



m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Simple encryption scheme

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
 plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

e.g.:

```
 Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Encryption key: mapping from set of 26 letters to set of 26 letters

Cryptography Techniques

- Symmetric key cryptography:
  - DES: Data Encryption Standard
  - AES: Advanced Encryption Standard
- Public key cryptography:
  - RSA : Rivest - Shamir -Adleman

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords are encrypted with the crypt(3) function (one-way hash) at few places.
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, "sdfo839f" is a good password
    - That is not my password
    - Please don't try it either
  - https://howsecureismypassword.net/

Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks

Denial of Service

- SYN flooding attack
- Send SYN packets with bogus source address
  - Why?
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state
- Solution: use “SYN cookies”
  - In response to a SYN, create a special “cookie” for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

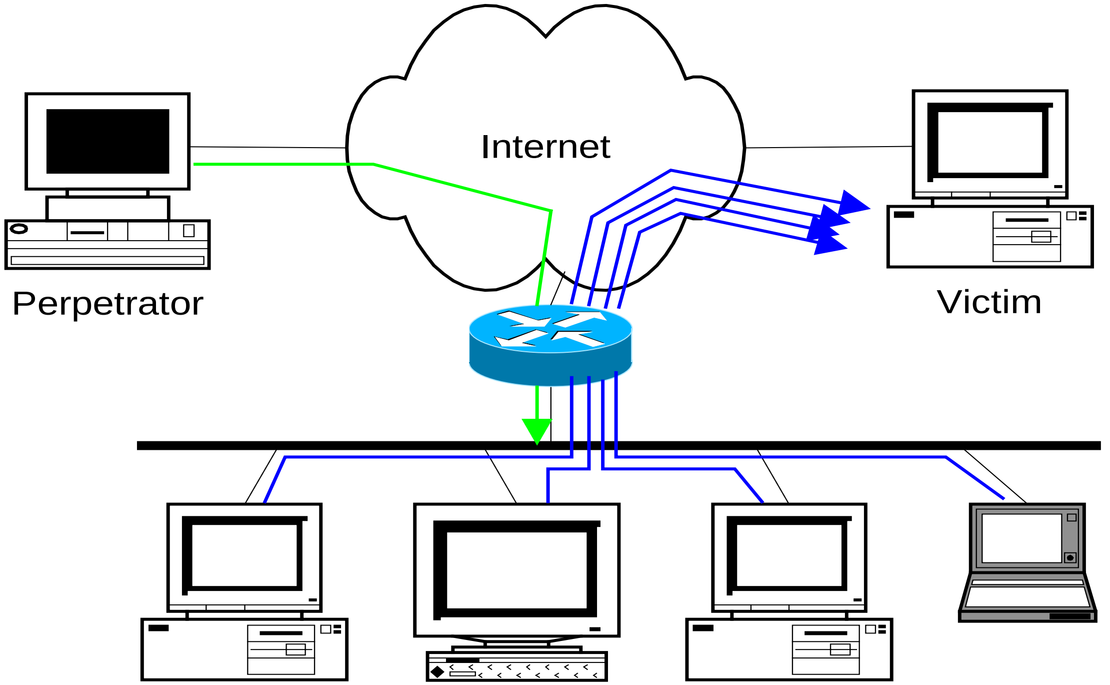
Denial of Service

- SMURF
  - Source IP address of a broadcast ping is forged
  - Large number of machines respond back to victim, overloading it

Denial of Service

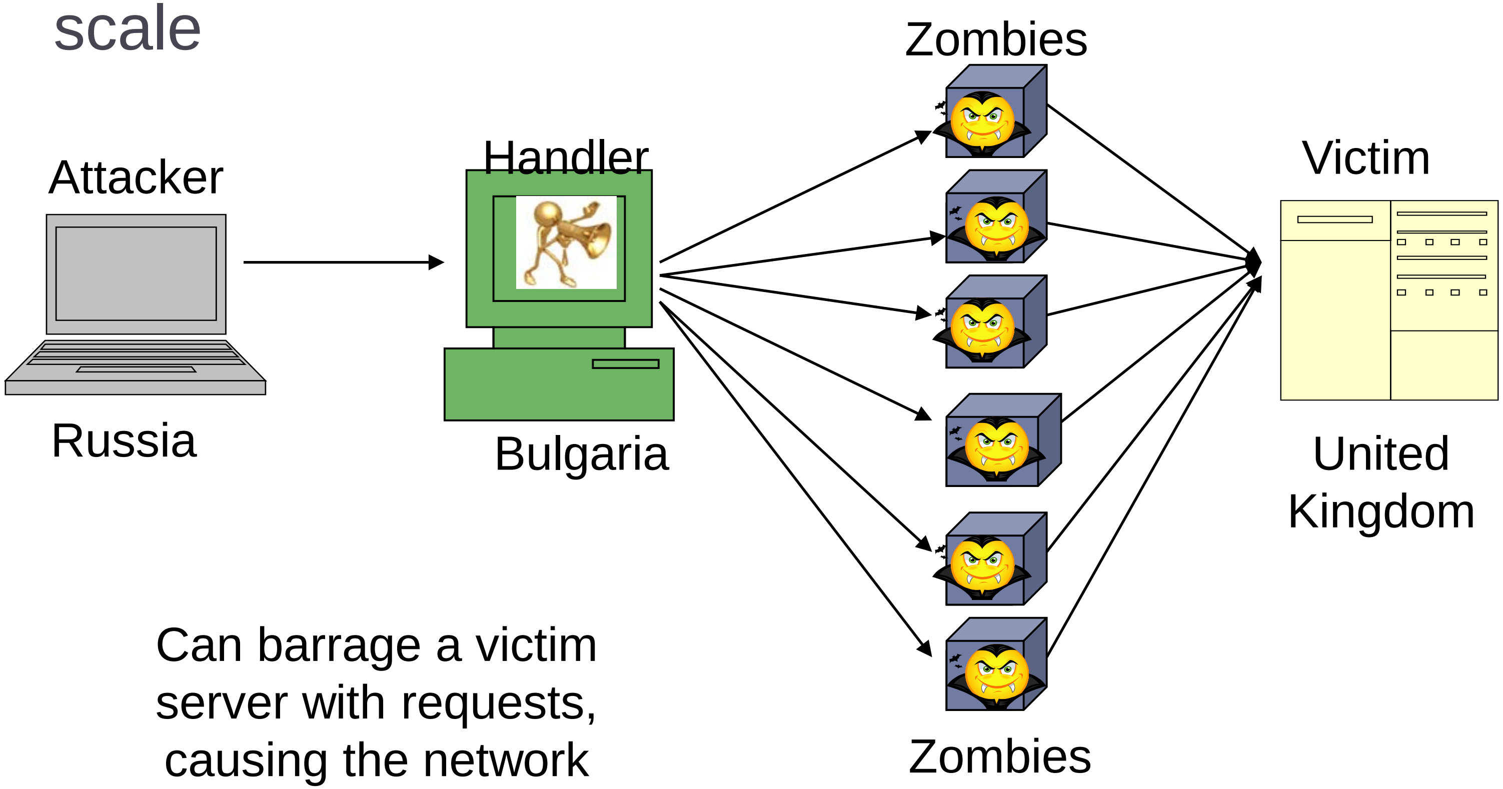
🟩 ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

🟦 ICMP echo reply



Denial of Service

- Distributed Denial of Service
  - Same techniques as regular DoS, but on a much larger scale



Can barrage a victim
server with requests,
causing the network
to fail to respond to anyone

TCP Attacks

- Recall how IP works…
  - End hosts create IP packets and routers process them purely based on destination address alone
- Problem: End hosts may lie about other fields which do not affect delivery
  - Source address – host may trick destination into believing that the packet is from a trusted source
    - Especially applications which use IP addresses as a simple authentication method
    - Solution – use better authentication methods

TCP Attacks

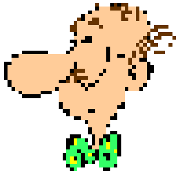
- TCP connections have associated state
  - Starting sequence numbers, port numbers
- Problem – what if an attacker learns these values?
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

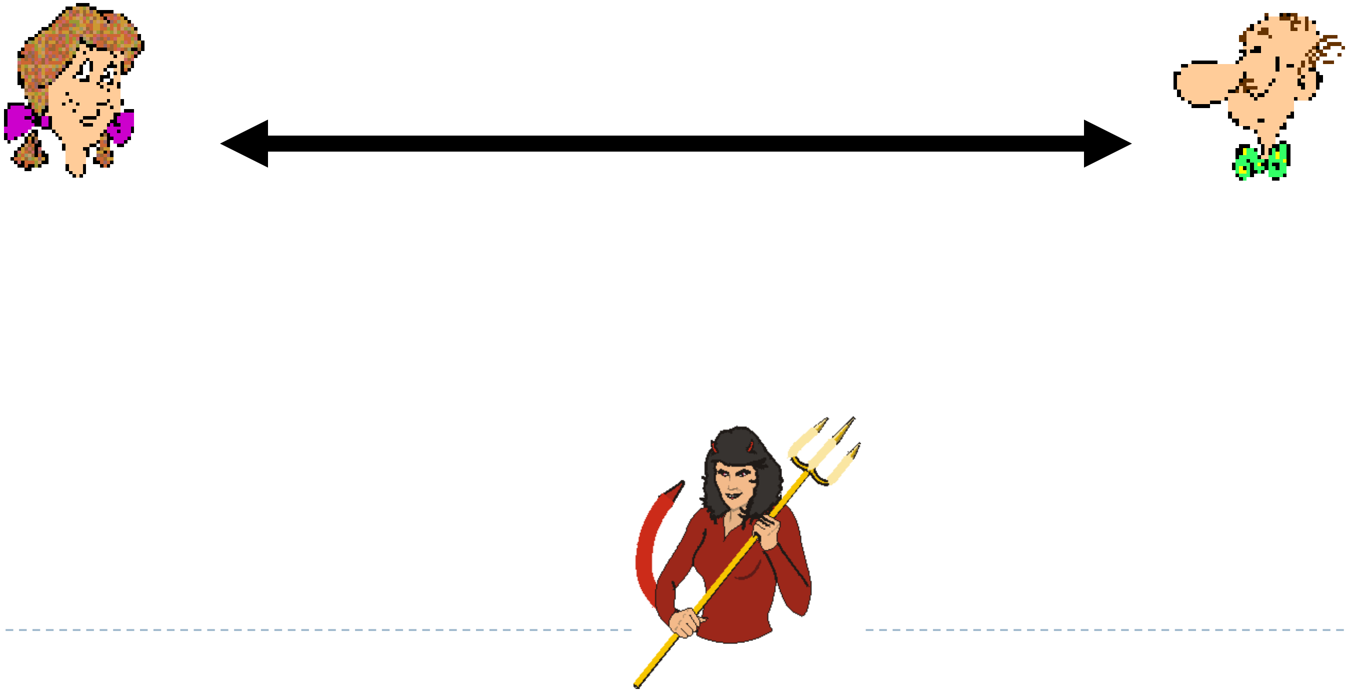
TCP Attacks

- Say hello to Alice, Bob and Mr. Trudy



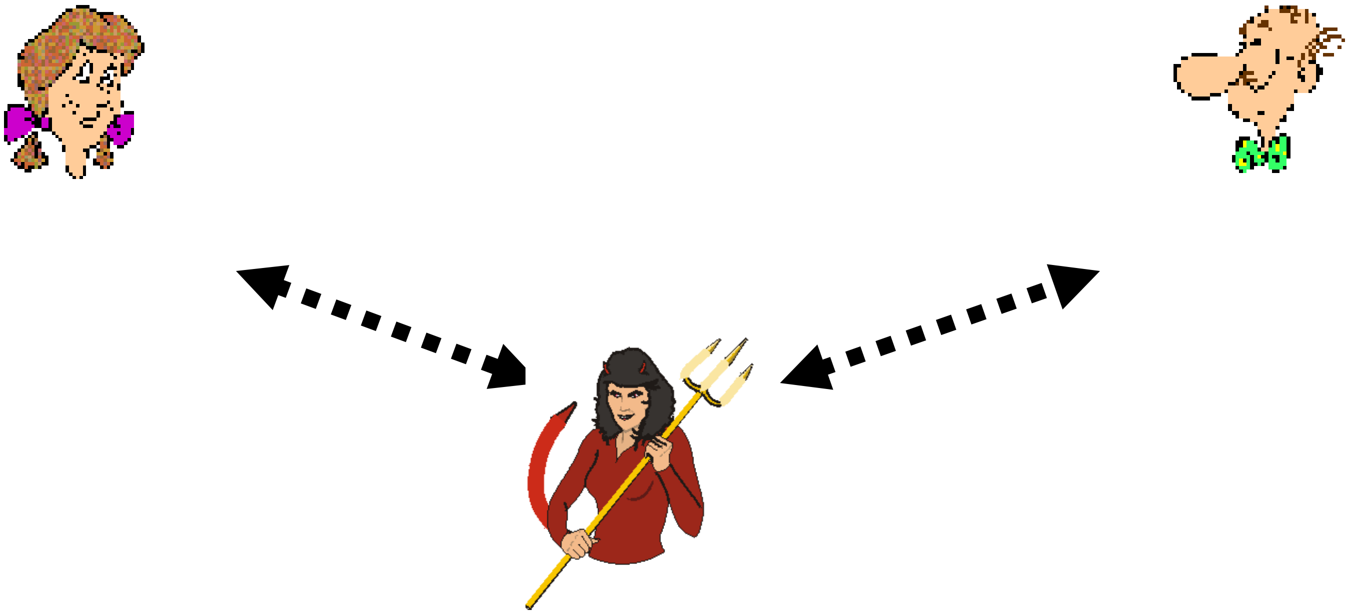
TCP Attacks

- Alice and Bob have an established TCP connection



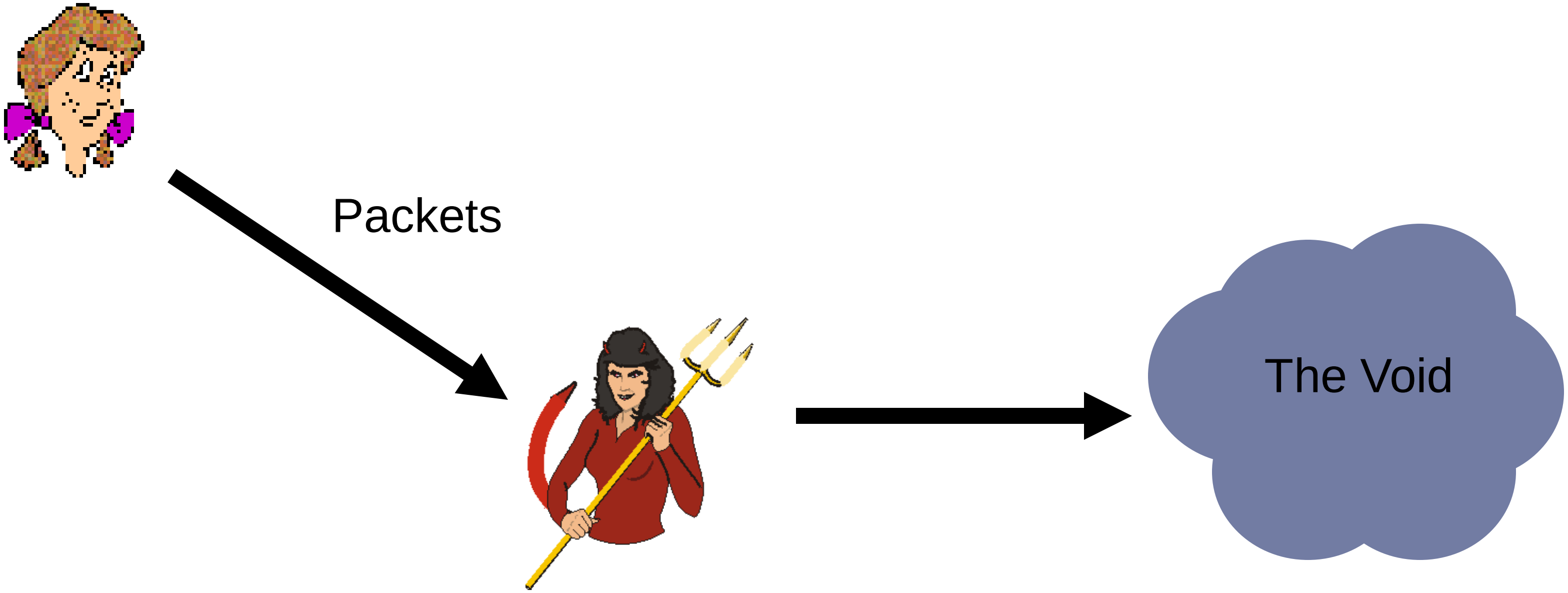
TCP Attacks

- Mr. Trudy lies on the path between Alice and Bob on the network
  - He can intercept all of their packets



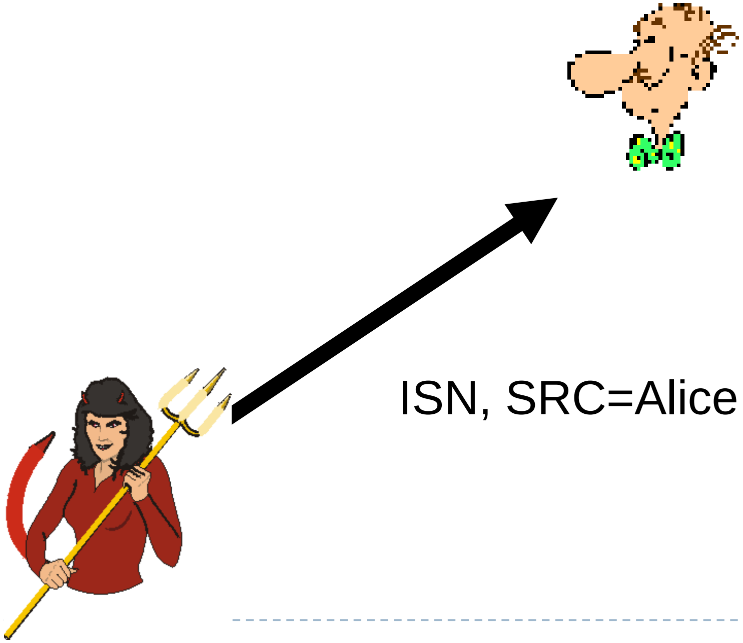
TCP Attacks

- First, Mr. Trudy must drop all of Alice’s packets since they must not be delivered to Bob (why?)



TCP Attacks

- Then, Mr. Trudy sends his malicious packet with the next ISN (sniffed from the network)



TCP Attacks

- How do we prevent this?
- IPSec
  - Provides source authentication, so Mr. Trudy cannot pretend to be Alice
  - Encrypts data before transport, so Trudy cannot talk to Bob without knowing what the session key is

IPsec services

- data integrity
- origin authentication
- replay attack prevention
- confidentiality

- two protocols providing different service models:
  - AH
  - ESP

Two IPsec protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

Packet Sniffing

- Recall how Ethernet works …
- When someone wants to send a packet to some else …
- They put the bits on the wire with the destination MAC address …
- And remember that other hosts are listening on the wire to detect for collisions …
- It couldn’t get any easier to figure out what data is being transmitted over the network!

Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium

Packet Sniffing

- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
  - Passwords are the most popular

Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the “harmed” stage, unless they have been specially trained
    - Think government here…

Social Problems

- Example:
  - Someone calls you in the middle of the night
    - “Have you been calling Egypt for the last six hours?”
    - “No”
    - “Well, we have a call that’s actually active right now, it’s on your calling card and it’s to Egypt and as a matter of fact, you’ve got about £2000 worth of charges on your card and … read off your card number and PIN and then I’ll get rid of the charge for you”

Conclusions

- The Internet works only because we implicitly trust one another
- It is very easy to exploit this trust
- The same holds true for software
- It is important to stay on top of the latest security advisories to know how to patch any security holes