Erik Guttman / Sun Microsystems
G. Malkin / Bay Networks
September 1997

Users' Security Handbook

Status of this Memo

Abstract

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

Acknowledgements

This document is the work of the Site Security Handbook Working Group of the User Services Area of the Internet Engineering Task Force. The group was chaired by Barbara Y. Fraser of the Software Engineering Institute at Carnegie Mellon University, who also edited the Site Security Handbook. Contributing authors to this document are: Erik Guttman/Sun Microsystems, Lorna Leong/Singapore Telecom.

Table of Contents

1. Who Cares? 3
1.1 Why Was This Written? 3
1.2 Who Should Read it? 3
1.3 Stuff You Should Know 3
2. The Commandments 4
3. READ.ME 4
4. The Wires have Ears 5
5. Just Do It 6
5.1 The Dangers of Downloading 6
5.2 Don't get caught in the Web 6
5.3 Email Pitfalls 7
5.4 Passwords 8
5.5 Viruses and Other Illnesses 9
5.6 Modems 11
5.7 Abandoned Terminals 12
5.8 File Protections 12
5.9 Encrypt Everything 13
5.10 Shred Everything Else 14
5.11 What program is this, anyway? 14
6. Paranoia is Good 15
7. Bad Things Happen 17
7.1 What to do if you suspect trouble 17
7.2 How to prepare for the worst in advance 18
8. Home Alone 18
8.1 Beware of Daemons 19

References 21
Editor's Address 21

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 their data and communication private and their 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.

1.2 Who Should Read it?

This document is targeted 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. Some of the handbook applies only to users who administer their own computers.

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 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. An "end-user" is everyone else.

A "security point of contact" is the person or help desk that you need to get ahold of if you suspect that there has been a computer security incident. If you are in a centrally administered site, your security point of contact will be somewhere within the central administration. If you are a home user, your point of contact will probably be an incident response team run by your Internet Service Provider. You need to know how to make contact in advance. There may be a phone number, Email address or the pager number of a system administrator that you should have on hand.

2. The Commandments

- Know who your security point of contact is.
- Keep passwords secret.
- Read manuals and turn on security features.
- Use a password locked screensaver or log out when you leave your desk.
- Don't let just anyone have physical access to your computer or your network.
- Be aware what software you run and very wary of software of unknown origin. THINK HARD before you execute downloaded software.
- Consider how private your data and Email need to be. Have you invested in privacy software and learned how to use it yet?
- Prepare for the worst in advance.
- Do not panic. Consult your security point of contact if possible before spreading alarm.
- Report security problems as soon as possible to your security point of contact.
- Keep yourself informed about what the newest threats are.

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 a site's technology and information assets must abide. As a user, you are obliged 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).

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 generally informs users what the "rules of the game" are.

Some of the guidelines in this document should be followed in all cases. Other guidelines, specifically those surrounding downloading software, may not be appropriate in all cases.

If you administer your own computer, you may decide that you are willing to take certain risks for the sake of convenience. This may be appropriate if your computer is used recreationally. If you use your computer for your business, you may not want to risk the data being stolen or damaged. It is really up to you. This document will

simply provide you with guidance and some idea of what you are getting yourself in for if you ignore caution.

4. The Wires have Ears

It is a lot easier to evesdrop on communications over data networks than to tap a telephone conversation. Any link between computers may potentially be insecure, as can any of the computers through which data flows. All information passing over networks may be worth evesdropping on, to someone, even if you think "No one will care about this..."

Information passing over a network may be read not only by the intended audience but can be read by others as well. This can happen to personal Email and sensitive information that is accessed via file transfer or the Web. Please refer to the "Caught in the Web" and "Email Pitfalls" sections for specific information on protecting your privacy. The point is that you need to take this very seriously.

As a user, your utmost concerns should, firstly, be to protect yourself against misuse of your computer account(s) and secondly, to protect your privacy.

Unless precautions are taken, every time you log in over a network, to any service, your password or confidential information may be stolen. It may then be used to gain illicit access to systems you have access to. In some cases the consequences are obvious: If someone learns your credit card number or can gain access to your bank account, you might find yourself losing some cash, quickly. What is not so obvious is that services which are not financial in nature may also be abused in rather costly ways. You may be held responsible if your account is misused by someone else!

Many Internet services involve remote logins. 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 in to a "dial-in" service where you make a connection via telephone and log in, say to an online service provider, as telephone lines are harder to evesdrop on than internet communications.

The risk is there when you are using programs to log in over a network. Many popular programs used to log in to services or to transfer files (such as telnet and ftp, respectively) send your name and password and then your data over the network without encrypting it.

The precaution commonly taken against password evesdropping 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 and small businesses. An increasing

number of products allow this to be done without fancy hardware, using cryptographic techniques. An example of such a technique is "SSH" (Secure Shell), which is both freely and commercially available

for a variety of platforms. Many products (including SSH-based ones) also allow user-data to be encrypted before it is passed over the network.

All these may sound very complex but it need not be, in practice. Ask your service provider how to log in securely and what to avoid. If you have a professional service provider they will give you detailed information. If secure login is not available, that itself is possibly good reason not to log in at all and to seek another service provider.

5. Just Do It

5.1 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.

You should decide ahead of time what risks are acceptable and then stick to this decision. It may be wise to simply avoid downloading any software from the network which comes from an unknown source to a computer storing business records, other valuable data and data which are potentially damaging (if the information was lost or stolen).

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

Be careful to store all downloaded files so that you will remember their (possibly dubious) origin. Do not, for example, mistake a downloaded program for a common program, say for doing directory listings.

Checking vital system files for corruption, tampering or malicious replacement is very tedious work to do by hand. Fortunately there are many virus detection programs available for PCs 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.

5.2 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

Dangers of Downloading."

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 browsers may download and execute programs on your behalf. You may disable these features. If you leave them enabled, be sure that you understand the consequences. You should read the security guide which accompanies your web browser as well as the security policy of your company (if you are accessing the Web from work.) You should be aware that downloaded programs may be quite risky to execute on your machine. (See "What program is this, anyway?").

Web pages often include forms. Be aware that, as with Email, data sent from a web browser to a web server is not secure. Several mechanisms have been created to prevent this, most notably SSL (Secure Sockets Layer). This facility has been built into many web browsers. It encrypts messages which are sent between the user's web browser to the web server so no one along the way can read it.

More and more software is downloaded, as part of 'normal' access to the World Wide Web. It is of course very dangerous to simply run software obtained from uncertain sources, for all the reasons discussed in the section "What Program is this, anyway?"

It is prudent to disable features which allow scripts, programs and the like to be downloaded and run on your computer. You should check with your site's administrative policy before you turn on such features.

If you administer your own machine, you may decide to allow Activex, Javascript, Java, etc. to run in your browser. There are a variety of techniques used to make downloaded programs safer. You should read about them and decide for yourself whether you trust these security mechanisms.

5.3 Email pitfalls

All the normal caveats apply to messages received via Email that you could receive any other way. For example, the sender may not be who he or she claims to be. If Email security software is not used, it is very difficult to determine for sure who sent a message. This means that Email is a 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. As the message moves between computers, and indeed as it sits in the user's mailbox waiting to be read, it is potentially visible to others. 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 via unprotected Email. Please refer to "The Wires Have Ears" section.

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

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 it up so that 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 the 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. If you are a home user, keep your mail files, indeed any sensitive files, on your home machine. You may also consider using an encryption program on your sensitive files.

Note that Email sent or received at work may not be private. Check with your employer, as employers may (in some instances) legally both read your mail and make use of it. The legal status of Email depends on the privacy of information laws in force in each country.

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 entitled "The Dangers of Downloading."

5.4 Passwords

Passwords may be easily guessed by an intruder unless precautions are taken. Your password should contain a mix of numbers, punctuation, and upper and lower case letters. Avoid all real words or combinations of words, license plate numbers, names and so on. The best password is a made up sequence (e.g., an acronym from a phrase you won't forget).

Resist the temptation to write your password down. If you do, keep it with you until you remember it, then shred it! NEVER leave a password taped onto a terminal or written on a whiteboard. You wouldn't write your PIN code on your automated teller machine (ATM) card, would you? You should have different passwords for different accounts, but no so many passwords that you can't remember them. You should change your passwords periodically.

You should also NEVER save passwords in scripts or login procedures as these could be used by anyone who has access to your machine.

Be certain that you are really logging into your system. Just because a login panel or prompt appears and asks you for your password does not mean you should enter it. Avoid unusual login screens and immediately report them to your security point of contact. If you notice anything strange upon logging in, change your password.

You should use "one time passwords" if you are logging in over a network, unless precautions have been taken to encrypt your password when it is sent over the network. (Some applications take care of that for you.) See "The Wires Have Ears" for more information on the risks associated with logging in over a network.

5.5 Viruses and Other Illnesses

The following definitions are quoted from the Internet User's Glossary [GLOSSARY].

Virus

> A program which replicates itself on computer systems by incorporating itself into other programs which are shared among computer systems.

Trojan Horse

> A program which carries within itself a means to allow the creator of the program access to the system using it.

Worm

A computer program which replicates itself and is self-propogating. Worms, as opposed to viruses, are meant to spawn in network environments.

Trojan Horse programs are dealt with in the "What program is this, anyway?" section. Worms should be considered a type of virus for the purposes of the discussion below.

Viruses are essentially unwanted pieces of software that find their way into a computer. What the virus may do once it has entered its host depends on several factors: What the virus has been programmed to do? What part of the computer system has the virus attacked? Some viruses are 'time bombs' which activate only when given a particular condition, such as reaching a certain date. Others remain latent in the system unless a particular afflicted program is activated. Still, there are others which are continually active, exploiting every opportunity to do mischief. A subtle virus may simply modify a system's configuration, then hide.

There are 3 ways to avoid viruses:

If you are responsible for maintaining your own computer, you should take some time to become aware of computer virus detection tools available for your type of computer. You should use an up to date tool (i.e., not older than a year). It is very important to test your computer if there has been a reported virus 'outbreak' in your organization or if you have been using freeware, other peoples' used floppy disks to transfer files, and so on.

If your computer system or account is centrally administered, do not use these tools. Consult your system administrator if you are curious what their strategy is regarding computer viruses.

1. Don't be promiscuous

If at all possible, be cautious about what software you install in your system. Do not run programs which origin you are unaware or unsure of. Do not execute programs or reboot using old diskettes unless you have reformatted them, especially if the old diskettes have been used to bring software home from a trade show, and so on.

Viruses have to get onto a computer somehow. Nearly all risk of viruses can be eliminated if you are extremely cautious about what files are stored on your computer. See "The Dangers of Downloading" for more details.

2. Scan regularly.

   Give your computer a regular check-up. There are excellent virus-checking and security audit tools for most computer platforms available today. Use them, and if possible, set them to run automatically.

3. Notice the unusual.

   It's not true that a difference you cannot detect is no difference at all, but it is a good rule of thumb. You should get used to the way your system works. If there is an unexplainable change (for instance, files you believe should exist are gone, or strange new files are appearing, disk space is 'vanishing') you should check to see if you have a virus.

If you are responsible for maintaining your own computer, you should take some time to be familiar with computer virus detection tools available for your type of computer. You should use an up-to-date tool (i.e., not older than three months). It is very important to test your computer if there has been a reported virus 'outbreak' in your organization or if you have been using freeware, other peoples' used floppy disks to transfer files, and so on.

If your computer system or account is centrally administered, you should use the tools recommended by the systems administration. You should report any virus you suspect has been passed onto your system. You should notify your site's systems administrators as well as the person you believe passed the virus to you. It is important to remain calm. Virus scares may cause more delay and confusion than an actual virus outbreak. Before announcing the virus widely, make sure you verify its presense using a virus detection tool, if possible with the assistance of technically competent personnel.

The best way to avoid problems with viruses is to keep important files backed up. That way, if worse comes to worse, you can always restore your system to its state before it was afflicted.

5.6 Modems

You should be wary about attaching anything to your computer, and especially something which allows data to flow. If your computer is centrally administered, you should get permission before you connect anything to your computer.

Modems present a special security risk. Many networks are protected by a set of precautions designed to prevent a frontal assault from public networks. If your computer is attached to such a network, you

must exercise care when using a modem. It is quite possible to use the modem to connect to a remote network while *still* being

connected to the 'secure' net. Your computer can now act as a hole in your network's defenses. Unauthorized users may be able to get onto your your organization's network through your computer!

Be sure you know what you are doing if you leave a modem on and set up your computer to allow remote computers to dial in. Be sure you use all available security features correctly. Many modems answer calls by default. You should turn auto-answer off unless you are prepared to have your computer respond to callers. Some 'remote access' software requires this. Be sure to turn on all the security features of your 'remote access' software before allowing your computer to be accessed by phone.

Note that having an unlisted number will not protect you from someone breaking into your computer via a phone line. It is very easy to probe many phone lines to detect modems and then launch attacks.

If you are a dial-in user, you should become familiar with what is normal behavior for your modem. If you detect a lot of sustained modem activity that cannot be explained by your work, it is possible that your system is being probed or accessed by a remote system.

5.7 Don't leave me...

Do not leave a terminal or computer logged in and walk away. Use password locked screensavers whenever possible. These can be set up so that they activate after the computer has been idle for a while.

Sinister as it may be, someone coming around to erase your work is not uncommon. If you remained logged in, anyone can come by and perform mischief for which you may be held accountable. For example, imagine the troubles you could be in for if nasty Email were sent to the president of your company in your name, or your account were used to transfer illegal pornography.

Anyone who can gain physical access to your computer can almost certainly break into it. This means that you should be careful with who you allow access to your machine. If this is impossible, it is wise to encrypt your data files kept on your local hard disk. It is wise to lock the door to one's office where the computer is stored, if possible.

5.8 File Protections

Data files and directories on shared systems or networked file systems require care and occasional oversight. There are two categories:

- Files to share

Shared files may be visible to everyone or to a restricted group

of other users. Each system has a different way of specifying this. Learn how to control sharing permissions of files and implement such control without fail.

- Protected files

  These include files which only you should have access to, but which are available to anyone with system administrator privileges. An example of this are files associated with the delivery of Email. You don't want other users to read your Email, so make sure such files have all the necessary file permissions set accordingly.

5.9 Encrypt Everything

Additionally, there are files that are private. You may have files which you do not wish anyone else to have access to. In this case, it is prudent to encrypt the file. This way, even if your network is broken into or the systems administrator turns into Mr. Hyde your confidential information will not be available. Encryption is also very important if you share a computer. A home computer may be used for preparing taxes and playing computer games by children. By backing up the data and using encryption, this kind of shared use may be done safely.

Before you encrypt files on a shared file server, you should check with your site's security policy. Some employers and countries expressly forbid the storing and/or transferring of encrypted files.

Be careful with the passwords or keys you use to encrypt files. Safely lock them away to keep them from others but also for your own security. If you lose them, you will lose your ability to decrypt your data as well! It may be wise to save more than one copy. This may even be required, if your company has a key escrow policy, for example. This protects against the possibility that the only person knowing a pass phrase may leave the company or be struck by lightning.

It should be noted that encryption programs, whilst readily available, are of widely varying quality. PGP (which stands for "Pretty Good Privacy") for example, offers a strong encryption capability. Many common software applications include the capability to encrypt data. The encryption facilities in these are typically very weak.

You should not be intimidated by encryption software. Easy to use software is being made available.

5.10 Shred Everything Else

You would be surprised what gets thrown away in the wast paper basket: notes from meetings, old schedules, internal phone lists, computer program listings, correspondence with customers, even market analyses. All of these would be very valuable to competitors, recruiters and even an overzealous (hungry?) journalist looking for a scoop. The threat of dumpster diving is real - take it seriously! Shred all potentially useful documents before discarding them.

You should also be aware that deleting a file does not erase it in many cases. The only way to be sure that an old hard disk does not contain valuable data may be to reformat it.

5.11 What Program is this, anyway?

Programs have become much more complex in recent years. They are often extensible in ways which may be dangerous. These extensions make applications more flexible, powerful and customizable. They also open the end-user up to all sorts of risks.

- A program may have "plug-in" modules. You should not trust the plug-ins simply because you are used to trusting the applications 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?

  Newer web browsers will allow "plug-in" modules to have "digital signatures." This will assist you in determining the source of the software, but you must still answer the questions posed above.

- 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 application components. Just because they integrate with products which are well-known does not mean that they can be trusted. Say you receive a mail message which can only be read if you download a special component. This component could be a nasty program which reformats your hard drive!

- Programs can use the network without making you 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 you. Say for example:

  > You download a game program from an anonymous file server. This appears to be a shoot-em-up game, but unbeknownst to you, it

transfers all your files, one by one, over the Internet to a cracker's machine! Or it might disconnect from your online

service, and dial into a server reached via a foreign telephone number, doing untold mischief and sending your phone bill through the roof in the process...

6. 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 plays a big part in helping an attacker slip through security barriers. This often proves to be an easy stepping stone onto the protected system if the attacker has no authorized access to the system at all.

Social engineering may be defined, in this context, as the act of gaining the trust of legitimate computer users to the point where they reveal system secrets or help someone, unintentionally, to gain unauthorized access to their system. Using social engineering, an attacker may gain valuable information and/or assistance that could help break through security barriers with ease. Skillful social engineers can appear to be genuine but are really full of deceit.

Most of the time, attackers using social enginering work via telephone. This not only provides a shield for the attacker by protecting his or her 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 the user to reveal more information on the system. The attacker may sound

really lost so as to make the user feel that he is helping a damsel in distress. Often, this makes people go way out their way

to help. 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. Site visits may pose a greater risk to the attacker as he may not be able to make an easy and quick get-away, but the risk may bring fruitful returns if the attacker is allowed direct access to the system by the naive user.

- Sometimes attackers can gain access into a system without prior knowledge of any system secret nor terminal access. Just like how one should not carry someone else's bags through Customs, no user should key in commands on someone's behalf. Beware of attackers who use users as their own remotely-controlled fingers to type away on the user's keyboard, commands the user does not understand which may harm the system. These attackers will exploit system software bugs and loopholes even without direct access to the system. The commands keyed in by the end-user may bring harm to the system, open his own account up for access to the attacker or create a hole to allow the attacker entry (at some later time) into the system. If you are not sure of the commands you have been asked to key in, do not simply follow instructions. You never know what and where these could lead to...

To guard against becoming a victim of social engineering, one 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 administrators, 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.

Most maintenance work will require special privileges which end-users are not given. Users should guard the use of their accounts, and keep it for their own use. Accounts should not be shared, not even temporarily with a maintenance staff or administrator. Systems administrators will have their own accounts to work with and will not need to access a system via an end-user's account.

Systems maintenance technicians who come on site should be accompanied by the local site administrator (who should be known to

you). If the site administrator is not familiar to you, or if the technician comes alone, it is wise to give a call to your known site administrator to check if the technician 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 or she claims to be, 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 not to reveal any secrets. If you are a systems administrator, there should 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 anyone else. Some companies assign a common account to multiple 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.

7. Bad Things Happen

This section concerns those who maintain their own computer systems. For those who have an account on a shared system or a centrally administered computer, very little in this section will apply to you. If you notice that your files have been modified or ascertain somehow that your account has been used without your consent, you should inform your security point of contact immediately.

The rest of this section concerns those whose systems are not centrally administered, such as home users or employees of small businesses.

7.1 What to do if you suspect trouble

The incident should be reported to your security point of contact. 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. Do not forget to re-install all security related fixes you had installed before the security incident. Obtain these from a verified, unsuspicious source.

7.2 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 network services are activated, 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. Keep up to date!

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. The system itself could be accessed again some time in future, if it has been compromised. This section describes issues and makes recommendations relevant to a home user of the Internet.

8.1 Beware of Daemons

A home system which uses PPP 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. Some services include:

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

There are in general two types of programs which operate on the Internet: Clients (like web browsers and Email programs) and Servers (like web servers and mail servers).

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 dee-mon). Many of the server software program names of internet daemons end in `d', like "inetd" (Internet Daemon) and "talkd" (Talk Daemon). These programs wait for clients to request some particular service from across the network.

There are four 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. This requires work: You have to stay in touch with the supplier of the software to get security updates. It is highly recommended that you keep up with security through on-line security forums. See [SSH] for a list of references.

  If security flaws in your server software 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.

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. See "The Wires Have Ears" which suggests precautions to take for remote log in.

If possible, activate all "logging" options in your server software which relates to security. You need to review these logs regularly in order to gain any benefit from this logging. You should also be aware that logs often grow very quickly in size, so you need to be careful they don't fill up your hard disk!

References

[GLOSSARY] Malkin, G, ed, "Internet User's Glossary", RFC 1983 (FYI 18), August, 1996.

[SSH] Frasier, Barbara, ed, "Site Security Handbook," RFC 2196 (FYI 8), June, 1996.

Security Considerations

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

Editor's Address

Erik Guttman
Sun Microsystems
Bahnstr. 2
74915 Waibstadt Germany

Phone: +49 7263 911701
Email: eguttman@eng.sun.com

Gary Scott Malkin
Bay Networks
8 Federal Street
Billerica, MA 01821

Phone: (508) 916-4237
Email: gmalkin@baynetworks.com