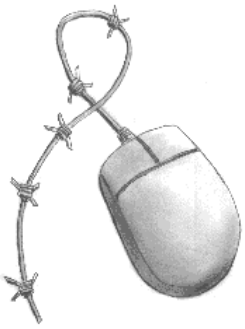
GreenNet CSIR Toolkit Briefing no. 14

Keeping Your System Secure

Basic information on how to protect systems and networks when working online



Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*, 2002.
http://www.internetrights.org.uk/

What's the problem?

There is always a certain amount of risk involved whenever you connect to the Internet. Once your computer interfaces with the Internet, that connection is open to scanning, probing, control, or malicious interference by any other computer hooked up to the 'Net.

By using good procedures for *information and network security* you can reduce the risks of connecting to the Internet. This briefing takes a general look at common and potential forms of disruption that can occur. It is aimed at:

- *Anyone who uses the Internet* for web and email services via service providers (level 1) - people who do not have any direct involvement in system security, but may themselves be the subject of attack or disruption for commercial or nuisance reasons;
- *People who operate* web sites or email lists or services on other people's servers (level 2) - people whose sites or services may be attacked or hijacked by others on the Internet for a variety of reasons;
- *Server operators or supervisors* with responsibility for security (level 3) - we cannot go into the level of technical detail that you probably need. This briefing provides a summary of issues to consider, however, and a list of invaluable sources of further information.

The implications for your Internet security will depend upon which of the three levels above you are operating at. Some issues are common to all levels; even if you use the Internet at level 2 or 3, therefore, you will still find it useful to read the sections on lower levels.

> In order to understand how services on the Internet can be disrupted, you need to have some idea of how the system works. You should refer to the GreenNet CSIR Toolkit Briefing no. 1, *Introduction to the Internet*, if you need more information on terms and concepts discussed in this briefing.

It is important to understand that there will always be risks in using the Internet as a communications medium; there will always be "buggy" software open to disruption and clever "crackers" discovering holes in security. These problems could only be totally resolved, however, by fundamental changes to the open nature of the network, thereby removing the major part of its value.

Why would someone seek to disrupt or take over your system? Motives vary:

- Cracking systems or hijacking computers for fun, but without causing disruption or problems;

- Damaging systems or hijacking computers for malicious pleasure;
- Hijacking computers via the Internet to assist cyber (computer-based) crime;
- Netspionage (Internet-enabled surveillance and spying) by states, corporations or other groups - in recent years this has become a cheap and popular way of obtaining information or intelligence on the use of the Internet by governments and other groups in society. These people may, like cyber criminals, commandeer others' computers to keep one step removed from their target).

There are two groups of *geeks* who play a role in disrupting network security:

- People who use the Internet for specific purposes and use certain features to achieve specific objectives, but do not actively break security barriers, are generally called hackers;
- People who actively break security features by exploiting the flaws in security systems, or force cracking security barriers, are known as *crackers*.

Unfortunately the media get the two confused. In general, *hackers* do not do anything unlawful - although they might skate around the boundaries of legality with some of the operations they undertake. They also tend to be open about their use of the technology.

Crackers tend, because of the unlawful nature of their activities, to work to a more mischievous agenda. This may just be a nuisance (when, for example, a web site is defaced), but it can also involve more complex computer fraud.

Level 1 - Basic users: *Internet usage and general security*

We start by considering security at a basic level, from the perspective of anyone using the Internet from home or from a corporate or academic network.

Any computer linked to the Internet is vulnerable to penetration by crackers. Some programs are more liable to disruption than others, however. Much of Microsoft's software (which dominates in 90% of the home and corporate desktop market), for instance, and in particular the *Windows* operating system, has very poor security.

Once connected to the 'Net, your system can be probed for information unless you take steps to prevent it. If you have some sort of malicious code or *malware* on your system, such as a worm or Trojan (see below), it may allow your system to be controlled from another site (*Back Orifice*, produced by the *Cult of the Dead Cow*1 hacker group, is an example of this). Malicious programs can also transmit sensitive data about you and your computer to crackers, enabling them to penetrate your system.

Most professional systems use *firewalls* to police the flow of information in and out of a computer; firewalls are computer programs that monitor the connections between your computer system and the rest of the local network or the Internet. You can buy firewalls for single PCs. Some very good firewalls are available free from the Internet (*Zone Alarm,*2 for example). These programs *register* those programs which are allowed to access the Net from your computer, prevent other software from using the 'Net without your approval and block requests that do not come directly from sites with which your registered software is communicating.

[1] See the *Cult of the Dead Cow* web site - http://www.cultdeadcow.com/

[2] *Zone Alarm* is available to buy online, but there is a minimal version available for free that performs very well. This software can be obtained from Zonelabs at http://www.zonelabs.com/ - the free version can also be downloaded from *ZDNet* at http://www.zdnet.com/downloads/stories/info/0,,0015P7,.html

Some firewalls, like Zone alarm, can interfere with your local network (if you have one). To remedy this you must specify the addresses used by computers on your local network to avoid them being blocked by the firewall.

The main risks for the single PC user are *viruses*, *Trojans* and *worms*, all of which go under the generic name of *malicious code*.

- Viruses are replicating programs that attach themselves to files and do specific damage to your system. Trojans and worms are fairly similar.
- Trojans are programs that quietly assimilate themselves from within files, but often are not damaging. Often, Trojans are written into commonly-used programs such as screen savers, or as scripted macros in word processing programs such as Word.
- Worms are single programs that distribute themselves across the 'Net, mining data as they go. Often they are designed to enter a system, log information about that system, such as passwords or stored security data such as encryption keys, and transmit it back to a base somewhere else on the 'Net.

Most viruses can be stopped with anti-virus software and regular scanning. Most Trojans will be picked up the same way. But newer viruses, and especially worms, may be missed by virus scanning.3 The only way you can be sure of not receiving malicious code is not to download and execute software from any *unvalidated* source on the 'Net; downloading from the web sites of major software companies is fine (in theory), but doing so from hobbyist web sites is definitely not.

Viruses *are* a threat to your system. However, many of the emails sent around the globe about new viruses are often hoaxes,4 designed to cause panic in an unsuspecting public.

Malicious code can be written into anything that executes a program. Therefore you must also ensure that programs that can use *macros*, such as word processors and spreadsheets, have their anti-virus features switched on.

You should never allow your email program or web browser to download and then automatically open any file from the 'Net that may contain executable code.

The main culprit here is *Microsoft Outlook*. Because of its ability to operate automatically it can be used by a malicious script, such as the *I Love You* or *SirCam* viruses. For better security, use an email program other than *Outlook*.

Even mainstream software can disclose information about your system. For example, if you download *Real Player 8* onto your system, and you have a firewall installed, you will see that when you are connected to the Internet Real Player will periodically try to open up a channel to communicate with its home base.

This is not necessarily a bad thing. But if you allow programs to access the 'Net and transmit data automatically, it is possible that, as part of that transaction, malicious code could be downloaded onto your system.

For example, if someone secretly uploaded a new version of the *Real Player* program to the Real Networks web site with a Trojan in it, it might take a few days for the site operators to notice the change. In that time it could have already infected your system through an automated connection to the Real Networks web site.

[3] If you want to find out the latest news on viruses, visit the *Symantec Anti-virus Research Centre's Online Encyclopaedia* at http://www.symantec.com/avcenter/ This site also gives information on how to deal with viruses.

[4] For information on viruses hoaxes and myths go to the *Vmyths.com* website at http://www.vmyths.com/

It is therefore not a good idea (quite apart from privacy and civil liberties issues) to allow software on your system to open connections to the 'Net, unless you know it is for a specific purpose. To police this, you should operate a firewall, such as the free version of *Zone Alarm*.

Dial-up connections for most stand-alone computers at home or in the office still operate at relatively slow speeds. This limits the ability of crackers to attack them; because the connection speed is slow, any large transaction of data would be very obvious. Furthermore, dial-up connections (as the term indicates) are only turned on when you actively choose to connect to the Internet. In the next few years, higher bandwidth systems such as ADSL (*Asymmetric Digital Subscriber Lines*) and ISDN (*Integrated Services Digital Network*) will become increasingly widespread; these connections are "always on".

An unmonitored connection will be vulnerable if not disconnected, so ADSL and ISDN offer massive opportunities for crackers. The high transfer speeds of these new broadband connections will equally mean that large quantities of data could be exchanged without you, the user, realising.

It is therefore essential that, before using any broadband connection, you invest in some form of firewall software to protect your system from unwanted intrusions.

Level 2 - Server and Web Site operators: *Network disruption and unauthorised access*

People who use servers and run web sites have an additional set of security problems beyond those of the ordinary Internet user.

These problems arise not only because of issues related to servers themselves (see the ***Level 3*** section below) but also because of the way you access the web or email services that you run.

The way you maintain your web site or server can also affect security. If you do not actually own and operate their server in-house there are usually four ways in which you can access your server or web site for maintenance:

- By renting space on "server farms"; these are companies that run large numbers of servers in one location and rent out space to others. Responsibility for front-line security generally falls on the site operators, so you get the level of security that you pay for. With cheap servers, responsibility for security of services such as email or web sites falls to whoever rents the server. If the person maintaining the server is inexperienced, and does not have up-to-date software or configuration information, services run on that server are likely to be wide open to crackers.
- By renting web space on servers; the server operator runs the server software for them. This is far simpler, and more popular, than the first option; server operators have greater control over the system, better enabling them to prevent cracker attacks. Web and other services such as email or list servers, however, are still susceptible to disruption and cracking, however. This is because if you are running an email list or web site on someone else's server, you have to use the Internet to communicate into your list or site, leaving you vulnerable.
- By having web space and email run from a local network. This is far more secure than the first two options, and many people in universities or large organisations do this. Local networks are usually isolated from the Internet, making cracker attacks more difficult. The local network may be used to update a web site, but that data is then usually transferred into a different area of the system for distribution on the Internet.
- By operating web sites where all updates are made manually by the server operators, who send them via email or through the postal system on disk. Few server operators use this method of

updating nowadays, as it is very labour intensive. But because all updates are handled within the server operator's own system it provides a high level of security.

As with most things in life, the level of security and safety you get on the Internet depends on how much you pay for it.

Large amounts of server space can be rented at low cost, for example, from server farms in the USA, provided that you operate all the software to run those services yourself. But, other than configuring a basic firewall, the companies operating the server provide very little security backup on your behalf. If anything goes wrong, it's your problem.

Conversely, some corporate Internet service providers will charge ten to fifty times the fee of a cheap server farm. They have staff available to continually monitor your Internet services for you, protecting them from attack, and tracking down the location of attackers if necessary.

If you operate sites on other people's hardware there are two main risks:

- That, through poor security or because of the lack of proper authentication, other people get access to your area or collection of web services; and
- That the server itself can be targeted for attacks that do not actually involve cracking.

There is also a general risk that the service provider's entire site will be hacked, but there is nothing you yourself can do about that. If you run Internet services on other people's systems the main risks are as follows.

Unauthorised access and defacing

If you run a web site and/or other services on other people's hardware you will usually have remote access to the system. This means that you have to make file transfers using a web browser or an FTP (*file transfer protocol*) program to update files on the operator's system. The only security protection you have for this type of access is usually an email address and a password. As your email address for this is usually the same as your ordinary email address, so a cracker can easily obtain half the key to break in. They then have only to get past the password protection. This can be done by -

- guessing the password - the cracker would usually do some background research on you to discover personal details that might give away a password;
- force cracking the password by throwing a dictionary of words at the site one at a time and seeing if any of them work (this can be easily picked up if someone is watching the data requests to the server, but you will not be aware of it if you have to police your own system);
- exploiting known holes in security to bypass the password authentication system - this is one of the most popular methods of entry (and is discussed in the next section).

As services become increasingly web-based, with growing use of web mail accounts, for example, and use of web pages for maintaining email lists, the opportunities for cracking access become greater.

Web mail may become a particular problem. Unlike dial-up services to an ordinary ISP, web mail is easily accessible from across the globe. Once cracked, a web mail account can be used for spamming, or some sort of denial of service action, or for sending hate mail anonymously.

The main reason for cracking file transfer access to a web site is to deface it. The cracker breaches security and then uploads new files to replace the existing ones or erase the entire site. If the server operator or people maintaining the web site do not keep regular backups of the site then the site will effectively be closed down. An example of this was in August 1999, when the well-known hate site *God Hates Fags* was cracked and a new web site, *God Loves Fags*, was uploaded in its place. Other high profile defacings have attacked government and corporate web sites.

Some sites, particularly where you also have to manage your own software, often use the Telnet protocol to allow access to the server. Whereas breaching the security on an FTP system usually permits access to files, breaching security via Telnet gives a cracker control over the server's software configuration. This enables the cracker to manipulate the server's resources to attack other sites, to covertly store data, or to selectively replace parts of the site to gather further sensitive information. For example, a server could be manipulated to record people's passwords for 'Net services such as email, to record their credit card numbers as part of e-commerce transactions, or to replace downloadable files with new versions containing Trojans or viruses.

If you do not change the access password to a site regularly, then crackers could potentially have regular access to the site for long periods of time. Likewise, if, following a breach, you do not change all passwords on the systems involved, a cracker could simply log back in and repeat the attack a few days later. However, this type of activity requires far more knowledge than it takes to crack file transfer security, and so this type of activity is restricted to truly professional crackers.

There is no simple solution to the problem of access authentication. If there is a problem with the password authentication system itself, that is an issue for your service provider.

If you access and run 'Net services remotely, the best ways of guarding against unauthorised access are to:

- Use an email address specifically for maintaining your site, rather then using your personal email address - this means any cracker will have to work harder to obtain your special email address; and
- Change your access password regularly, using passwords that are a random string of alphanumeric characters.

Redirection of domain names

The *Internet Protocol*[5] uses numeric addresses rather than domain names. If your site is based upon a domain name, then the ability of people to access your site is entirely reliant upon the numeric address pointer stores alongside your domain name on a *name server*.

There have been a number of incidents where, either accidentally or intentionally, the name server database has been altered to redirect site access. For example, the domain name entry for *The Web* in Canada was changed at the request of someone not involved with the organisation, and all requests for the Web's site were redirected to a server in Hong Kong.

Control of domain names for commercial exploitation

The issue of *cyber-squatting* has recently received considerable attention. This is where someone buys up certain domain names, and instead of using them tries to extort money for their return from corporations or individuals who would want them.

[5] See GreenNet CSIR Toolkit Briefing no. 1, *Introduction to the Internet*

There have also been cases where companies have used the courts to press a claim on the basis of intellectual property rights in order to seize control of a domain name[6]. When presented with a court order as a result of this sort of legal action, the company running the name servers will immediately change the database (and hence the domain name of the subject of the action).

There have been cases where existing groups have been the subject of action by newer companies. The most celebrated instance of this kind is *etoy*7. *etoy* was set up as Internet arts group in 1994, but an online toy trader, *eToy Inc.*, which set up in 1996, took out a court action on the grounds that it had rights to *etoy* as a brand name. With the assistance of other hacktivists, *etoy* led an online campaign against the *eToy* web site and severely disrupted the company's online trading system. This action, and the publicity it generated, assisted in lowering the company's share price; as a result of the financial damage this cause, *eToy* eventually gave up their rights to the domain name.

The main national *name servers* have good security. The redirection or diversion of requests for a particular domain name, therefore usually requires some sort of formal action (either deliberately - as in the case of *etoy* - or by mistake - as in the case of *The Web*) to redirect the domain to another server. As branding becomes more pervasive, however, and intellectual property laws are strengthened, this may become more common. The growing backlash against hacktivist and protest groups on the 'Net may also see certain domains removed at a result of national law.

Site blocking

Site blocking software is used with the intention of protecting public morality or preventing children accessing sites with "adult" content.8 The most popular programs are *NetNanny*, *KinderGuard*, *Surfwatch*, *CyberPatrol* and *CyberSentry*. In some countries, and particularly in the USA, the use of blocking software in certain institutions such as public libraries, and even higher education establishments, is becoming mandatory. Some governments (in South East Asia, for instance) use site blocking to ensure that users within their country are only able to access certain sites.

Blocking software programs cause problems, however, because they are a fairly crude instrument. Most of them use a *blacklist* of sites, stored in a pre-set list. Judgements on which sites should go on the list are, reportedly, made by the writers of the software. As the lists are encrypted, the user cannot tell which sites are being blocked by the system.

Some groups of hackers have recently cracked the encryption to reveal the range of sites actually blocked, and in the process have revealed a clear political agenda on the part of the software writers. People who have decrypted the lists have subsequently faced legal action on the grounds that they have infringed "proprietary database rights" under recent international intellectual property agreements.[9]
Recent studies have revealed inconsistencies and double standards in the way sites are blocked. Although hate sites may be blocked in the USA, for example, conservative Christian family-oriented sites which launch attacks on minority groups have been permitted10.

The *Electronic Privacy Information Center*11 (EPIC), again in the USA, illustrates just how crudely blocking

[6] For more information see the GreenNet CSIR Briefing no.7 on *Intellectual Property Rights*

[7] There is a site detailing the events in the 'Toy War' at http://www.toywar.com/ For a general article on the whole saga go to http://www.heise.de/tp/english/inhalt/te/5843/1.html

[8] The *Electronic Freedom Foundation* maintain a detailed resource page on content filtering and blocking at http://www.eff.org/pub/Net_info/Tools/Ratings_filters_labelling/

[9] See GreenNet CSIR Briefing no.7 on *Intellectual Property Rights*

[10] *Wired*, *Filters Kow-towing to Hate?* - http://www.wired.com/news/politics/0,1283,36621,00.html

[11] EPIC, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* - http://www.epic.org/reports/filter-report.html

software operates; in educational establishments it actually hampers students trying to carry out research as part of their studies.

Blocking may also indirectly affect sites that contain no restricted content. For example, if the server you use is also used by a proscribed site, access to all sites on that server may be blocked, not just those perceived as problematic.

What can you do?

The simplest way to avoid all of the problems above is not to have a domain name, but instead be a subdirectory of your service provider's main domain. That way, the only means for removing your site would be to close the service provider's site - which would probably involve legal action against authorities.

Level 3 - Server operators: *System cracking and flooding attacks*

For you are a system operator, security is crucial to running a successful system.

If there are security flaws someone will get to know about them sooner or later. Your system could then become a target for crackers. Your server may also become a target for hackers or *hacktivists* (hackers with a political or social cause) because of its content or purpose.

Server security can be jeopardised by:

- Flooding and denial of service (DoS) attacks;
- Problems with email and lists;
- System probing and cracking attacks; and
- Exploiting holes in system security.

> Server security is a complex and constantly changing area. Ensuring good system security requires you as a server operator to keep up-to-date with the latest information. It is not possible to offer solutions here to the problems highlighted below, but sources of information are included in the section *'further information and research'* towards the end of this briefing.

Flooding and denial of service (DoS)

As a security issue *flooding* and *denial of service* (DoS) can affect both users and operators of servers. We include it here because the only way of defeating these attacks is through maintenance and modification of the server.

A DoS attack involves showering a site with requests for information, or emails, or with certain IP signals that the server must answer. A variety of tactics can be used in DoS attacks. Their aim is to queue more requests at the server than the server is capable of handling. This slows the response of the server, and under certain conditions may even close it down.

If you are a server operator, *flooding* and DoS attacks can cause instability in your server system and leading to a crash. Because they generate large amounts of traffic, flooding attacks may mask a direct attack on the system's security features by crackers using *force cracking* techniques.

The name server can be a weak point in the network. But your Internet connection, and especially the capacity of that connection, are more significant points at which your system could be vulnerable to DoS attacks.

There are two ways of mounting DoS attacks:

- The most high profile attacks, such as those against online traders in early 2000, involved crackers taking over servers with poor security and then showering e-commerce servers with data requests. E-commerce systems, by their nature, have good security. But by picking low-security servers with high-capacity connections one or two crackers were able to generate enough traffic on the network to close down these high-security systems.
- Some protest actions have involved DoS attacks on web sites (for example, the etoy campaign noted earlier, or the Zapatista Tribal Port Scan12); these are known as fully distributed attacks. This involves getting thousands or tens of thousands of people to individually request data using automated web tools. Such actions can have great democratic potential and legitimacy, it can be argued. There is also no simple defence against them.

DoS attacks may target:

- email, web, Telnet or IRC services;
- the router (the device where the line from the Internet enters the system and which directs packets of data to various servers); or
- flaws in the operating system used on the server (this usually involves sending abnormal data packets to the server, causing it to crash).

> Your main defence against DoS attacks is to update or patch your server software to manage those attacks that target flaws in the operating system and software.

DoS attacks can be characterised according to three generic types:

- Those that seek to exploit the operation of the Transmission Control Protocol/Internet Protocol (TCP/IP) system;
- Those that seek to exploit flaws in the software that implements the TCP/IP system; and
- "Brute force" attacks.

The following are the most common forms of DoS attack:

- The SYN Flood attack: When servers initiate connections over the 'Net they send signals to synchronise the transmission of data. The requesting server sends a SYN signal, and the receiving server responds with ACK, to which the requesting server responds with another ACK. But rather than sending the second ACK, the requesting (and attacking) server sends another SYN signal. As the receiving server keeps receiving SYN signals it queues these requests and waits for an ACK signal in response - but to no avail. In the end the server clogs up with SYN requests. Linux, Solaris, and Windows NT/95 are all vulnerable to SYN Flood attacks, although patches can be installed to minimise the impact on the system. Another version of this attack is the NMAP attack. NMAP is the port scanner (see below) that opens connections with ports and then resets them. It can be made to do so at such high volumes as to cause DoS.
- The Land attack: The Land attack is a modification of the SYN Flood attack. In the Land attack the source IP address in the packet is forged or "spoofed" as a non-existent address, or even as an

[12] The *Zapatista Tribal Port Scan* (ZTPS) system, http://www.thing.net/~rdom/ecd/ecd.html

address on the target systems' own network. Windows 95 is vulnerable to Land attacks. Filtering out bad IP addresses at the firewall is one method of defeating Land attacks.

- The Ping of Death attack: The hacker creates abnormally large IP data packets and sends them to the target system. Unless the system screens them out, when they are processed they cause it to hang or crash. Solaris, Unix, Linux and FreeBSD are susceptible to Ping attacks, unless they are updated or patched to screen out excessively large packets.
- The Teardrop attack: When a collection of packets are sent out over the 'Net they can be broken up and sent by different routes. Data within the packets provides information on which packets should be inserted where when they are reassembled at the destination. In the Teardrop attack these data values are modified so that they overlap, causing the system to hang or crash.
- The Smurf attack: This involves sending Internet Control Message Protocol (ICMP) echo requests to a network. The network then broadcasts an echo back. Due to the addressing of the packet this clogs the local network around the server with ICMP traffic. if the source address is spoofed from another network on the Internet, it will flood that network too. Windows NT/95, Unix and Linux systems are susceptible to Smurf attacks, but they can be prevented if you turn off the ICMP packet broadcast feature on the network (but this is not always possible).
- The UDP Flood attack: The UDP (User Datagram Protocol) attack generating UDP packets and then echoing them off another system on the 'Net - so clogging up both systems. UDP packets are meant for the testing and diagnostics of internal/local networks. They are not meant to be passed over the 'Net at all. All common server systems are susceptible to the UDP Flood attack, but if all UDP packets are screened at the firewall (since no UDP packer should ever cross a firewall to or from the Internet) the attack can be defeated.

Other kinds of attack are:

- Brute force DoS attacks are often attacks from low security servers commandeered by crackers. There is basically no defence against brute force attacks. It is simply a matter of capacity. If your Internet connection, or your routers or servers, do not have the capacity to serve the requests then you system will be closed down;
- Mass-participation protest tools such as those developed by the *Electronic Disturbance Theater* (for the Zapatistas campaign) and *the electrohippie collective*.[13]

Problems with email and lists

Email is one of the most widespread features of the 'Net, and one of the most personal. It is can be used as a means of "getting even" between people or groups. The biggest problem that arises here is *email bombing*. This involves the repeated sending of emails, usually containing large amounts of data, to one address, in order to flood the user with email.

At server level, a sufficiently large email bomb can shut down the email system either:

- by simply filling the storage space allotted to the email system (a particular problem if the emails contain large amounts of incompressible data, such as graphics); or
- by the sending of a single email so large (in excess of 32 or 48 megabytes) that the mail handling system cannot cope with the traffic and it shuts down.

At user level, you can deal with the problem by setting up *filters* for email programs to divert emails from problematic addresses to the trash bin.

[13] See *Occasional Paper 1: Client Side Denial of Service* by *the electrohippie collective* - listed in the 'archive' section at http://www.fraw.org.uk/ehippies/

At server level things are more difficult. The server, as part of the email handling system or the firewall, can reject data from certain locations. This has been done routinely for some time to reject emails from those providers who allow *spammers* to use their email systems. Programs can also be obtained to monitor email traffic and *kill* any excessively large emails from a restricted number of addresses. But for protest-related email bombing, where thousands of individuals send only a few small emails (a fully distributed attack), defeating the bombing tactic is very difficult.

Another problem relating to email is the *use of lists*. This is becoming less of a problem today, as more lists require you to confirm consent before you are put on a list. Previously, someone else could put you on a large number of lists in order to bomb you with email.

There are still potential problems with email lists. For example, if a hacker can determine what the content of the confirmation email sent to the target's address will be, they can impersonate or spoof that person's email address using an insecure POP mail server (of which there are a number, many of them for free services that have started up recently). Then, after subscribing, the hacker can send the confirmation email as it came from the user to join the target to the list.

Problems have also been caused where lists have been linked to other lists, so flooding subscribers with emails. Undoing the problem can be a tedious process, as the target, or list moderator, will have to be unsubscribed from each list individually.

Probing and cracking attacks

We have already looked at the cracking and defacing of web sites. Cracking via the server itself, particularly if it was badly set up or configured, offers far more scope than the rather hit-and-miss attempts to gain access for file transfers or web mail. This is because much of the Internet is based around standard operating systems, using standard utilities for certain tasks. By knowing what software or operating system a server is using the cracker can employ different techniques to circumvent the security or authentication systems used.

Local attacks

An attack from within the network is actually far more likely to succeed, because of the availability of information about the system and those who operate it, than a remote attack. Likewise, *local* attacks do not have the problem of negotiating the firewall.

The potential for attack via the local network, for example by volunteers or temporary workers within an organisation's own system, should never be discounted. People on the inside may also be able to perform the necessary probing and research to enable external attacks more quickly.

Remote attacks

We will now focus on *remote* attacks, that is, attacks across the Internet. The first step in carrying out any cracking activity is to gather evidence about the server from a variety of sources:

- Knowing the server's domain name can produce a variety of information, kept within the database of the name server, which is extracted using standard utilities. These utilities quiz the InterNICs about who owns which names. Basic research can also be aided by the finger, rusers and whois services on servers; these services are becoming more restricted, however due to growing security concerns and new data protection laws (particularly in the EU).

- A request to the name server's database will give the numeric address for the server or servers operated by the target. When these are known network scanners are used to identify which ports on the system are in use, and for what services.
- When the cracker has established what types of service the site has, they can use specific tools to test the security features of specific services. This will also throw up additional information such as the type of firewall being used. This information may even be disclosed by simply opening up a Telnet or manual FTP connection to the target site. This type of activity used to be difficult because of the need to have a super user (or root) account on a Unix system to use these utilities, but the availability of Linux for home PCs makes it much easier to use these utilities. In any case, good crackers will write their own.
- When the configuration of the system has been identified, the cracker can write or download from the 'Net, tools with which to challenge the various services, looking for holes in the security through which to gain access. They could also attempt to force-crack password-protected ports, such as the Telnet service; if you, as the server operator, are not carrying out traffic analysis you will allow such attacks to go unchallenged (see below).

With sufficient knowledge, luck or patience, a cracker may gain access to your system. The level of access they gain may vary. But once inside, they could upload utilities to crack internal security and gain access to password and log files, in order to gain *super user* control. If the server is connected to a local network, the cracker could *tunnel* their way into other clients and servers connected to that network.

The ability of a cracker to gain access is largely determined by the skill of whoever is running the server. This is particularly true of the recent growth of Linux as a server system. New network systems like Linux and Microsoft work very well, but the ease with which they can be set up often means that not all security features are enabled, and some services that aid the work of the cracker may not be disabled.

Making your server more secure

Making a server secure is a vast subject, made more complex by the peculiarities of different hardware, operating systems and software. Software and hardware is always imperfect, so as fast as some problems are fixed, new ones can arise (see *security holes* below).

Here, then, is a general outline of steps you should take to make your server more secure.

1. *Procedures and audit:* Procedures are boring, but necessary. Even simple things can make all the difference:
    - Making sure that everyone obeys the rules on the naming of passwords;
    - Ensure that regular network and port scanning is carried out from inside and outside the system.

There are many guides and examples of good practice for procedures for computer security. Look around until you find ones that match your organisation's structure and needs.

2. *Check the installation*: Servers are often installed using a standard operating system, with server applications loaded on top. In the best of all possible worlds the *box* should only perform one function, such as server, workstation, network administration, etc. This enables you to disable or delete unnecessary services and utilities.
    - For Internet servers, all unused services should be disabled;
    - If you are purely using a web, FTP or email server, then other services such as Telnet, News, Finger, etc, should be disabled;
    - If you are not going to use the system for setting up new software, you might consider

removing the run-time environments for Java and Visual Basic, as well as the development utilities installed by default, such as compilers and debuggers; they will just assist the work of the cracker.

3. *Plug the holes*: Research the security history of your main applications, and in particular any services that come into contact with the Internet, as well as the firewall itself. You may need to install patches to these applications, or even a total upgrade.
4. *Implement logging and tracking systems:* To find out if you have an elephant in the fridge you look out for footprints in the butter. You can do this on a server by enabling tracking and logging. There are two aspects to it:
   - *File integrity* - using some sort of checksum or integrity system, you regularly scan the files on the system and look for alterations, in particular in the binary and configuration files.
   - *Traffic analysis* - using a utility to monitor the use of processes within the operating system, and the resources allocated to users, you can look out for abnormalities (also see *intrusion detection* below).

   Most server systems, such as Unix, Linux or Windows NT, come with some sort of logging and tracking system. But because these systems come as standard they are very easily modified by crackers to erase the traces of their access into the server. It is therefore also useful to have some sort of non-standard or proprietary tracking and logging system. A cheaper option may be to write the logs to a write-once media such as a CD-R disc so that changes cannot be retrospectively erased.
5. *Firewalls and filtering*: Installing a firewall is no guarantee of security in itself. It must be properly configured with a set of rules that reflect the structure and patterns of operation of the server. This can be complex where the server performs other functions; people usually install another box on a network between the router and the server, to act as a stand-alone firewall between the Internet and the server. As well as a firewall, you should introduce some sort of filtering, such as *ipchains*. Filtering utilities will reject rogue packets such as those associated with DoS attacks, but it can also be useful for rejecting packets from sites that are behaving in a way consistent with some sort of scanning or probing prior to a cracker attack. The latest filtering software can also include features such as *masquerading*, where the software responds to potential probing from a remote site by shunting those requests into a sort of decoy server environment.
6. *Intrusion detection*: Whilst the firewall is your main method of preventing intrusion, it should never be relied upon exclusively. Intrusion detection systems are programs that monitor system activity, based on user-defined rules, in a similar way to firewalls. They can quickly scan the system logs, looking for abnormalities, or physically monitor the system's ports, looking for abnormal or excessive levels of activity (although this uses far more system resources). There is a wide range of intrusion detection systems available. You should use them regularly to detect modifications to your system. Using a program is a less tedious and more thorough way of checking system logs for changes or deletions than doing so manually.
7. *Update regularly*: New holes are always being discovered in operating systems and applications. To ensure that you keep your system secure you should regularly browse the postings from security groups and update your system where necessary.

The most essential aspect of security is to make sure you regularly back up your system's content, and store that information off-line. If your system performs regular backups to storage devices on the network, these backups would be open to deletion or corruption if your site and network were cracked.

If you must store backups online, do so on write-once media such as CD-R disks. Keeping regular copies of your system backups (especially the system logs) on CD-R disks is also a convenient way of tracing the period over which a cracker may have gained access to the system.

Security holes

As hackers and crackers find new holes in systems, the security industry churns out a new patch. The problem is they tell everyone, including crackers who may not have known about the security hole before.

If you run a server it is essential to keep up-to-date with security news. There are many sources of free information:

- *Software vendors* - the originators of software will have areas of their web sites devoted to security issues. Do not rely on this, though; software companies are sometimes reluctant to make public news of a serious flaw in their product);
- *Security web sites* - some security sites on the Internet are run software vendors, and others by security teams. The security team sites tend to be better, because they also cover issues such as viruses and new tools developed by crackers;
- *Security Lists* - there are a number of email lists available on security, but they vary in subject and quality. You'll need to try a few to find what is most useful for you.

As a general rule, you should view newer software and operating systems as less secure than older versions. This is because the new systems have not yet had the *install time* for security experts to study their performance in detail. *Windows 2000* and the Microsoft *IIS* web server is a good example of this; after the initial triumphant launch, they were the subject of many security advisories a few months later.

Open source software, such as the software that runs under the GNU/Linux operating system, is generally considered more secure, because the technical operation of the programs has had time for careful and independent study of potential holes in security.

Closed source software, from the major software vendors, is not subject to the same type of *peer review* as open source software. It must first be picked apart to find the holes in it.

Most online resources for system security are based in the USA:

- CERT[14] is the premiere site for regular and quality reporting on security holes. It also provides many good practice guidelines on security, intrusion detection and incident reporting for server operators.
- The Forum of Incident Response and Security Teams (FIRST) sites[15] provide bulletins and country-specific information.
- US Government web sites on network and information security - the US Government has spent large sums of money on computer security over recent years (as have a number of other governments), and the results of its work are distributed widely over the Internet.
- Infrastructure protection sites are aimed primarily government and large corporate systems, but much of the information on these sites is relevant to the small server operator.

If you discover a serious vulnerability you should seek to patch it as soon as possible. Many of the vulnerabilities discovered and reported are specific to a certain operating system or software package, and so may not be applicable to you. But once a security flaw is reported, crackers who have access to such reports may try to exploit that particular weakness.

[14] CERT is part of the Software Engineering Institute at Carnegie Mellon University - http://www.cert.org/

[15] The national FIRST teams have a central site at http://www.first.org/

Further information and research

The best way to improve security is to understand the system you are working with. We list below a number of books and web sites that may help you.

Online resources:

- ❑ For a large list of links to security resources try the following sites -
  - CERT security archives - http://www.cert.org
  - 'The Security Portal' - http://securityportal.com/
  - The 'InfoWar' Information Security Site - http://www.info-sec.com/
  - For more general information on hackers, crackers and 'Info War' see the main 'Info War' web site - http://www.infowar.com/
- ❑ Mailing lists on security -
  - The CERT mailing list for advisories and bulletins - for a free subscription email majordomo@cert.org including in the body of the message the phrase *subscribe cert-advisory*
  - *The Security Portal's Weekly Newsletter* - for a free subscription go to http://securityportal.com/subscribe.html
  - *SANS Newsbites*, The SANS Weekly Security News Overview - for a free subscription email sans@sans.org with the subject *Subscribe NewsBites*
  - *Virus Myths* web site email list on virus hoaxes - for a free subscription go to http://vmyths.com/news.cfm
  - InfoWar's *Internet Crime News* List - for a free subscription email icnlist@infowar.com with *mode_digest* as the first line of the message
- ❑ Major computer, information security and hacker web sites (not included in the list above):
  - 'US Dept. of Justice Cyber Crime Division' - http://www.cybercrime.gov/
  - 'Security Focus' (general reports/security issues) - http://www.security-focus.com/
  - '@ stake research labs' - http://www.atstake.com/research/index.html
  - 'Security News Network' (hacking/defacing) - http://www.atstake.com/security_news/
  - 'Cult of the Dead Cow' - http://www.cultdeadcow.com/
  - 'Net Ninja' resources - http://netninja.com/

Books:

- Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network
  Anonymous (Mark Taber ed.), second edition 1998, Sams Publishing. ISBN 0 672 31341 3.
  RRP, $49.99/£46.95.
- Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation
  Anonymous (Randi Roger ed.), first edition 2000, Sams Publishing. ISBN 0 672 31670 6
  RRP, $39.99/£28.99.
- Hacking Exposed - Network security secrets and solutions
  Joel Scambray, Stuart McClure and George Kurtz, second edition 2001, Osborne/McGraw-Hill.
  ISBN 0 072 12748 1. RRP, $39.99/£29.99.

- Hacking Linux Exposed - Linux security secrets and solutions
  Brian Hatch, James Lee, George Kurtz, first edition 2001, Osborne/McGraw-Hill.
  ISBN 0 072 12773 2. RRP, $39.99/£29.99.
- The Complete Idiot's Guide to Protecting Yourself Online
  Preston Gralla, 1999, QUE Alpha Books. ISBN 0 789 72035 3. RRP, $16.99/£15.99.

The GreenNet Internet Rights Project

GreenNet[16] is the UK member of the Association for Progressive Communications[17] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project[18]. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series[19] that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

[16] GreenNet - http://www.gn.apc.org/
[17] APC - http://www.apc.org/
[18] CSIR Project - http://rights.apc.org/
[19] http://www.internetrights.org.uk/

Free Documentation License:

For more information about the Civil Society Internet Rights Project, or if you have questions about the briefings, contact ir@gn.apc.org.