ELEC5616 COMPUTER & NETWORK SECURITY

Lecture 18:

Network Protocols II

SOURCE ROUTING

Both IPv4 and IPv6 allow the sender (rather than routers) to specify routes that packets take through a feature known as source routing (a.k.a ‘path addressing’).

In strict source routing, the sender specifies each hop that the packet takes through the network (IP Header: SSRR)

In loose source routing, the sender only specifies a group of hosts the packet must transit through. (IP Header: LSRR)

This allows a remote attacker to facilitate non-blind attacks (whereas they previously could only mount blind attacks as they do not receive reply packets).

Source routing can be turned off in the kernel.

SOURCE ROUTING

Many kernels are configured to ignore source routing.

Many firewalls/routers block source routed packets and may optionally trigger alarms.

PORT SCANNING

Port scanning is the process of sending packets to all ports on a machine (or range of machines) to audit available (open) services.

```
# nmap 192.168.0.1-255

Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on cosmic.spectre.net (192.168.0.1):
Port    State       Protocol  Service
22      open        tcp       ssh
139     open        tcp       netbios-ssn

Interesting ports on orbital.spectre.net (192.168.0.2):
Port    State       Protocol  Service
7       open        tcp       echo
9       open        tcp       discard
21      open        tcp       ftp
25      open        tcp       smtp
42      open        tcp       nameserver
53      open        tcp       domain
80      open        tcp       http

Nmap run completed -- 255 IP addresses (2 hosts up) scanned in 10 seconds
```

OS FINGERPRINTING

OS fingerprinting is the process of scanning machines using peculiarities in the IP stack in order to identify the vendor and operating system version.

```
# nmap -O 192.168.0.2

Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on orbital.spectre.net (192.168.0.2):
Port    State       Protocol  Service
7       open        tcp       echo
9       open        tcp       discard
13      open        tcp       daytime

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=10629 (Worthy challenge)
Remote operating system guess: Windows 2000 RC1-RC3

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

FIREWALLS

A firewall is a packet filtering gateway which aims to limit the number of exposed services on a connection (aka a wall with holes in it):

Static packet filtering gateways look at a set of static rules known as access control lists (ACLs). Static packet filters are fast but reasonably weak (and difficult to maintain).

Dynamic packet filtering gateways aims being more intelligent about what packets to allow (e.g. by stateful inspection of packet headers).

Application level gateways attempt to enhance the security further through acting as a proxy (allowing user authentication and not allowing direct IP connections between the inside and the outside) but are more complicated still and don’t support all services (hence aren’t used that often).

FTP BOUNCE ATTACKS

FTP servers can be used to launch “bounce” attacks.

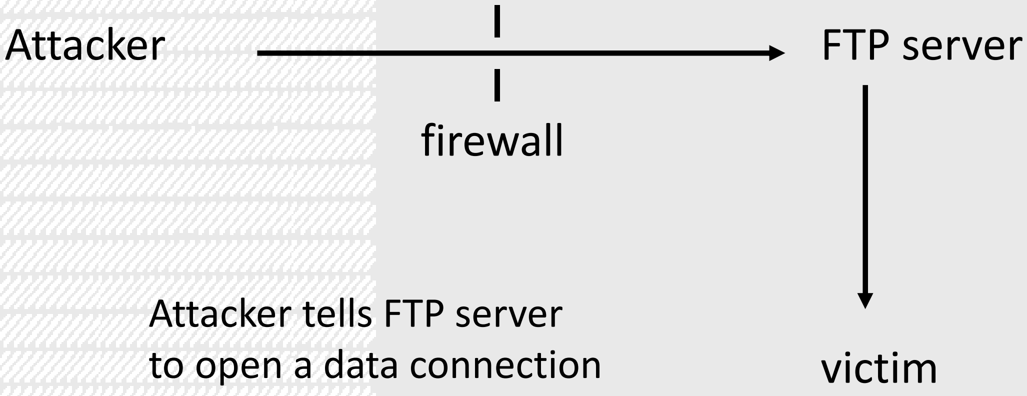
An example of an attack a firewall doesn’t help against.

Take the following example:

- Attacker finds FTP server located behind a firewall, allowing connections with writeable directory.
- Attacker logs in and uploads a file containing SMTP commands for a spoofed mail message.
- Attacker then uses PORT command to point to a victim’s mail port.
- Attacker then uses RETR command to initiate file transfer.
- The FTP server will then connect to the victim’s mail port, uploading valid mail commands (and, for example, can send mail pretending to be the FTP server).

(http://en.wikipedia.org/wiki/List_of_FTP_commands)

FTP BOUNCE ATTACKS



Attacker

firewall

FTP server

victim

Attacker uploads
SMTP dialog:

```
hello pizza.com
mail from: server.goodguy.com
rcpt to: victim.goodguy.com
data
hello there!
.
end
```

Attacker tells FTP server to open a data connection to the victim’s SMTP port and “upload” the file.

Victim gets (believable) spoofed email

TRACEROUTE

Traceroute is a network debugging utility designed to map out the pathway between two hosts over IP by monotonically increasing the time-to-live (TTL) field in the IP header.

The TTL field is used to limit the number of hops a packet may across the network before it expires.

On expiry, a ICMP error message is generated (time to live exceeded in transit).

By monotonically increasing the TTL field we will receive such an error message from every host along the path the packet takes to the destination (and hence a route).

TRACEROUTE

```
# traceroute cassius.ee.usyd.edu.au
traceroute to cassius.ee.usyd.edu.au (129.78.13.49), 30 hops max, 40 byte
packets
 1  * * *
 2  sydney-atm.vic-remote.bigpond.net.au (61.9.128.189)  34.477 ms  35.317
ms  32.934 ms
 3  202.12.157.72 (202.12.157.72)  34.205 ms  36.603 ms  32.927 ms
 4  fastethernet4-1-0.win4.Melbourne.telstra.net (139.130.61.117)  32.514 ms
34.914 ms  35.385 ms
 5  FastEthernet0-0-0.lon20.Melbourne.telstra.net (203.50.79.30)  34.258 ms
32.954 ms  33.645 ms
 6  optvs.lnk.telstra.net (139.130.6.26)  38.416 ms  34.988 ms  35.881 ms
 7  GigEth1-0-0.sn2.optus.net.au (202.139.190.16)  47.587 ms  46.593 ms
48.402 ms
 8  NSW-RNO-Dom.sn2.optus.net.au (202.139.18.114)  51.023 ms  58.395 ms
49.161 ms
 9  usyd-atm-chippendale.nswrno.net.au (203.15.123.36)  81.577 ms  91.889 ms
91.788 ms
10  su-ti.gw.usyd.edu.au (129.78.226.241)  85.420 ms  78.939 ms  91.274 ms
11  * * *
12  * * *
13  cassius.ee.usyd.edu.au (129.78.13.49)  94.850 ms  100.272 ms *
```

FIREWALKING

Firewalking is the process of determining the access control lists (ACLs) of packet filtering gateways (e.g. firewalls, routers, etc.) similar to traceroute.

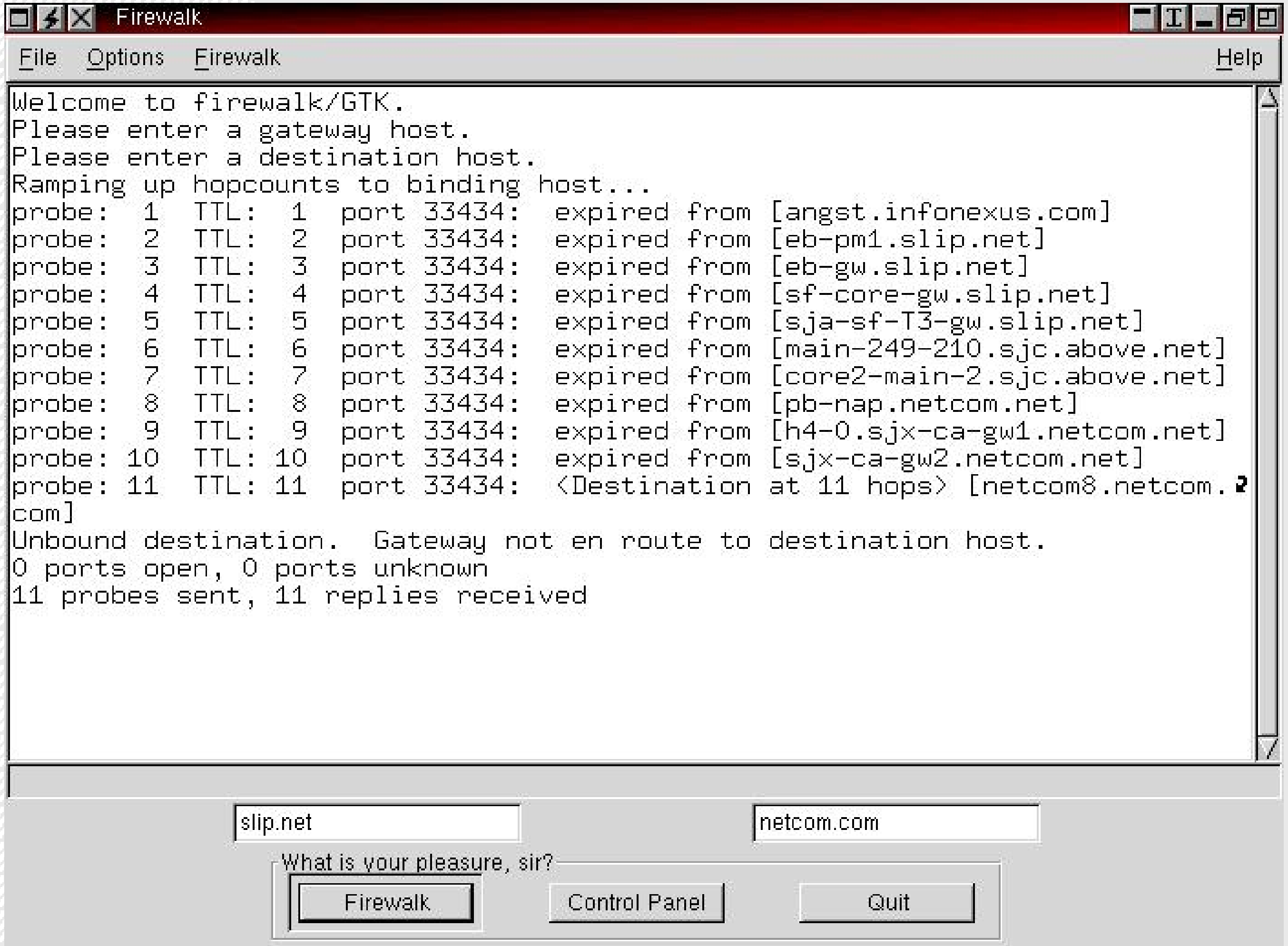
The firewalk scan works by sending out packets with a TTL one greater than the targeted gateway.

If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit a TTL exceeded in transit message (which we get back).

If the gateway host does not allow the traffic, it will likely drop the packets on the floor and we will see no response.

Through such scanning ACLs on a gateway or firewall can be determined.

FIREWALKING



```
Welcome to firewalk/GTK.
Please enter a gateway host.
Please enter a destination host.
Ramping up hopcounts to binding host...
probe:  1  TTL:  1  port 33434:  expired from [angst.infonexus.com]
probe:  2  TTL:  2  port 33434:  expired from [eb-pm1.slip.net]
probe:  3  TTL:  3  port 33434:  expired from [eb-gw.slip.net]
probe:  4  TTL:  4  port 33434:  expired from [sf-core-gw.slip.net]
probe:  5  TTL:  5  port 33434:  expired from [sja-sf-T3-gw.slip.net]
probe:  6  TTL:  6  port 33434:  expired from [main-249-210.sjc.above.net]
probe:  7  TTL:  7  port 33434:  expired from [core2-main-2.sjc.above.net]
probe:  8  TTL:  8  port 33434:  expired from [pb-nap.netcom.net]
probe:  9  TTL:  9  port 33434:  expired from [h4-0.sjx-ca-gw1.netcom.net]
probe: 10  TTL: 10  port 33434:  expired from [sjx-ca-gw2.netcom.net]
probe: 11  TTL: 11  port 33434:  <Destination at 11 hops> [netcom8.netcom.
com]
Unbound destination.  Gateway not en route to destination host.
0 ports open, 0 ports unknown
11 probes sent, 11 replies received
```

slip.net

netcom.com

IPSEC

IPsec is the working group on security aiming at securing the Internet architecture (both IPv4 and IPv6).

The two main features of IPsec are:

- Authentication Header (AH)
  - Authentication and integrity
- Encapsulated Security Payload (ESP)
  - For confidentiality and sometimes authentication or integrity

Packets can use AH and/or ESP

Algorithm independent

IPsec does not protect against

- Traffic analysis
- Non-repudiation
- Denial-of-service

IPsec is used to set up virtual private networks (VPNs)

AUTHENTICATION HEADER

The Authentication Header (AH) provides authentication (and possibly integrity) only.

- Transport mode is applicable only to host implementations and provides protection for upper layer protocols, in addition to selected IP header fields.
- Tunnel mode is where it protects the entire inner IP packet, including the entire inner IP header.

The authentication algorithm used is defined by a security association. Suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., DES) or one-way hash functions (e.g., MD5 or SHA-1).

ENCAPSULATING SECURITY PAYLOAD

The Encapsulating Security Payload (ESP) provides confidentiality for packets. Likewise to the AH, it can be used in both transport (between two hosts) and tunnel (an IP tunnel between two gateways) modes.

ESP is algorithm independent. Common cyphers used include 3DES, DES, CAST128 and Blowfish.

SECURITY ASSOCIATION

The Authentication Header defines a Security Association to use for a particular link (or connection: UDP/TCP):

Authentication algorithm and mode

Authentication key(s)

Encryption algorithm and mode

Encryption key(s)

Presence / absence of a crypto synchronisation/IV

Lifetime of a key or when key change should occur

Lifetime of the security association

Source address of the security association

Sensitivity level (SECRET / CLASSIFIED etc)

Again the issue here is key distribution & management.

IKE / IKE V2

“Internet Key Exchange”

Protocol used to set up Security Association in IPsec.

Uses X.509 certificates for authentication which are pre-shared or distributed using DNS (DNSSEC) and Diffie Hellman to set up a shared secret.

Runs as IKE daemon in user space.

ADDRESS RESOLUTION PROTOCOL

ARP (Address Resolution Protocol) is used to map IP addresses to hardware addresses.

A table called the ARP cache is used to store each MAC address and its corresponding IP address.

When a packet sent to a host machine on a network arrives at a router, it asks queries via ARP the MAC address that matches the destination IP address. The ARP program looks this up in the ARP cache:

- If it finds the address the ARP program provides it
- If no entry is found for the IP address, ARP broadcasts a request packet to all the machines on the network based on that IP address. A machine that recognizes the IP address as its own replies. ARP updates the ARP cache for future reference and then sends the packet to that MAC address.

SPOOFING ARP

ARP is one of the simplest but most fundamental protocols on the Internet.

Lack of strong authentication means manipulating ARP is trivial, and allows many powerful attacks to be accomplished, including many on higher level secure protocols (e.g. ssh, ssl)

Poisoning the ARP cache of targets

MAC flooding

Man in the middle

Connection hijacking

Denial-of-service

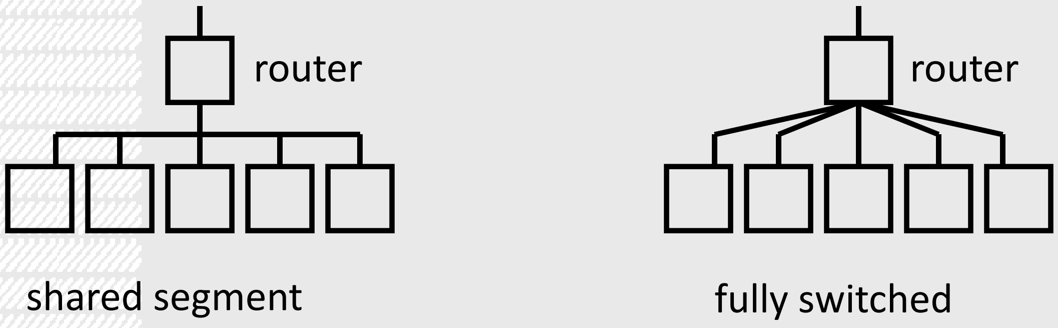
Cloning

ARP ATTACKS

As time passes, networks are migrating towards being <u>fully switched</u>. This is where each host is on a separate network cable so the number of machines sharing a particular connection are minimised.

Increases network performance

Increases security as sniffing a particular link will yield traffic only to/from that host, not all hosts on the local network



ARP ATTACKS

ARP facilitates Mallory to trivially launch man-in-the-middle attacks against Alice and Bob:

- Mallory poisons the ARP cache of Alice and Bob
- Alice associates Bob's IP with Mallory's MAC
- Bob associates Alice's IP with Mallory's MAC
- All of Alice and Bob's traffic will now go through Mallory

<u>This works even if the network is fully switched</u>.

What if Bob is a gateway or router?

- <u>All traffic flowing through that router goes via Mallory.</u>

OTHER ARP ATTACKS

MAC flooding where an attacker sends spoofed ARP replies at a high rate to the switch, eventually overflowing the port / MAC table. Most switches then revert back to “full broadcast” mode (i.e. forwarding all traffic on all ports).

Denial-of-service attacks where ARP caches are updated with non-existent MAC addresses, causing valid frames to be dropped.

Connection hijacking

Cloning

PREVENTING ARP SPOOFING

ARP spoofing is difficult to prevent:

- enabling MAC binding at a switch
- implementing static ARP tables

MAC binding makes it so that once an address is assigned to an adapter it cannot be changed without authorisation.

Static ARP management is only realistically achieved in a very small network. In a large dynamic network, it would be impossible to manage the task of keeping the entries updated.

`arpwatch` for Unix based systems monitors changes to the ARP cache and alerts administrator as to the changes.

DNS

Many of the earlier problems we have discussed are a result of authentication through source IP address (and the ability of an attacker to spoof it).

Many other applications also extend trust to other hosts based on their names (known as name addresses) e.g. cassius.ee.usyd.edu.au.

The domain name service (DNS) performs the mapping between IP address and name address.

ATTACKS ON DNS

Similar to ARP, DNS by default does not have any form of authentication.

The ability to subvert DNS through hacking the nameserver or poisoning the cache leads to many potential attacks:

- subversion of r* commands, NFS (file sharing), /etc/hosts.equiv and other transitive trust relationships.
- impersonation attacks (e.g. webserver)
- denial-of-service

DNSSEC

Suite of IETF extensions to secure DNS using digital signatures, including origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. DNSSEC-bis is a subsequent improvement for scalability.

New DNS record types:

- RRSIG
- DNSKEY
- DS
- NSEC
- NSEC3
- NSEC3PARAM

Each lookup returns RRSIG DNS record, a digital signature which can be verified via public key in DNSKEY. DS record is used in authentication of DNSKEYs using the chain of trust. NSEC and NSEC3 records are used for robust resistance against spoofing.

INFRASTRUCTURE ATTACKS

The Internet Control Message Protocol (ICMP) is used to communicate error messages and network conditions across IP.

Like other infrastructure protocols, strong authentication is absent

ICMP Redirect messages can be spoofed “redirecting” traffic (although doesn’t work any more)

ICMP error messages can be spoofed telling target hosts that a victim is unavailable (hence knocking the victim off the air).

Most firewalls block ICMP into and out of the network properly.

Since “ping” uses ICMP echo this means that sometimes all ICMP is allowed to pass (or ping is broken).

OTHER INFRASTRUCTURE ATTACKS

Likewise all other infrastructure protocols (e.g. RIP, EGRP, BGP, OSPF) are open.

Other common attacks involving domain names involve subverting the process of domain name registrars (e.g. social engineering Verisign) in order to change root nameserver records.

ITS GOING TO GET WORSE

Stealthy, anonymous, encrypted, one-way communications difficult to detect or trace.

Collaboration: bot nets assembled from every Internet device.

The “ubernets”: dark nets (probably several already exist)

Mobility ever increasing.

Automated agents pretending to be humans (already here- ChatBots on dating sites, etc)

Software to confuse biometric forensics (e.g. keystroke analysis)

Still expecting a major attack on the mobile phone network globally… any day now

WHAT WE NEED TO DO

Rebuild the Internet from the ground up, using strong building blocks.

Build strong authentication into every component.

Audit trails and authentication for packets.

A global network for co-operation.

Out-of-band network control.

Stronger languages, better programming practices, better network design, better quality control.

Secure default configurations out of the box.

An Internet police force.

Everyone playing their part.

REFERENCES

Papers

Read Security Problems in the TCP/IP suite (Bellovin)

Protocol Tools

Dsniff, ettercap, nmap, arpwatch, fragrouter, metasploit