CERT Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections

Original issue date: January 23, 1995
Last revised: September 23, 1997
Updated Copyright Statement

A complete revision history is at the end of this file. **The IP Spoofing portion of this advisory has been superseded by CA-96.21**

The CERT Coordination Center has received reports of attacks in which intruders create packets with spoofed source IP addresses. These attacks exploit applications that use authentication based on IP addresses. This exploitation leads to user and possibly root access on the targeted system. Note that this attack does not involve source routing. Recommended solutions are described in Section III below.

In the current attack pattern, intruders may dynamically modify the kernel of a Sun 4.1.X system once root access is attained. In this attack, which is separate from the IP spoofing attack, intruders use a tool to take control of any open terminal or login session from users on the system. Note that although the tool is currently being used primarily on SunOS 4.1.x systems, the system features that make this attack possible are not unique to SunOS.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

This description summarizes both the IP spoofing technique that can lead to root access on a system and the tool that intruders are using to take over open terminal and login connections after they get root access. We are currently seeing attacks in which intruders combine IP spoofing with use of the tool. However, these are two separate actions. Intruders can use IP spoofing to gain root access for any purpose; similarly, they can highjack terminal connections regardless of their method of gaining root access.

IP spoofing
To gain access, intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker.

Examples of configurations that are potentially vulnerable include

- routers to external networks that support multiple internal interfaces
- routers with two interfaces that support subnetting on the internal network
- proxy firewalls where the proxy applications use the source IP address for authentication

The IP spoofing attacks we are currently seeing are similar to those described in two papers: 1) "Security Problems in the TCP/IP Protocol Suite" by Steve Bellovin, published in _Computer Communication Review_ vol. 19, no. 2 (April 1989) pages 32-48; 2) "A Weakness in the 4.2BSD Unix TCP/IP Software" by Robert T. Morris. Both papers are available by anonymous FTP from

ftp://ftp.research.att.com/dist/internet_security

Bellovin paper: ipext.ps.Z
Morris paper: 117.ps.Z

Services that are vulnerable to the IP spoofing attack include

SunRPC & NFS
BSD UNIX "r" commands
anything wrapped by the tcp daemon wrappers - site dependent; check your configuration
X windows
other applications that use source IP addresses for authentication

Hijacking tool
Once the intruders have root access on a system, they can use a tool to dynamically modify the UNIX kernel. This modification allows them to hijack existing terminal and login connections from any user on the system.

In taking over the existing connections, intruders can bypass one-time passwords and other strong authentication schemes by tapping the connection after the authentication is complete. For example, a legitimate user connects to a remote site through a login or terminal session; the intruder hijacks the connection after the user has completed the authentication to the remote location; the remote site is now compromised. (See Section I for examples of vulnerable configurations.)

Currently, the tool is used primarily on SunOS 4.1.x systems. However, the system features that make this attack possible are not unique to SunOS.

The CERT Coordination Center has been informed that any services that use Kerberos for authentication should not be vulnerable to an IP spoofing attack. For more information about Kerberos, see

ftp://rtfm.mit.edu/pub/usenet/news.answers/kerberos-faq

Also note that the information and solution described in this advisory does not address the issue of mobile IP spoofing.

II. Impact

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall.

After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

III. Solutions

A. Detection

IP spoofing
If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack. Netlog is available by anonymous FTP from

ftp://net.tamu.edu/pub/security/TAMU/netlog-1.2.tar.gz
MD5 checksum: 1dd62e7e96192456e8c75047c38e994b

Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

Hijacking tool
When the intruder attaches to an existing terminal or login connection, users may detect unusual activity, such as commands appearing on their terminal that they did not type or a blank window that will no longer respond to their commands. Encourage your users to inform you of any such activity. In addition, pay particular attention to connections that have been idle for a long time.

Once the attack is completed, it is difficult to detect. However, the intruders may leave remnants of their tools. For example, you may find a kernel streams module designed to tap into existing TCP connections.

B. Prevention

IP spoofing
The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

The following vendors have reported support for this feature:

Bay Networks/Wellfleet routers, version 5 and later
Cabletron - LAN Secure
Cisco - RIS software all releases of version 9.21 and later
Livingston - all versions

3COM, Cisco Systems, and Morning Star Technologies have provided detailed information, which you can find in Appendix A of this advisory.

If you need more information about your router or about firewalls, please contact your vendor directly.
If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

NOTE: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to do so.

Additional information about protecting yourself from IP spoofing attacks is in Updates section at the end of this file; these updates were added after the initial release of the advisory.

Hijacking tool
There is no specific way to prevent use of the tool other than preventing intruders from gaining root access in the first place. If you have experienced a root compromise, see Section C for general instructions on how to recover.

C. Recovery from a UNIX root compromise

1. Disconnect from the network or operate the system in single-user mode during the recovery. This will keep users and intruders from accessing the system.
2. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as *cmp(1)* located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX *sum(1)* program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

   -- or --

   Reload your system from the vendor's media.
3. Search the system for new or modified setuid root files.

   ```
   find / -user root -perm -4000 -print
   ```

   If you are using NFS or AFS file systems, use ncheck to search the local file systems.

   ```
   ncheck -s /dev/sd0a
   ```

4. Change the password on all accounts.
5. Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.

Appendix A: Vendor Information

3COM

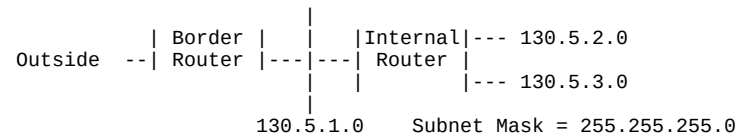
The following information has been provided by 3COM for their customers.

Begin Text Provided by 3COM

```
The following examples illustrate how NETBuilder software can be
configured to support the CERT Advisory recommendations.  Each of
these examples assumes that the value of the -IP FilterDefAction
parameter is configured to Forward.

Example 1:

This example illustrates a two-router solution where the internal
network is configured with non-contiguous IP network numbers.  The
filters are installed on the border router which can only have two
interfaces.  In a two-port router, an output filter on one port is
equivalent to an input filter on the other port.  Please refer to
Figure 1:

Figure 1: Non-Contiguous IP Networks



                          |
            | Border |    |    |Internal|--- 10.0.0.0
 Outside  --| Router |----|----| Router |
                          |    |        |--- 20.0.0.0
                          |
                     30.0.0.0


The border router is configured with the following filters:

 ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 >
           10.0.0.0/0.255.255.255 Discard

 ADD -IP FilterAddrs 20.0.0.0/0.255.255.255 >
           20.0.0.0/0.255.255.255 Discard

 ADD -IP FilterAddrs 30.0.0.0/0.255.255.255 >
           30.0.0.0/0.255.255.255 Discard

 ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 <>
           20.0.0.0/0.255.255.255 Discard

 ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 <>
           30.0.0.0/0.255.255.255 Discard

 ADD -IP FilterAddrs 20.0.0.0/0.255.255.255 <>
           30.0.0.0/0.255.255.255 Discard

This configuration prevents the external attack and allows the
internal router to route traffic between networks 10.0.0.0, 20.0.0.0,
and 30.0.0.0.  This configuration also works for the cascade topology
shown in Figure 2.


Figure 2: Non-Contiguous IP Networks (alternate topology)

                          |                    |
            | Border |    |    |Internal|    |    |Internal|
 Outside ---| Router |----|----| Router |----|----| Router |--- 10.0.0.0
                          |                    |
                          |                    |
                     30.0.0.0           20.0.0.0


Example 2:

The second example illustrates a two-router solution when the internal
```

network is configured with multiple subnets of the Class B network address - 130.5.0.0. The subnet mask is 255.255.255.0. Please refer to Figure 3.

Figure 3: Subnets on the Internal Network



The border router is configured with the following filter:

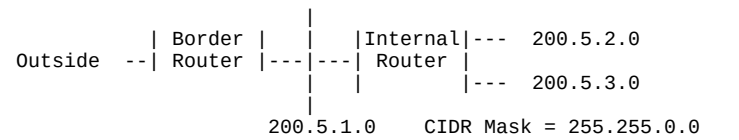
```
ADD -IP FilterAddrs 130.5.0.0/0.0.255.255 >
        130.5.0.0/0.0.255.255 Discard
```

This configuration prevents the external attack and allows the internal route to route traffic between all subnetworks of 130.5.0.0. In this example, a single filter can protect multiple subnets.

Example 3:

The final example illustrates a two-router solution when the internal network is configured with contiguous IP network numbers. Assume the service provider has provided the subscriber with the CIDR block 200.5.0.0/255.255.0.0. Please refer to Figure 4:

Figure 4: Multiple Contiguous IP Networks



The border router is configured with the following filter:

```
ADD -IP FilterAddrs 200.5.0.0/0.0.255.255 >
         200.5.0.0/0.0.255.255 Discard
```

This configuration prevents the external attack and allows the internal router to route traffic between supernets of 200.5.0.0/255.255.0.0. In this example, a single filter can protect multiple contiguous IP networks numbers assigned as a CIDR block.

End Text Provided by 3COM

Cisco Systems

The following information has been provided by Cisco Systems for their customers.

Begin Text Provided by Cisco

```
The defense is to set up your internet firewall router to deny packets
from OUTSIDE your network that claim to have a source address INSIDE
your network.

example configuration:

access-list 101 deny ip 131.108.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 101 deny ip 198.92.93.0 0.0.0.255 0.0.0.0 255.255.255.255
[..rest of your firewall goes here..]

and so on, where access list 101 describes all possible source
addresses on YOUR network.  The example above describes a network with
internal source addresses of 131.108.x.x and 198.92.93.x

Note: If you use only the two line example described above without any
other access-list commands, ALL TRAFFIC will be stopped on your interface
since the implicit action of an unmatched access-list is to deny packets.

If you only want source address spoofing protection and nothing else, add
the line

access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

to the end of the earlier example.  This is NOT an optimal solution since
there are many other possible attacks barring the IP spoofing fixed here.

There are articles on this topic on the CIO information service and various
USENET mailing lists.  You can telnet to cio.cisco.com or point your WWW
browser at http://www.cisco.com.

Anyway!  Once you have defined an appropriate access list you can apply them
to the vulnerable interfaces.

Assuming your interface serial 0 faces the Internet:

 interface serial 0
 description interface facing the big, bad Internet
 ip access-group 101 in

for a router running 9.21 or later.

If you DO NOT have 9.21, an upgrade is NOT required if your internet
firewall is a two port router (which it should be).  Simply
apply access-list 101 as described above to the LAN interface and not
the serial interface.

example:

 interface ethernet 0
 description LAN port on my internet router
 ip access-group 101

The essence of this defense is that any packets coming from the internet that
claim to be from your network are tossed, thereby preventing the style of
attack described below.

Also, for good measure, ALL INTERNET FIREWALLS should have the global
command

no ip source-route

Which helps prevent other forms of spoofing attack from outside.


For further discussion of sequence number guessing attacks, see papers
by Morris and also Bellovin in

ftp://ftp.research.att.com/dist/internet_security/117.ps.Z
ftp://ftp.research.att.com/dist/internet_security/ipext.ps.Z
```

End Text Provided by Cisco

Morning Star Technologies, Inc.

The following information has been provided by Morning Star Technologies for their customers.

Begin Text Provided by Morning Star

TO ALL USERS OF MORNING STAR PRODUCTS:

Here is how to configure your Internet interface to prevent such attacks:

1) Locate the packet filter file controlling your interface to the Internet. For users of Morning Star PPP, this will usually be /etc/ppp/Filter, /usr/etc/ppp/Filter, or /usr/lib/ppp/Filter. Users of Express routers should look in the file called Filter. Check your pppd (or frd for frame relay users) command line for a possibly different filter filename, or look for `ifconfig [interface] filter [filename]' commands in your Express router's rc.boot file.

2) Within the packet filter file, locate the individual filter specification used by your Internet connection. It will begin with either the hostname or IP address of the remote side of a PPP connection, the local hostname or IP address of a frame relay, Ethernet, or RF modem connection, or the special keyword `default' for any type of connection.

3) Within the appropriate filter specification, locate the `pass' filter.

4) Add the following line to the beginning of the pass filter:

```
!ip_opt=srcrt
```

This will cause all transmitted or received IP packets with Source Routing options to be discarded.

5) Determine the IP network number or numbers of your internal network or networks. Insert a set of lines similar to the following pair following the source route rule described in step 4) above for each internal network number.

```
!recv/src/[network-number]
!send/dst/[network-number]
```

This will block all received packets containing a source IP address in your internal network, and will block the transmission of all packets containing a destination IP address in your internal network. For example, we have Class B network 137.175, so our Filter file contains

```
!ip_opt=srcrt
!recv/src/137.175.0.0
!send/dst/137.175.0.0
```

If you don't have a whole IP network, you'll also need to specify a netmask. For example, an organization that has both the Class C network 192.1.1.0 and the Class-C-sized 10.1.220.0 segment of the Class A net 10 would add these lines

```
!ip_opt=srcrt
!recv/src/192.1.1.0
!send/dst/192.1.1.0
!recv/src/10.1.220.0/255.255.255.0
!send/dst/10.1.220.0/255.255.255.0
```

FURTHER NOTE:

Do not configure any of your systems to trust any of the Unix `r' commands (rlogin, rsh, etc.) from any machine outside your firewall. Such systems can be spoofed as easily as internal machines, but spoofed packets cannot be detected at your firewall.

GETTING MORE HELP:

If you need any help with these modifications, call our customer support hotline at +1 800 558 7827 or send us e-mail at support@MorningStar.Com. When sending e-mail, please include the phrase CERT SECURITY PROBLEM in your Subject: header. We will provide assistance with this to all Morning Star customers, even for those without current customer support agreements. If you do not have a current support agreement, use the phrase `CERT SECURITY PROBLEM' when asked for your customer support number.

End Text Provided by Morning Star

The CERT Coordination Center thanks Eric Allman, Steve Bellovin, Keith Bostic, Bill Cheswick, Mike Karels, and Tsutomu Shimomura for contributing to our understanding of these problems and their solutions.

UPDATES

Additional steps you can take to address IP spoofing:

For IP spoofing to be successful, intruders rely on two machines to trust each other through the use of the .rhosts file or the /etc/hosts.equiv file. By exploiting applications that use authentication based on IP addresses (e.g., rsh and rlogin), intruders can gain user or root access on targeted hosts.

We suggest that you use TCP wrappers to allow access from only a select few machines. Although this is not a complete solution, it does reduce your susceptibility to attack. Alternatively, change the configuration of your Internet gateway so that rlogin and rsh from the Internet to hosts in your domain are blocked. If that is not possible, disable the rlogin and rsh services on all of your hosts.

Some sites have turned off source routing thinking that this would prevent IP spoofing attacks. This is NOT the case. Although we encourage sites to turn off source routing this does not prevent IP spoofing attacks. To prevent such attacks it is necessary to undertake packet filtering as described in the advisory.

In addition to the attacks described in this advisory, we are now seeing attacks in which intruders gain access to a site using loopback IP addresses rather than IP addresses particular to that site.

We recommend that in addition to the packet filtering suggestions described in Section III B of the advisory, you configure the filtering router to filter inbound packets in the following IP ranges:

```
127.0.0.0       -       127.255.255.255         (loopback)
10.0.0.0        -       10.255.255.255          (reserved)
172.16.0.0      -       172.31.255.255          (reserved)
192.168.0.0     -       192.168.255.255         (reserved)
```

Finally, we encourage you to consider using network monitoring tools to check for signs of IP spoofing attacks. Argus is a network monitoring tool that uses a client-server model to capture data and associate it into "transactions." The tool provides network-level auditing; it can verify compliance to a router configuration file, and information is easily adapted to protocol analysis, intrusion detections, and other security needs. Argus is available from ftp://ftp.net.cmu.edu/pub/argus-1.5.

Revision History

```
Sep. 23, 1997  Update Copyright statement
Dec. 19, 1996  Updates section - reminder
Sep. 24, 1996  Supersession statement modified
Sep. 19, 1996  Superseded by CA-96.21 [IP spoofing portion only]
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
               Appendix A - added vendor information as it was received: Cisco
               Systems, Morning Star Technologies, and 3COM.
May 10, 1996   Updates section - added pointer to the Argus tool.
Aug. 04, 1995  Updates section - added more information on IP spoofing
               and recommendations for detecting such activity.
Aug. 04, 1995  Sec. I - added notes about Kerberos and mobile IP spoofing.
```