Internet and CyberSecurity 101

U.S. National Cybersecurity,

10/5/06

presented by: Martin Casado

Network vs. Internet

- a **network** is a system of computers that talk over some communication medium: phone line (analogue modem, DSL), cable, fiber etc.

- the **Internet** is a global network owned and operated by many different groups with often conflicting interests, ideals, goals, agendas, and policies

Today ...

- What makes up the Internet
- How the Internet works
- How the Internet doesn't work

.. and remember ... the information presented here is a GROSS oversimplification.

Core vs. Edge

- The Internet can be roughly broken into the "Core" and the "Edge"
- The Internet "Edge" is composed of computers used by people to send or receive content
- The "Core" are all the computers that move traffic between computers on the "Edge"

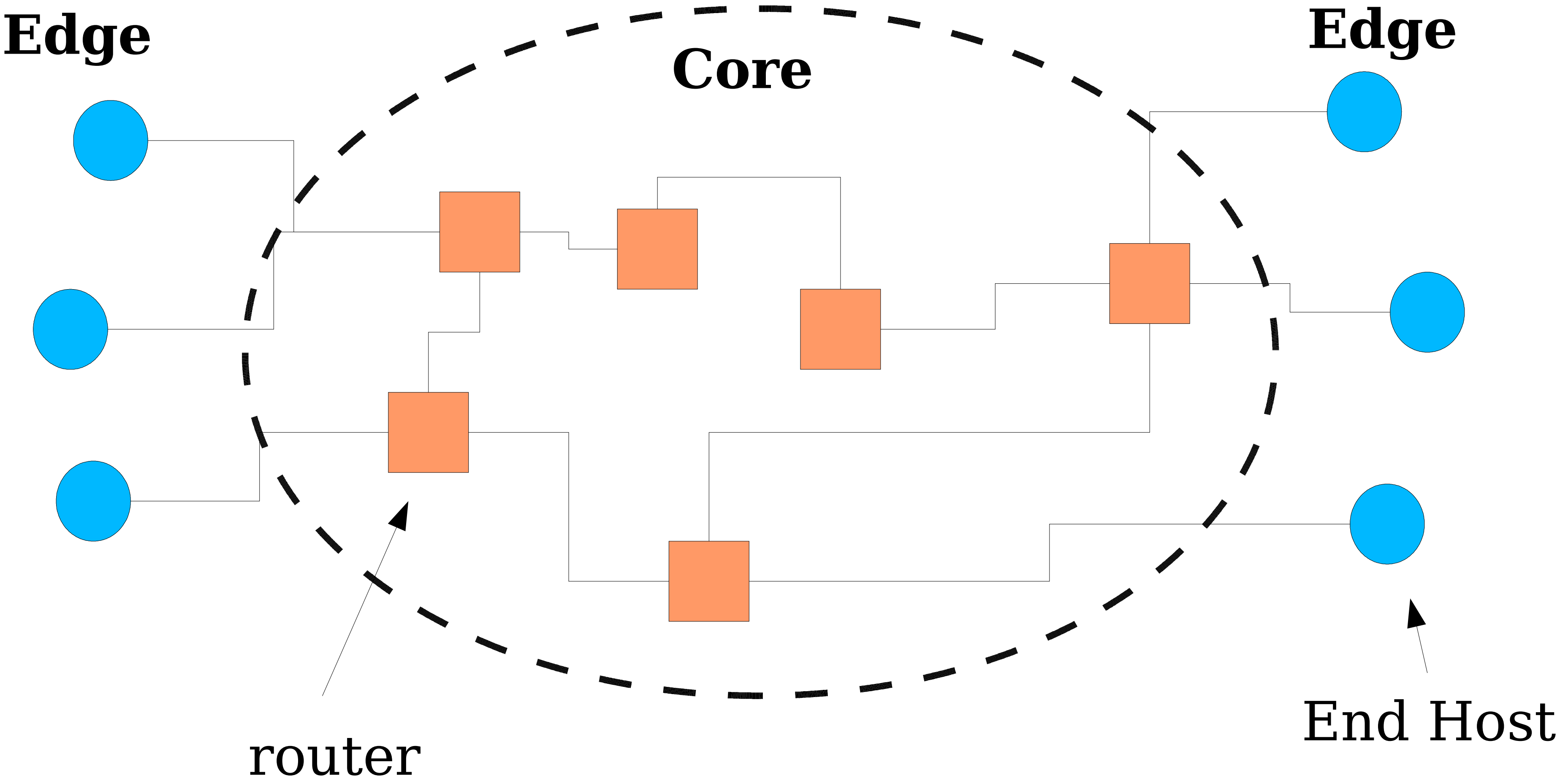
“Edge” Computers

- home computers
- computers that host web pages
- educational computers
- business computers
- governmental computers

“Core” computers

- Routers : try to figure out how traffic goes from point A to point B (on the Internet)

Core vs. Edge



Who Owns the Core?

- Mostly owned by private companies (ISPs)
- Can think of Internet as an aggregation of smaller networks
- Companies are often multi-national (what might be the implications of this?)
- Many names you've heard of, AT&T, MCI, Sprint

IP Addresses

- Any computer on the Internet can talk to any other (mostly)
  (yeeks! Once you plug in, everyone is your neighbor!)
- Computers “find” each other through virtual addresses” called “IP addresses”
- If someone knows the IP address of your computer, can talk to you

What are IP Addresses?

- Just numbers (with dots in them)
  123.114.23.4
  10.15.46.32

- Really just a value from 1 to (2^32 - 1) represented in octets (chunks of 2^8)

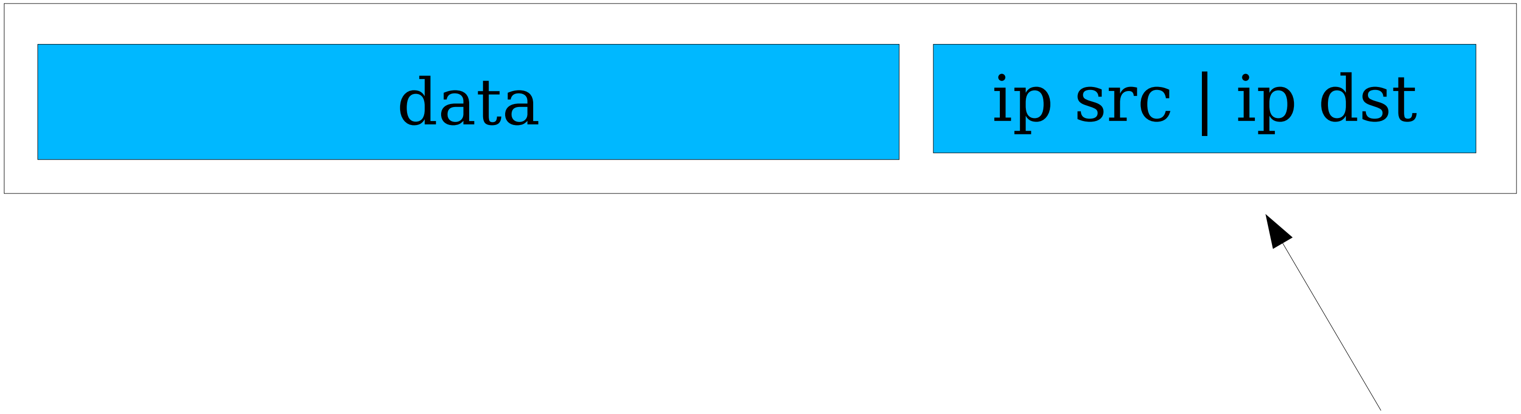
IP Addresses Cont …

Note: Since so many computers are on the Internet; a person, or computer program, can choose an IP at random (just a number remember!) and it will likely be assigned to a computer

- this process of iterating through lots of IP Addressess looking for a target is called "SCANNING"

How Computers Talk

- Send "packets" of information (called IP packets or IP datagrams)
- Packets contain IP address of recipient and send plus data



Packet "header"

Packets in the Core

- Packets are moved or “routed” from the sender to the receiver based on the destination IP address
- Note that, routers (computers in the core) ONLY look at the destination
- Sources can lie about who they are: “source spoofing”

IP Packets Cannot be Used for Reliable Services

- If a computer (router, sender, end-host) is too busy, will drop packets
- If the header gets corrupted, packet gets dropped
- Data can get corrupted
- If a router dies, packets will get lost

Transmission Control Protocol (TCP)

- Almost all communications on the Internet use higher-level mechanism (TCP)
- TCP uses IP packets plus black magic to ensure...
  - Data will not be corrupted
  - Data will not be lost
  - Data will arrive in the order it was sent
- Plus! TCP black magic makes source forging REALLY hard!

User Datagram Protocol (UDP)

- Sometimes want to send data quickly, and don't need so much magic
- Who cares if you loose a bullet or two in quake?
- Who cares if bullets come out of order?
- Not used very often (except for DNS)

Servers

- Some computers are only used to house services such as web pages or email
- Typically only offer services and aren't used like home computers
- Often located as close to the core as possible (in some basement downtown)

Servers cont ...

- When connecting to a website, connecting to a server
- When getting your email, connecting to a server

Clients

- Programs that connect to services on servers (used by you me and Aunt Bev)
- Web browsers (mozilla, ie, safari etc.)
- Email clients (outlook, Eudora, ...)

Domain Name System (DNS)

- IP addresses are hard to remember (and boring) … why not use names instead?
- Computers in the core map names to IP addresses
  - www.google.com
  - www.stanford.edu
- Called DNS servers
- "root" name servers most important!
  - Heavily guarded in unmarked buildings

Checking News on the Web
(putting it all together)

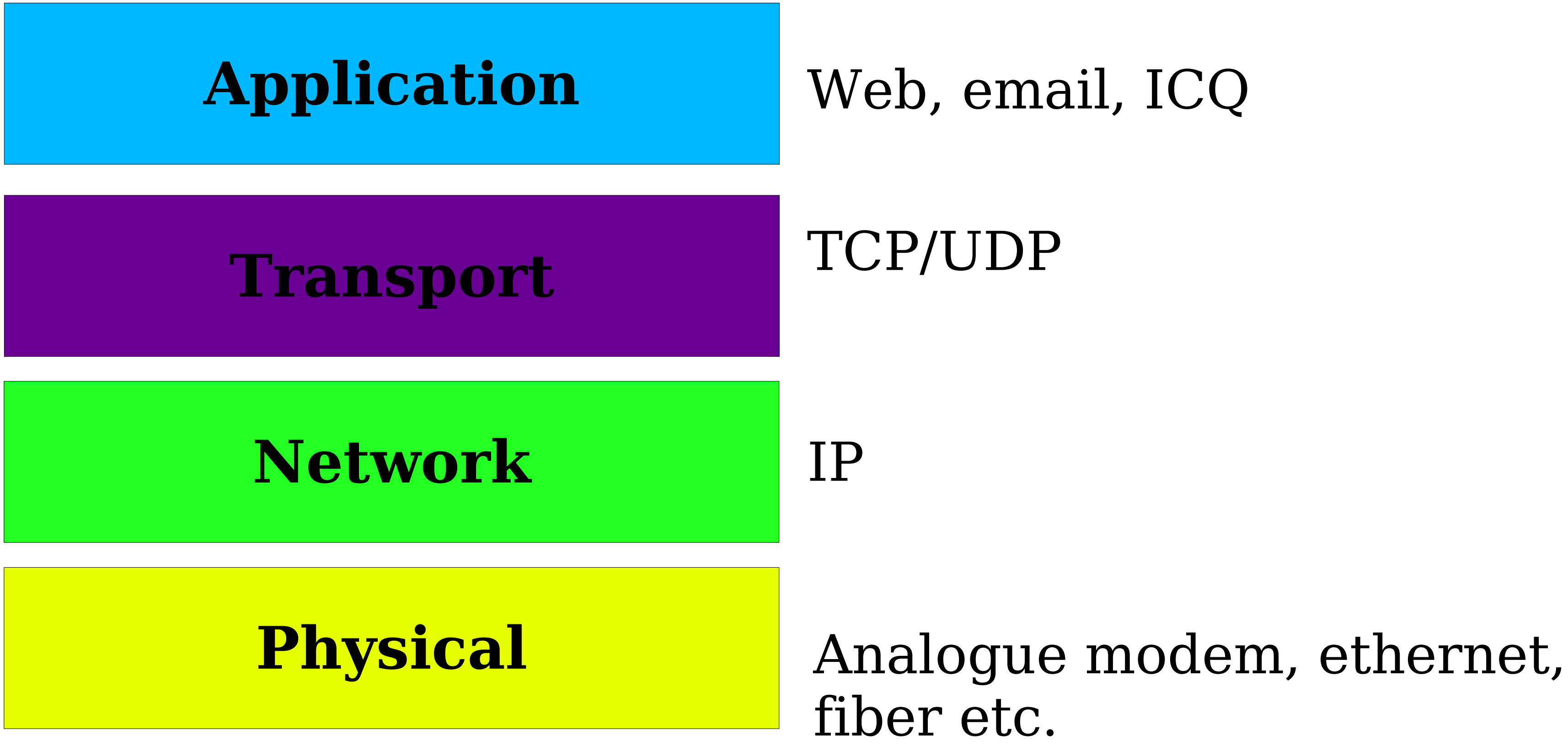
- Sit down at computer and load web browser
- Type in “news.google.com”
- My computer asks DNS server to map news.google.com to IP address
- DNS server responds with “64.233.167.99” (what could happen if server lies?!)
- Computer then asks Google's web server for news
- Google's web server responds
- procrastinate

Ports

- A server can host multiple services (e.g. Web and email)
- Each service has a unique “port” (just another number) that clients connect to
- Ports are standardized on the Internet (80 www, 25 sending email, 21 ftp)
- Hackers see look to see what services are on a host by “port scanning”

The Layered Model

(another way to look at things)



Application Web, email, ICQ

Transport TCP/UDP

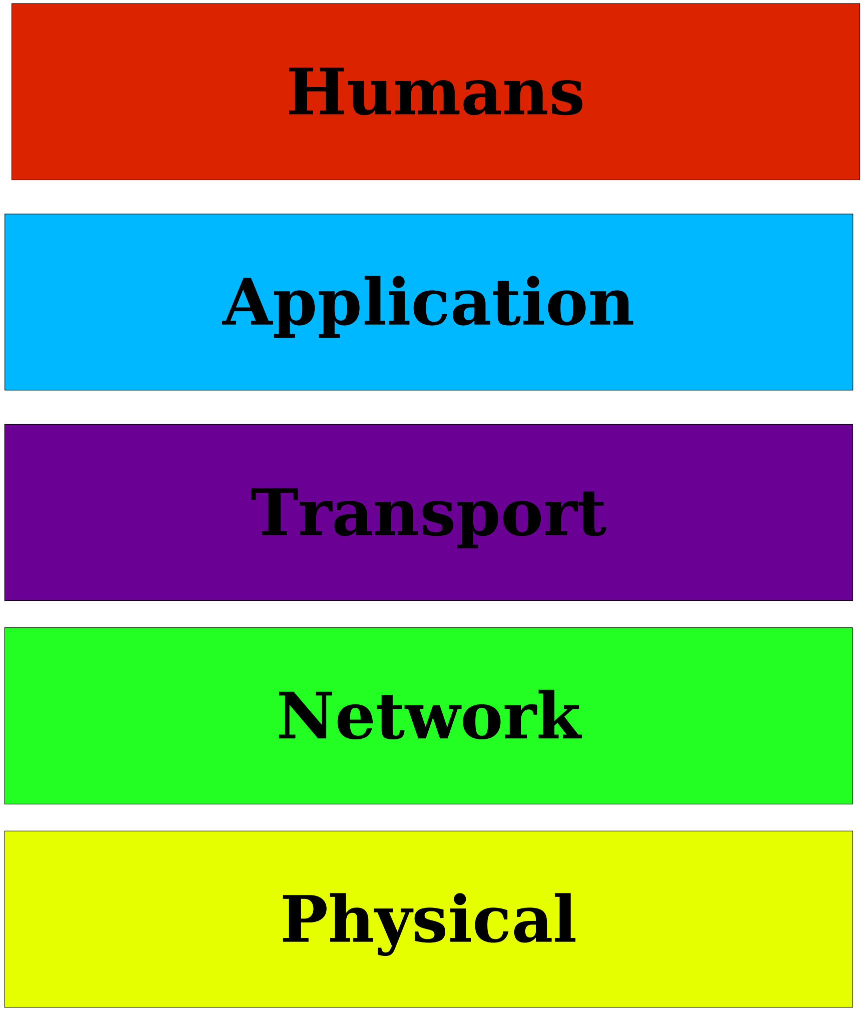
Network IP

Physical Analogue modem, ethernet, fiber etc.

Each Layer Has its Own Vulnerabilities

- Physical
  - I chop your wires or bomb your building
- Network
  - I forge my source address
- Transport
  - I send too many TCP connection requests and freeze your computer
- Application
  - I send a web request to your server to make it croak

Oh ... and Don't Forget the Weakest Layer of All



Humans

Application

Transport

Network

Physical

Humans are Vulnerable!

- Susceptible to beer, chocolate and the opposite sex
- Not experts (and shouldn't be!)
- Often don't care

Attack Classifications

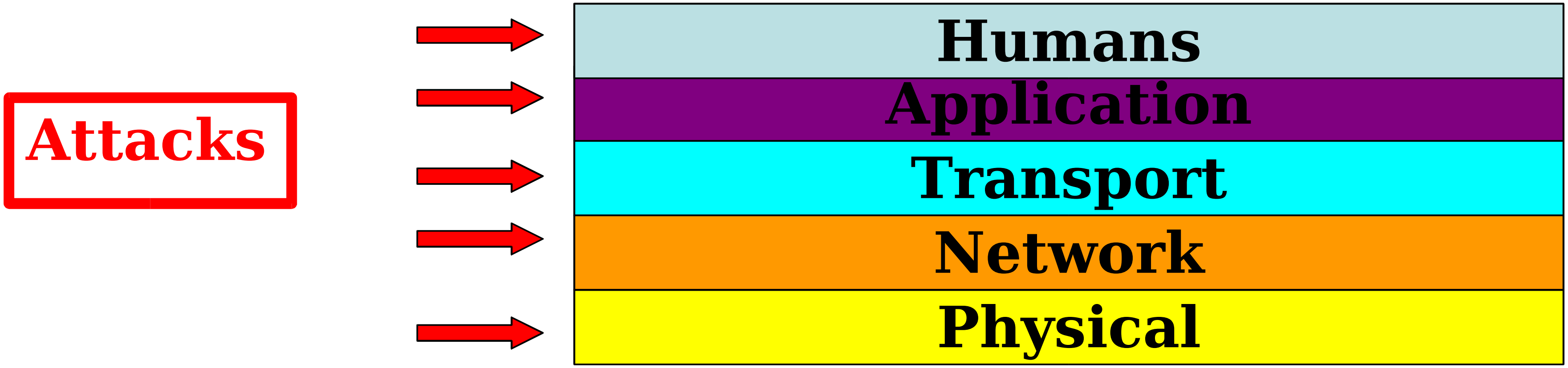
(not mutually exclusive)

Vulnerabilities & Attacks

The nature of the network technologies, protocols, and operators are the basis for attacks.

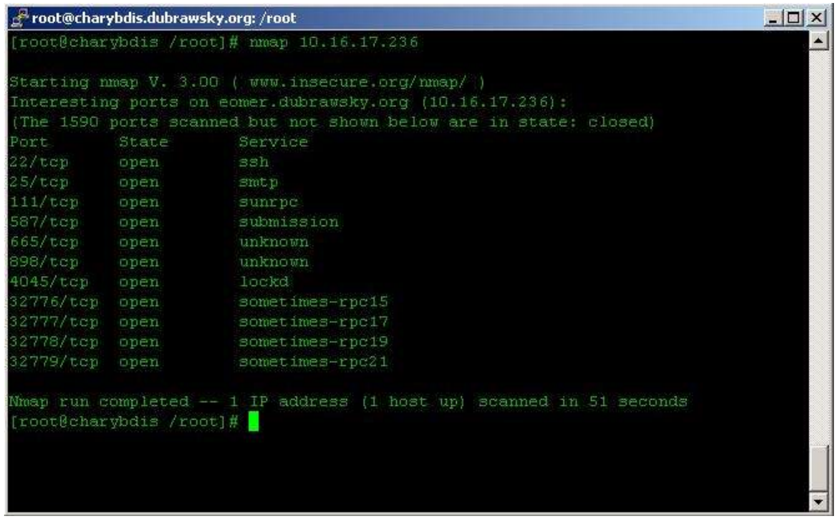
Attacks can (and will) come at vulnerabilities in every layer.

Big Question: What is it about the Internet architecture that causes these vulnerabilities to exist?



Scanning & Fingerprinting

What is it?



```
[root@charybdis /root]# nmap 10.16.17.236

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on eomer.dubrawsky.org (10.16.17.236):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
111/tcp    open        sunrpc
587/tcp    open        submission
665/tcp    open        unknown
898/tcp    open        unknown
4045/tcp   open        lockd
32776/tcp  open        sometimes-rpc15
32777/tcp  open        sometimes-rpc17
32778/tcp  open        sometimes-rpc19
32779/tcp  open        sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 51 seconds
[root@charybdis /root]#
```

Reconnaissance technique to explore networks, classify + analyze connected hosts, and identify potential vulnerabilities.

Example: nmap security scanner

Exploits

What is it?

The use of vulnerabilities in or misconfiguration of software or hardware to gain access to information or resources on a system.

Exploits may be manual or automated.

worms/viruses are exploits with code to facilitate propagation.

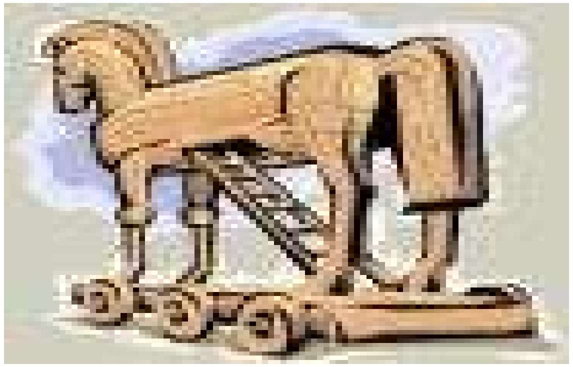
example: Blaster worm exploits RPC bug

Trojaned Software

What is it?

Software/Hardware with hidden functionality that its use allows an attacker an avenue to access a system or its information.

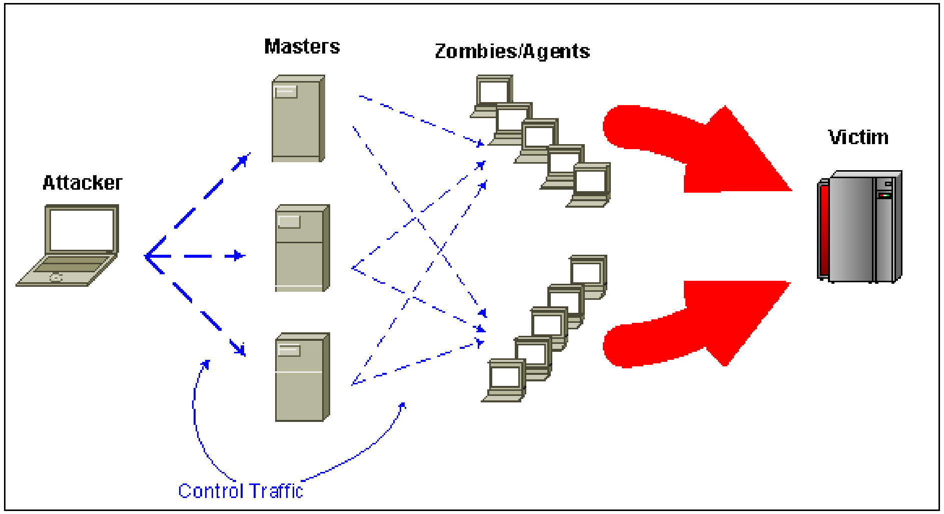
This is sometimes also referred to as a “backdoor”.



Example: A free copy of MSWord downloaded off of Kazaa may have been modified to include a trojan leading to a compromise.

Denial of Service

What is it?



The malicious consumption of resources in order to make a system <u>incapable of fulfilling its designed role</u>.

Attacks are often “distributed” to increase resource consumption (zombies or botnets).

example: SYN flood against Yahoo

Social Engineering Attack

What is it?

Any attempt that employs non-technical means to attack a system. Often the attacker uses information gleaned from outside sources to produce false credentials (dumpster diving).

Attacks are often hybrid, relying on human and technical factors.

example: Beagle virus used email domain name to pose as a message from the user’s ISP.

Access Control Failures

What is it?

- Failure to set up adequate access control
  - Default configurations
  - Privilege revocation

Example: default administrator password for windows

Authentication Failures

What is it?

Some authentication schemes are better than others:

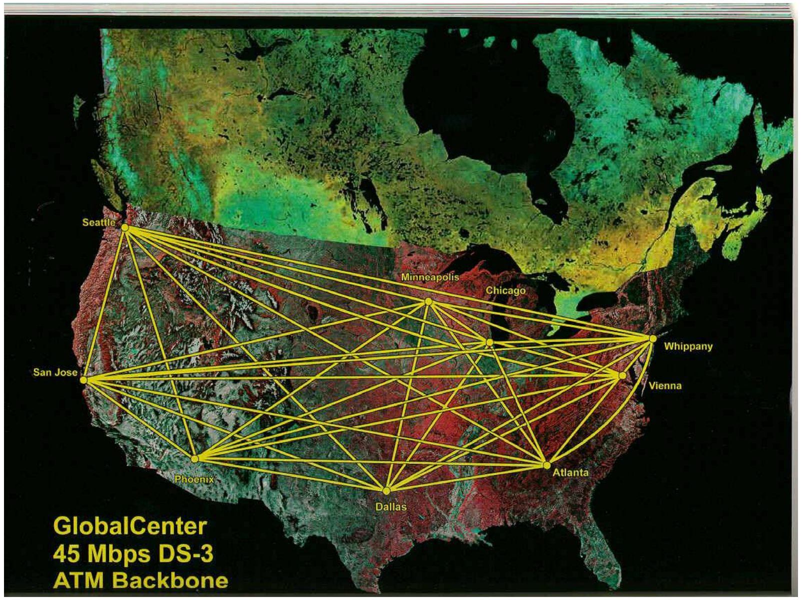
- Passwords
- Public Key Crypto

Example: phishing schemes that steal passwords break the authentication model.

If you have forgotten y password, please call our Internet Help Line

Infrastructure Attack

What is it?



An attack against the core systems that operate as the Internet infrastructure. Attacks can be either physical or virtual, often focusing on central points of failure.

example: Attack on root DNS servers.

Insider Threats

What is it?

Attacks that exploit an existing trust relationship to harm the overall security of a system.

example: former employee uses knowledge of a company’s network systems and passwords to steal customer information entrusted to the company

Traffic Sniffing/Modification

What is it?

Using access to a link or infrastructure system to examine or modify the contents of Internet traffic. Similar to a phone tap, with ability to change contents.

example: ISP’s potential for information gathering

Don’t Forget

Attacks are only one of the reasons systems can fail.   There are many other, perhaps less exciting, ways systems are vulnerable.

Internet Security Mechanisms

What is Cryptography

A critical **TOOL** in securing information systems and their communications.

- You may have heard of:
  - SSL
  - Trusted Computing
  - Public Key Cryptography
  - Tripwire

Cryptography Overview

Crypto can great hard guarantees (backed by math) in the digital world similar to those we have long relied upon for security in the physical world:

- Data Encryption (privacy)
  - “No one else can read my message”
- Data Integrity
  - “My message has not been modified”
  - “My message is from who it says it is”

Also provides for some improved authentication schemes.

Problems with Crypto

- Bad Standards
  - WEP, CSS
- Bad Implementation
  - IE, OpenSSL
- Weak back-end
  - Weak link, insider attacks
- Encryption is often slow & cumbersome

"those who think that their problem can be solved by simply applying cryptography don't understand cryptography and don't understand their problem"

(mutually attributed by B. Lampson and R. Needham to each other)

Attack Detection/Prevention

Firewalls – Software to inspect packets, compare them to rules and drop traffic specified by these rules.

Intrusion Detection/Prevention Systems (IDS/IPS) – Software to inspect traffic flows for signatures or other behavior that appears to be malicious.

Anti-Virus Software – Inspects files for signs of infectious programs and eliminates them.

These mechanisms can either be deployed on individual hosts or on dedicated network servers.

Patching

Fix vulnerabilities in software that may lead to exploitation. Patch management is major hidden cost to companies.

Important:

- Gap between release of patch + first exploit “in the wild” is shrinking (Witty worm and zero-days).

- Often patches are not applied to critical systems because updates sometimes have conflicts that can break software running on the systems.

Do we patch?

Check out: “Security Holes? Who Cares” by Eric Rescorla. : http://www.rtfm.com/upgrade.pdf

Process, Education & Risk Assessment

Often forgotten as security mechanisms:

- Having well-defined and consistent preparation, response, and recovery plans across an organization.

- Attempting to secure humans, often the weakest link.

- Determining the danger associated with each potential vulnerability.

The End!