Users' Security Handbook

Status of this Memo

   This document is an Internet-Draft. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   To learn the current status of any Internet-Draft, please check the
   "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow
   Directories on ds.internic.net (US East Coast), nic.nordu.net
   (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific
   Rim).

Abstract

   The Users' Security Handbook is the companion to the Site Security
   Handbook (FYI 8). It is intended to provide users with the
   information they need to keep their networks and systems secure.

Table of Contents

[1](#). **Who Cares?**

   This document is meant to provide guidance to the end users of
   computer systems and networks on what they can do to keep those
   systems and networks secure. It is a companion document to the Site
   Security Handbook [SSH].

[1.1](#) **Why Was This Written?**

   This handbook is a guide which end users can follow to help keep
   their computer systems and networks more secure. It contains hints
   and guidelines, dos and don'ts, and anecdotes chosen to help codify
   the information in users' memories.

   This guide is meant to be a framework which sites can build upon to
   create handbooks to distribute to their users. However, it can stand
   as a users' security guide in its own right.

[1.2](#) **Who Should Read it?**

   This document is targetted towards end users of computer systems and
   networks. This includes users working in small, medium and large
   corporate and campus sites, as well as users working from home PCs
   with modems.

   System and network administrators may wish to use this document as
   the foundation of a site-specific users' security guide; however,
   they should consult the Site Security Handbook first.

[1.3](#) **Stuff You Should Know**

   For the purposes of this document, a "site" is any individual or
   organization that owns and uses computer or network resources. These
   resources may include host computers, routers, servers, or other
   devices that may be accessed from outside the site (e.g., from the
   Internet).

   The "Internet" is the global data network which connects users via
   the TCP/IP suite of protocols.

   An "administrator" is an individual or group which is responsible for
   the day-to-day maintenance and operation of the site's hardware and
   software. A "user" is everyone else.

2. **The ?? Commandments**

3. **READ.ME**

If there were only one thing a user should read before connection to
the Internet, it would be the security policy of the user's home
network. A security policy is a formal statement of the rules by
which users who are given access to an site's technology and
information assets must abide. As a user, you are obligated to
follow the policy created by the decision makers and administrators
at your site. When using an outside network, you are obligated to
follow its Acceptable Use Policy (if it has one).

3.1 What is a Security Policy for?

A security policy exists to protect a site's hardware, software and
data. It explains what the security goals of the site are, what
users can and cannot do, what to do when problems arise and who to
contact, and to generally inform users what the "rules of the game"
are.

3.2 Why You should Follow it

There was once a student who spent four years working on his degree,
but made a tragic mistake at the end of his senior year. He
carelessly left his account, which contained the only copy of all of
his thesis data and writings, logged on when he went home. Some
malicious sole deleted all of his work. This caused the poor student
to fail to graduate and renege on his ROTC scholarship conditions,
and the US government demanded an immediate payback of the $65,000
which had been payed on his behalf.

That's why you should follow it.

4. **Just Do It**

4.1 Passwords

4.2 Viruses and Other Illnesses

4.3 Modems

4.4 Abandoned Terminals

[5](#). Paranoia is Good

   Many people do not realise it but social engineering is a tool which
   many intruders use to gain access to computer systems. The general
   impression that people have of computer break-ins is that they are
   the result of technical flaws in computer systems which the intruders
   have exploited. People also tend to think that break-ins are purely
   technical. However, the truth is that social engineering does play a
   big part in helping an attacker slip through security barriers as
   this could prove to be an easy stepping stone onto the protected
   system if the attacker has no authorised access to the system at all.

   Social engineering may be defined, in this context, as the act of
   talking legitimate computer users into revealing system secrets so as
   to gain information required to break through security barriers. An
   attacker who is good at social engineering can appear to be genuine
   but is really full of deceit.

   Most of the time, attackers using social enginering work via
   telephone calls. This not only provides a shield for the attacker by
   protecting his identity, it also makes the job easier because the
   attacker can claim to be a particular someone with more chances of
   getting away with it.

   There are several types of social engineering. Here are a few
   examples of the more commonly used ones:

      An attacker may pretend to be a legitimate end-user who is new to
      the system or is simply not very good with computers. This
      attacker may approach systems administrators and other end-users
      for help. This "user" may have lost his password, or simply can't
      get logged into the system and needs to access the system
      urgently. Attackers have also been known to identify themselves
      as some VIP in the company, screaming at administrators to get
      what they want. In such cases, the administrator (or it could be
      an end-user) may feel threatened by the caller's authority and
      give in to the demands.

      Attackers who operate via telephone calls may never even have seen
      the screen display on your system before. In such cases, the
      trick attackers use is to make details vague, and get you to

reveal more information on the system. The attacker may sound
really lost so as to make you feel you are helping a damsel in
distress. Often, this makes people go all the way out to help the
"poor user." The user may then reveal secrets when he is off-
guard.

An attacker may also take advantage of system problems that have
come to his attention. Offering help to a user is an effective
way to gain the user's trust. A user who is frustrated with
problems he is facing will be more than happy when someone comes
to offer some help. The attacker may come disguised as the
systems administrator or maintenance technician. This attacker
will often gain valuable information because the user thinks that
it is alright to reveal secrets to technicians.

To guard against becoming a victim of social engineering, the
important thing to remember is that passwords are secret. A password
for your personal account should be known ONLY to you. The systems
administrators who need to do something to your account will not
require your password. As administrator, the privileges they have
will allow them to carry out work on your account without having you
to reveal your password. An administrator should not have to ask you
for your password.

Systems maintenance technicians who come on-site should be
accompanied by the site administrator (who should be known to you).
If the site administrator is not familiar to you, or if the
technician(s) comes alone, it is wise to give a call to your known
site administrator to check if the technician(s) should be there.
Yet many people will not do this because it makes them look paranoid
and it is embarrassing to show that they have no, or little trust in
these visitors.

Unless you are very sure that the person you are speaking to is who
he claims to be, then no secret information should ever be revealed
to such people. Sometimes, attackers may even be good enough to make
themselves sound like someone whose voice you know over the phone.
It is always good to double check the identity of the person. If you
are unable to do so, the wisest thing to do is to reveal no secrets.
If you are a systems administrator, there would be security
procedures for assignment and reassignment of passwords to users, and
you should follow such procedures. If you are an end-user, there
should not be any need for you to have to reveal system secrets to
another user. Some companies assign a common account to several
users. If you happen to be in such a group, make sure you know
everyone in that group so you can tell if someone who claims to be in
the group is genuine.

Finally, it is always wise to take the trouble to locate your site's
user (security) manual and read it. Most sites would have some
security guidelines for end-users. Knowing more about security and
practicing guidelines will help to protect you, the end-user, in the
end. Security guidelines have been drawn up for a purpose, so end-
users should observe and practise security procedures as much as
possible.

[6](). The Wires have Ears

Yes they do. The walls may too, but the wire can reveal much more
than listening at the door ever could. The way computers carry on
conversations on subnets is a lot like the way people communicate at
parties. There's lots of different conversations going on all at
once, and despite the fact that trying to listen to every
conversation at the same time is pretty confusing, it's very easy for
anyone close enough to you to listen to just what you're saying. The
big diffence here is that at parties you can see the people around
you, but with computer networks you don't know every place the wire
goes, so if someone's evesdropping on your computer conversation
you'll never know it.

Most of the chatter that goes on over most computer networks these
days is almost exactly like computers sending post cards to each
other. A postcard contains two addresses, one so the post office
knows where it's going, and another so if it can't be delivered to
that address, it can come back to the person who sent it; it also has
some sort of message the person sending it wants to tell the person
they're sending it to. When you mail someone a postcard, it goes to
the local post office, through the post office chain to the
neighborhood branch of the person you're sending it to, then finally
to their house. The same thing happens when you're using your
computer network. The role of the post office is replaced by the
network routers. It's easy to see how anyone that comes into contact
with that postcard is capable of reading the message that's on it.
Any computer that comes into contact with your computer's post cards
can see the message that's on it, too. Just as anyone that can read
your post card can make a photocopy of it (and send it to anyone else
they want to see it), any computer that sees your corespondence on
the net can save the messages you're sending, and make copies. At
first glance you may think it only applies to email, and places where
you type messages in, but it doesn't. If you're transfering a
program to, or getting a program from, another computer, that program
can be stolen just as easily as a personal message to your mother.
Once it's on the wire, it open season.

It gets worse. There are many tools on the market right now that are

designed to make debugging of problems on computer networks easy.
These tools are meant to help network administrators optimize
productivity on their networks, so the end user is ultimately the
target of these benefits. Unfortunately these tools also give anyone
that uses them the ability to listen to everything everyone on the
subnet they're plugged into has to say, and by the nature of their
design, allows it to be done in a very intelligent way. The tools
will select specific things out of network traffic, allowing people
to target you, passwords, email, whatever they like. Most also allow
them to save these packets, and once that's been done, they can do
anything they want with the information.

Data encryption is a fancy sounding term, but the difference it makes
on a subnet is very easy to understand. Data encryption takes those
postcards, and puts them in envelopes, sending them to the same
address so the message being sent between the two computers can still
get there, and placing your return address on it so it can get back
if necessary. The big difference is that now the message the
computer is sending is hidden inside the envelope, and even though
someone intercepting it can see the envelope, it can't be read unless
they know how to open the envelope. It's the ability to use
different types of envelopes, and prevent others from knowing how to
open their envelope that differentiates different types of data
encryption mechanisms from each other, and is what makes them so
fancy.

The basic concept here is pretty simple. People can see what your
doing, and the details of what you're saying if they want to. The
last part of this is important to realize; it helps you tune you're
paranoia accordingly. How important is what you're doing, or what
you're saying? If it's something of national security, you can bet
if anyone knows your doing it, they're interested in reading it. Is
what your doing something very personal to you? Even if you think no
one's interested in it, is it something you don't mind them knowing?
Somewhere in between lies the actual risk.

7. Incident Handling

7.1 Identifying a Breakin

Unfortunately there are no hard and fast rules, only some signs which
can be of use. Modern computers and network programs often do a lot
of work while the user is idle. So just because the computer seems
quite busy when you are not actively using it does not necessarily
imply that a computer has been broken into. Indeed, many of the
indications listed below must be considered suspicious only in the
extreme.

   - Massive disk activity. This might indicate someone is copying
     files from your system to a remote location.

   - Abnormally poor performance. Note that this may occur for many
     reasons. There should be other clues before you suspect a
     breakin.

   - Strangely intense and prolonged network activity. This might arise
     if your home system is being probed for vulnerabilities.

   - System files have modification dates more recent than can be
     explained.

   - Sometimes a hacker with a puerile imagination will flaunt the fact
     he or she has violated a system. An obnoxious message may appear,
     or the system may make irritating noises.

[7.2] What to do if you suspect trouble

   The incident should be reported to your network administrator. For
   home users, report the incident to your Internet Service Provider.
   They will tell you what the next step should be.

   If you suspect that your home computer has a virus, that a malicious
   program has been run, or that a system has been broken into, the
   wisest course of action is to first disconnect the system from all
   networks. If available, virus detection or system auditing software
   should be used.

   If it becomes clear that a home system has been attacked it is time
   to clean up. Ideally, a system should be built back up from scratch.
   This means erasing everything on the hard disk. Then you install the
   operating system and then all additional software the system needs.
   It is best to install the operating system and additional software
   from the original distribution diskettes or cd roms, rather than from
   backup storage. The reason for this is that a system may have been
   broken into some time ago, so the backed up system or program files
   may already include some altered files or viruses. Restoring a
   system from scratch is tedious but worth while.

[7.3] How to prepare for the worst in advance

   - Read all user documentation carefully. Make sure that it is clear
     when services are being run on your computer. If daemons are
     present, make sure they are properly configured (set all
     permissions so as to prevent anonymous or guest logins, and so on).
     Increasingly, many programs have networking capabilities built in
     to them. Learn how to properly configure and safely use these

     features.

   - Back up user data. This is always important. Backups are normally
     thought of as a way of insuring you will not lose your work if a
     hard disk fails or if you make a mistake and deletes a file.
     Backing up is also critical to insure that data cannot be lost due
     to a computer security incident. One of the most vicious and
     unfortunately common threats posed by computer viruses and Trojan
     Horse programs is erasing a computer's hard disk.

   - Obtain virus checking software or security auditing tools. Learn
     how to use them and install them before connecting to a public
     network. Many security tools require that they are run on a
     "clean" system, so they can compare the present state to the
     pristine one. Thus, it is necessary to do some work ahead of time.

   - Upgrade networking software regularly. As new versions of programs
     come out, it is prudent to upgrade. Security vulnerabilities will
     likely have been fixed. The longer you wait to do this, the
     greater the risk that security vulnerabilities of the products will
     be well known and some network assailant will exploit them.

8. Home Alone

   A home system can be broken into over the Internet if a home user is
   unwary. The files on the home system can be stolen, altered or
   destroyed. A computer can acquire a virus, which can degrade or even
   completely halt the system. A computer can house a "Trojan Horse"
   program, which surreptitiously leaks information, files and so forth
   to someone elsewhere on the Internet. The Trojan Horse can also
   provide a hacker with a back door into a computer, effectively
   allowing an assailant access any time the computer is connected to
   the Internet.

8.1 How to pick an ISP

   There are really three ways to use the Internet: with an online
   dial-in service, with a direct connection to the Internet, or with a
   hybrid system which does some of both. You should ascertain which
   type of account you have from your service provider. Each one has
   its own security implications for the home user.

   Examples of an online dial in service would be a BBS or a dial-in
   unix system which allows terminal access only. The BBS or Unix
   system may be directly connected to the Internet and provide services
   to a community, such as Email, usenet news, chatting forums, file
   downloading or even text based World Wide Web access. In this case

privacy and downloading issues are important, but the home system is
effectively unable to directly connect to the Internet. This means
that the home system can't run network services, so this serious
class of problems simply cannot arise. Still, it is wise to find out
what the service provider or sysop recommends for safe storage of
files. For example: Many Unix shell accounts provide a method for
users to publish web pages. It is important to understand how to
adjust the file permissions of files in your home directory in this
case to prevent others from being able to access all of your data.

A home system which uses PPP or SLIP to directly connect to the
Internet is increasingly common. These systems are at the greatest
risk if they run certain kinds of programs called "services." If you
run a service you are in effect making your computer available to
others across the network. Services include:

- File servers (an NFS server, 'file sharing' turned on on a PC)
- An FTP server
- A Web server

If you want to run services on your system, see the section "Beware
of Daemons" below.

The single most important question to ask your service provider is:
"What stands between me and the Internet?"

Some connections to the Internet are direct, others are made behind
various protective barriers. In simplest terms, these mechanisms
prevent anyone from the outside of a trusted network from sending
messages into the trusted network. The 'firewall' is usually set up
so as to allow some information to pass in, such as Email. Users on
the inside of the trusted network can initiate connections to other
computers outside of the protective barriers. If a barrier has been
set up, the most important things to learn as a user are:

- What protection does this afford?
- What inconveniences does it entail?

Some online services provide a combination of dial-in and direct
connection to the Internet. The online services are often accessed
by applications furnished by the service provider. If these
applications communicate with the online services directly, using a
modem, for example, the system is not exposed to internet based
attacks. Some online services, however, provide the ability to also
use TCP/IP networking in addition to their proprietary applications.
This means that software which is not part of the online service's
furnished application suite will be able to connect to Internet
services in general. If this is the case, you should be conscious

   what sort of network applications you use while online. See "What
   program is this, anyway?", above.

Email and BBS pitfalls

   Many users of the Internet avail themselves of a narrow range of
   services such as Email and on-line bulletin board services.

   All the normal caveats apply to messages received via Email that you
   could receive any other way: the sender may not be who he or she
   claims. It is very difficult to determine for sure who sent a
   message. This means that Email is not suitable way to conduct
   business. It is very easy to forge an Email message, so that it
   appears to come from anyone.

   Another security issue you should consider when using Email is
   privacy.

   Email passes through the Internet from computer to computer. The
   addressee will remove it from their mail repository eventually, when
   he or she reads the message. The problem is that as the message
   moves from computer to computer, and indeed as it sits in the
   repository waiting to be read, it is possibly visible to others. The
   vulnerability exists in each link in the chain of computers and
   networks between the sender and the receiver of an Email message.

   For this reason it is wise to think twice before sending confidential
   or extremely personal information via Email. You should never send
   credit card numbers and the like in Email.

   To cope with this problem there are privacy programs which are
   available. Some mail programs make use of PEM, "Privacy Enhanced
   Mail." There is also a popular program which is widely available
   called PGP, "Pretty Good Privacy." To use them you need a mail
   program which employs this privacy protection software.

   Privacy software requires that the sender and receiver exchange some
   information beforehand. This means that it is not easy to send
   private messages to strangers. In general though this is not a
   problem, since confidential information is normally only sent to
   people you have established contact with beforehand.

   One service many Email users like to use is Email forwarding. This
   should be used very cautiously. Imagine the following scenario:

      A user has an account with a private Internet Service Provider and
      wishes to receive all her mail there. She sets up so her Email at
      work is forwarded to her private address. All the mail she would

receive at work then moves across the Internet until it reaches
her private account. All along the way, the Email is vulnerable to
being read. A sensitive Email message sent to her at work could
be read by a network snoop at any of many stops along the way the
Email takes.

Remember to be careful with saved mail. Copies of sent or received
mail (or indeed any file at all) placed in storage provided by an
Internet service provider or BBS may be vulnerable. The risk is that
someone might break into the account and read the old mail.
Precautions against this are:

- Keep your mail files, indeed any sensitive files, on your home
  machine.

- Consider using an 'encryption program' on your sensitive files. It
  should be noted that encryption programs, while easily available,
  are of widely varying quality. PGP offers a strong encryption
  capability.

Internet Service Providers, BBS operators and commercial online
services often provide some assurances of confidentiality of user
data to their subscribers. It pays to read the fine print and ask
the right questions. Just how confidential is a user's data? Just
how competent are the operators of a given online service?

Note that Email sent or received at work is not private, and
employers may legally both read your mail and make use of it.

Many mail programs allow files to be included in mail messages. The
files which come by mail are files like any other. Any way in which
a file can find its way onto a computer is possibly dangerous, like a
disease vector. If the attached file is merely a text message, fine.
But it may be more than a text message. If the attached file is
itself a program or an executable script, extreme caution should be
applied before running it. See the section below entitled "The
Perils of Downloading."

8.3 Don't get caught in the Web

The greatest risk when web browsing is downloading files. Web
browsers allow any file to be retrieved from the Internet. See "The
Perils of Downloading" below.

For the most part, browsing the World Wide Web is a harmless
activity. Web pages consist of text, images, and sounds for the most
part. These are transmitted to a web browsing program, and made
available to the user. The catch here is that web browsing programs

are very complicated and getting more complicated all the time. The
more complicated a program is, the less secure it is considered to
be. The reason for this is that all programs have flaws, the more so
the larger the program. Flaws can very often be exploited by a
network based attacker to gain unintended access to a computer.
Features which seem harmless can be manipulated via seemingly
unrelated program weaknesses in order to provide a way to malign or
gain illicit access to a computer system.

Many web browsers are downloading files even when it is not entirely
obvious. Thus, the risk posed by actively downloading files may be
present even if you do not actively go out and retrieve files
overtly. Any file which you have loaded over the network should be
considered possibly dangerous (even files in the web browser's
cache.) Do not execute them by accident, as they may be malicious
programs.

Web pages often include forms. Be aware that as with Email, the data
sent from a web browser to a web server passes through many computers
and interconnecting networks before it reaches its destination. Any
one of those networks or systems could possibly have compromised
network security. Thus, any personal or financially valuable
information that is sent using a web page entry form may be
evesdropped on. Several mechanisms have been created to prevent
this, most notably "SSL" or the Secure Sockets Layer. This encrypts
the message which is sent from the user's web browser to the web
server so no one along the way can read it.

One paranoid note to add here. Due to export laws in the US, only
very weak encryption may be added to products which are for export.
Since most companies export their products, they use a very weak form
of encryption in conjunction with SSL. The pertinent detail is how
many 'bits' the 'key' has. The more bits, the better. If the key
has only 40 bits, you have reason for concern.

8.4 The Dangers of Downloading

An ever expanding wealth of free software has become available on the
Internet. While this exciting development is one of the most
attractive aspects of using public networks, you should also exercise
caution. Some files may be dangerous. Downloading poses the single
greatest risk to a home system.

It is prudent to decide ahead of time what risks are acceptable and
then stick to this decision. A home system which contains business
records or other valuable and potentially damaging data (if the
information were lost or stolen), it may be wise to simply avoid
downloading any software from the network which comes from any

unknown source.

If the machine has a mixed purpose, say recreation, correspondence
and some home accounting, perhaps the user will hazard some
downloading of shareware applications. He or she takes some risk of
acquiring software which is not exactly what it purports to be.

Ways to minimize the risk:

- Avoid floppy disks which have been in many different computers.
  Especially avoid booting up the computers with these disks in the
  default boot drive. This may not seem like a network security
  issue, but if files downloaded from the network are stored on a
  floppy disk, and the disk is then left in the default boot drive it
  is potentially just as bad as if the disk were freshly brought home
  from a hacker's convention.

- Get to know your computer's system directory. The files located
  there control how the computer works, whether it works, how secure
  it is and so on. If any of those files gets modified without the
  user having explicitly doing it, something might have been done to
  them by a virus or a trojan horse program.

Checking system files is very tedious work to do by hand.
Fortunately there are many virus detection programs available forPCs
and Macintosh computers. There are security auditing programs
available for Unix based computers. If software is downloaded from
the network, it is wise to run virus detection or auditing tools
regularly.

8.5 Downloading continued: What Program is this, anyway?

Programs have become much more complex in recent years.

- A program may have "plug-in" modules. You should not trust the
  Plug- ins simply because you are used to trusting the application
  they plug into. For example: Some web pages suggest that the user
  download a plug in to view or use some portion of the web page's
  content. Consider: What is this plug-in? Who wrote it? Is it
  safe to include it in your web browser?

- Some files are "compound documents." This means that instead of
  using one single program, it will be necessary to run several
  programs in order to view or edit a document. Again, be careful of
  downloading component applications. Just because they integrate
  with products which are well known does not mean that they can be
  trusted.

   - Downloading an application which has the same name as a well known
     application is dangerous. This is a well known ploy to trick
     users. You might accidentally run the downloaded program thinking
     it is the well known application. Files which have the same name
     as system files, utilities or start up batch files are especially
     dangerous.

   - Programs can use the network without making the user aware of it.
     One thing to keep in mind is that if a computer is connected, any
     program has the capability of using the network, with or without
     informing the user. Say for example a game program is downloaded
     from an anonymous file server. This appears to be a shoot-em-up
     game, but unbeknownst to the user, it is transferring all the
     user's files, one by one, over the Internet to a hacker's machine!
     The only indication that this is underway might be that there is a
     lot of disk and network activity. This example is meant to
     illustrate the dangers of downloading and running software of
     unknown origins.

8.6 Remote login

   Many Internet services involve logging in remotely. A user is
   prompted for his or her account name and password. If this
   information is sent through the network without encryption, the
   message can be intercepted and read by others. This is not really an
   issue when you are logging into a "dial-in" service where you make a
   connection via a telephone and logs in, say to an online service
   provider.

   Where it is a risk is when you are using telnet, rlogin, FTP or other
   services which allow access to computers across the Internet.

   A very serious risk for a home user is if he or she runs a remote
   login service on their home machine. This allows the home user to
   log in to their home machine from other computers on the Internet.
   This can be quite convenient. The danger is that someone will
   secretly observe the logging in and be able to masquerade as the user
   whenever they choose in the future.

   The precaution commonly taken against this by larger institutions,
   such as corporations, is to use one-time password systems. Until
   recently this has been far too complicated and expensive for home
   systems. A program called "ssh" allows secure remote login and file
   transfer, and may be appropriate for a technically capable home user.
   The best policy then is to not run a remote log in service on your
   home computer.

8.7 **Beware of Daemons**

There are in general two types of programs which operate on the
Internet. There first is servers, which provide such services as
http (World Wide Web), and DNS (Domain name service.) The other is
clients, such as web browsers.

Most software which runs on home systems is of the client variety;
but, increasingly, server software is available on traditionally
client platforms (e.g., PCs). Server software which runs in the
background is referred to as a "daemon" (pronounced deemon). Many of
the server software program names end in `d', like "inetd" (Internet
Daemon) and "talkd" (Talk Daemon).

There are three very important things to keep in mind as far as the
security implications of running services on a home computer. First
and most important,

- If a server is not properly configured it is very vulnerable to
  attack over a network. It is vital, if you run services, to become
  familiar with how to properly configure them. This is not easy,
  and may require training or technical expertise.

- All software has flaws, and flaws exploited deviously can be used
  to breach computer security. If you run a server on your home
  machine you have to stay aware: If security flaws in it are
  discovered you will need to either stop using the software or apply
  "patches" or "fixes" which eliminate the vulnerability. The
  supplier of the software, if it is a decent company or freeware
  author, will supply information and updates to correct security
  flaws. These "patches" or "fixes" must be installed.

- As a rule of thumb, the older the software, the greater the chance
  it has known vulnerabilities. This is not to say you should simply
  trust brand new software either! Frequently it takes time to
  discover even obvious security flaws in servers.

- Some servers start up without any warning. There have been Web
  Browsers and telnet clients in common use which automatically start
  FTP servers if not explicitly configured to not do so. If these
  servers are not themselves properly configured, the entire file
  system of the home computer can become available to anyone on the
  Internet.

In general, any software MAY start up a network daemon. The way to
be safe here is to know the products you are using. Read the manual,
and if any questions arise, call the company or mail the author of
free software to find out if you are actually running a service by

using the product.

References

   [SSH]   Frasier, Barbara, ed, "Site Security Handbook," RFC ??? (FYI
            8), June, 1996.

Security Considerations

   This document discusses what computer users can do to improve
   security on their systems.

Editor's Address

   Gary Scott Malkin
   Bay Networks
   53 Third Avenue
   Burlington, MA 01803

   Phone: (617) 238-6237
   EMail: gmalkin@baynetworks.com