draft-ietf-ssh-users-09.txt
Site Security Handbook WG

Erik Guttman / Sun Microsystems
Lorna Leong / COLT Internet
G. Malkin / Bay Networks
October 7, 1998

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.

Table of Contents

Part One: Introduction

This document provides guidance to the end-users of computer systems and networks about what they can do to keep their data and communication private, and their systems and networks secure. Part Two of this document concerns "corporate users" in small, medium and large corporate and campus sites. Part Three of the document addresses users who administer their own computers, such as home users.

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 [RFC2196].

A glossary of terms is included in an appendix at the end of the document introducing computer network security notions to those not familiar with them.

1. READ.ME

Before getting connected to the Internet or any other public network, you should obtain the security policy of the site that you intend to use as your access provider, and read it. 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.

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.

2. The Wires have Ears

It is a lot easier to eavesdrop 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 eavesdropped on, 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 "Don't Get Caught in the Web" and "Email Pitfalls" sections for specific information on protecting your privacy.

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 network 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 gains 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 network services involve remote log in. A user is prompted for his or her account ID (ie. username) 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 more difficult to eavesdrop 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 username and password and then your data over the network without encrypting them.

The precaution commonly taken against password eavesdropping 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. However, an increasing number of products allow this to be done without fancy hardware, using cryptographic techniques. An example of such a technique is Secure Shell [SSH], which is both freely and commercially available for a variety of platforms. Many products (including SSH-based ones) also allow data to be encrypted before it is passed over the network.

Part Two: End-users in a centrally-administered network

The following rules of thumb provide a summary of the most important pieces of advice discussed in Part Two of this document:

- Know who your security point-of-contact is.
- Keep passwords secret at all times.
- Use a password-locked screensaver or log out when you leave your desk.
- Don't let simply 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.
- 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.

3. Watch out!

3.1. 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.

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 another program just because they have the same name. This is a common tactic to fool users into activating programs they believe to be familiar but could, in fact, be dangerous.

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 FTP 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!

Many corporate environments explicitly prohibit the downloading and running of software from the Internet.

3.2. 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."

Web browsers are downloading files even when it is not entirely obvious. Thus, the risk posed by 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. (Remember, programs are files, too. You may believe you have downloaded a text file, when in fact it is a Trojan Horse program, script, etc.)

Web browsers may download and execute programs on your behalf, either automatically or after manual intervention. 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. You should be aware that downloaded programs may be 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 Secure Sockets Layer [SSL]. This facility has been built into many web browsers. It encrypts data sent between the user's web browser to the web server so no one along the way can read it.

It is possible that a web page will appear to be genuine, but is, in fact, a forgery. It is easy to copy the appearance of a genuine web page and possible to subvert the network protocols which contact the desired web server, to misdirect a web browser to an imposter.

That threat may be guarded against using SSL to verify if a web page is genuine. When a 'secure' page has been downloaded, the web browser's 'lock' or 'key' will indicate so. It is good to double-check this: View the 'certificate' associated with the web page you have accessed. Each web browser has a different way to do this. The certificate will list the certificate's owner and who issued it. If these look trustworthy, you are probably OK.

3.3 Email Pitfalls

All the normal concerns 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 itself is a not a suitable way to conduct many types

of business. It is very easy to forge an Email message to make it appear to have 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 a 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 other sensitive data via unprotected Email. Please refer to "The Wires Have Ears."

To cope with this problem, there are privacy programs available, some of which are integrated into Email packages.

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.

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. 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."

3.4 Passwords

Passwords may be easily guessed by an intruder unless precautions are taken. Your password should contain a mixture of numbers, upper and lower case letters, and punctuation. Avoid all real words in any language, 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), such as "2B*Rnot2B" (but don't use this password!)

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 not 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 prompt appears and asks you for your password does not mean you should enter it. Avoid unusual login prompts and immediately report them to your security point-of-contact. If you notice anything strange upon logging in, change your password.

Unless precautions have been taken to encrypt your password when it is sent over the network, you should, if possible, use "one-time passwords" whenever you log in to a system over a 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.

3.5 Viruses and Other Illnesses

Viruses are essentially unwanted pieces of software that find their way onto a computer. What the virus may do once it has entered its host, depends on several factors: What has the virus 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 until a particular afflicted program is activated. There are still others which are continually active, exploiting every opportunity to do mischief. A subtle virus may simply modify a system's configuration, then hide.

Be cautious about what software you install on your system. Use software from "trusted sources", if possible. Check your site policy before installing any software: Some sites only allow administrators to install software to avoid security and system maintenance problems.

Centrally-administered sites have their own policy and tools for dealing with the threat of viruses. Consult your site policy or find out from your systems administrator what the correct procedures are to stay virus free.

You should report it if a virus detection tool indicates that your system has a problem. 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 presence using a virus detection tool, if possible, with the assistance of technically-competent personnel.

Trojan Horse programs and worms are often categorized with viruses. Trojan Horse programs are dealt with in the "What Program is This, Anyway?" section. F the purposes of this section, worms should be considered a type of virus.

3.6 Modems

You should be careful when attaching anything to your computer, and especially any equipment which allows data to flow. You should get permission before you connect anything to your computer in a centrally-administered computing environment.

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 also 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 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.

3.7 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 seem, 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. Therefore, be cautions regarding who you allow
access to your machine. If physically securing your machine is not possible, it is wise to encrypt your data files kept on your local hard disk. If possible, it is also wise to lock the door to one's office where the computer is stored.

3.8 File Protections

Data files and directories on shared systems or networked file systems require care and maintenance. There are two categories of such systems:

- 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.

3.9 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. For example, a home computer may be shared by roomates who are friends but prefer to keep their Email and financial information private. Encryption allows for shared yet private usage.

Before you encrypt files you should check your site's security policy. Some employers and countries expressly forbid or restrict the storing and/or transferring of encrypted files.

Be careful with the passwords or keys you use to encrypt files. Locking them away safely not only helps to keep them from prying eyes but it will help you keep them secure too; for 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.

Whilst encryption programs are readily available, it should be noted that the quality can vary widely. 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.

3.10 Shred Everything Else

You would be surprised what gets thrown away into the waste-paper basket: notes from meetings, old schedules, internal phone lists, computer program listings, correspondence with customers and 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.

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

- Some programs are downloaded automatically when accessing web pages. While there are some safeguards to make sure that these

programs may be used safely, there have been security flaws discovered in the past. For this reason, some centrally-administered sites require that certain web browser capabilities be turned off.

4. 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(s). 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 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. In the same way that 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 commands on the user's keyboard that the user does not understand, commands 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 the need for 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 them 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.

Part Three: End-users self administering a networked computer

The home user or the user who administers his own network has many of the same concerns as a centrally-administered user. The following is a summary of additional advice given in Part Three:

- Read manuals to learn how to turn on security features, then turn them on.
- 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.
- Keep yourself informed about what the newest threats are.

5. Make Your Own Security Policy

You should decide ahead of time what risks are acceptable and then stick to this decision. It is also wise to review your decision at regular intervals and whenever the need to do so arises. 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 is potentially damaging if the information was lost or stolen.

If the system has a mixed purpose, say recreation, correspondence and some home accounting, perhaps you will hazard some downloading of software. You unavoidably take some risk of acquiring stuff which is not exactly what it seems to be.
It may be worthwhile installing privacy software on a computer if it is shared by multiple users. That way, a friend of a roommate won't have access to your private data, and so on.

6. Bad Things Happen

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. When you do not know who your security point-of-contact is, try calling your Internet service provider's help desk as a first step.

6.1 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 ensuring you will not lose your work if a hard disk fails or if you make a mistake and delete 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 be run on a "clean" system, so that comparisons can be made between the present and pristene states. Thus, it is necessary for some work to be done 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 become known and be exploited by some network assailant. Keep up to date!

- Find out who to contact if you suspect trouble. Does your Internet Service Provider have a security contact or Help Desk? Investigate this before trouble happens so you won't lose time trying to figure it out should trouble occur. Keep the contact information both online and offline for easy retrieval.

There are 3 ways to avoid problems with viruses:

1. Don't be promiscuous

If at all possible, be cautious about what software you install on your system. If you are unaware of or unsure of the origin of a

program, it is wise not to run it. Obtain software from trusted sources. 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 other potentially security-vulnerable places.

Nearly all risk of getting infected by 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 system 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 and regularly. Also, install updates of these tools regularly and keep yourself informed with new virus threats.

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 and disk space is 'vanishing'), you should check for the presense of viruses.

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 you have been using freeware, other peoples' used floppy disks to transfer files, and so on.

6.2 What To Do if You Suspect Trouble

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.

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.

If it becomes clear that a home system has been attacked, it is time

to clean up. Ideally, a system should be rebuilt from scratch.
This means erasing everything on the hard disk. Next, 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 worthwhile. Do not forget to re-install all security related fixes you had installed before the security incident. Obtain these from a verified, unsuspicious source.

6.3 Email

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 may be vulnerable. The risk is that someone might break into the account and read the old mail. Keep your mail files, indeed any sensitive files, on your home machine.

7. 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, if compromised, could be accessed again some time in the future. This section describes issues and makes recommendations relevant to a home user of the Internet.

7.1 Beware of Daemons

A home system which uses PPP to connect directly 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 Internet server software programs that run as daemons have names that

end in `d', like "inetd" (Internet Daemon) and "talkd" (Talk Daemon). When set to run, 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 are concerned. First and most important,

- If a server is not properly configured, it is very vulnerable to being attacked over a network. It is vital, if you run services, to be familiar with the proper configuration. This is often 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 issues 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 soon as possible.

- As a rule of thumb, the older the software, the greater the chance that it has known vulnerabilities. This is not to say you should simply trust brand new software either! Often 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 home user running a remote login service on his home machine faces very serious risks. This service allows the home user to log in to his home machine from other computers on the Internet and can be quite convenient. But the danger is that someone will secretly observe the logging in and then be able to masquerade as the user whenever they choose to do so 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 relate 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!

7.2 Going Places

Remote logins allow a user privileged access onto physically remote systems from the comfort of his own home.

More and more companies are offering their employees the ability to work from home with access to their computer accounts through dial-up connections. As the convenience of Internet connectivity has led to lowered costs and wide-spread availability, companies may allow remote login to their systems via the Internet. Customers of companies with Internet access may also be provided with remote login accounts. These companies include Internet service providers, and even banks. Users should be very careful when making remote logins.

As discussed in "The Wires have Ears" section, Internet connections can be eavesdropped on. If you intend to use a remote login service, check that the connection can be done securely, and make sure that you use the secure technologies/features.

Connections may be secured using technologies like one-time passwords, secure shell (SSH) and Secure Sockets Layer (SSL). One-time passwords make a sniffed password useless to the intruder, while secure shell encrypts data sent over the connection. Please refer to "Don't Get Caught in the Web" for a discussion on SSL. Secure services such as these have to be made available on the systems to which you log in remotely.

7.3 Secure It!

Administering your own home computer means you get to choose what software is run on it. Encryption software provides protection for data. If you keep business records and other sensitive data on your computer, encryption will help to keep it safe. For example, if you ran a network service from your home computer and missed setting restrictions on a private directory, a remote user (authorised or not) may gain access to files in this private directory. If the files are encrypted, the user will not be able to read them. But as with all forms of encryption running on any system, the keys and passwords should first be kept safe!

8. A Final Note

This document has provided the reader with an introduction and as

much concise detail as possible. Present security issues go out of date quickly, and although effort has been made to keep discussions

general, examples given may not be relevant in the future as the Internet and computer industry continue to grow.

Just as home-owners are now taking increased cautions at the expense of convenience, to secure their homes in the changing world we live in, computer network users should not ignore security. It may be inconvenient, but it is always better to be safe than sorry.

Appendix: Glossary of Security Terms

Acceptable Use Policy (AUP)

A set of rules and guidelines that specify in more or less detail the expectations in regard to appropriate use of systems or networks.

Account

See (Computer) Account

ActiveX

Microsoft's system that allows webpages to run (active) application code from a websource on the client system, bypassing various controls.

Anonymous and Guest Log In

Services may be made available without any kind of authentication. This is commonly done, for instance, with the FTP protocol to allow anonymous access. Other systems provide a special account named "guest" to provide access, typically restricting the privileges of this account.

Auditing Tool

Tools to analyze computer systems or networks in regard to their security status or in relation to the set of services provided by them. COPS (Computer Oracle Password and Security analyzer) and SATAN (Security Administrator's Tool for Analyzing Networks) are famous examples of such tools.

Authentication

Authentication refers to mechanisms which are used to verify the identity of a user. The process of authentication typically requires a name and a password to be supplied by the user as proof of his identity.

Centrally-Administered Network

A network of systems which is the responsibility of a single group of administrators who are not distributed but work centrally to take care of the network.

Certificate

A certificate is used to verify digital signatures. Say, an Email message contains a digital signature which says "I am from Bob". To verify this, Bob's key will have to be used to check it. Without getting Bob's key, recipients may, instead, rely on certificates (which certify that the key actually belongs to Bob) to verify the source of the message.

Clean System

A computer which has been freshly installed with its operating system and software obtainied from trusted software distribution media. As more software and configuration are added to a computer, it becomes increasingly difficult to determine if the computer is 'clean' or has been compromised by viruses, trojan horse or misconfiguration which reduces the security of the system.

Client

Depending on the point of view, a client might be a computer system which an end-user uses to access services hosted on another computer system called a server. 'Client' may also refer to a program or a part of a system that is used by an end-user to access services provided by another program (for example, a web browser is a client that accesses pages provided by a Web Server).

Compound Documents

A 'document' is a file containing (a set of) data. Files may consist of multiple parts: a plain document, an encrypted document, a digitally-signed documents or a compressed document. Multi-part files are known as compound documents and may require a variety of programs to be used in order to interpret and manipulate it. These programs may be used without the user's knowledge.

(Computer) Account

This term describes the authorization to access a specific computer system or network. Each end-user has to use an account,

which consists most probably of a combination of user name and password or another means of proving that the end-user is the person the account is assigned to.

Configuring Network Services

The part of an administrator's task that is related to specifying the conditions and details of network services that govern the service provision. In regard to a Web server, this includes which Web pages are available to whom and what kind of information is logged to review the use of the Web server.

Cookies

Cookies register information about a visit to a web site, for future use by the server. A server may receive information of cookies of other sites as well which create concern in terms of breach of privacy.

Cracker

These term is used to describe attackers, intruders or other bad guys that do not play by the rules and try to circumvent security mechanisms and/or attack individuals and organisations.

Daemons (inetd, talkd, etc.)

These are processes that run on computer systems to provide services to other computer systems or processes. Typically, daemons are considered "servers".

Decrypting

The process of reversing the encryption of a file or message to recover the original data in order to use or read it.

Default Account

Some systems and server software come with preconfigured accounts. These accounts may be set up with a predefined (username and) password to allow anyone access and aare often put there to make it convenient for users to login initially. Default accounts should be turned off or have their predefined passwords changed, to reduce the risk of abuse to the system.

Dial-in Service

A way of providing access to computer systems or networks via a telecommunications network. A computer uses a modem to make a telephone call to a another modem, which in turn provides 'network access service'. See also: PPP.

Digital Signature

A digital signature is created by a mathematical computer program. It is not a hand-written signature nor a computer-produced picture

of one. The signature is like a wax seal that requires a special stamp to produce it, and is attached to an Email message or file. The origin of the message or file may then be verified by the digital signature (using special tools).

Downloaded Software

Software packages retrieved from the Internet (using, for example, the FTP protocol).

Downloading

The act of retrieving files from a server on the network.

Email Bombs

A denial-of-service attack caused by too many Email being received by a server to the stage where the server runs out of resources.

Email Packages

To communicate via electronic mail, an end-user usually makes use of an Email client that provides the user-interface to create, send, retrieve and read Email. Various different Email packages provide the same set of basic functions but have different user-interfaces and perhaps, special/extra functions. Some Email packages provide encryption and digital signature capabilities.

Email Security Software

Software like PGP provides security functionalities like encryption (and decryption) to enable the end-user to protect messages and documents prior to sending them over a possibly insecure network.

Encrypting / Encryption

This is a mathematical process of scambling data for privacy protection.

Encryption Software

The software that actually provides the needed functionality for end users to encrypt messages and files. PGP is one example.

End-User

An (human) individual that makes use of computer systems and

networks.

Files (programs, data, text and so on)

Files include user data, but also programs, the computer operating system and the system's configuration data.

File Server

A computer system that provides a way of sharing and working on files stored on the system among users with access to these files over a network.

File Transfer

The process of transfering files between two computer systems over a network, using a protocol such as FTP or HTTP.

Fixes, Patches and installing them

Vendors, in response to the discovery of security vulnerabilities, provide sets of files that have to be installed on computer systems. These files 'fix' or 'patch' the computer system or programs and remove the security vulnerability.

FTP (File Transfer Protocol)

A protocol that allows for the transfer of files between an FTP client and FTP server.

Group of Users

Security software often allow permissions to be set for groups (of users) as opposed to individuals.

Help Desk

A support entity that can be called upon to get help with a computer or communication problem.

Internet

A collection of interconnected networks that use a common set of protocols called the TCP/IP stack to enable communication between the connected computer systems.

Key Escrow

Keys are used to encrypt and decrypt files. key escrow is used to store keys for use by third parties to access the data in encrypted files.

Keys Used to Encrypt and Decrypt Files

To make use of encryption, an end-user has to provide some secret, in the form of some data, usually called a key.

Log In, Logging into a System

This is an action performed by an end-user, when he authenticates himself to a computer system.

Log In Prompt

The chracters that are displayed when logging into a system to ask for user name and password.

Logged In

If an end-user has successfully proven to have legitimate access to a system, he is considered to be logged in.

Logging

Systems and server software often provide the ability to keep track of events. Events may be configured to be written out to a file known as a log. The log file can be read later and allows for system failures and security breaches to be identified.

Masquerade (see Remote Log In)

Anyone who pretends to be someone they are not in order to obtain access to a computer account is said to be in 'masquerade'. This may be accomplished by providing a false user name, or stealing someone else's password and logging in as him.

Network File System (NFS, file sharing with PCs, etc.)

NFS is an application and protocol suite that provides a way of sharing files between clients and servers. There are other protocols which provide file access over networks. These provide similar functionality, but do not interoperate with each other.

Networking Features of Software

Some software has features which make use of the network to retrieve or share data. It may not be obvious that software has networking features.

Network Services

Services which are not provided on the local computer system the end-user is working on but on a server located in the network.

One-Time Passwords (OTP)

Instead of using the same password over and over again, a different password is used on each subsequent log in.

Passphrase

A passphrase is a long password. It is often composed of several words and symbols to make it harder to guess.

Password-Locked Screensaver

A screen saver obscures the normal display of a monitor. A password-locked screensaver can only be deactivated if the end-user's password is supplied. This prevents a logged-in system from being abused and hides the work currently being done from passers-by.

Patch

See "Fixes, Patches and installing them"

Permissions

Another word for the access controls that are used to control the access to files and other resources.

PGP (Pretty Good Privacy)

PGP is an application package that provides tools to encrypt and digitally sign files on computer systems. It is especially useful to encrypt and/or sign files and messages before sending them via Email.

Plug-in Modules

Software components that integrate into other software (such as web browsers) to provide additional features.

Point-of-Contact, Security

In case of security breaches or problems, many organisations provide a designated point-of-contact which can alert others and take the appropriate actions.

PPP (Point to Point Protocol)

PPP is the mechanism which most end-users establish between their PC and their Internet service provider, that effectively provides the PC with a "host" status (level with other servers

on the network), enabling them to make
further Internet connections
(eg. Email, chat etc)

Privacy Programs

Another term for encryption software that highlights the use of this software to protect the confidentiality and therefore privacy of the end-users that make use of it.

Remote Access Software

This software allows a computer to use a modem to connect to another system. It also allows a computer to 'listen' for calls on a modem (this computer provides 'remote access service'.) Remote access software may provide access to a single computer or to a network.

Remote Log In

If an end-user uses a network to log in to a system, this act is known as remote log in.

Security Features

These are features which provide protection or enable end-users and administrators to assess the security of a system, for example, by auditing it.

Security Policy

A security policy is written by organisations to address security issues, in the form of "do's" and "don'ts". These guidelines and rules are for users with respect to physical secruity, data security, information security and content (eg. rules stating that sites with sexual content should not be visited, and that copyrights should be honoured when downloading software, etc).

Server

A server is a computer system, or a set of processes on a computer system providing services to clients across a network.

Shared Account

A common account is one which is shared by a group of users as opposed to a normal account which is available to only one user. If the account is misused, it is very difficult or impossible to know which of users was responsible.

Sharing Permissions

Many computer systems allow users to share files over a network. These systems invariably provide a mechanism for users to use to control who has permission to read or overwrite these files.

Site

Depending on the context in which this term is used, it might apply to computer systems that are grouped together by geographical location, organizational jurisdiction, or network addresses. A Site typically refers to a network under a common administration.

SSH (Secure Shell)

SSH provides a protocol between a client and server, allowing for encrypted remote connectivity.

SSL (Secure Sockets Layer)

This protocol provides security services to otherwise insecure protocols which operate over a network. SSL is typically used by web browsers to encrypt data sent to and downloaded from a server.

Systems Administrator

The individual who maintains the system and has system administrator privileges. In order to avoid errors and mistakes done by this individual while not acting as an administrator, he/she should limit the time he/she acts as an administrator (as known to the system) to a minimum.

System Administrator Privileges

System administrators have more rights (greater permissions) as their work involve the maintenance of system files.

System Files

The set of files on a system that do not belong to end-users, which govern the functionality of the system. System files have a great impact on the security of the system.

Telnet

A protocol that enables remote log in to other computer systems over the network.

Terminal

A dumb device that is connected to a computer system in order to provide (text-based) access to it for users and administrators.

Terms of Service (TOS)

See "Acceptable Use Policy (AUP)".

Threats

The potential that an existing vulnerability can be exploited to compromise the security of systems or networks. Even if a vulnerability is not known, it represents a threat by this definition.

Trojan Horse

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

Virus

A program which replicates itself on computer systems by incorporating itself (secretly and maliciously) into other programs. A virus can be transferred onto a computer system in a variety of ways.

Virus Detection Tool

Software that detects and possibly removes computer viruses, alerting the user appropriately.

Vulnerability

A vulnerability is the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

Web Browser Cache

This is the part of the file system that is used to store web pages and related files. It can be utilized to reload recently accessed files from the cache instead of loading it every time from the network.

Web Browser Capabilities

The set of functionalities on a web browser for use by the end-user. This includes the set of plug-ins available.

Web Server

A server program that provides access to web pages. Some web servers provide access to other services, such as databases, and directories.

Worm

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

Acknowledgments

The User Security Handbook was a collaborative effort of the Site Security Handbook Working Group of the IETF. There were also others who made significant contributions --- Simson Garfinkle and Eric Luiijf provided very helpful feedback on this document. The Glossary contribution by Klaus-Peter Kossakowski is much appreciated.

References

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

[RFC2196] Fraser, Barbara, ed, "Site Security Handbook," RFC 2196 (FYI 8), September, 1997.

Security Considerations

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

Authors' Addresses

	Erik Guttman	Lorna Leong	Gary Malkin
	Sun Microsystems	COLT Internet	Bay Networks
	Bahnstr. 2	250 City Road	8 Federal Street
	74915 Waibstadt	City Forum, London	Billerca, MA 01821
	Germany	England	USA
Phone:	+49 7263 911701	+44 171 390 3900	+1 508 916 4237
Email:	erik.guttman@sun.com	lorna@colt.net	gmalkin@baynetworks.com