Internet 101

U.S. National Cybersecurity,
Technical Breakout #1
10/5/04

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.
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
- Internet Cafe's
“Core” computers

- **Routers**: try to figure out how traffic goes from point A to point B (on the Internet)
- In the core, **routers** use a mechanism called **BGP** to figure out where to send the packets next (this is a big technical and political rathole!)
Core vs. Edge

Edge

Core

Edge

router

End Host
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
Edge is you, me and aunt Bev
(and business, and gov and edu)

- Plug into Internet through an ISP
- ISP charges us to use their bandwidth
- ISPs charge other ISPs to lease lines
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)
  123.114.23.4
  10.15.46.32

• Really just a value from 1 to \(2^{32} - 1\)
  represented 4 in octets (chunks of 2^8)
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 Addressesss 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 sender, plus data

```
data | ip src | ip dst
```

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 lose a bullet or two while playing 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
- When listening to music online, 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!
  - Only 13!
  - 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 uses TCP to ask Google's web server for news
- Google's web server responds
- I 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.
IP runs on everything, everything runs on IP
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 bad request to your web server that makes it croak
Oh ... and Don't Forget the Weakest Layer of All

- Humans
- Application
- Transport
- Network
- Physical

You, me, aunt Bev
Humans are Vulnerable!

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