TCP/IP and its Weaknesses and Vulnerabilities

Peter Shipley

shipley@dis.org

+1 510 849 2230

Outline

This lecture will cover basics security problems relating to TCP/IP Networks and applications.

Most of the exploits discussed will be on the network level although a few examples of application level attacks will be discussed

This lecture is geared toward Novices

Outline

- Types of Attacks
- Methods of Attacks
- What is TCP/IP
- Why do we need TCP/IP
- Known Problems with TCP/IP

Types of Attacks

- Disclosure of information
- Destruction of data (malicious intent)
- Alteration of data (forgery)
- Denial of Service (DOS)

Disclosure of Information

- Attacks against the confidentiality of data.
- Attempts to disclose otherwise private information such as finances, personal letters or information, proprietary documentation or marketing strategies.
  - Password or Email Sniffers

Destruction of Data

Deletion or “wiping” of information stored on a server (or even of the server itself).

Alteration of Data

Editing of data to hide or falsify data

- Inserting or substituting data in a IP stream (TCP session Hijacking)
- UDP data stream alteration
- Website re-design

Denial of Service

Malicious attacks designed to prevent the victim server or that server's clients from accessing resources that would otherwise be available.

Methods of Attacks

- Common System Exploits
  - Attacks against System Services
- IP/Network Vulnerabilities
  - Attacks against the TCP & IP Protocol

Common System Exploits

- Attacks against System Services
  - WWW
  - DNS (Domain Naming System)
  - Mail Services
  - RPC

What is the best protection

- 24 hour firewall/network monitoring
- Policy Management & Enforcement
- IDS (Intrusion Detection Systems)

What Is TCP/IP

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network. It was developed by a community of researchers centered around the ARPAnet.

The ARPAnet eventually became what we now know as the Internet.

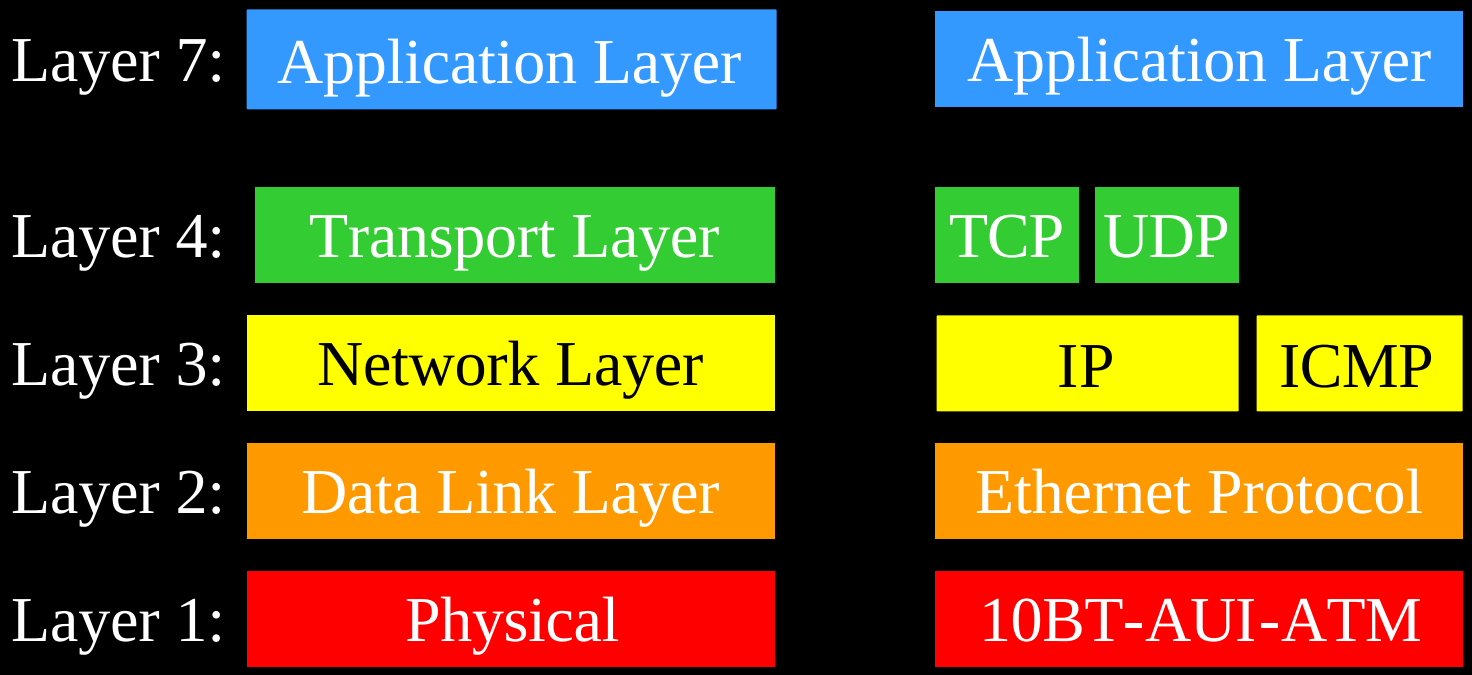
Why Do We Need TCP/IP

TCP/IP allows our computer to communicate and share and pass information and services.

Examples of such services are:

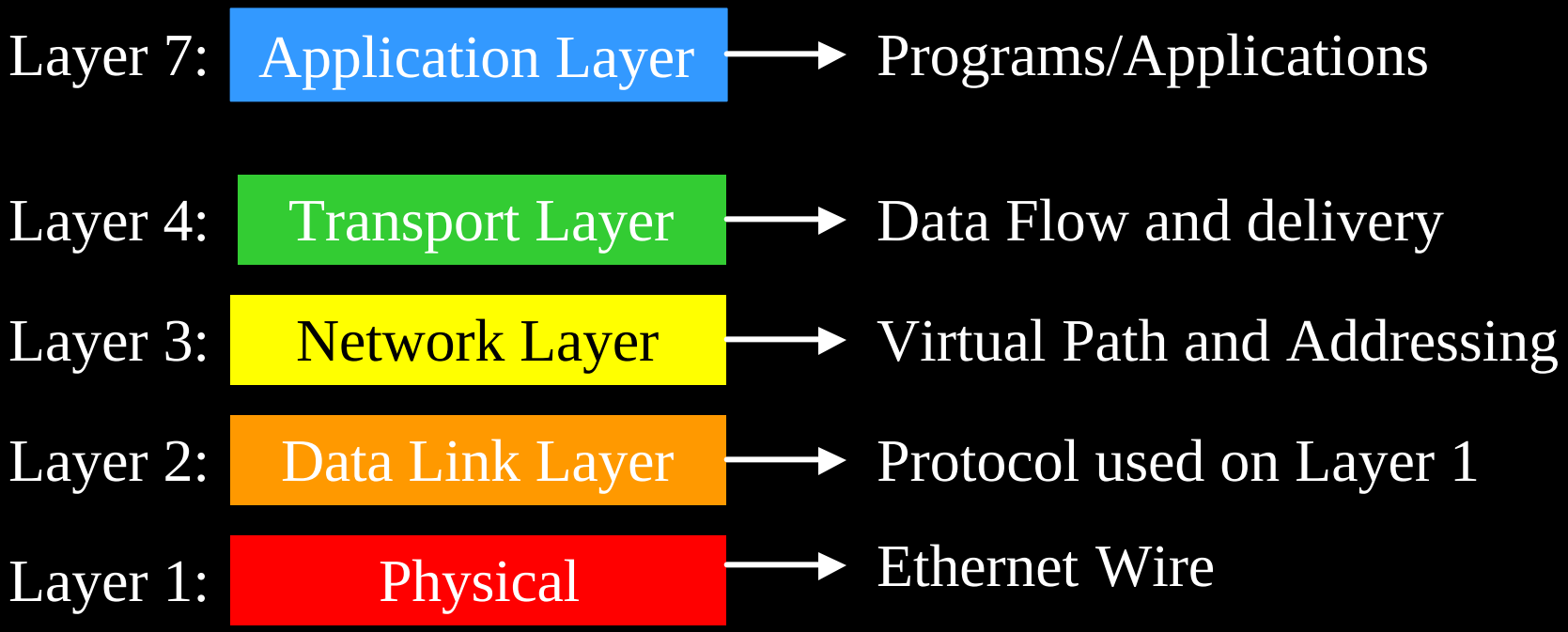
- FTP - File Transfer Protocol
- WWW - World Wide Web
- SMTP - Email
- Remote login access

How the Protocols come together



Each protocol layer is built up from supporting protocols.

How the Protocols come together



Each layer's security is also built from supporting protocols.

TCP Three Way Handshake

TCP relies on a three way handshake when establishing a connection.

This ensures that both sides agree that a connection has been established and data can be transmitted reliably.

Three Way Handshake

1: Send SYN seq=x

2: Send SYN seq=y, ACK x+1

3: Send ACK y+1

Three Way Handshake

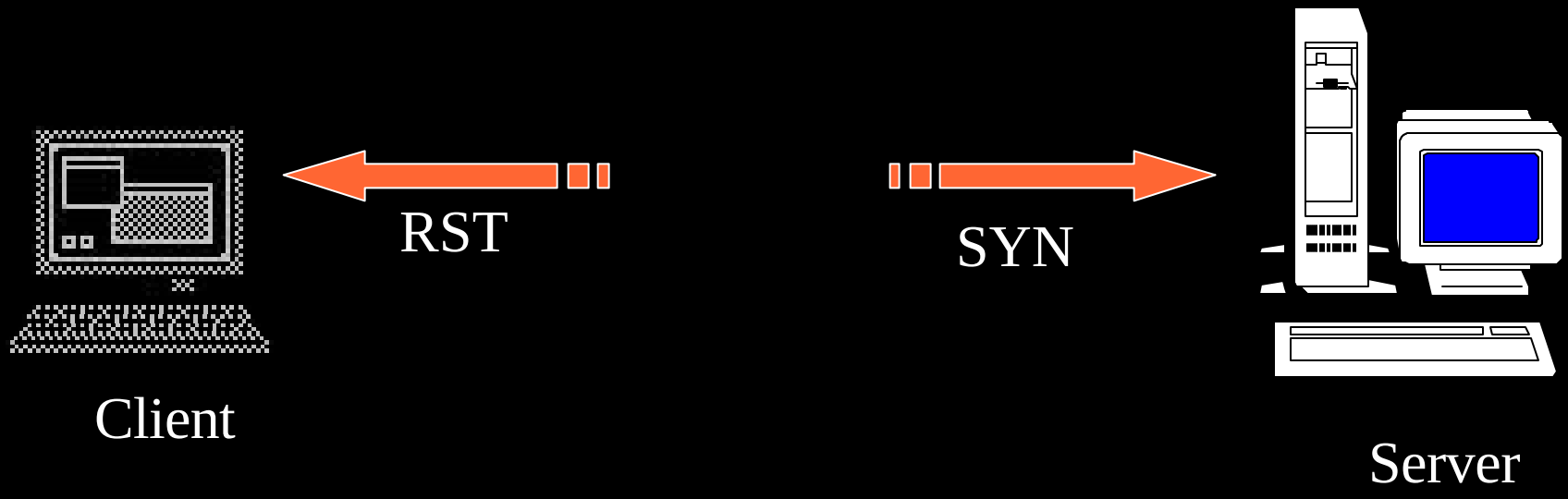
The Three Way Handshake guarantees that both sides are ready to exchange data, and it allows both sides to agree on a initial sequence number synchronization and data window size.

Normal Connection Failure

There are several methods of failure for a TCP/IP connection. The most common method is for a connection to be reset/rejected by the receiving/answering host.

This is most commonly done by the receiving/answering system.

Normal Connection Failure



Normal Connection Failure

In some cases, if there is a IP filtering router between the client/originating host and the server/receiving host, the filtering router will filter-block the SYN and send a RST or ICMP unreachable message or sometimes just drop the SYN (blackhole) and send nothing back. this is a drop vs. reject.

Layer 7 / Application Layer

Layer 7: Application Layer → Programs/Applications

Microsoft IIS

An under-documented feature of Microsoft's IIS server is the ability to do remote administration from the URL:

http://www.domain.com/issadmin

Microsoft IIS-1.0

To crash a IIS-1.0 server:

```
GET ../../../../ HTTP/1.0
```

or

```
http://www.server.com/../../../../
```

Microsoft IIS-2.0

To crash a IIS-2.0 server:

```
GET “../..\ HTTP/1.0
```

Microsoft IIS-3.0

To crash a IIS-3.0 server:

```
GET /?foo=XX< *1180>XX HTTP/1.0
```

Apache 1.1.1

- A directory listing of a web server can be obtained even if there is a index.html file present.
- On a browser request the URL:

  http://www.server.com/////////////////////////////////
  ///[many]///////
- You will get a listing of the files instead of the contents of the index.html file.

Apache 1.1.1 (with cookies)

- A buffer overflow condition exists in the cookie processing code of the server that can be exploited to obtain a shell or run commands on as the servers userid.

FTP Bounce Attack

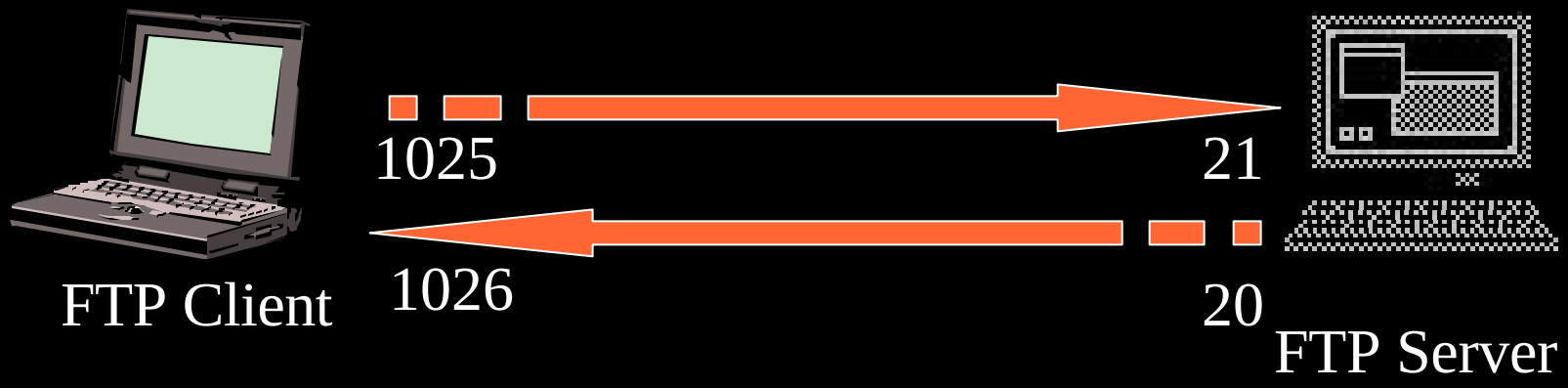
By manipulating ftp daemon that supports the “PASV” command it is possible to establish third-party one-way connections through the ftp host.

FTP Bounce Attack

This can be used to

- Transfer data anonymously
- Slip past application based firewalls
- Remotely portscan

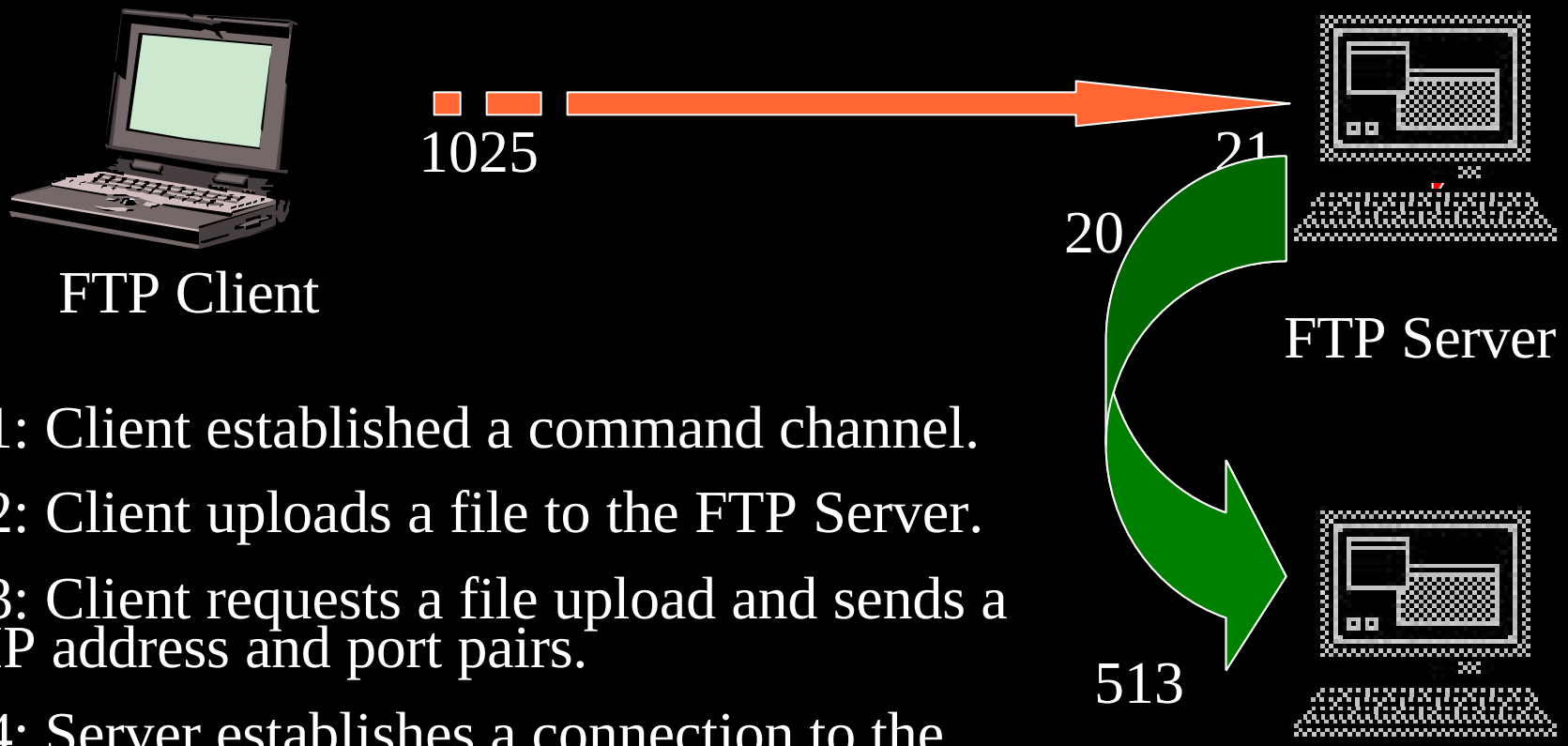
Normal FTP Connection



1: A connection is established to the servers FTP port from a high numbered port to port 21 on the server. Login / Password are sent over this connection.

2: When the client wants to receive a file it opens a local (high) port a message to the server to connect to that port and transmit the requested data.

FTP Bounce Attack



1: Client established a command channel.

2: Client uploads a file to the FTP Server.

3: Client requests a file upload and sends a IP address and port pairs.

4: Server establishes a connection to the given IP address and port pairs.

5: Server send data to Internal Server.

FTP Bounce Attack

- The best fix for this is to upgrade your ftp daemon.
- Some firewalls that filter command and content can also block this attack but it is not advisable to rely on this security strategy.

DOS IP Attacks

A majority of IP based attacks tend to be DOS based :

- ICMP_ECHO flooding
- ICMP_ECHOREPLY flooding
- UDP loop flooding
- TCP SYN flooding
- SYN sniping
- Large packet (Ping of Death)
- Fragment overflow (TearDrop)

Level 3 attacks

Attacks

- Unfortunately, the IP stack is susceptible to a plethora of attacks.

Layer 4 / Transportation Layer

Layer 4: Transport Layer → Data Flow and delivery

Ping Flooding

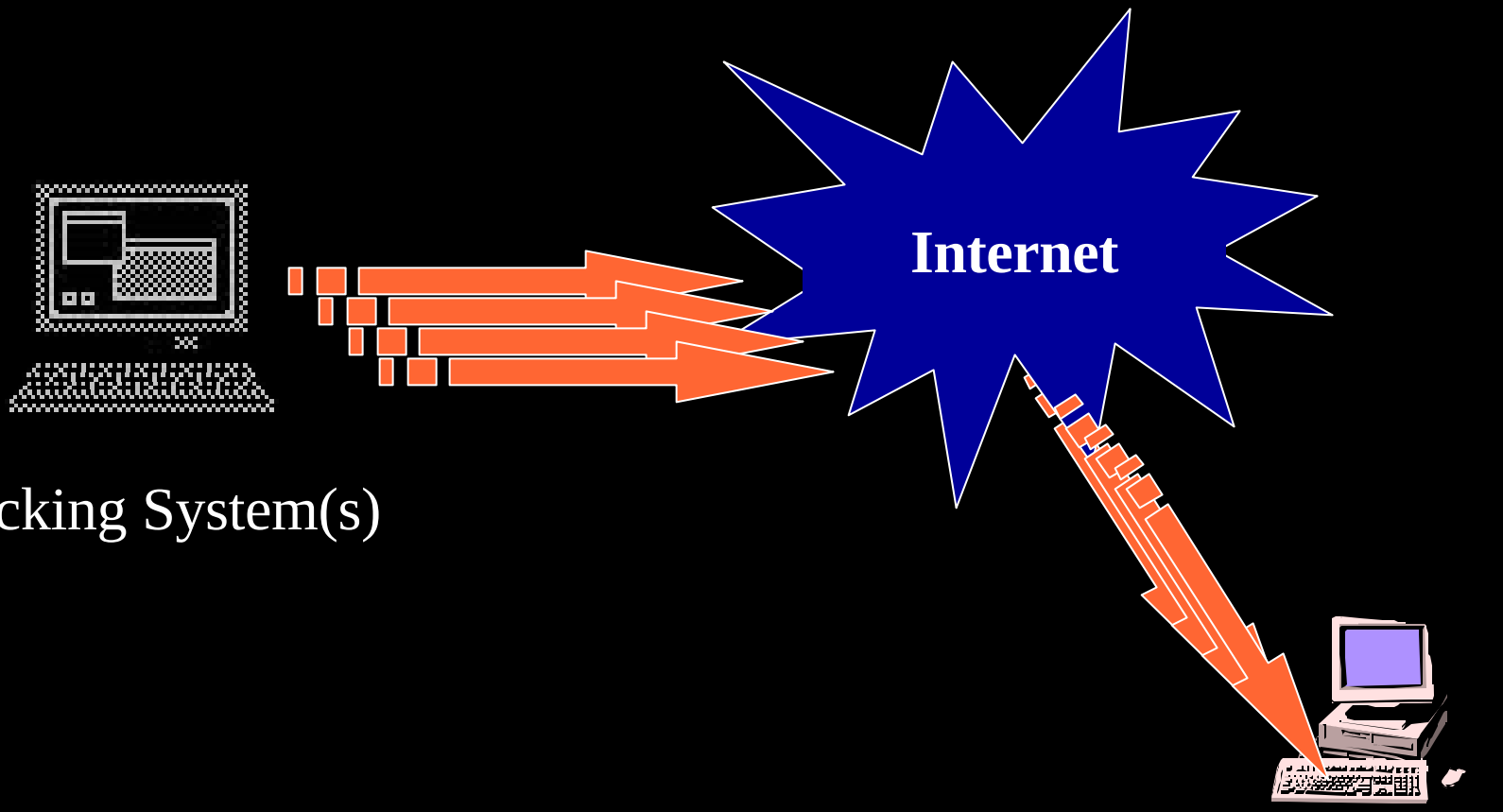
Ping Flooding is a denial of service (DOS) attack involving flooding the victims with IP traffic, thus saturating the remote site's available bandwidth.

- Allows an attacker to inhibit network connectivity to the target network
- High-bandwidth beats low bandwidth
- Spoofable, thus easy to hide source

Ping Flooding

Instead of sending ICMP echo packets (AKA ping packets), any type of IP packet can be sent.

Ping Flooding



Ping Flooding

To be effective, the attacker site needs significantly greater bandwidth than the victim site.

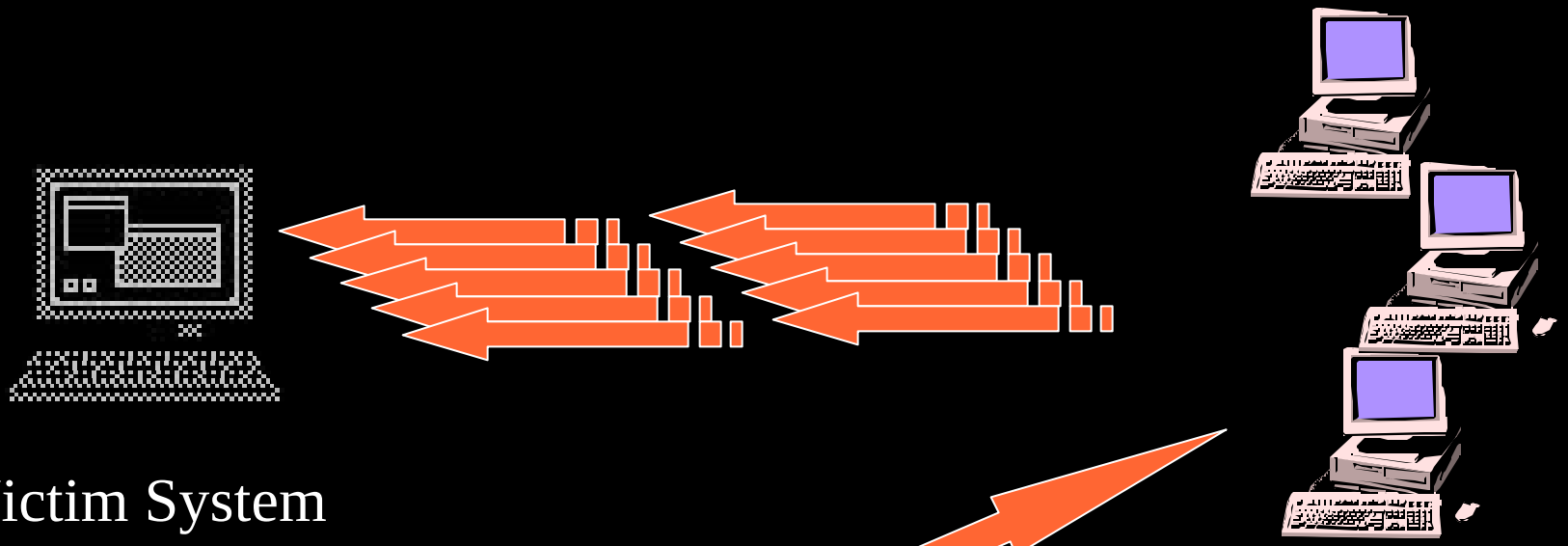
A typical defense is to filter ICMP_ECHO packets at the router level. This defense may be easily countered by sending ICMP_ECHOREPLY packets instead.

“Smurf” Attacks

The “Smurf” attack is a modification of the classic ping flood attack

Instead of sending ICMP echo packets (aka ping packets) from your system to the victims host/network, a packet is to sent to a broadcast address of intermediate network with a forged return address of the victim’s host.

“Smurf” Attacks



Victim System

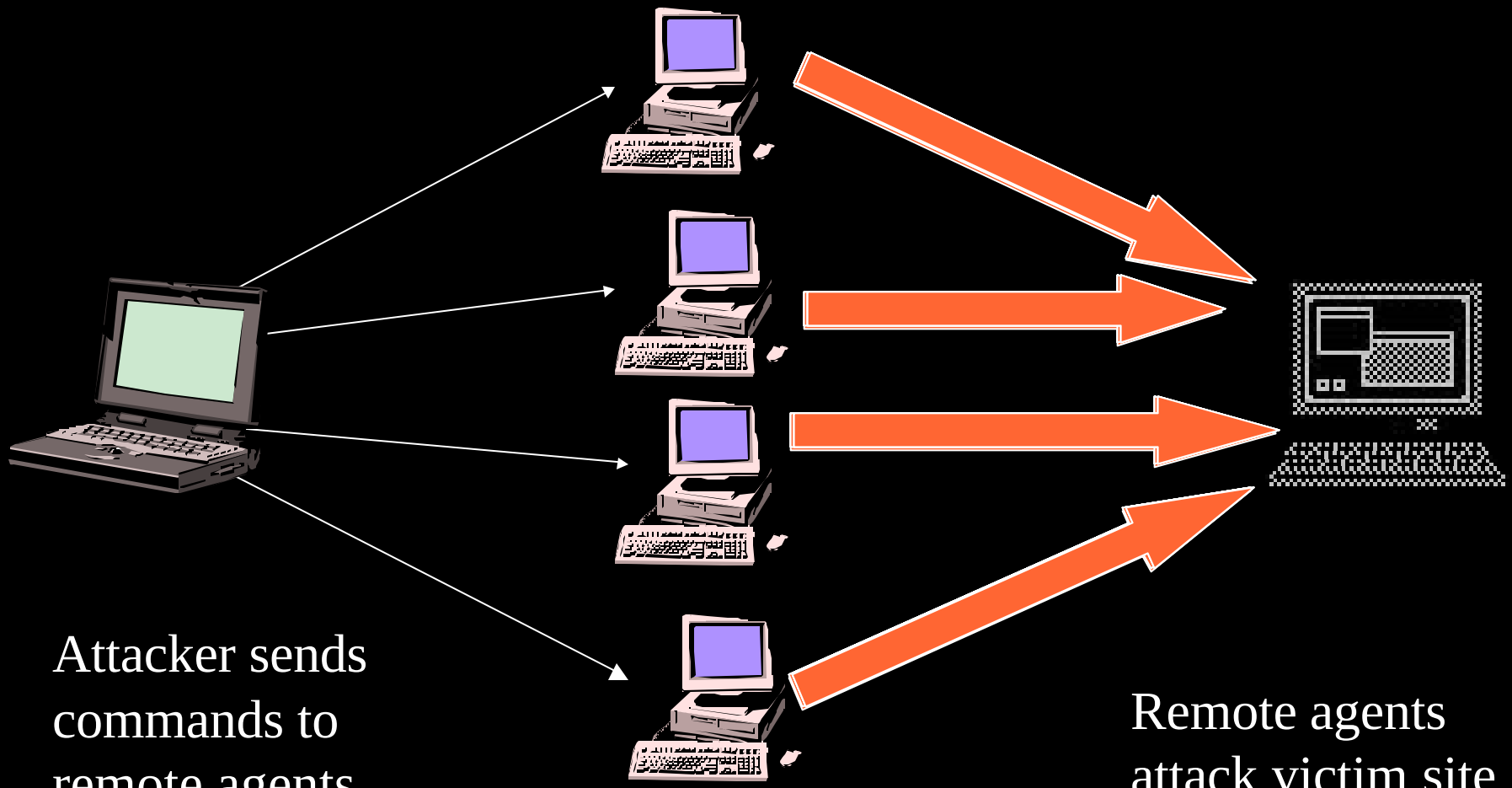
A Networks of Systems

A Single System

“Smurf” Attacks

As with ICMP Echo Flood attacks, the best protection is through IP filtering of ICMP_ECHOREPLY packets.

DDos Attacks



Attacker sends commands to remote agents

Remote agents attack victim site

DDos Attacks

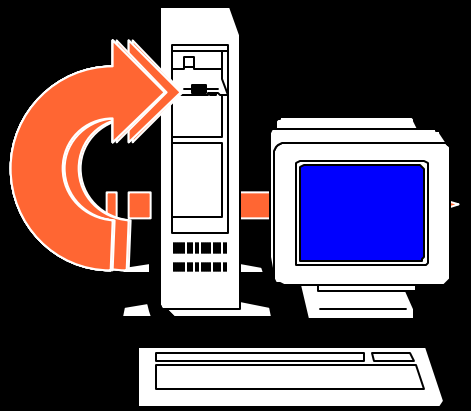
- Similar to “Smurf” attacks
- Attacker does not have to be online during attack
- Near Impossible to defend against
- Best defense is to not to be a “tool”.

UDP Echo Looping

- UDP Echo Spoofing is a Denial of Service (DOS) attack that causes the system to UDP echo data (port 7) packets to itself till the local LAN is saturated or the packet is lost for other reasons.
- This attack allows an attacker to hang a host in addition to causing high congestion on a network.
- It’s close to impossible to detect the source (duo to spoofing).

UDP Echo Looping

Attacker



Victim System

UDP Echo Looping

Variations of this includes sending to a broadcast address or to the localhost address.

UDP Echo Looping

There are patched versions of inetd that will block these attacks.

IP filtering will also help protect unpatched systems.

Layer 3 / Network Layer

Layer 3: Network Layer → Virtual Path and Addressing

SYN Flooding

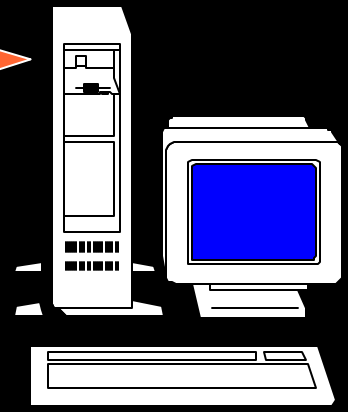
SYN Flooding is a Denial of Service (DOS) attack that exploits a “feature” in the TCP/IP protocol stack (a layer 4 attack).

- Allows attacker to deny access to any TCP based service
- Attacks on a port per port basis
- Denied access to legitimate clients

SYN Flooding

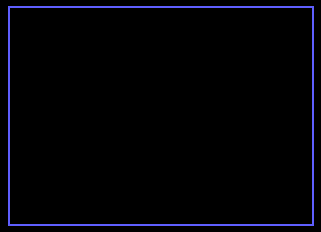
Attacker

SYN

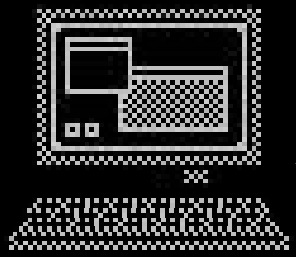


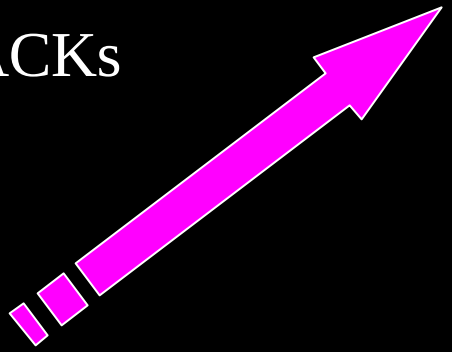
ACKs

Victim System



Non-existent System





Legitimate client

SYN Flooding

- Remote access to “victim system” is blocked.
- The attacks take very little bandwidth from an attacker’s site. (Can be done from a 14.4 modem dialup).
- Close to impossible to detect the source (duo to spoofing).

SYN Flooding

- Most current Operating Systems are resistant to SYN Flood attacks.
- Strong IP filtering will also help protect some spoofing.

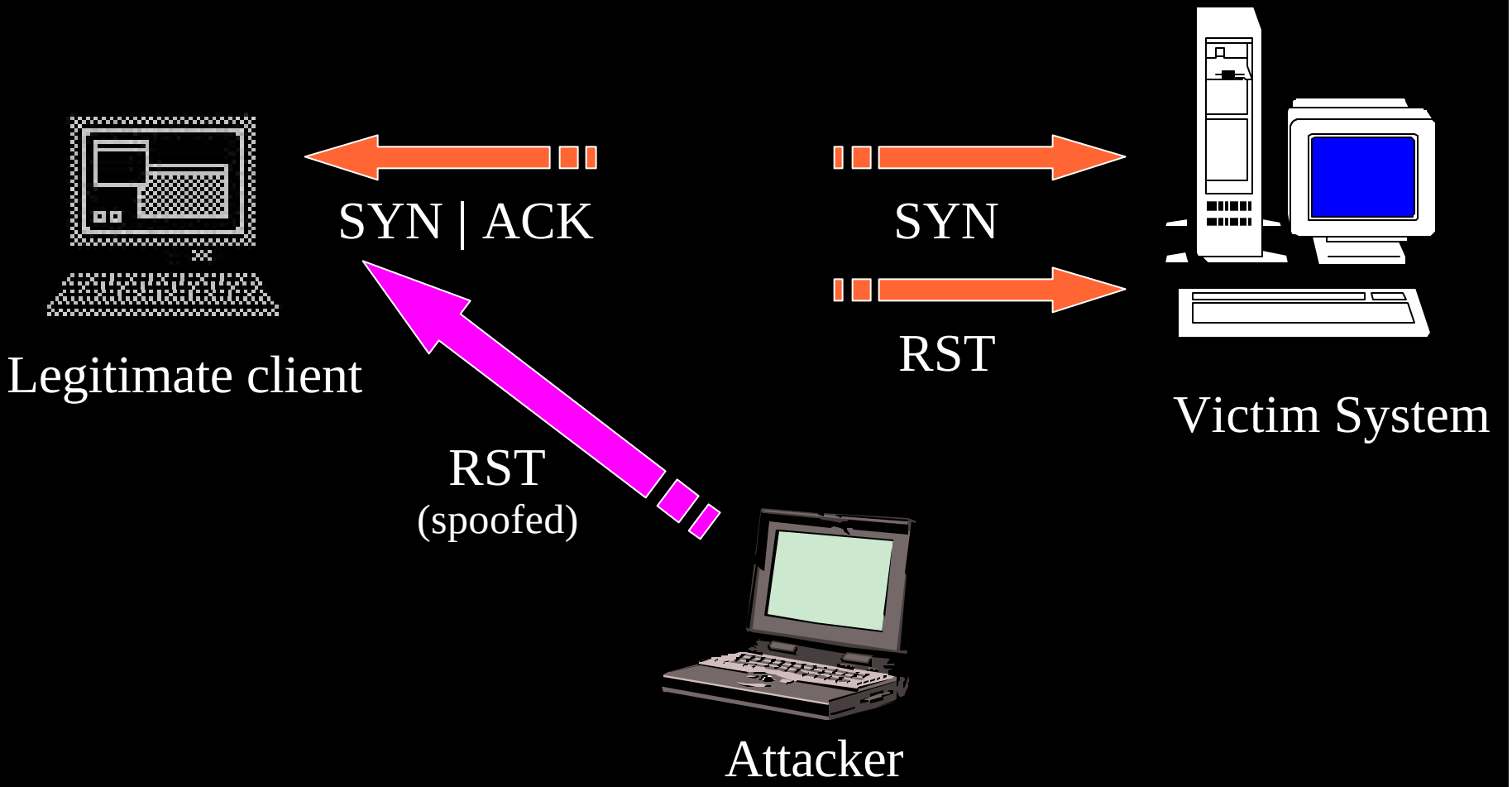
SYN Sniping

SYN Sniping is a Denial of Service (DOS)

RST (reset) packets are spoofed thus causing a connection to fail to become established.

A layer 4 attack

SYN Sniping



SYN Sniping

- Remote access to “victim system” is selectively blocked.
- Requires access to the local or intermediate network.
- Close to impossible to detect the source (due to spoofing).

SYN Sniping

- It is possible to “snip” connections in a blind attack.
- This is basically done by spraying randomly sequenced RST packets as a known connection.
- When you get lucky and stumble onto the correct sequence number the connection will drop (this may take while).

SYN Sniping

Can be inhibited with the use of “smart” hubs and segmented networking.

Ping Of Death

- The “Ping of Death” attack involves sending a unexpectedly large IP packet to the victim host.
- While this is most commonly sent as a ICMP_ECHO packet (AKA: ping), this attack may be done with almost any IP packet type.
- Attacks an implementation bug in the layer 3 code.

Ping Of Death

- Most OSs have patches available to correctly deal with such IP packets
- Up stream protection can be done at the router/IP filter level by not forwarding illegal packets (packet size > 65515), (although with fragmentation, this can be difficult to filter/stop).

Ping Of Death

One option is filter fragmented IP and TCP packets.

This solution can also inhibit connectivity from some remote sites that are forced to fragment due to high network congestion or bad network design on there local LANs.

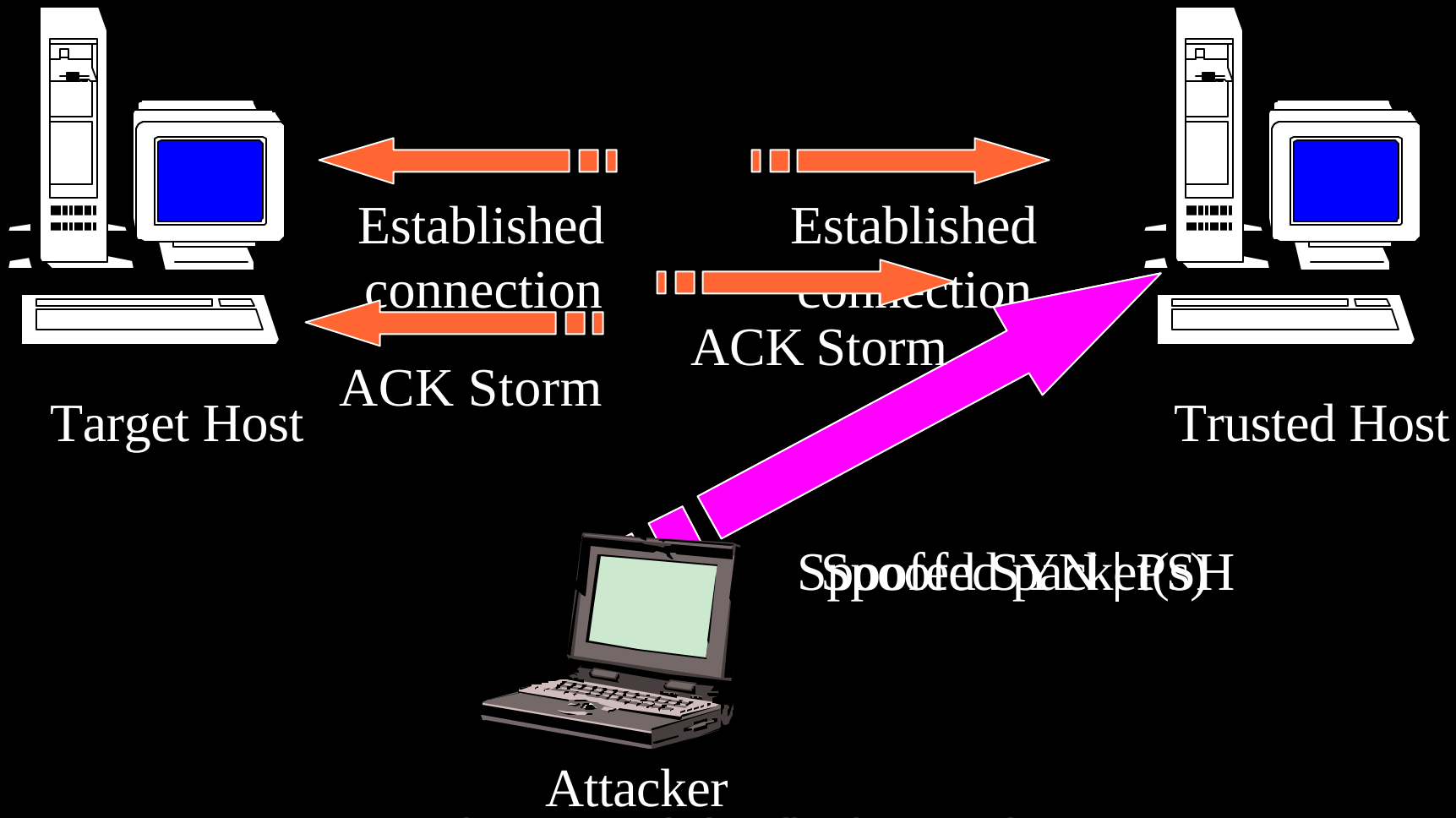
TCP Session Hijacking

By predicting the IP sequence number a large number of impersonation attacks become possible:

Allows an attacker to inject data or take over a pre-established connection

This attack can only be done on a from a local LAN (ISO Layer 1).

TCP Session Hijacking



TCP Session Hijacking

- The attacker desynchronizes the established connection.
- While the connection is desynchronized, the attacker may inject data into the “established connection”.
- Eventually, the connection die as a result of a ACK storm between the legitimate hosts.

TCP Session Hijacking

The best protection from hijacking is a "smart" hub or "switch" and good network monitoring.

Other Attacks

- Port scanning
- DNS cache poisoning
- SNMP attacks
- TCP Hijacking

TCP Port Scanning

TCP port scanning is a term which refers to the technique of sequentially connecting to IP ports and determining if there is a daemon running on that port.

TCP Port Scanning

TCP Port 7 (echo) is open
TCP Port 9 (discard) is open
TCP Port 20 (ftpd) is open
TCP Port 22 (sshd) is open
TCP Port 25 (smtpd) is open

TCP Port Scanning

There are several permutations of how to do the scanning (mostly to designed to evade logging and detection)

- Full (normal scanning)
- Half-open
- Stealth

TCP Port Scanning

The traditional (and easiest to implement method of scanning) is to connect to and open every possible port on the target system.

This is also the easiest to log and detect.

TCP Port Scanning

"Half Open" is a technique in which the scanning program sends a SYN packet to each port and counts the receipt of SYN|ACKs (optionally sending a RST in reply to the SYN|ACKs).

Since a TCP connection is never fully established, user level utilities such as tcp_wrappers will not log the connection.

TCP Port Scanning

- "Stealth" port scanning takes advantage of the behavior characteristics of some TCP stack implementation.
- The concept is that closed ports *tend* to reply to FIN packets with the proper RST.
- Open ports, on the other hand, tend to ignore the packet in question.
- Thus, available ports can be determined based on RST response packets.

TCP Port Scanning

"Stealth" port scanning also has the ability to evade some IDS systems and some firewalls that realy on filtering the SYN packets

TCP Port Scanning

Sequential probes are trivial to spot.

There are many tool that do this for you by sniffing your local network or examining the system log (syslog) files.

- tcplog
- netstat
- abacus

Layer 3 / Network Layer

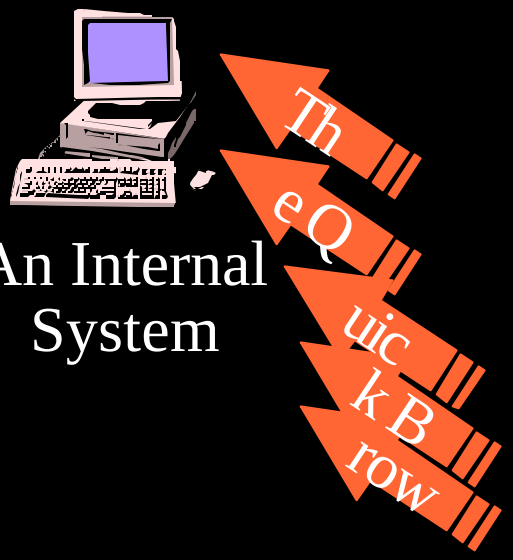
Layer 3: Network Layer → Virtual Path and Addressing

IP Fragmentation

The TCP/IP protocol standard supports the ability to fragment a IP packets into smaller packets.

This to accommodate IP transmissions over congested networks or with nets smaller MTU sizes.

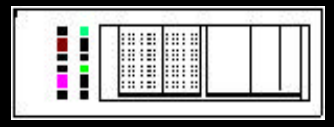
IP Fragmentation



An Internal System

1: A (long) packet is through a router

2: The router breaks (fragments) the packet into smaller packets



An External System

A Router

IP Fragmentation (problems)

- Hops IP Filter based firewalls
  - Tiny Fragment attack
- Evades IDS and some sniffers
  - Tiny Fragment attack
  - Overlapping Fragments
- DOS attacks
  - Teardrop
  - Exhaust system resources (Fragment Tracking)

IP Fragmentation (Evasion)

- Evading IP Filters through the use of tiny fragments
  - Packets may evade many IP filtering systems by reducing their size to the point that the IP rules can not identify the content on the of the packet.
  - A solution to this is addressed in RFC 1858

IP Fragmentation (Evasion)

- Fragmented Packets can evade IDS
  - A majority of IDS fail to attempt to analyze and inspect the contents of fragmented packets. (Secnet:98)

IP Fragmentation Attacks

- Overlapping Fragment Attacks (AKA: “Teardrop”)
- IP Fragment Flooding
- Micro Fragments
- Overlapping Fragment Attack (hiding data)

Overlapping Fragment Attacks

- Some implementations of the TCP/IP IP have bugs in the IP fragmentation re-assembly code and thus do not properly handle overlapping IP fragments.
- “Teardrop” is a widely available attack tool that exploits this vulnerability.

Overlapping Fragment Attacks

There are patches available for Windows that make it resistant to this attack.

Linux systems should be upgraded to the current release.

IP filtering will also help protect unpatched systems.

IP Fragmentation Flooding

- Any TCP/IP implementation has to deal with fragmented packets of one form or another
- A DOS attack can be executed by sending random IP fragments to a system.

IP Fragmentation Flooding

This will cause the system to buffer these fragments awaiting other IP or TCP fragments to reassemble the packets with.

A DOS attack situation can exist in cases where a joining fragment never arrives, thus causing a system to run low on memory and CPU resources.

Micro Fragments

One common method to circumvent IP filter based routers is to fragment one's IP packets sufficiently so that the encapsulated TCP header can not be analyzed and filtered.

This technique can also be used to evade detection from current IDS systems.

IP Fragmentation (Overlapping)

- Overlapping fragments can be used to evaded the detection of an IDS system if the IDS fails to reassemble the overlapping in the same manor as the OS it is shielding (Secnet:98 RFC-1858)

IP Fragmentation (Overlapping)

Both IP and TCP packets can be fragmented, this is supported by the protocol

A problem occurs when the packets fragments parts overlap, because the standard does not specify the priority of the data (that is if the new data or the old data has precedent when there is a overlap.

IP Fragmentation (Overlapping)

- Given a set of overlapping packets:

- Favoring Old Data:

- Favoring New Data:

IP Fragmentation (DOS)

Overlapping Fragment attack

Some implementations of the TCP/IP IP have bugs in the IP fragmentation re-assembly code and thus do not properly handle overlapping IP fragments.

System crashes due to buggy IP code (lunix and NT)

AKA: “teardrop attack”

IP Fragmentation Attacks

Some implementations of the TCP/IP IP have bugs in the IP fragmentation re-assembly code and thus do not properly handle overlapping IP fragments. Teardrop is a widely available attack tool that exploits this vulnerability.

IP Fragmentation

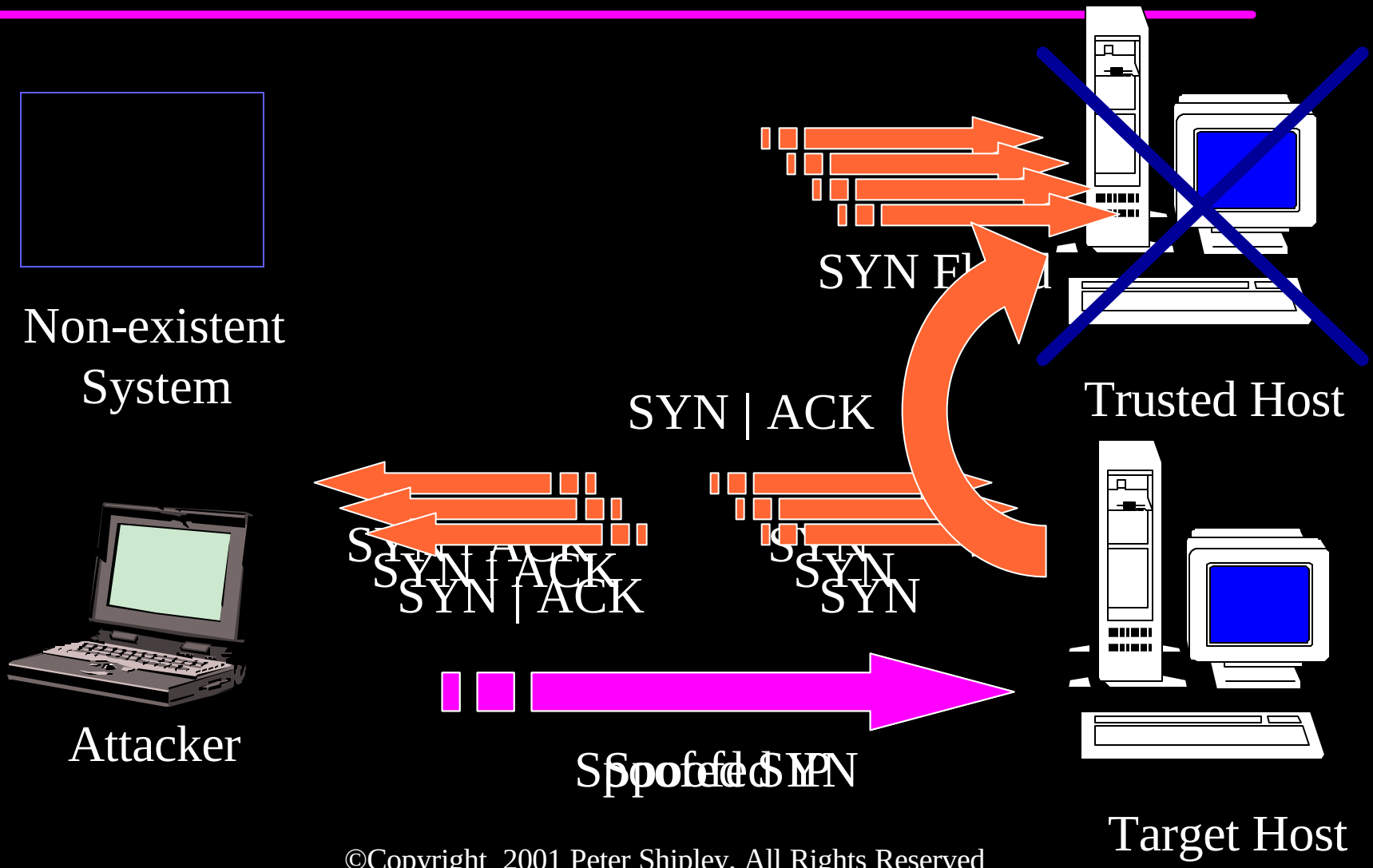
- On a healthy network IP fragmentation is very rare.
- Filter fragments at the router level (1%✍5% of sites have problems connecting
- RFC 1858 (solution?)
- See also RFCs 791 & 815

IP Sequence Prediction

By predicting the IP sequence number a large number of impersonation attacks become possible:

- Allows an attacker to gain access to a machine
- Exploits trust relationships
- Blind attacks

IP Sequence Prediction



IP Sequence Prediction

- Trusted System is SYN Flooded.
- Attacking system establishes a number of connections to Target System. Thus an attacker can predict the next IP Sequence number
- A connection is spoofed from Trusted System to Target System. Trusted system can not dispute the connection due to SYN Flood.

IP Sequence Prediction

- Most OSs now randomize their sequence numbers to thwart prediction
- This attack can be prevented with IP filtering to inhibit IP spoofing
- Crypto login authentication system will also inhibit the establishment of login sessions

Layer 2 / Data Link Layer

Layer 2: Data Link Layer → Protocol used on Layer 1

Other Attacks

- Sniffing (passwords, data, email)
- ARP cache poisoning

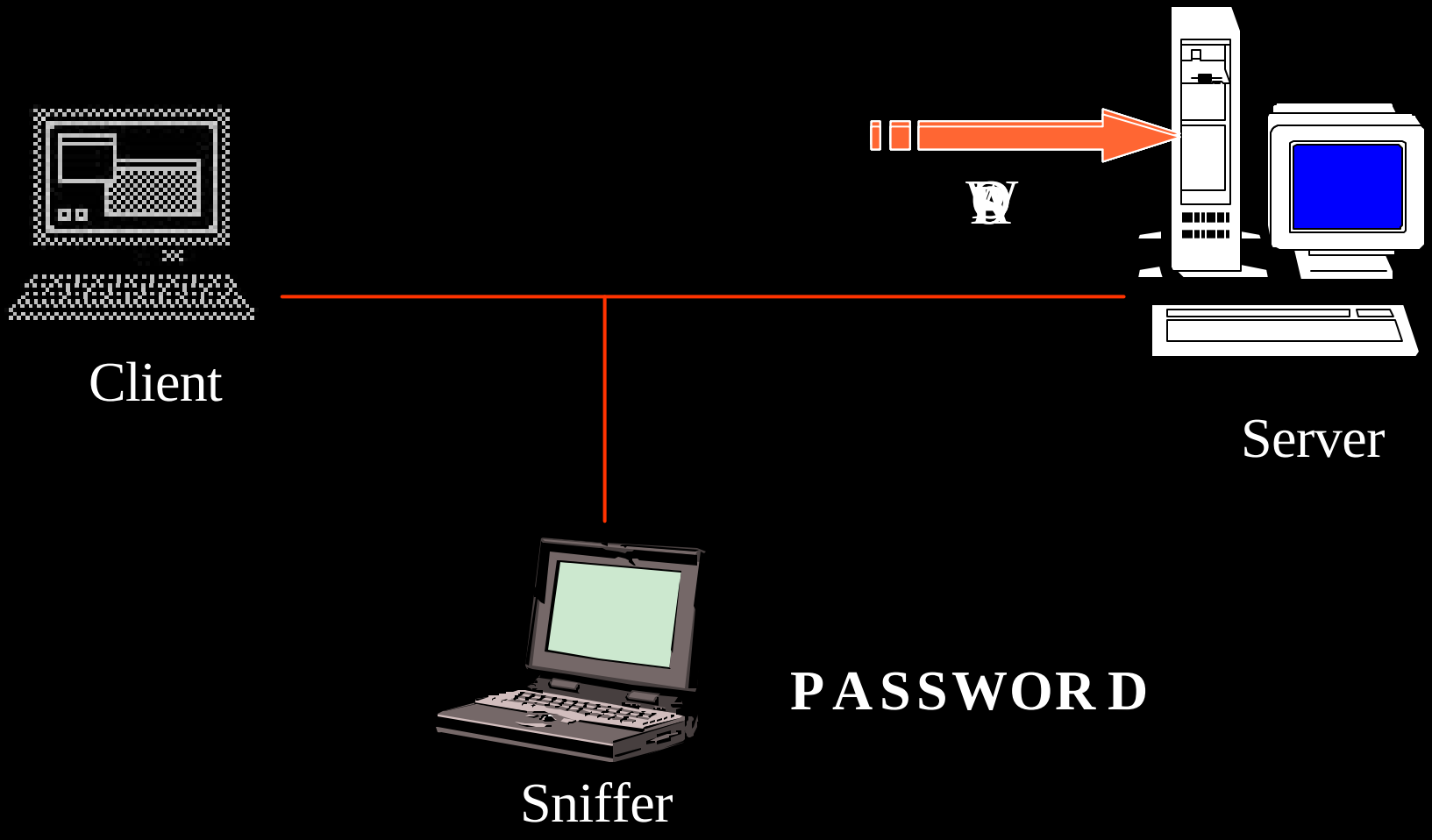
Sniffers / Data Interception

"Sniffing" is a term used to describe the action of eavesdropping on a network.

It is extremely common for system intruders to install a "sniffer" on a system to collect information to be harvested at a later time.

85% - 95% of Internet attacks are sniffer based.

Sniffers / Data Interception



Sniffers / Data Interception

Services affected:

- telnet
- rlogin
- pop / IMAP
- http / WWW
- ftp
- SMTP
- SNMP
- rpc/ NFS
- Just to name a few...

Sniffers / Data Interception

- The best protection from sniffing is a “smart” hub or “switch”.
- Use SSH or another encrypting client for network communications.
- Whenever possible, remove support for promiscuous mode from the kernel.

Sniffers / Data Interception

As with any statement about sniffing one must reference AntiSniff by those fun loving guys at the l0pht.

http://www.l0pht.com/antisniff/

AntiSniff is a unique program that can detect most sniffers remotely on a local network.

ARP Cache Poisoning

On a local ethernet network communication relies on each ethernet interface having a unique MAC address (a property of a ethernet interface card).

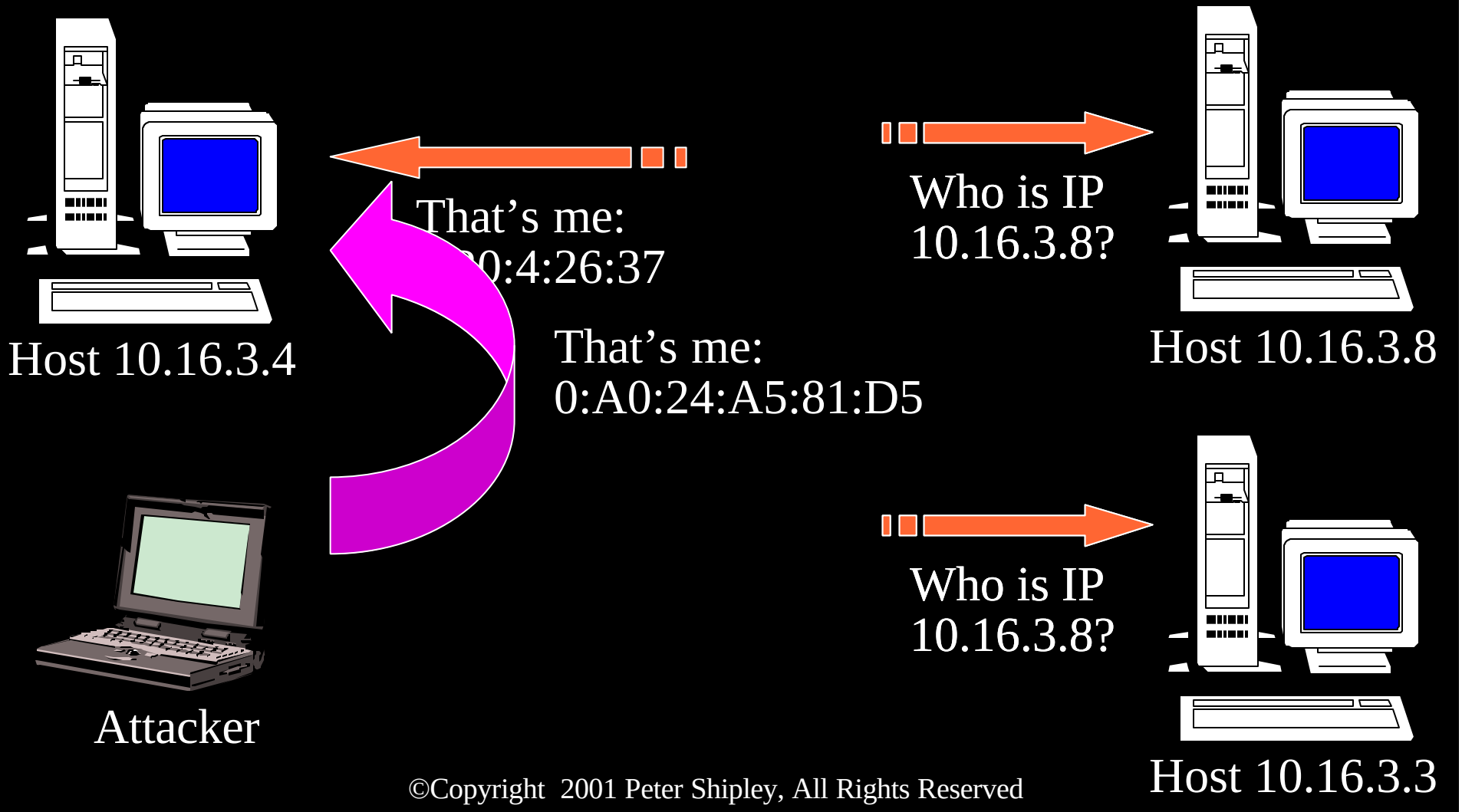
The “table” a system maintains that maps MAC addresses to system IP address is referred to as an “ARP” table.

ARP Cache Poisoning

At the ethernet level it is possible to insert erroneous information into a system's ARP cache

- Permits an someone to impersonate any machine on a LAN
- Many Deny Of Service (DOS) attacks are possible
- Intercept / Redirect Ethernet Communications

ARP Cache Poisoning



ARP cache poisoning

- Again, the best protection from sniffing is a “smart” hub or “switch”.
- Whenever possible remove support for promiscuous mode from the kernel
- Run network monitors such as arp-watch
- Also on stable networks, arp-addresses can be “permanently” inserted into the table

  arp -s 10.16.3.40 0:1:C0:61:40:5C pub
- But is is not a solution for transient networks (or DHCP based networks).

DNS Cache Poisoning

Domain Name System (DNS) is one of the Internet fundamental building blocks, providing a distributed host information database used for the mapping of host names and IP address and their inverse mappings.

(a layer 7 attack)

Normal DNS Resolution

Legitimate Client

www.acme.com is at 192.168.34.78

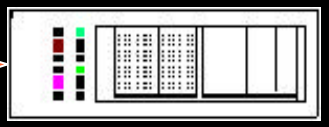
What is the IP for www.acme.com?

DNS Server

Referral to .com server

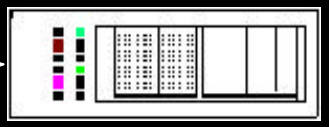
Answer for www.acme.com

www.acme.com?



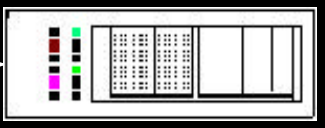
“.” Server

www.acme.com?



.com Server

www.acme.com?



acme.com Server

Normal DNS Resolution

While this seems expensive, it is actually quite efficient if you add the concept of caching.

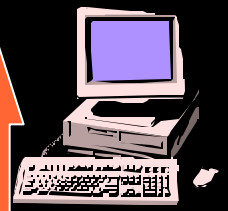
Thus the DNS server does not have to send a query to “.” to relearn where .com is located, etc...

DNS Cache Poisoning

One vulnerability of DNS is the cache.

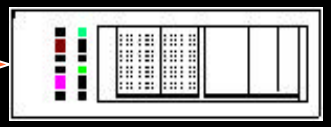
By inserting erroneous information into a server's cache, someone can redirect network connection and/or block access to remote sites.

DNS Cache Poisoning



Legitimate Client

www.acme.com?



“.” Server

www.acme.com
is at 127.0.0.1

What is the IP for
www.acme.com?

DNS Server

Www.acme.com?

Spoofed Answer for
www.acme.com

www.acme.com
is at 127.0.0.1

Attacker

DNS Cache Poisoning

This can be best prevented by installing current versions of bind/named.

Modern versions track pending queries and serialize them to thwart such spoofing.

SNMP

SNMP = **S**imple **N**etwork **M**anagement **P**rotocol

Used primarily a run and manage mid to large size networks.

Defined in RFC 1155, 1157, 1901-1910

UDP ports 161 & 162

SMNP Attacks

Most OS and network appliances manufactured these day supports SNMP to one degree or another.

Because of this, is has become a service activated by default and thus it existence is may times ignored or forgotten about.

SMNP Attacks

- Turn off Power (UPS system)
- Current configurations
  - Software Versions
  - Packet Filter
  - Contact Info
- Reconfigure systems/routers
- Map and Query remote networks and connectivity
- Traffic Monitoring/redirection

What to Do?

- 24 hour network monitoring
- IDS (Intrusion Detection Systems)
- Policy Enforcement

Other References

- http://www.l0pht.com/~weld/netcat/
  - A simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts
- http://www.rootshell.com/
  - A moderate collection of exploits and scripts

Other References

- http://www. securityfocus.com/
  - Bugtraq searchable archives
  - known bug archives
- http://www.attrition.org/
  - clear reviews of current news.

Other References

Books

- TCP/IP Illustrated Volume 1
  W. Richard Stevens
  Addison-Wesley
  1994
  ISBN:0-201-63346-9

- TCP/IP Network Administration - 2nd Edition
  Craig Hunt
  O'Reilly & Associates
  1998
  ISBN: 1-56592-322-7

Other References

- WWW

• TCP/IP FAQ Frequently Asked Questions (1999-07) Part 1 of 2

http://www.cis.ohio-state.edu/hypertext/faq/usenet/internet/tcp-ip/tcp-ip-faq/part1/faq.html

• TCP/IP FAQ Frequently Asked Questions (1999-07) Part 1 of 2

http://www.cis.ohio-state.edu/hypertext/faq/usenet/internet/tcp-ip/tcp-ip-faq/part1/faq.html

TCP/IP and its Weaknesses and Vulnerabilities

Peter Shipley

shipley@dis.org

+1 510 849 2230