

Lecture 8: Network Security

David Lie
ECE1776

1

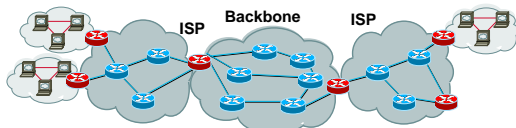
Outline

- Networking 101
- Network Hacking
- Protocol Vulnerabilities
 - TCP weaknesses
 - BGP/EGP, Spoofing
 - Snooping
 - DDOS, Smurf
- Network Security
 - Border Security: Firewalls, Proxies
 - Encryption: VPN, IPSEC, SSH/SSL



2

Internet Infrastructure

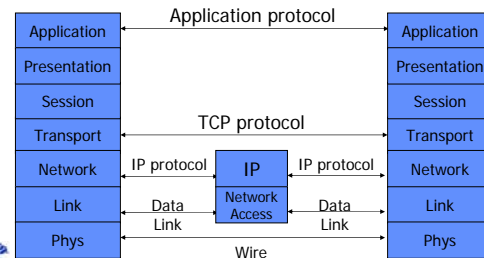


- Local and interdomain routing
 - IP routes traffic
 - BGP for routing control
- Domain Name System
 - Find IP address, indexing



3

OSI TCP/IP Protocol Stack



4

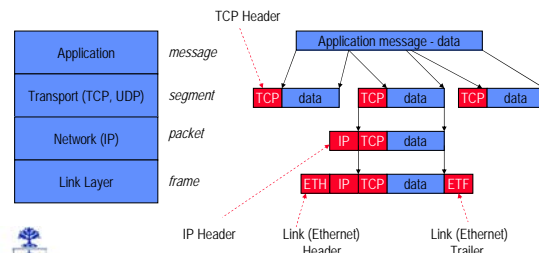
Layer Functions

Layer	Key Unit	Function
Physical	Bit	Electrical signals on the wire, signaling schemes
Link	Frame	Transmission error recovery, framing
Transport	Packet	Routing, packetization, TCP/UDP/CMP
...	...	OS level stuff, API (connections, sockets, etc...)
Application		Application level protocol

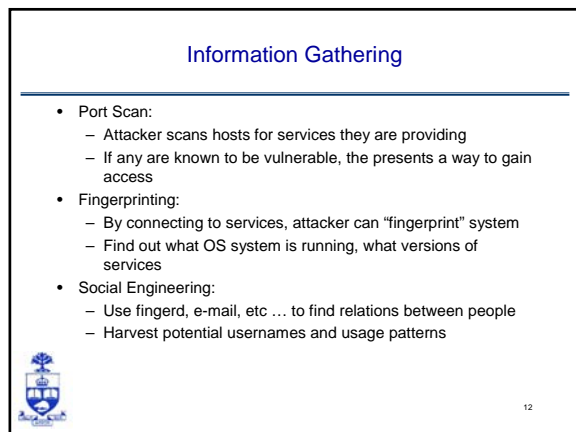
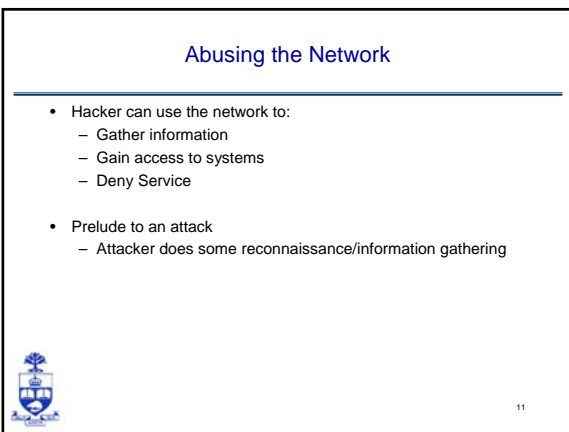
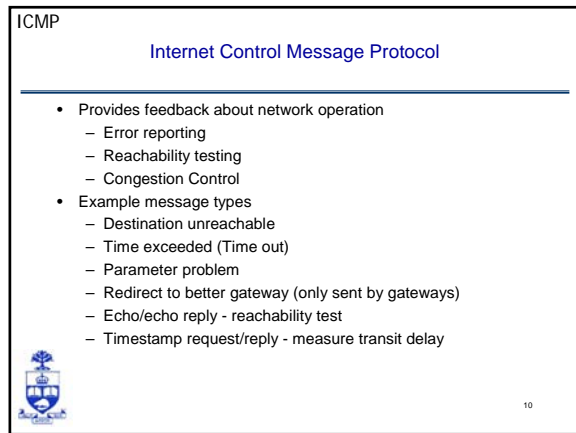
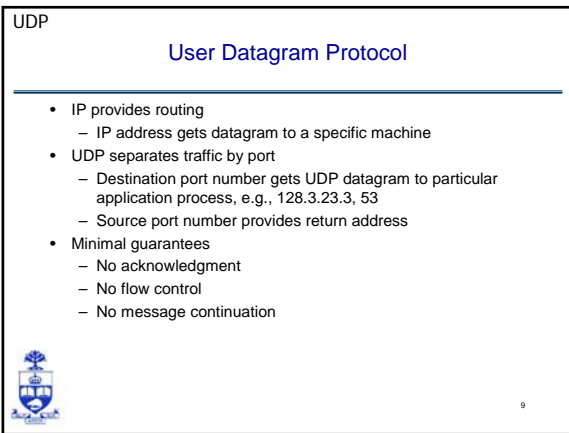
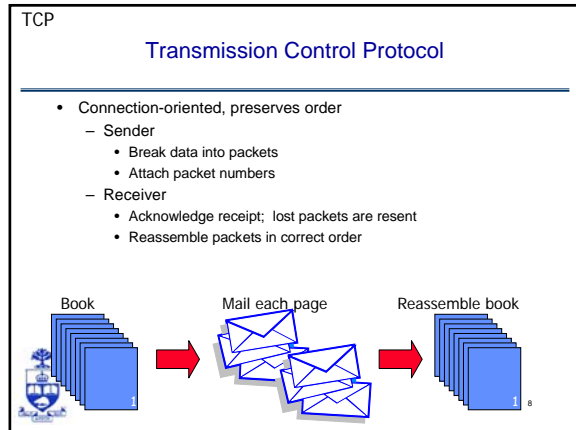
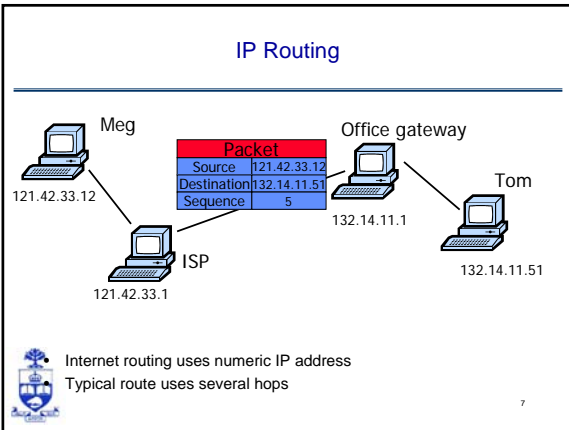


5

Data Formats



6



Nmap Port Scan

```
blackcomb:~% nmap picton.eecg.toronto.edu
Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2004-03-22 10:01 EST
Interesting ports on picton.eecg.toronto.edu (128.100.10.141):
(The 1632 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
9/tcp    open  discard
13/tcp   open  daytime
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
37/tcp   open  time
53/tcp   open  domain
79/tcp   open  finger
110/tcp  open  pop3
111/tcp  open  rpcbind
113/tcp  open  auth
143/tcp  open  imap
....
```



13

Some Other Network Security Attacks

- Eavesdropping, packet sniffing
 - Network packets pass by untrusted hosts
- TCP session hijacking
 - TCP sequence numbers are predictable
- Routing attacks
 - Attacks on BGP/EGP
- DNS Name Spoofing
 - Claim the identity of a host
- Denial of Service
 - Distributed Denial of Service, Smurf, SYN Flooding
- These attacks discussed in [Security Problems in the TCP/IP Protocol Suite](#), Steven M. Bellovin



14

Denial of Service

- Attacks that make networks inaccessible for legitimate users:
- Using up resources
 - Bandwidth: Distributed attacks, Smurf attacks
 - Host memory: SYN Flooding attacks
 - Operation: Ping of Death



15

Yahoo DOS

To: <nanog@merit.edu>
Subject: Yahoo offline because of attack (was: Yahoo network outage)
From: Declan McCullagh <declan@wired.com>
Date: Mon, 07 Feb 2000 20:31:24 -0500

Yahoo told me on the phone that it's a malicious attack, and Global Center says the same thing. In Yahoo's words: "a coordinated distributed denial of service attack." We've got a brief story up at: <http://www.wired.com/news/business/0,1367,34178,00.html> The problem apparently originated with a router. But what kind of attack could have taken the network offline for that period of time and not affected other Global Center customers? I mean, there had to have been a gaping security hole somewhere: It looks like the routes got lost for (nearly) all of the Yahoo network, but no other non-Yahoo sites...

-Declan



16

Routers Blamed for Yahoo Outage by Declan McCullagh and Joan

- Most of Yahoo unreachable for three hours on
- Attackers reportedly laid siege...
 - Denying millions of visitors access ...
- An engineer at another company ...
 - told Wired News outage due to misconfigured equipment
- Details remained sketchy...
- A Yahoo spokesperson called it a "coordinated distributed denial of service attack"



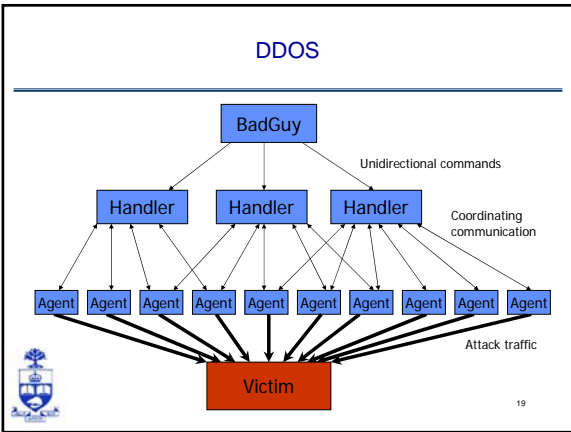
17

What happened?

- Coordinated effort from many sites
- Sites were compromised
 - According to Dittrich's DDoS analysis,
 - trinoo and tfn daemons found on of Solaris 2.x systems
 - systems compromised by exploitation of buffer overrun in the RPC services statd, cmsd and ttdbserverd
- Compromised machines used to mount attack



18



Trin00

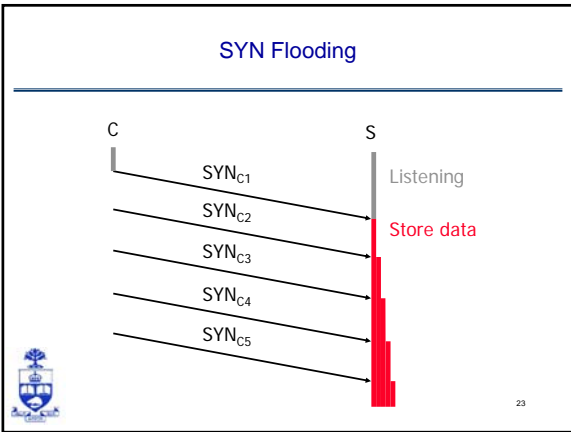
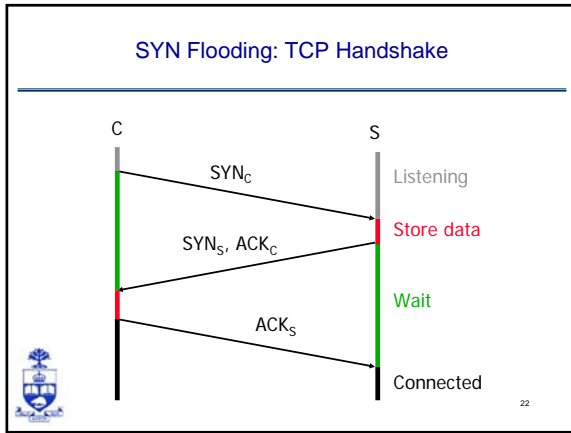
- Installed on various Solaris systems in 1999
- Commands can be given:
 - Client to Handler to Agent to Victim
 - Attacks through UDP flood
 - Command strings were all 3 characters or less (avoid showing up if standard "strings" command is run)
 - Ask handlers to retrieve a list of agents
- Passwords protect handlers and agents of Trin00 network, though sent in clear text
 - Passwords were hardcoded into clients in crypt() format
- Uses cron to start a process so extra entry is created in crontab
- Warns if there is another connection to avoid detection

20

Tribal Flood Network (TFN)

- Client to Daemon to Victim
- TCP, SYN and UDP floods
- No passwords for client
- Client-Daemon communication only in ICMP
- Needs root access
- Fixed payload size
- Does not authenticate incoming ICMP

21



SYN Flooding

- Attacker sends many connection requests
 - Spoofed source addresses
- Victim allocates resources for each request
 - Connection requests exist until timeout
 - Fixed bound on half-open connections
- Resources exhausted \Rightarrow requests rejected

24

Protection against SYN Attacks

[Bernstein, Schenk]

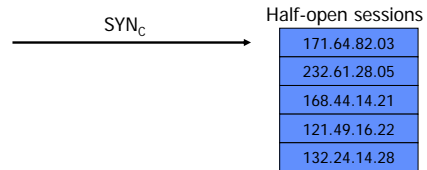
- Client sends SYN
- Server responds to Client with SYN-ACK cookie
 - $sqn = f(\text{src addr, src port, dest addr, dest port, rand})$
 - Server does not save state
- Honest client responds with ACK(sqn)
- Server checks response
 - If matches SYN-ACK, establishes connection

See <http://cr.jp.to/syncookies.html>



25

Random Deletion



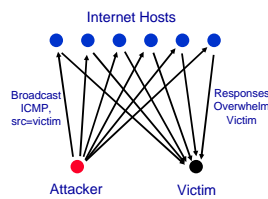
- If queue is full, delete random entry
 - Legitimate connections have chance to complete
 - Fake addresses eventually deleted
- Easy to implement, some improvement



26

Smurf Attack

- Choose victim
 - Idea: Flood victim with packets from many sources
- Generate ping stream (ICMP Echo Req)
 - Network broadcast address with spoofed source IP set to victim
- Wait for responses
 - Every host on target network will generate a ping reply (ICMP Echo Reply) to victim
 - Ping reply stream can overload victim



Prevention: Turn off ping? Authenticated IP addresses?



27

“Ping of Death”

- Windows machines contained a programming error
 - Machine would crash or reboot
 - Packets of this length are illegal, so programmers did not account for them
- Solutions:
 - Patch
 - Filter out ICMP packets



28

More Recently

Date: Fri, 19 Mar 2004 17:15:56 -0500 (EST)
 From: Eugenia Distefano <eugenia@eecg.toronto.edu>
 To: David Lie <lie@eecg.toronto.edu>
 Subject: Re: Honeybot activity

I have seen these in the logs of the eecg web servers too. The campus switches have been bombarded with these packets as well and apparently 3Com switches reset when they get these packets. This has caused the campus backbone to be up and down most of yesterday. The attack seems to start with connection attempts to port 1025 (Active Directory logon, which fails), then 6129 (DameWare backdoor, which fails), then 80 (which works as the 3Com's support a web server, which can't be disabled as far as we know). The HTTP command starts with 'SEARCH /x90x02xb1x02.....' (the 'xb1x02' goes on for quite a while), then goes off into a continual pattern of 'x90'



29

Some Solutions

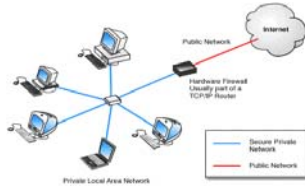
- Solutions based around controlling access to networks
- Border Security to control access:
 - Firewalls
 - Proxies/Bastion Machines
- Cryptographic Solutions to control access:
 - IPSEC
 - VPN's
 - SSH/SSL



30

Border Security

- Try and stop bad guys from entering
- Firewall:
 - Simple machine who's main operation is to block access



31

Firewalls

- Minimal machines:
 - Provide few services, less likely of compromise
- Types of firewalls

Type	Complexity	Description
Packet Filtering	Simple	Usual filters based on src address, destination port, only sees headers
Host or Personal	Simple	Runs on the host system. Filters same as packet, but may also filter outgoing connections based on application
Stateful Inspection	More complex	Packet reassembly to see data portion, examines packet payloads, connections

32

Proxies

- These are programs that mimic applications but do some inspections/performance enhancement
 - Examples are web proxies, ftp proxies, news proxies, etc...
 - May filter content:
 - E.g. web proxies may remove ads, dangerous code
 - May also improve performance by caching content for many users

33

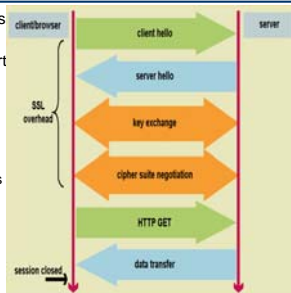
Cryptographic protection

- Solutions above the transport layer
 - Examples: SSL and SSH, Protect against session hijacking and injected data
 - Do not protect against denial-of-service attacks caused by spoofed packets
- Solutions at network layer
 - IPSec, VPN's
 - Can protect against
 - session hijacking and injection of data
 - denial-of-service attacks using session resets

34

SSH/SSL

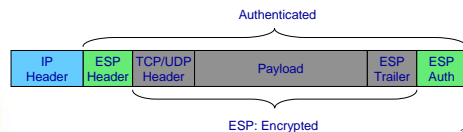
- Secure Shell/Secure Sockets Layer
 - SSL also called Transport Layer Security (TLS)
 - Establishes encrypted channel for communications
 - Establishes a private session with public keys
 - All communications encrypted with private key



35

IPSec


- Developed by IETF as part of IPV6
 - Designed to address security problems in IPV4
 - Session hijacking
 - Host spoofing
 - Snooping
- IPSec packet:
 - TCP header + Data are encrypted and hashed to form **Encapsulated Security Payload (ESP)**
- More discussion in [A Cryptographic Evaluation of IPSec](#) Bruce Schneier



36

Virtual Private Networks (VPNs)


- Very common security solution for companies now:
 - Netscreen bought by Juniper for \$3.3 Billion
 - Can be built on top of SSL or IPSec infrastructure
 - Works well with firewalls
 - User outside the firewall needs to get inside the firewall safely
 - Encrypted “tunnel” or channel is negotiated with firewall
 - User’s packets going to hosts behind the firewall get translated so they look like they’re coming from an internal IP
 - From the user’s point of view, they are “inside” the private network



37


Summary

- Network Hacking
 - Reconnaissance, Social Engineering, Fingerprinting
- Protocol Vulnerabilities
 - Snooping
 - TCP sequence number predication
 - BGP/EGP, DNS Spoofing
 - DDOS, Smurf, Ping of Death
- Network Security
 - Border Security: Firewalls, Proxies
 - Cryptographic Solutions: VPN, IPSEC, SSH/SSL



38

Extra Slides




39

IP Internet Protocol

- Connectionless
 - Unreliable
 - Best effort
- Transfer datagram
 - Header
 - Data


Version	Header Length
Type of Service	
Total Length	
Identification	
Flags	Fragment Offset
Time to Live	
Protocol	
Header Checksum	
Source Address of Originating Host	
Destination Address of Target Host	
Options	
Padding	
IP Data	



40

IP Protocol Functions (Summary)


- Routing
 - IP host knows location of router (gateway)
 - IP gateway must know route to other networks
- Error reporting
 - IP reports discards to source
- Fragmentation and reassembly
 - If packets smaller than the user data



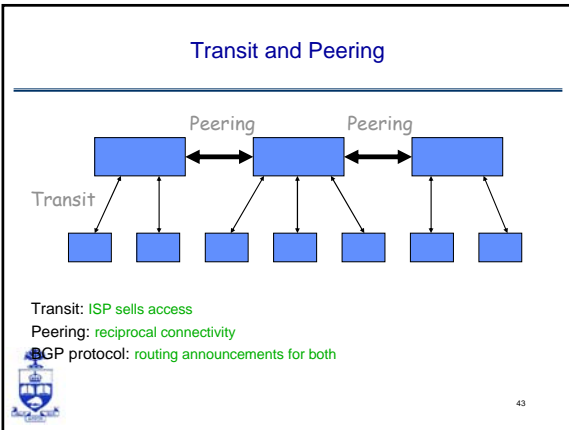
41

BGP overview

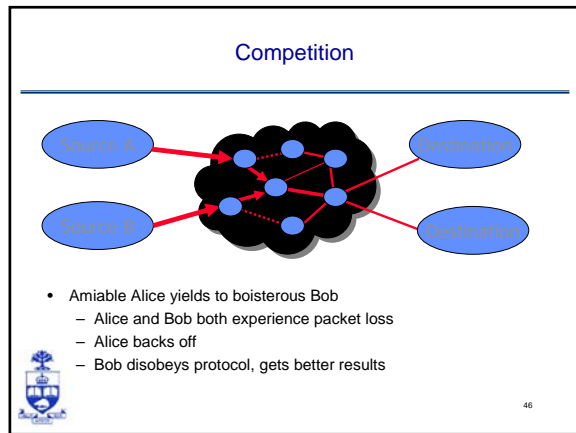
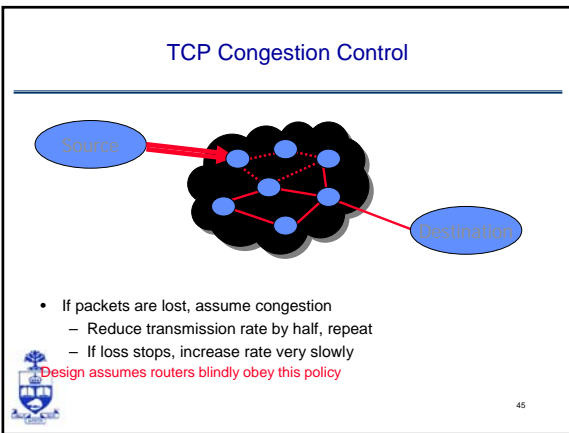
- Iterative path announcement
 - Path announcements grow from destination to source
 - Subject to policy (transit, peering)
 - Packets flow in reverse direction
- Protocol specification
 - Announcements *can* be shortest path
 - Nodes allowed to use other policies
 - E.g., “cold-potato routing” by smaller peer
 - Not obligated to use path you announce



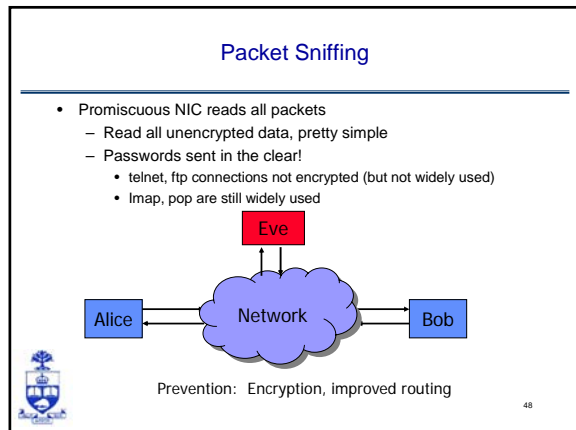
42



- ### Issues
- BGP convergence problems
 - Protocol allows policy flexibility
 - Some legal policies prevent convergence
 - Even shortest-path policy converges slowly
 - Incentive for dishonesty
 - ISP pays for some routes, others free
 - Security problems
 - Potential for disruptive attacks
- 44



- ### TCP Attack on Congestion Control
- Misbehaving receiver can trick sender into ignoring congestion control
 - Receiver: duplicate ACK indicates gap
 - Packets within seq number range assumed lost
 - Sender executes fast retransmit algorithm
 - Malicious receiver can
 - Send duplicate ACK
 - ACK before data is received
 - needs some application level retransmission – e.g. HTTP 1.1 range requests ... See RFC 2581
 - Solutions
 - Add nonces – ACKs return nonce to prove reception
- See: Savage et al., TCP Congestion Control with a Misbehaving Receiver
- 47



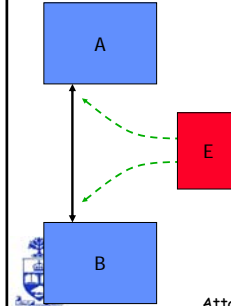
TCP Connection Hijacking

- Each TCP connection has an associated state
 - Sequence number, port number
- Problem
 - Easy to guess state
 - Port numbers are standard
 - Sequence numbers often chosen in predictable way



49

IP Spoofing Attack



- A, B trusted connection
 - Send packets with predictable seq numbers
- E impersonates B to A
 - Opens connection to A to get initial seq number
 - SYN-floods B's queue
 - Sends packets to A that resemble B's transmission
 - E cannot receive, but may execute commands on A

Attack can be blocked if E is outside firewall.



50

TCP Sequence Numbers

- Need high degree of unpredictability
 - If attacker knows initial seq # and amount of traffic sent, can estimate likely current values
 - Send a flood of packets with likely seq numbers
 - larger bandwidth => larger flood possible
- Reported to be safe from practical attacks
 - Cisco IOS, OpenBSD 2.8-current, FreeBSD 4.3-RELEASE, AIX, HP/UX 11i, Linux Kernels after 1996
 - Solaris 2.6 if strong seq numbers turned on:
 - Set TCP_STRONG_ISS to 2 in /etc/default/inetinit.
 - HP/UX, IRIX 6.5.3, ... if so configured



51

Routing Vulnerabilities

- Source routing attack
 - Can direct response through compromised host
- Routing Information Protocol (RIP)
 - Direct client traffic through compromised host
- Exterior gateway protocols
 - Advertise false routes
 - Send traffic through compromised hosts



52

Source Routing Attacks

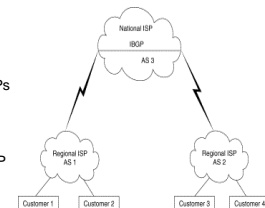
- Attack
 - Destination host may use reverse of source route provided in TCP open request to return traffic
 - Modify the source address of a packet
 - Route traffic through machine controlled by attacker
- Defenses
 - Gateway rejects external packets claiming to be local
 - Reject pre-authorized connections if source routing info present
 - Only accept source route if trusted gateways listed in source routing info



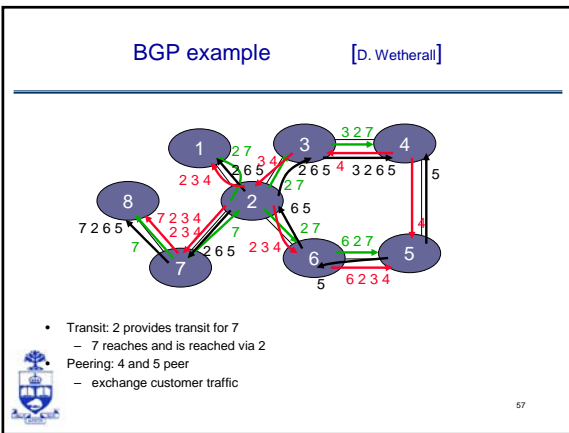
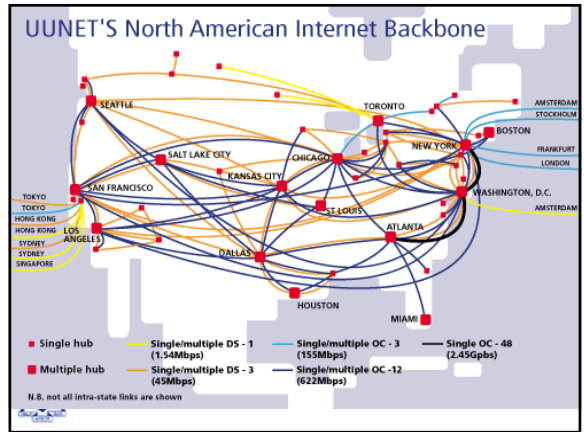
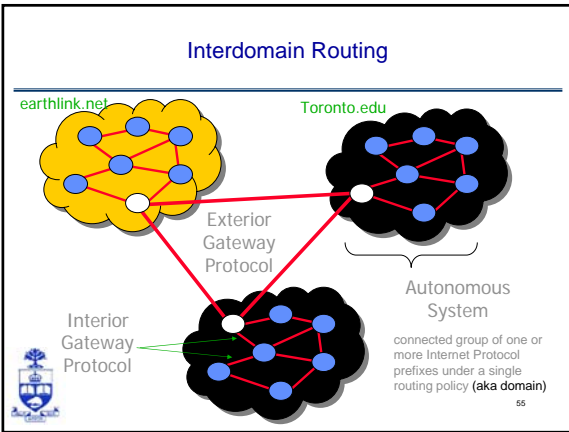
53

Routing Table Update Protocols

- Border Gateway Protocol: BGP
 - Protocol that gateways use to exchange routing information
- Interior Gateway Protocols: IGPs
 - Used for gateways within and autonomous system (AS)
- Exterior Gateway Protocol: EGP
 - used for communication between different autonomous systems



54



Routing Information Protocol (RIP)

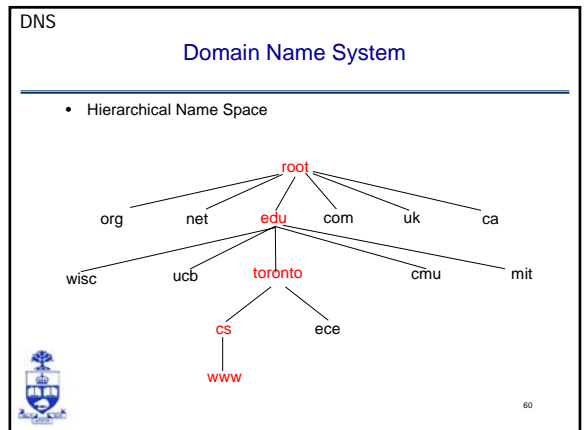
- Attack
 - Intruder sends bogus routing information to a target and each of the gateways along the route
 - Impersonates an unused host
 - Diverts traffic for that host to the intruder's machine
 - Impersonates a used host
 - All traffic to that host routed to the intruder's machine
 - Intruder inspects packets & resends to host w/ source routing
 - Allows capturing of unencrypted passwords, data, etc

58

Routing Information Protocol (RIP)

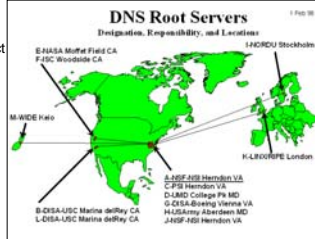
- Defense
 - Paranoid gateway
 - Filters packets based on source and/or destination addresses
 - Don't accept new routes to local networks
 - Interferes with fault-tolerance but detects intrusion attempts
 - Authenticate RIP packets
 - Difficult in a broadcast protocol
 - Only allows for authentication of prior sender

59



DNS Root Name Servers

- Root name servers
- Local name servers contact servers when they cannot resolve a name



61

DNS name spoofing

- Many services authenticated by hostname:
 - Hosts.equiv
 - .rhosts
 - Mail filters
 - NIS/NIS+
- Attacking DNS server is a valuable asset:
 - Change entries to allow your host to become trusted



62

DNS Implementation Vulnerabilities

- Reverse query buffer overrun in BIND Releases 4.9 (4.9.7 prior) and Releases 8 (8.1.2 prior)
 - gain root access
 - abort DNS service
- MS DNS for NT 4.0 (service pack 3 and prior)
 - crashes on chargen stream
 - telnet ntbbox 19 | telnet ntbbox 53



63

Inherent DNS Vulnerabilities

- Users/hosts typically trust the host-address mapping provided by DNS
- Problems
 - Zone transfers can provide useful list of target hosts
 - Interception of requests or compromise of DNS servers can result in bogus responses
 - Solution – authenticated requests/responses



64

Bellovin/Mockapetris Attack

- Trust relationships use symbolic addresses
 - /etc/hosts.equiv contains friend.stanford.edu
- Requests come with numeric source address
 - Use reverse DNS to find symbolic name
 - Decide access based on /etc/hosts.equiv, ...
- Attack
 - Spoof reverse DNS to make host trust attacker



65

Reverse DNS

- Given numeric IP address, find symbolic addr
- To find 222.33.44.3,
 - Query 44.33.222.in-addr.arpa
 - Get list of symbolic addresses, e.g.,
 - 1 IN PTR server.small.com
 - 2 IN PTR boss.small.com
 - 3 IN PTR ws1.small.com
 - 4 IN PTR ws2.small.com



66

Attack

- Gain control of DNS service for domain
- Select target machine in domain
- Find trust relationships
 - SNMP, finger can help find active sessions, etc.
 - Example: target trusts host1
- Connect
 - Attempt rlogin from compromised machine
 - Target contacts reverse DNS server with IP addr
 - Use modified reverse DNS to say addr is host1
 - Target allows rlogin



67

Defense against this attack

- Double-check reverse DNS
 - Modify rlogind, rshd to query DNS server
 - See if symbolic addr maps to numeric addr
- Use another service besides DNS
 - SSH hostkeys
 - NIS servers keep their own name/IP maps



68