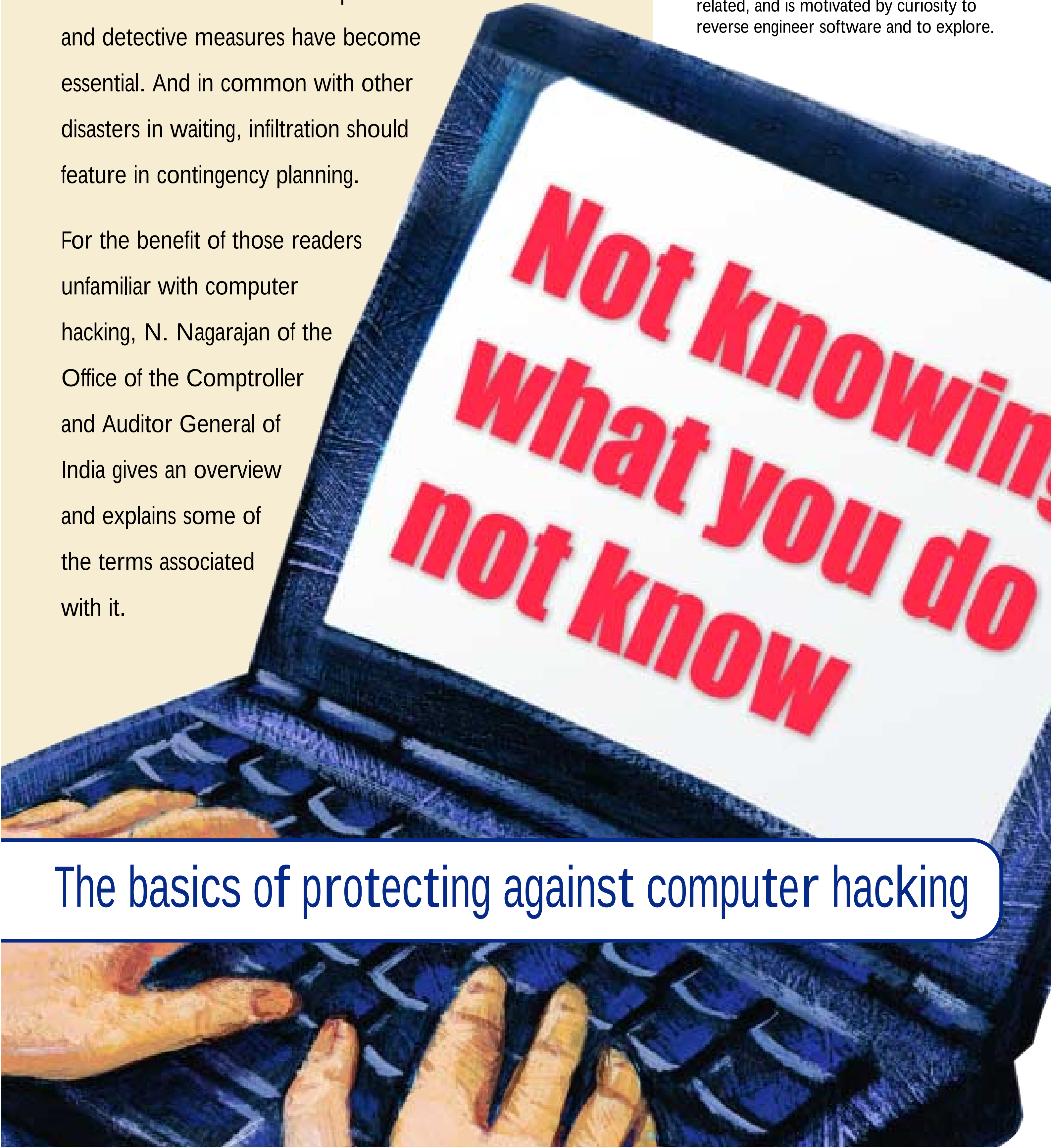
You can manage what you know about; it's what you don't know about that creeps up and stabs you. For the IT manager, computer hacking is one such sword of Damocles for which sensible preventive and detective measures have become essential. And in common with other disasters in waiting, infiltration should feature in contingency planning.

For the benefit of those readers unfamiliar with computer hacking, N. Nagarajan of the Office of the Comptroller and Auditor General of India gives an overview and explains some of the terms associated with it.

The hacker

Technically, a *"hacker"* is someone who is enthusiastic about computer programming and all things computer related, and is motivated by curiosity to reverse engineer software and to explore.



The basics of protecting against computer hacking

The term *"cracker"*, on the other hand, describes those who apply hacking skills to gain *unauthorised* access to a computer facility, often with sinister motives. But *"cracking"* never really caught on, perhaps due to the grey area that exists between the two activities and to the media's widespread use of *"hacking"* as a term synonymous with computer crime. I will not therefore try to buck the trend in this article.

Computer hacking

Hacking is in some ways the online equivalent to burglary; in other words *breaking into* premises against the wishes of the lawful owner - in some jurisdictions a crime in itself - from which other criminal acts such as theft and/or damage generally result.

Computer hacking refers to gaining *unauthorised* access to, and hence some measure of control over, a computer facility, and most countries now have specific legislation in place to deter those who might wish to practice this art and science. In some jurisdictions, unauthorised access alone constitutes a criminal offence, even if the hacker attempts nothing further. However, in practice, hackers generally have a particular target in mind, so their unauthorised access leads to further acts, which national law might also define as criminal activities. These can be summarised under the headings of unauthorised:

- **obtaining of confidential information:** perhaps the major growth area in computer crime is "identity theft", in other words the obtaining of personal information that can then be used to commit other serious offences, usually in the area of fraud. However, other motives include espionage (both governmental and commercial secrets) and the obtaining of personally sensitive information that might be used for tracing people, deception and blackmail;
- **alteration or deletion of data and code:** most organisations now depend to some extent on computerised information systems, and any act resulting in significant corruption or deletion of corporate data could have serious implications on their ability to transact business;
- **degradation or cessation of service:** acts that result in systems being unable to carry their workload or that fail altogether, could also have serious business implications;
- **use of computer resources:** this impact is really inherent in the previous three, but it's worth mentioning separately because an emerging problem is the use by hackers of other people's systems (extending to home PCs) to store illegally obtained data or to mount attacks on other systems. There are documented cases of systems hacked in this way - sometimes referred to as "zombies" because they are no longer in the full control of their unsuspecting owners - being used to store child pornography and material that breaches copyright law (e.g. copyrighted music files), to mount distributed denial of service attacks on other systems, and to distribute spam e-mail.

Finally, it's worth emphasising that the term "hacker" applies both to outsiders and to otherwise authorised personnel who misuse their system privileges, or who impersonate higher privileged users. This sad fact needs to be recognised when formulating corporate security policy.

The Ten Immutable Laws of Security

1 If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.

2 If a bad guy can alter the operating system on your computer, it's not your computer anymore.

3 If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

4 If you allow a bad guy to upload programs to your web site, it's not your web site any more.

5 Weak passwords trump strong security.

6 A machine is only as secure as the administrator is trustworthy.

7 Encrypted data is only as secure as the decryption key.

8 An out of date virus scanner is only marginally better than no virus scanner at all.

9 Absolute anonymity isn't practical, in real life or on the web.

10 Technology is not a panacea.

Source - www.microsoft.com/technet

Just another security update for Microsoft Internet Explorer

Are You on a Network?

If your computer is part of a managed network, contact your organization's system administrator before making changes to your computer.

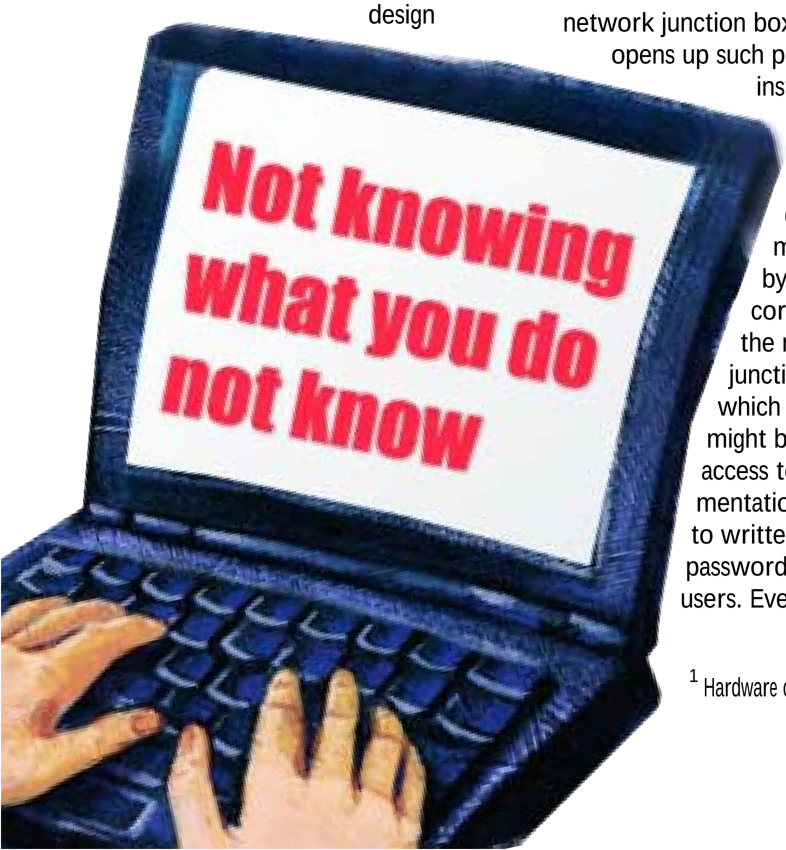
Why We Are Issuing This Update

A number of security issues have been identified in Microsoft® Internet Explorer that could allow an attacker to compromise a Microsoft Windows®-based system and then take a variety of actions. For example, an attacker could run programs on a computer used to view the attacker's Web site. This vulnerability affects computers that have Internet Explorer installed. (You do not have to be using Internet Explorer as your Web browser to be affected by this issue.) You can help protect your computer by installing this update from Microsoft.

Source - Microsoft Security Bulletin MS03-032

Approaches to hacking

There are several basic strategies for hacking a computer facility: physical intrusion; password attacks; network access; web server attacks; and e-mail attacks, but there are a multitude of tactics that can be used to implement them. For example, security flaws (or design weaknesses) in infrastructure software and communications protocols offer seemingly endless tactical possibilities, as is evidenced in the never-ending stream of security updates (see example).



Physical intrusion: an attacker's work is made easier by gaining physical access to a machine's keyboard or to network junction boxes. Physical access opens up such possibilities as installing a keystroke logger[1]; installing unauthorised hardware devices (e.g. linking a modem that bypasses the corporate firewalls to the network); tapping junction boxes through which network traffic might be analysed; gaining access to system documentation, printouts and to written notes of their passwords left by reckless users. Even access to confidential waste can prove fruitful. Perhaps the quickest and easiest way to gain physical access to an organisation's computer facilities is to join the contract cleaning force, which often works unsupervised and outside normal office hours.

Password attacks: obtain a valid password to the system and you become just another legitimate user. This is particularly dangerous where the hacked account has special privileges assigned to it that permit wide-ranging system access and use. A successful password attack is both difficult to detect and difficult to prevent because password security depends largely on the user. Keystroke loggers and social engineering (see terminology below) are methods of capturing passwords, while people often share their personal passwords with others, write them on notes that they attach to their terminals, and fail to change them periodically. Password cracking programs perform an elaborate process of guessing 'weak' passwords by trial and error, using combinations of words from different languages, names (places, people, characters in books), jargon, slang, and acronyms. These are tried backwards, in two-word combinations, in combinations with numbers substituted for letters, etc. Vendors often ship infrastructure software with the administrator account passwords set to default values; because these are widely known in the hacking community, they provide an easy route into a computer facility if left unchanged.

Network Access and Web Server Attacks: computers forming part of a local area network that is in turn

[1] Hardware or software than captures the user's keystrokes, including their passwords.

connected to the Internet are exposed to a range of potential logical access risks. A network's primary purpose is to permit users to access resources and exchange information, but hackers can also use the network for the same purpose. There are different ways to achieve unauthorised access under this heading, many being technically sophisticated. One set of approaches exploits features of networking software that make it accessible from outside the network. Another set exploits browsers; for example, browsers maintain or have access to information about the user and computer that a hacker can exploit. A hacker could also cause a browser to launch an "applet" (a program that runs in conjunction with the browser) to hack the computer or network, or to send back information that is not normally accessible from outside. Once access is gained, "island hopping" through the network is sometimes possible by exploiting trusted relationships between interconnected computers - *the fact is that a network of computers that trust each other is only as secure as its weakest link*.

The basic solutions to this family of security risks are to keep abreast of vendor security updates - such as the Microsoft example illustrated - and to maintain an effective "firewall"[2].

Email Attacks: e-mail is a major route into networked computers. Typically, a Trojan horse program is buried within an innocuous-looking attachment to an e-mail message (see the *Autorooter* example). The Trojan is launched when the attachment is opened (or sometimes viewed) and covertly passes control of the computer to the hacker.

Managing common vulnerabilities

A compromised system can be a self-inflicted injury due simply to the basic precautions having being ignored:

- ensure that your computer has good physical security, consistent with both its value in terms of replacement cost and the consequences that could stem from its data being disclosed or destroyed. Secure sensitive areas; manage access keys; consider installing intruder alarms. Ensure communications junction boxes are secured and inspect them periodically for signs of tampering - network administration packages can detect unauthorised physical devices connected to the network. Provide a secure waste disposal service for computer printouts and removable media;
- formulate a sensible password policy for authenticating users and *enforce it*. Consider the need to strengthen password authentication with tokens or biometrics. Disable unnecessary services and accounts promptly;
- systems administrators occupy positions of extreme trust; it follows that they should themselves be trustworthy. Be very careful who you permit to have system administrator-level access to your network particularly when hiring new staff or appointing people to cover for absences. Consider implementing a policy of "least privilege"[3] and review periodically the privileges that have been allocated, to whom and for what purpose;
- infrastructure software - in particular the operating system and firewalls - generates logs that record who is using (or attempting to use) the system, for what purpose and when. This information can prove vital in detecting unauthorised activity - for example, attempted access to particularly sensitive accounts or files - and system use at unusual times. Logs should be reviewed frequently - it may be necessary to develop or purchase a log monitoring and analysis package to enable key system messages to be detected quickly. An unplanned increase in

Autorooter

...a Trojan horse, potentially spread by e-mail, which exploits a Windows vulnerability to allow a hacker to gain control of infected computers.

This DCOM-RPC exploit only affects Windows XP/2000 Pro/NT computers, which can use Remote Procedure Call. As the Trojan is incapable of spreading by itself, the file reaches computers through infected e-mail messages, inside files downloaded from the Internet or even on floppy disks.

When run, Autorooter creates files, including RPC.EXE, which exploit the operating system vulnerability by opening communication port 57005 and logging on with the same privileges as the computer's user. It also downloads a file called LOLX.EXE, which opens a backdoor in the computer. After that, the infected computer is at the mercy of the hacker who can gain remote control through the port created.

Because it doesn't show any messages or warnings that may indicate that it has reached the computer, Autorooter is difficult to recognise.

[2] A combination of hardware and software that limits external access to networked computers and resource.

[3] The least level of privilege consistent with performing a particular role.

disc storage, slower than expected network performance and suspicious-looking outbound connections can be other indicators that you have a cuckoo in the nest;

- make sure that your system files (including the Registry) are well protected from unauthorised change. Apply the principle of least privilege to limit what users are able to do. Implement a change control procedure to ensure at least two people are involved in important system changes and that all changes are recorded. Periodically audit your system software for unauthorised executables;
- never run or download software from an untrusted source (the source from which it was obtained might not be the same as the developer). If you run a web site, you should control closely what visitors can do; in particular, you should only permit programs on the site that you obtained from a trusted developer;
- typically, a new virus or Trojan does the greatest amount of damage early in its life when few people are able to detect it. Thus, an out of date virus scanner is only marginally better than no virus scanner. New viruses and Trojans are created virtually every day, so it's vital to keep your scanner's signature file up to date - virtually every vendor provides a means to obtain free updated signature files from their web site.

When you're satisfied that the basics are both in place and operating, why not consider hiring a reputable firm of security specialists to undertake a "penetration testing" programme to assess the extent to which your scheme of control rests on solid foundations rather than on sand?

It's vital to appreciate that:

- security consists of both technology and policy; that is, it's the combination of the technology and how you use it that ultimately determines how secure your systems are;
- security is journey, not a destination. It's not a problem that can be "solved" once and for all, but a continual series of moves and countermoves between the good guys and the bad guys;
- the key is to ensure that you have good security awareness, appropriate security policies (*that you enforce*), and that you exercise sound judgment.

Planning for hacking incidents

So, you discover that your system has been hacked. What next? Well, first it's necessary to backtrack and consider planning for this possibility. Sit down with colleagues and write down a strategy to guide your response, exactly as you would for any other aspect of contingency planning. Who will form your incident response team? What are your goals going to be and in what order of priority? In most cases they are likely to be first, to prevent further intrusion, then to identify the vulnerabilities that led to the attack, assess the damage and consider what remedial action needs to be taken (e.g. what would you do were you to suspect identity theft?). Will you assign resources to identifying the intruder? Will you involve the police?

One of the first points to consider is whether to disconnect from your external networks to limit damage and prevent further infiltration to other trusted networks. Assuming the attack is external, remaining connected may leave the hacker able to observe and negate the response team's actions. Organisations that have reliable (i.e. successfully tested) disaster recovery arrangements in place may find it comparatively easy to transfer their key operations to a disaster recovery site while they thoroughly investigate and sanitise their home site.

You should consider the extent to which you back up your firewall and other significant logs. Assuming the vulnerability that gave rise to the attack is not apparent, you may need to look back, perhaps weeks, to identify when and how the intrusion occurred (another plus in favour of frequent log reviews). Furthermore, should events finish up in the hands of the police, the police are likely to need the evidence contained in your logs to support a prosecution.

You will also need to consider who to inform when you discover the problem. This will involve striking a balance between those who need to be involved in the investigation, top management - but only when you have concrete proposals to make to them - and everyone else, at least until the evidence has been preserved.

Investigation needs to be thorough; focusing on a single vulnerability before restoring service might overlook the existence of backdoors that the hacker has inserted to enable easy re-entry later. A thorough investigation will involve advanced networking techniques, adeptness with software tools, system administration, data/system recovery, technical skills that might not be at your immediate disposal. Thus, it might be prudent in

The hackers' hit parade

Security firm Qualys produces a real-time index of the vulnerabilities that are the current favourites of the Internet's computer hacking community. You can obtain details of each vulnerability by clicking on each entry in the 'ID' column of the vulnerability table.

http://www.qualys.com/services/threats/current.html.

Responding to intrusions

- understand the extent and source of an intrusion;
- protect sensitive data contained on systems;
- protect the systems, the networks and their ability to continue operating as intended;
- recover systems;
- collect information to better understand what happened. Without such information, you may inadvertently take actions that can further damage your systems;
- support legal investigations.

Source: www.cert.org

your planning to identify reputable security specialists well versed in penetration testing that might be called upon to assist with sanitising and rebuilding your systems.

In addition to identifying the system vulnerabilities exploited by the hacker, a critical review and reconciliation of activated accounts (particularly those of guests, supposedly disabled accounts and those whose presence can't be explained) and their associated system privileges, while tedious, could reveal other unused entry points the hacker has set up against a rainy day; likewise, you should confirm the status of all interconnected 'trusted' systems.

Scan the system for Trojans. These are typically identified by antivirus packages, but their scan engines have varying degrees of success, particularly if not up-to-date, so scan using (up-to-date versions of) several packages.

Note: there is more information on incident response at...

http://www.cert.org/security-improvement/modules/m06.html

Conclusion

In the context of computer hacking, *knowing what you do not know* is manageable, hence the importance of good preventive and detective measures, such as log review and intrusion detection systems. The less fortunate are those who remain in self-inflicted ignorance - maybe for weeks or months - that their system has been infiltrated and their business is being damaged.

Regardless of the strength of your preventive and detective measures, *be prepared for hacking incidents*, particularly if your organisation relies heavily on networks (the Internet, WANs and LANs) for its operations and customer services. Should you fall victim, a thorough investigation of a compromised system - while disruptive, time-consuming, expensive, and tedious - is essential. The temptation is to give in to pressure to resume operations quickly by closing the obvious vulnerabilities and trusting to luck that the system is clean. That could easily be a false economy.

Some terminology

Buffer overflows - are due partly to a characteristic of some programming languages, such as C, which poor programming practices then exacerbate. An overflow occurs when a program attempts to store more data in temporary storage area, or "buffer", than it can hold. Since buffers are of finite size, the extra information overflows into adjacent buffers thereby corrupting or overwriting the valid data held in them. This would normally cause a program failure or even a system crash, but a skilfully crafted overflow can also be exploited as a form of security attack. The attacker can gain control by creating an overflow containing code designed to send new instructions to the attacked computer, hence the relevance of buffer overflows to hacking.

Firewall - the online equivalent of the 'man on the door' who, when a visitor arrives in the foyer, asks for proof of identity, checks the appointments book, contacts the host, issues a temporary pass and perhaps inspects the visitor's baggage before permitting - or denying - entry.

A network firewall sits at the junction point or gateway between two networks - usually a private network and a public network such as the Internet - its purpose being to reduce the risk to networked computers of intrusion. It may be a hardware device or software running on a secure host computer. In either case, a firewall has at least two network interfaces, one for the network it is protecting and one for the untrusted network to which it is exposed. Because firewalls cannot decide for themselves whether traffic is hostile or benign, they must be programmed with rules (a "security policy") that govern the types of traffic to allow or deny.

In addition to guarding external connections, firewalls are also sometimes used internally to provide additional security by segregating sub-network that give access to highly sensitive applications.

Honey Pots - decoy servers or systems designed to gather information about attackers. A honey pot, which is set up to be easier prey for attackers than genuine production systems, incorporates modifications that enable intruders' activities to be logged and traced. The theory is that when an intruder breaks into a system, they will return. During subsequent visits, additional information can be gathered and additional attempts at file, security, and system access on the Honey Pot can be monitored and saved. Most firewalls can be configured to alert system administrators when they detect traffic entering or leaving a honey pot.

Identity theft - involves taking over an individual's identity by stealing critical private information, such as the Social Security number, driver's license

Example of a buffer overflow vulnerability

The Phone Book Service that runs on Internet Information Services (IIS) 5.0 has an unchecked buffer (a temporary data storage area that has a limited capacity but no specification for the amount of information that can be written into it) in the code that processes requests for phone book updates. A specifically malformed HTTP request from a malicious user can cause a buffer overflow in the Phone Book Service, which might allow the malicious user to run unauthorized code on the server, or cause the service to fail.

Source: extract from a Microsoft security update.

number, address, credit card number, or bank account number. The identity thief can then use the stolen information to obtain loans or credit lines to buy goods and services under the stolen name. Identity thieves typically change the consumer's mailing address to hide their activities.

Intrusion detection - the art and science of detecting when a computer or network is being used inappropriately or without authority. An ID system monitors system and network resources and activities and, using information gathered from these sources, alerts system administrators on identifying possible intrusion.

Firewalls (see above) work only at a network's point of entry with packets as they enter and leave the network. An attacker that has breached the firewall can roam at will through a network - this is where an ID system becomes important.

Intrusion Prevention - systems monitor for suspicious activity with the aim of proactively blocking potential attacks. Typically, an IP system comprises a software agent that resides near to the host's operating system kernel, which monitors system calls before they reach the kernel using a rules engine to identify potentially suspicious activity. This can then be halted, or the systems administrator alerted. A drawback is that IP systems can respond to legitimate activities and generate false alarms. Defining exceptions can reduce such false alarms, but there are pros and cons to this.

Keystroke logger (or keylogger) - is a program that runs in the background recording all keystrokes. Once logged, the keystrokes are returned to the hacker who peruses them carefully to identify passwords and other useful information that could be used to compromise the system, or be used in a social engineering attack. For example, a keylogger will reveal the contents of all e-mail composed by the user. Keylogger programs are commonly included in rootkits and remote administration Trojans. A keystroke logger can also take the form of a hardware device, independent of the operating system, which plugs in between the keyboard and the main system (for PCs). They simply record what is typed at the keyboard; the hacker can later retrieve the device and examine its contents.

Phishing - occurs when a consumer receives a deceptively legitimate looking e-mail from what appears to be a reputable company (see Spoofing). The e-mail might ask a recipient to, for example, update their credit card information, and/or provide other personal details to avoid their account being terminated. Another approach is for the sender of the message to offer a service, for example to protect their credit cards from possible fraud. Those stung by phishing are victims of "identity theft" (see above).

Attempted identity theft

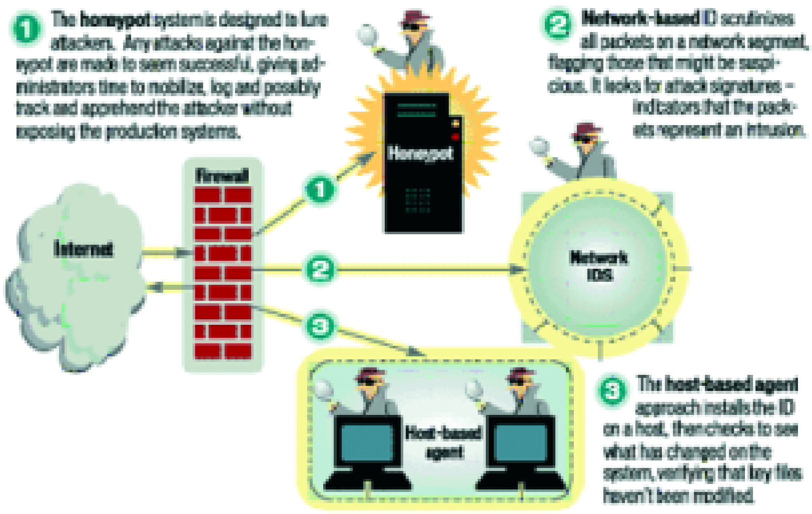
National Australia Bank customers became targets for an e-mail fraud in which they were sent (grammatically incorrect) requests, purportedly from the bank, requesting them to connect to the NAB web site.

"Dear valued customer," it read, *"Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety."* The e-mail encouraged recipients to click a link in the body of the message, which then connected them to a site that mimicked the NAB Web site but that had been set up to capture their login and password details.

The scam used a message previously used to targeted other banks' customers.

Intrusion-Detection Systems

ID stands for intrusion detection, which is the art of detecting inappropriate, incorrect or anomalous activity. ID systems that operate on a host to detect malicious activity are called host-based ID systems. ID systems that operate on network data flows are called network-based ID systems. These two systems can be used in conjunction with each other.



1 The **honeypot** system is designed to lure attackers. Any attacks against the honeypot are made to seem successful, giving administrators time to mobilize, log and possibly track and apprehend the attacker without exposing the production systems.

2 **Network-based** ID scrutinizes all packets on a network segment, flagging those that might be suspicious. It looks for attack signatures – indicators that the packets represent an intrusion.

3 The **host-based agent** approach installs the ID on a host, then checks to see what has changed on the system, verifying that key files haven't been modified.

Rootkit - a collection of tools and utilities that a hacker can use to hide their presence and gather data to help them further infiltrate a network. Typically, a rootkit includes tools to log keystrokes (see keylogger above), create secret backdoor entrances to the system, monitor packets on the network to gain information, and alter system log files and administrative tools to prevent detection.

Social engineering - in his book, *The Art of Deception: Controlling the Human Element of Security*[4], arch hacker Kevin Mitnick poses the question: why bother attacking technology when the weakest link lies not in the computer hardware or software, but in humans who can be tricked into giving up their passwords and other secrets? Mitnick goes on to state that social engineering *"uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. The social engineer is able to take advantage of people to obtain information with or without the use of technology."*

Spoofing - in essence a technique that depends on forging the identity of someone or something else ("masquerading"), the aim being to alter the trust relationship between the parties to a transaction.

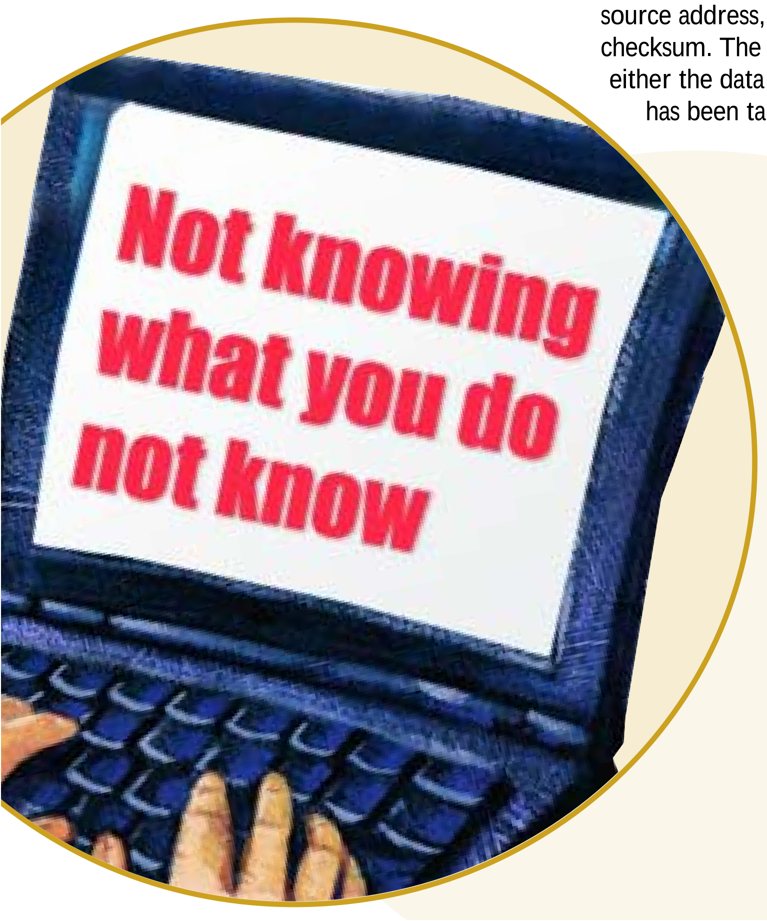
In the online world, there are different flavours of spoofing. A hacker might employ sophisticated e-mail spoofing to make it appear that an e-mail requiring the victim to confirm their account details, including such information as their logon ID and password, has been sent by a reputable person or organisation (see "phishing" and "social engineering" above).

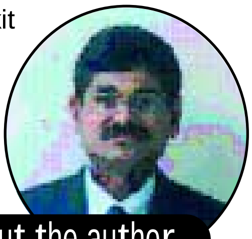
IP spoofing is another common form of online camouflage, in which a hacker attempts to gain unauthorised access to a computer or network by making it appear that a packet has come from a trusted machine by spoofing its unique Internet IP address. A countermeasure is to use of a Virtual Private Network (VPN) protocol, a method that involves encrypting the data in each packet as well as the source address using encryption keys that a potential attacker doesn't have. The VPN software or firmware decrypts the packet and source address, and performs a checksum. The packet is discarded if either the data or the source address has been tampered with.

Trojan horse - a name derived from the classic Trojan horse in Homer's Iliad. After spending many months unsuccessfully besieging the fortified city of Troy, the Greeks evolved a strategy. They departed leaving behind them as a gift a large wooden horse, which the citizens of Troy brought into town. Unknown to them the horse contained Greek warriors, who at night jumped out and opened the city gates letting in the Greek army who had been in hiding.

In the IT environment - and setting aside the legitimate use of network administration tools - Trojans are generally considered a class of "malware" that, like their predecessor, contain covert functionality. They act as a means of entering a target computer undetected and then allowing a remote hacker unrestricted access and control. They generally incorporate a rootkit (see above).

[4] Wiley, ISBN 0-471-23712-4





About the author

N. Nagarajan CISA joined the Office of the Comptroller and Auditor General of India in 1989, and is presently employed as Senior Deputy Accountant General in Mumbai. In addition to his wide experience in auditing IT (particularly in the field of Electronic Data Interchange) and in training staff in IT audit skills, Nararajan has also worked as a developer of pensions systems.

Nagarajan's international work includes audit assignments at the United Nations in New York, and a two year secondment to the Office of the Auditor General of Mauritius where he was involved in training staff and in the audit of EDI systems operated by the Customs department. Nagarajan has been published in a number of international journals.