The inetd Program

Today's UNIX systems use the Internet daemon, **inetd**, to centralize the handling of lightweight Internet services. The Internet daemon listens and accepts connections on many network ports at the same time. When a connection is received, **inetd** automatically starts up the appropriate TCP-based or UDP-based server running under the appropriate UID. The Internet daemon also simplifies the writing of application-specific daemons themselves, as each daemon can be written so that it reads from the network on *standard input* and writes back to the network on *standard output,* all with no special calls from the Berkeley socket library being required.

The **inetd** daemon is run at boot time as part of the startup procedure. When **inetd** starts executing, it examines the contents of the */etc/inetd.conf* file to determine which network services it is supposed to manage. The program will reread its configuration file if it is sent a HUP signal.

A sample *inetd.conf* file is shown below: Note that in this example, services that are not considered "secure" have been disabled.

```
#  Internet server configuration database
#
#ftp            stream      tcp     nowait      root        /usr/bin/ftpd ftpd
#telnet         stream      tcp     nowait      root        /usr/sbin/telnetd telnetd
#shell          stream      tcp     nowait      root        /usr/sbin/rshd rshd
#login          stream      tcp     nowait      root        /usr/sbin/rlogind rlogind
#exec           stream      tcp     nowait      root        /usr/sbin/rexecd rexecd
#uucp           stream      tcp     nowait      uucp        /usr/sbin/uucpd uucpd
#finger         stream      tcp     nowait      nobody      /usr/sbin/fingerd fingerd
#tftp           dgram       udp     wait        nobody      /usr/sbin/tftpd tftpd
#comsat         dgram       udp     wait        root        /usr/sbin/comsat comsat
talk            dgram       udp     wait        root        /usr/sbin/talkd talkd
ntalk           dgram       udp     wait        root        /usr/sbin/ntalkd ntalkd
#echo           stream      tcp     nowait      root        internal
#discard        stream      tcp     nowait      root        internal
pop-3           stream      tcp     nowait      root        /usr/sbin/tcpd  popper  -c  -C  -p  2
auth            stream      tcp     nowait      nobody      /usr/sbin/tcpd  identd  -o  -E  -i
```

Each line of the *inetd.conf* file contains at least six fields, separated by spaces or tabs:

Service Name:

Specifies the service name that appears in the /etc/services file. **inetd** uses this name to determine which port number it should listen to. If you are testing a new service or developing your own daemon, you may wish to put that daemon on a nonstandard port. Unfortunately, **inetd** requires that the service name be a symbolic value such as *smtp*, rather than a numeric value such as *25*.

Socket Type:

Indicates whether the service expects to communicate via a stream or on a datagram basis.

Protocol Type:

Indicates whether the service expects to use TCP- or UDP-based communications. TCP is used with *stream* sockets, while UDP is used with *dgram* or datagrams.

Wait/Nowait

If the entry is "wait," the server is expected to process all subsequent connections received on the socket. If "nowait" is specified, **inetd** will fork() and exec() a new server process for each additional datagram or connection request received. Most UDP services are "wait," while most TCP services are "nowait," although this is not a firm rule. Although some man pages indicate that this field is used only with datagram sockets, the field is actually interpreted for all services.

User

Specifies the UID that the server process will be run as. This can be *root*, UID 0, *daemon*, UID 1, *nobody*, often UID 2 or 65534, or any other user of your system. This field allows server processes to be run with fewer permissions than *root* to minimize the damage that could be done if a security hole is discovered in a server program.

Command Name and Arguments

The remaining arguments specify the command name to execute and the arguments passed to the command, starting with *argv[0].*

Some services, like echo, time, and discard, are listed as "internal." These services are so trivial that they are handled internally by **inetd** rather than requiring a special program to be run. Although these services are useful for testing, they can also be used for denial of service attacks. You should therefore disable them.

You should routinely check the entries in the */etc/inetd.conf* file and verify that you understand why each of the services in the file is being offered to the Internet. Sometimes, when attackers break into systems, they create new services to make future break-ins easier. If you cannot explain why a service is being offered at your site, you may wish to disable it until you know what purpose it serves. In many circumstances, it is better to disable a service that you are not sure about than it is to leave it enabled in an effort to find out who is using it at a later point in time. If somebody is using the service, they are sure to let you know. One easy way to list all of the services that are enabled is:

```
$ grep -v "^#" /etc/inetd.conf
talk        dgram       udp     wait        root        /usr/sbin/talkd talkd
ntalk       dgram       udp     wait        root        /usr/sbin/ntalkd ntalkd
pop-3       stream      tcp     nowait      root        /usr/sbin/tcpd popper -c -C -p 2
auth        stream      tcp     nowait      nobody      /usr/sbin/tcpd identd -o -E -i
```

When we look at the */etc/inetd.conf* file on a Solaris 10 system, we see in the comments that

```
# This file is no longer directly used to configure inetd.
# The Solaris services which were formerly configured using this file
# are now configured in the Service Management Facility using inetadm.
```

Checking the man pages for **inetadm** we have

```
The inetadm utility provides the following capabilities for
     inetd-managed SMF services:

         o    Provides a list of all such services installed.

         o    Lists the services' properties and values.

         o    Allows enabling and disabling of services.

         o    Allows modification of the services' property
              values, as well as the default values provided by
              inetd.
```

Checking what services are enabled/disabled in Sparc2.cs.clemson.edu

```
$ /usr/sbin/inetadm
ENABLED   STATE          FMRI
disabled  disabled       svc:/application/x11/xfs:default
disabled  disabled       svc:/application/x11/xvnc-inetd:default
enabled   online         svc:/application/font/stfsloader:default
disabled  disabled       svc:/application/print/rfc1179:default
disabled  disabled       svc:/network/talk:default
disabled  disabled       svc:/network/ftp:default
disabled  disabled       svc:/network/stlisten:default
disabled  disabled       svc:/network/stdiscover:default
disabled  disabled       svc:/network/nfs/rquota:default
disabled  disabled       svc:/network/security/krb5_prop:default
enabled   online         svc:/network/security/ktkt_warn:default
disabled  disabled       svc:/network/uucp:default
disabled  disabled       svc:/network/comsat:default
disabled  disabled       svc:/network/swat:default
disabled  disabled       svc:/network/rpc/metamh:default
enabled   online         svc:/network/rpc/cde-calendar-manager:default
disabled  disabled       svc:/network/rpc/rstat:default
disabled  disabled       svc:/network/rpc/metamed:default
disabled  disabled       svc:/network/rpc/ocfserv:default
disabled  disabled       svc:/network/rpc/mdcomm:default
disabled  disabled       svc:/network/rpc/spray:default
enabled   online         svc:/network/rpc/cde-ttdbserver:tcp
enabled   online         svc:/network/rpc/gss:default
disabled  disabled       svc:/network/rpc/rex:default
disabled  disabled       svc:/network/rpc/rusers:default
enabled   online         svc:/network/rpc/smserver:default
disabled  disabled       svc:/network/rpc/wall:default
disabled  disabled       svc:/network/rpc/meta:default
disabled  disabled       svc:/network/shell:default
disabled  disabled       svc:/network/shell:kshell
```

```
disabled  disabled       svc:/network/discard:dgram
disabled  disabled       svc:/network/discard:stream
disabled  disabled       svc:/network/chargen:dgram
disabled  disabled       svc:/network/discard:stream
disabled  disabled       svc:/network/chargen:dgram
disabled  disabled       svc:/network/chargen:stream
disabled  disabled       svc:/network/tname:default
disabled  disabled       svc:/network/daytime:dgram
disabled  disabled       svc:/network/daytime:stream
disabled  disabled       svc:/network/telnet:default
disabled  disabled       svc:/network/rexec:default
disabled  disabled       svc:/network/finger:default
disabled  disabled       svc:/network/login:eklogin
disabled  disabled       svc:/network/login:klogin
disabled  disabled       svc:/network/login:rlogin
disabled  disabled       svc:/network/echo:dgram
disabled  disabled       svc:/network/echo:stream
disabled  disabled       svc:/network/cde-spc:default
disabled  disabled       svc:/network/time:dgram
disabled  disabled       svc:/network/time:stream
enabled   online         svc:/network/rpc-100235_1/rpc_ticotsord:default
enabled   online         svc:/network/sgi_fam_1-2/rpc_tcp:default
```