The ABC of Computer Security

Paul Ducklin, Sophos Plc, Oxford, England

Part #tr00018t/990401

SUMMARY

This White Paper gives an introduction to computer security and its significance for businesses, followed by an alphabetical guide to common security measures and threats.

Introduction

At first, it might seem as though a computer security company would need to take extra-special security precautions and that the lessons that could be learned from it would not be generally applicable. This is rather like suggesting that it is more important for policemen to lock their front doors than it is for the rest of us to do so.

Of course, the police are more thorough about certain things: they tend to check the credentials and personal history of prospective employees more thoroughly than other organisations, for example. This does not mean, however, that the rest of us are right to be more casual about employee vetting. Being casual probably reflects the fact that we do not have to worry as much because the risks and costs of making a mistake are lower.

Where security is concerned, there are often many issues which we overlook, knowing that we can dismiss our oversight at a later stage and fall back on the explanation that the necessary precautions were deemed economically non-viable. This is bad practice: we need to ensure our rejection of any specific precaution, on the basis of cost, is firmly justified.

As information technology becomes increasingly critical to success in business, so does computer security.

Insisting upon a solid financial case for those security precautions that will be adopted is vital. It is equally important to have a solid business case for precautions which are not taken. Fortunately, many security matters can be addressed with various levels of intensity. This means that security-related spending decisions are rarely binary ("should we do this or not"), but often decisions of degree ("how much effort should we expend on this?").

As information technology becomes increasingly critical to success in business, so does computer security. At the same time, the technology required to deliver some forms of protection is becoming more complex. Encryption schemes, for example, which were considered excellent a decade ago may now be only satisfactory or even inadequate, a result of computers being sufficiently more powerful and more numerous. Similarly, encryption algorithms which today seem invincible, may appear to be of little or no use ten years from now.

Technology, however, is not the answer to all computer security matters. In fact, as computers are regarded increasingly as consumer items, and as more home users (as opposed to companies) connect to, use and rely upon the Internet, physical security becomes an increasingly important part of computer security. After all, PCs are now just as popular with household burglars as televisions and video recorders.

Similarly, computer security is an increasingly important part of physical and personal security. Today, bankcard PINs, for example, are virtually as common as telephone numbers. Personal details can be easily acquired and manipulated, thanks to the computer. The motivation for using such personal information is usually positive or morally neutral—but not always.

Computer security is an increasingly important part of physical and personal security. Personal details can be easily acquired and manipulated, thanks to the computer.

Security, whether in a computer security company or not, has many topics to be considered and acted upon. With this in mind, this article presents an A-Z of issues intended to offer food for thought for those interested in creating or enhancing security in their company. It is presented from the point of view of a computer security researcher and considers matters from a "worst case" perspective. If it seems overly worrying at times, consider this: just because you're not paranoid doesn't mean they're not out to get you!

Authentication

This tool is probably the most commonly used, and misused, in the computer security armoury. Authentication refers to the act of verifying that a specific user is allowed to access a specific network or computer. This is usually done with a password—something, it is assumed, only the legitimate user will know.

All decent password schemes rely on encryption technology which ensure that actual passwords don't have to be sent across the network, where they might be "sniffed" (see the section **LAN Analysers**).

Unfortunately, encryption is difficult to do well, so some password schemes suffer from cryptographic weaknesses, making them vulnerable to attack. Often, these weaknesses are only discovered once the password mechanism is used widely. Read relevant newsgroups or specialist security journals to keep up-to-date on known attacks against authentication schemes used on your networks.

Passwords are the only authenticator for a user. They should therefore be hard-to-guess and also be changed frequently.

Passwords are also often the only authenticator for a user. They should therefore be hard-to-guess (which makes them harder to remember and thus more likely to be written down—a bad thing). They should also be changed frequently (which makes them more likely to be kept simple, and therefore easier to guess—another bad thing).

For one way of avoiding these problems, see **Hand-Held Authenticator**.

Building Security

The physical security of your premises is an important part of computer security.

The physical security of your premises is also an important part of computer security. "Chipping", which involves breaking into a company and stealing computer chips, is a common crime today. Chips, including CPUs and memory chips, are generally easy to remove from computers, valuable, difficult to trace and straightforward to dispose of.

In the same way that highwaymen sometimes found it quicker to hack off fingers than to ask the victims to remove their rings, chippers often ruin PC cases, motherboards and peripheral components during their thieving operations. The cost of recovery is usually far greater than the value of the stolen items.

Speak to the police for advice on the physical protection of your assets. Be aware that social engineers (see **Social Engineering**) find it easy to derive information about the number, type and even location of your computers via innocent-sounding telephone calls or emails.

Cryptography

Cryptography is the technology that allows computer users to keep information secret, and is mentioned liberally throughout this glossary. The field is highly specialised, often gruesomely mathematical, and continually developing.

A good introduction to current trends in cryptography can be found in some of the specialised newsgroups on the Internet (see **Usenet**).

Digital Signatures

Digital signatures are concerned with ensuring that an object does not change, rather than with preventing others from accessing it.

Like most security technologies, digital signatures use cryptographic techniques. They are concerned with ensuring that an object does not change, rather than with preventing others from accessing it. Clearly, you want know whether anybody has tampered with a trusted document as you can only continue to trust it so long as its contents remain unaltered.

One problem with digital signatures is that their implications are often misunderstood. Some people assume that because something (an active Web page or a program for example) is signed, it is therefore of good character. This is not always true, in much the same way that people who hold passports are often, but not always, honest citizens.

Make sure that you understand what a digital signature is, and, more importantly, what it is not.

Escrow

Legally, escrow is a deed held by a third party which takes effect when a stated condition is fulfilled. In computer security, the word is used most commonly in connection with cryptographic keys. The idea is that you give your decryption key to a third party, who can then use it on your behalf should the need arise.

This is positive when "the need" is an emergency (for example, if you are severely injured or incapacitated), but worrying when "the need" is the desire of the government to take a peek at your correspondence. The numerous civil liberties debates that have arisen over key escrow have overshadowed an obvious use of the technique in the information technology arena: the escrow of source code.

Negotiated properly, source escrow allows you access to the code of bespoke applications you have commissioned if the vendor becomes unwilling or unable to support you. At the same time, it protects the vendor's intellectual property as long as the vendor continues to do business with you.

Hand-held Authenticator

Rather than rely on passwords remembered by users, some administrators are using hand-held authenticators. These are usually credit-card sized (or smaller) devices that can perform specialised cryptographic calculations that are used to enhance login security.

Typically, a user will log in, and the server will produce a so-called challenge—a sequence of digits displayed on the screen. The user will type this challenge into the authenticator, which produces a response—also a sequence of digits. These digits are used as the password. By requiring a PIN to be entered on the authenticator before it can be used, the card is rendered useless if it is lost. Similarly, if the authenticator is taken back from the user by the administrator, that user's network access is automatically and immediately terminated.

This solves the problem of password lifetime—each "password" is used once only, so network sniffers are out of luck. It also simplifies the management and revocation of passwords for users who leave. Though these are compelling arguments for using authenticators, they do increase the cost of adding a new user to the network, and necessitate a change in operating culture.

Java

Java is a programming language. It is similar to C++, but tries to disallow the use of certain styles of programming which are believed to produce coding errors. However,

Java itself is not secure. Thus, Java applications are not inherently safe simply because they are written in Java. Malicious programs, including viruses, are possible in Java just as they are possible in C, Pascal or assembler.

Java itself is not inherently secure. However the environment supports things called "applets"; applications run in a protective "sandbox" that should protect them from viruses.

However, the Java environment supports things called "applets", which are applications that run in a carefully managed environment. Theoretically, viruses and other common types of malicious software will be unable to succeed in the applet environment of the so-called Java Virtual Machine.

Be sure to understand the difference between Java itself (the language); Java applications (which are programs like EXE files); Java applets (which are programs which run in a protective cocoon, called a "sandbox"); and Javascript (which isn't Java at all, but rather a Web scripting language with a similar name).

Key Search

Encryption systems typically rely on a "key". If the encryption is any good, there will be only two ways to break it: either get the user to reveal the key, or try every possible key. The latter is called a key search.

The more possible encryption keys there are, the longer and more difficult a key search becomes.

The more possible keys there are, the longer and more difficult a key search becomes. Generally speaking, this means that the more bits in a key, the longer it will take to recover the key by brute force.

Sometimes, however, strong cryptosystems that support long keys are weakened by the way they are implemented. Some American cryptosystems discard some of the key, shortening it artificially in order to satisfy USA arms regulations that control the export of cryptographic "munitions". Others reduce the key space inadvertently by allowing only certain characters to be used, or by silently converting lower case characters in the key into upper case, or something similar. Weakening the interface can make a strong encryption system weak.

LAN Analysers

On some LANs, every data packet travelling on the network is up for grabs. Although packets are usually marked with a particular sender and a particular recipient, the packet might not be invisible to other computers on the network.

A LAN Analyser is a computer which "sniffs" packets off the network so they can be analysed at a later stage. Such a tool can be used for good (e.g. for troubleshooting), but also for evil (e.g. for recovering passwords or data from a network session).

Encryption is an obvious way to render recovered data useless to "sniffers"—see **Cryptography**.

Misuse of Computers

In the UK, misusing a computer is a criminal offence.

In the UK, misusing a computer is a criminal offence. There are two major sorts of offence under the Computer Misuse Act:

- Unauthorised access
- Unauthorised modification.

This means that hackers are now punishable, even if they merely "look around".

There are some people keen to deploy the Computer Misuse Act to bring hackers to book. Write the following address in your diary:

The Computer Crime Unit
New Scotland Yard
2 Richbell Place
WC1N 3LA
England

Tel: 0171 2301177

Fax: 0171 2301275

See also **Authentication**, **LAN Analysers** and **Viruses**.

Network Managers

Typically, network managers have considerable power—they can usually add new users, alter security profiles, view and edit auditing information, and even read from and write to all files on the network.

Generally speaking, lodging this sort of power with one individual or group of individuals is not a good idea— administrators who are able to manipulate their own audit trails are effectively operating unaudited.

Unfortunately, some network operating systems do not allow the clean separation of administrative and audit functions (NetWare 3.x and most versions of Unix, for instance, have the notion of a "superuser" or "supervisor", who always has almighty power over the system).

On the other hand, some operating systems allow administrators to restrict themselves so drastically that they are no longer able to access the network at all. Actually, this can be a good sign as the job (and powers) of administration can be carefully and safely subdivided.

Overflow Attacks

Overflow attacks involve connecting to a permitted service on a remote computer and then sending more data than that computer expects to receive, causing it to crash or malfunction.

Overflow attacks involve connecting to a permitted service on a remote computer—sometimes the very service by which authentication is carried out—and then sending more data than the remote computer expects to receive. In theory, the programmer should have guarded against such an event by detecting and discarding erroneous input. In practice, programmers sometimes forget such checks, or code them incorrectly.

This may allow an attacker to provoke the remote computer to misbehave—often simply to crash, but sometimes to go wrong in a malevolently coordinated way.

The continued existence of overflow attack bugs in server operating systems shows how vulnerable system administrators are to apparently minor oversights by programmers.

Read relevant newsgroups or specialist security journals to keep up to date on known weaknesses in services used on your networks.

Quality Assurance

Quality Assurance (QA), or the lack of it, affects administrators every time they install new software. The stability of a system after a new program is installed is generally directly proportional to the quality of that program.

QA methods are used before, during and after the creation of a new program with the aim of ensuring that it will behave correctly when used.

Since formally *proving* the quality and correctness of software is mind-numbingly complex, time-consuming and expensive, it is impractical for anything but the most specialised (usually military) applications. In the real world, QA methods are used before, during and after the creation of a new program with the aim of ensuring that it will behave correctly when used.

No real-world software will be perfect. But the obvious flaws in some popular programs suggest that their QA could have been rather better. Unfortunately, some vendors cannot vouch at all for the quality of the software they sell because they may have bought, or be licensing, a substantial part (or possibly even 100%) of their technology from another company.

One of the benefits of smaller, independent producers of specialist software is that a competent manufacturer in this sector will be able to provide hard evidence of a comprehensive, scientific and repeatable QA regimen.

For security software, quality is especially important. For real certainty, ask for a guided tour of the security company (though bear in mind that key areas are likely to be off limits).

Remailers

When you send an email across the Internet, information about its starting point, its destination and some details of the route that it has taken will be available in the message headers as it travels. This makes the true source of many emails traceable. To the sender, this may or may not be desirable.

Some remailer services will obfuscate or completely disguise the true source of an email. But email anonymity is often illusory so keep your threatening or actionable emails.

Some remailer services will obfuscate or completely disguise the true source of an email. Basically, they work by accepting a message of the form "from X to Remailer, but really to Y", and then remailing it in the form "from Remailer to Y". This gets the message from X to Y, but in such a way that Y cannot trace its route back to X.

In the example above, Y receives the message but cannot reply to X, because any reply will be delivered to the remailer, not to the original sender. Obfuscated mails, which can be replied to but in which the recipient of the reply is non-obvious, are nevertheless possible.

To allow anonymous replies, the remailer might accept a message of the form "from X to Remailer but really to Y", and relay this message as "from Remailer-Z to Y". The remailer will then remember the rule "replies to Z are actually for X". Any reply directed at Remailer-Z is then rerouted to X. Even if X and Y do not know each other's identity, the remailer knows how to connect them together.

What this means is that mails received via the Internet may not be exactly what they seem. If they are offensive, they may not be directly traceable, and threats returned to the apparent sender may be out of place, or out of order.

On the other hand, email anonymity is often illusory (the remailer, at least, knows who the true sender was), so you may as well preserve threatening or actionable emails received by your organisation, in case their headers do contain useful information. The Computer Crime Unit would certainly like you to keep anything which might be used in evidence (see also **Misuse of Computers**).

Social Engineering

Often, the most effective attack against a technology-centric company is cultural. Instead of spending dozens of CPU-years trying to crack a password by brute force (see **Key Search)**, simply persuade someone who knows the password to tell it to you.

By masquerading as someone who has the right to know, social engineers are able to con their victims into revealing information.

This is social engineering, and is most easily carried out by telephone. By masquerading as someone who has the right to know, social engineers are able to con their victims into revealing information.

Pretending to be a support specialist assigned to fix a problem with the network is a common guise (many users are only too keen to "help" someone who claims to be trying to help them). Posing as an employee of a telemarketing company is another (users are often happy to reveal details about their company and their network if they believe that their answers are simply being marked down in some kind of anonymous survey matrix).

One problem with social engineering attacks is that it is often easy for attackers to obtain, or to guess, complete lists of internal telephone extensions. This means that they do not have to succeed at once: they can call user after user until they encounter someone who will believe their patter.

To counter this, your users need someone to whom they can report suspicious phone calls or emails. Without central reporting, patterns of attack are unlikely to emerge.

Trawling

As the name suggests, network trawling (or 'trolling') involves a broad, often mindless, search for information on a network, usually the Internet. Hackers with time on their hands may spend hours drifting through the oceans of material on the Internet, saving anything that takes their fancy. Alternatively, they might program scripts to perform an automated trawl. Libraries of viruses, malicious programs and hacking tips can be built up in this way with relatively little effort.

In a directed attack, a hacker who has entered your network might try to trawl through as much of it as possible, retrieving everything of even minor interest. By catching a very large number of fish, the hacker hopes also to catch a small number of especially tasty fish without needing to identify the location of the better fish first. Anything useless can easily be discarded later.

If you routinely monitor usage patterns on your network, you should be in a good position to notice systematic attempts to violate security and trawl your servers.

Usenet

Usenet is a worldwide-distributed set of newsgroups available via the Internet. Used sensibly it can help you keep abreast of security issues.

Usenet is a worldwide-distributed set of newsgroups available via the Internet. Users post questions, discussions, and ideas to newsgroups which interest them and others with similar interests reply.

Some Usenet groups are of a dangerous, dubious or even illegal nature. Pornography, viruses and hacking tips are commonly exchanged via Usenet, for example.

Used sensibly, though, Usenet discussion groups can be an excellent forum for staying abreast of security-related risks and fixes. To save bandwidth, you should ask your news server to retrieve only those groups that are of interest to users inside the company.

Viruses

These days, almost everybody has had, or knows someone who has had, a computer virus. These self-replicating programs are generally much more dangerous than a stand-alone malicious program—they tend to spread super-linearly rather than linearly, and are therefore more likely to become widespread, and to be passed on to someone outside the company.

The threat is also a rapidly changing one. Currently, between 300 and 600 new viruses appear each month, which corresponds to 10 or 20 new viruses per day. Viruses now exist which infect diskettes, program files, Word documents, Excel spreadsheets, Java applications, Access databases, batch scripts, and more.

Clearly, up-to-date anti-virus software is the answer, so that you can prevent viruses (rather than simply detecting them after they infect computers inside the company).

SOPHOS

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • UK • Tel 01235 559933 • Fax 01235 559935
Sophos Pty Ltd • Level 4 • 725 George Street • Sydney • NSW 2000 • Australia • Tel 02 9212 1600 • 02 92121788
Sophos Plc • 2 Place de la Défense • BP 240 • 92053 Paris la Défense • France • Tel 01 46 92 24 42 • Fax 01 46 92 24 00
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251

www.sophos.com