

Security Problems Related to Address Resolution

- Introduction to Address Resolution
 - 2 types of address resolution
 - The Domain Names to IP address resolution
 - The IP to MAC (Medium Access Control) address using address resolution protocol (ARP)

Security Problems Related to Address Resolution

- Domain Name Server
 - Computers use IP addresses to talk with one another in the Internet
 - It is often difficult to remember the IP addresses of other computers in a network
 - Domain Name Server (DNS) provides a service that maps host names to IP addresses
 - IP addresses and their associated host names are stored in databases in the DNS

Security Problems Related to Address Resolution

- DNS Spoofing

- However DNS was not designed to be secure, it is susceptible to DNS Spoofing
- Why?
 - Because a computer is able to advertise a false IP address for itself
 - It is easy to setup a DNS resolver and feed it with false data

Security Problems Related to Address Resolution

- Two types of common DNS Spoofing
 - A malicious DNS advertises false IP address to a victim
 - Java applets could be created to spoof IP addresses

Security Problems Related to Address Resolution

- How to Prevent DNS Spoofing
 - Two ways to prevent it:
 - (a) Perform ‘paranoid’ checking on the Web Server
 - (b) Use a properly configured firewall to provide a reliable DNS lookups

Security Problems Related to Address Resolution

- What is ARP and how ARP works?
 - Address Resolution Protocol (ARP) is a protocol used by IP (Internet Protocol) which map IP network addresses to the hardware addresses which. The protocol is used when IP is used over Ethernet.
 - For Example :

IP Address	MAC address
197.15.3.1	0A:4B:00:00:07:08
197.15.3.2	0A:4B:00:00:07:00
197.15.3.3	0A:5B:00:00:01:03

Security Problems Related to Address Resolution

- Every Ethernet board manufactured come with an equipped 48 bit Ethernet address. The board sent and receives frames based on 48 bit Ethernet addresses. They know nothing about 32-bit IP addresses.
- These mapping is done in the ARP client and server processes operate on all computers using IP over Ethernet.
- For example, an IP address of 192.169.20.1 is mapped to a Ethernet MAC address of OA:4B:00:00:07:08, so the sender will know that the IP address of 192.169.20.1 belong to which machine.
- The processes are normally implemented as a part of the software driver of the network interfaces card

Security Problems Related to Address Resolution

- There are four types of ARP message, which may sent by the ARP protocol
 - ARP request
 - ARP reply
 - RARP request
 - RARP reply

Security Problems Related to Address Resolution

- The format of an ARP message is shown below:

0	8	15	16	31
Hardware Type		Protocol Type		
HLEN	PLEN	Operation		
Sender HA (octets 0-3)				
Sender HA (octets 4-5)		Sender IP (octets 0-1)		
Sender IP (octets 2-3)		Target HA (octets 0-1)		
Target HA (octets 2-5)				
Target IP (octets 0-3)				

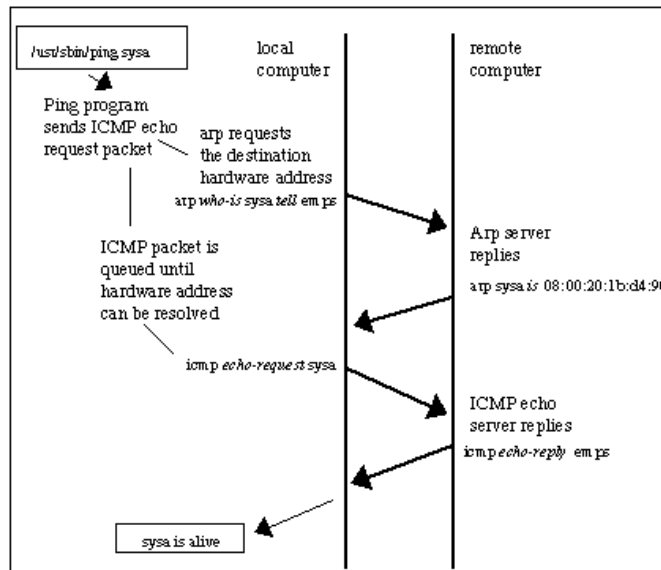
- Format of an ARP message used to resolve the remote MAC address

Security Problems Related to Address Resolution

- In order to reduce the number of address resolution requests, the client normally caches the resolved addresses for a short period of time
- The size of the ARP caches is of a finite size, it will become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow unchecked
- The cache is periodically flushed of all entries

Security Problems Related to Address Resolution

- The figure below shows an example of the use of ARP when a computer tries to contact
- a remote computer on the same LAN (known as “sysa”) using the ping program. It is assumed that no previous IP datagrams have been received from this computer and
- therefore ARP must be used to identify the MAC address of the remote computer



Security Problems Related to Address Resolution

- ARP Spoofing
 - machines communicates using ARP is that authentication is based on the hardware address only
 - A hacker can exploit this MAC address authentication by disabling a trusted host and spoofing it MAC address. So in doing this the trusting machine is deceived that the hacker's machine is the trusted host.
 - ARP spoofing can be prevent by either stopping the usage of ARP for obtaining the MAC address of the trusted host by keeping a permanent entry of the MAC address of the trusted host in the ARP caches of the trusting machine.

Security within DNS

- Dynamic Environment
- Cache Poisoning
- Java Applet Vulnerability

Dynamic Environment

Problem:

The DNS and DHCP services must be available to the client systems to provide host name and IP address updates immediately for those mobile users within the dynamic environment.

Solution:

The solution for against this DHCP attack is to set up a firewall to block incoming DHCP packers, DHCP packets should only pass through within the local area network, as well as making the Domain Name more secure.

Cache Poisoning

Problem:

There is a process where attacks are made efforts on the cache data of DNS in order to misdirect and intercept packets on domain name servers.

Solution:

New DNS standards have fixed this bug by establishing discrete cache update security configuration that specify exactly which server has the authority to provide cache updates.

Java Applet Vulnerability

Problem:

The Java applet vulnerability would have been working in conjunction with a hacked DNS server owned and access to some domains in order to carry out the attack.

Solution:

A fix for the applet security manager is to be stricter deciding which computers that an applet is allowed to connect to. System needs to take note of the actual IP address that the applet truly came from, and thereafter only an applet to connect to that exact same numerical address.

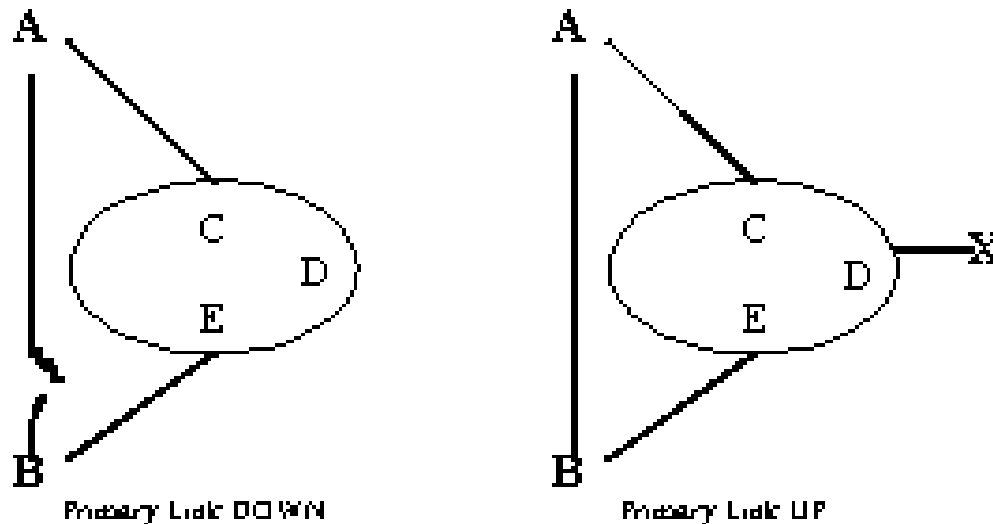
IP spoofing

- Occur on the TCP/IP protocol suite
- complex technical attack where an attacker sends out packets using an IP address other than its own
- What is TCP/IP?
 - comprised of two protocols, TCP and IP
 - designed in the early 1980's with no security taken into consideration
 - IP source addresses provide identification, not authentication

Man-in-the-middle attack

- Packet sniffs on link between 2 end points, and can therefore pretend to be one of the connection.
- attacks are often implemented using network packet sniffer and routing/transport protocols
- Routing redirect is redirecting routing information from the original host to the hacker's host

Source Routing



Legitimate:

$B \rightarrow A$ "reply via C,D,E"

Source Routing Attack:

$B(X) \rightarrow A$ "reply via C,D,X"

Figure 1. Source Routing

(Adapted from <http://www.cis.ohio-state.edu/~dolske/gradwork/cis694q/>)

IP Spoofing

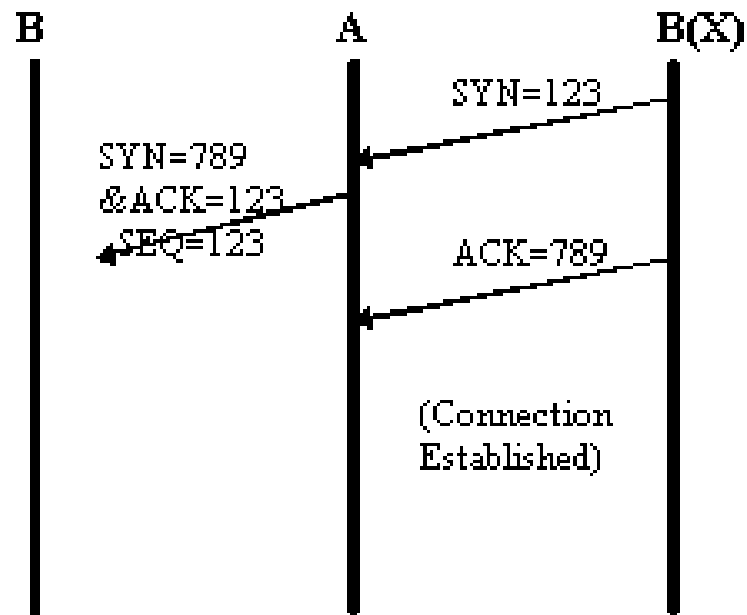


Figure 2. IP Spoofing via Sequence Guessing

(Adapted from <http://www.cis.ohio-state.edu/~dolske/gradwork/cis694q/>)

SYN Flooding

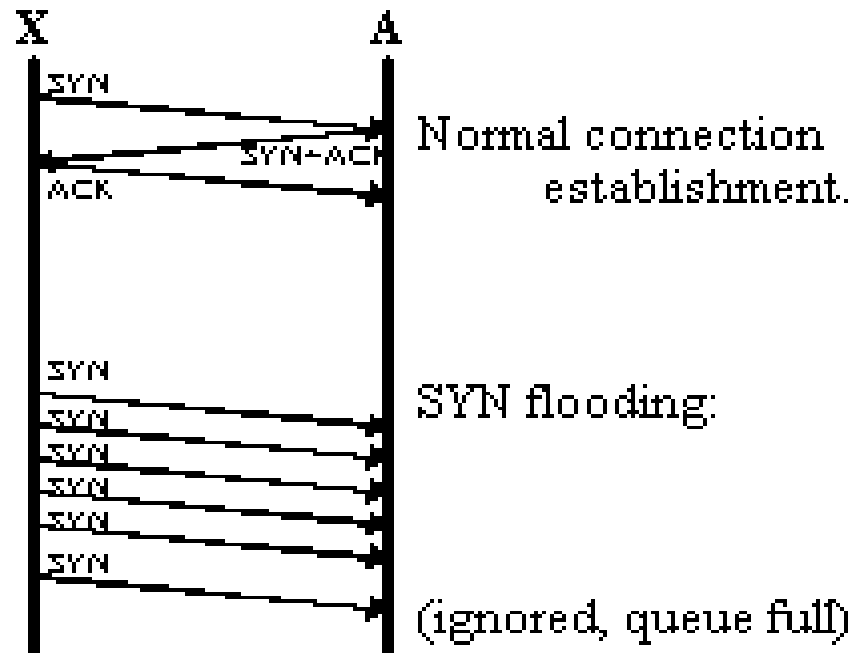


Figure 3. SYN Flooding

(Adapted from <http://www.cis.ohio-state.edu/~dolske/gradwork/cis694q/>)

What can be done to prevent IP Spoofing Attacks?

- *likelihood of IP spoofing attacks can be reduce by configuring the network to reject packets from the Internet that claim to originate from the local address*
- done with proper router configuration in a router
- **Note: If the network trusts foreign hosts**, routers will not protect against a spoofing attack that purports to originate from those hosts
- If you allow internal addresses to access through the outside portion of the firewall, you are vulnerable to attacks too

Conclusion

- All these problems are caused by the trust-relationship between one host and the other
- With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets
- To prevent IP spoofing is by using IPv6 or IPsec instead of IPv4, which include two new characteristics authentication header and encapsulated security payload.
- Application-level firewalls should be used to filter off the unauthorised incoming IP packets and reliable DNS should be deployed to perform a thorough domain names and IP addresses checking and mapping