

Computer Solutions

(Bill Ridgeway)

Telephone: 020 8422 7570

7 Sandringham Crescent, HARROW, HA2 9BW

Email: info@1001solutions.co.uk

Website: 1001solutions.co.uk

Threat prevention

Overview

Threat prevention may, for convenience, be considered as two related subjects; physical threat prevention (access control) and electronic threat prevention (software and hardware).

Accessing information on a computer may be likened to a hurdles race where each hurdle represents a layer of security. At each 'hurdle' the computer user needs to remember and type in user names and passwords. However, anyone determined enough can, through various means, plough through each hurdle to reach the finish line (access information). Threat prevention is, therefore, inherently flawed and should be regarded as a deterrent not as a complete solution.

There is a chance a thief will see the computer as a means of making money and will be thinking only of selling it on. However, a clever thief (or the clever purchaser) may realise there may be more value in using the data on the computer either as a means of identify theft or for blackmail. This latter possibility may be more likely if the computer came from the likes of an accountant or solicitor.

Two 'rules of thumb' need to be considered –

the inconvenience of security measures varies in direct proportion to the amount of security (more door locks and window locks increase inconvenience in locking and unlocking and decreases the chance of a successful burglary); and

the consequence of security measures varies in indirect proportion to the amount of security (more door locks and window locks decreases the consequences of a successful burglary).

Threat prevention (electronic)

Electronic threats to computers may be classified as follows –

Adware

Programs that facilitate delivery of advertising content to the user through their own window, or by utilizing another program's interface. In some cases, these programs may gather information from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other location in cyber-space.

Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger adware by accepting an End User License Agreement from a software program linked to the adware or from visiting a website that downloads the adware with or without an End User License Agreement.

Dialers

Programs that use a computer or modem to dial out to a 00xx (international) or 09xx (premium rate) number or FTP site, typically to accrue charges. Diallers can be installed with or without a user's explicit knowledge, and may perform their dialling activity without a user's specific consent prior to dialling.

Hack Tools

Tools that can be used by a hacker or unauthorized user to attack, gain unwelcome access to or perform identification or fingerprinting of your computer. While some hack tools may also be valid for legitimate purposes, their ability to facilitate unwanted access makes them a threat. Hack tools also generally: -

Attempt to gain information on or access hosts surreptitiously, utilizing methods that circumvent or bypass obvious security mechanisms inherent to the system it is installed on, and/or

Facilitate an attempt at disabling a target computer, preventing its normal use.

One example of a hack tool is a keystroke logger -- a program that tracks and records individual keystrokes and can send this information back to the hacker. Also applies to programs that facilitate attacks on third-party computers as part of a direct or distributed denial-of-service attempt.

Joke Programs

Programs that alter or interrupt the normal behaviour of a computer, creating a general distraction or nuisance. Joke programs generally do not themselves engage in the practice of gathering or distributing information from the user's computer.

Remote Access

Programs that allow one computer to access another computer (or facilitate such access) without explicit authorization when an access attempt is made. Once access is gained, usually over the Internet or by direct dial access, the remote access program can attack or alter the other computer. It may also have the ability to gather personal information, or infect or delete files. They may also create the risk that third party programs can exploit its presence to obtain access. Such remote access programs generally: -

Attempt to remain unnoticed, either by actively hiding or simply not making their presence on a system known to the user, and/or

Attempt to hide any evidence of their being accessed remotely over a network or Internet.

Means by which these programs provide access may include notifying a remote host of the machine by sending its address or location, or employing functionality that wholly or partially automates access to the computer on which the program is installed.

Security Risks

Threats that do not meet the definitions of Viruses, Trojan horses, Worms, or other expanded threat categories, but which may present a threat to a computer and its data, an unwanted nuisance to the user, or exhibit other unexpected or unwanted results when the threat is present and functioning. This category includes programs that encrypt or otherwise attempt to obfuscate some of their functionality, making it difficult to determine whether they fall into one of the other categories.

Spyware

Programs that have the ability to scan systems or monitor activity and relay information to other computers or locations in cyber-space. Among the information that may be actively or passively gathered and disseminated by Spyware: passwords, log-in details, account numbers, personal information, individual files or other personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage or other computing habits.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger spyware by accepting an End User License Agreement from a software program linked to the spyware or from visiting a website that downloads the spyware with or without an End User License Agreement.

Viruses, Worms and Trojan Horses

A virus is a program or code that replicates itself onto other files with which it comes in contact; that is, a virus can infect another program, boot sector, partition sector, or a document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though many can do damage to a computer or a user's data as well.

A worm is a program that makes and facilitates the distribution of copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive via exploitation of a system vulnerability or by clicking on an infected e-mail.

A Trojan horse portrays itself as something other than what it is at the point of execution. While it may advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. A Trojan horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort. The malicious functionality of a Trojan Horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

Wireless technology

In the same way that anyone with the appropriate equipment may receive broadcast stations anyone with the appropriate equipment may receive wireless data transmissions.

The problem is that someone sitting in a car in front of your house, or your neighbour next door may also be able to pick up your signal, use your bandwidth to surf the internet and, if you do not have the proper access controls in place, even access the files on your computer.

There are security mechanisms that you can enable to help prevent this. You can turn on encryption on the WAP, which will require that all wireless users know the password to be able to connect (if your WAP and wireless computers support it, use WPA encryption instead of WEP, as it's stronger). You can turn off SSID broadcasting, which will prevent your WAP from sending out its network name (Service Set Identifier) over the air to show up in others' list of available networks. You can enable MAC filtering, which allows you to specify that only computers with the physical addresses (an address that's programmed into each network interface card) you list are allowed to connect.

Many people don't do any of these things, leaving the network wide open for anyone to connect. If you've travelled with your wireless-equipped laptop, you may have seen other people's networks pop up in your list of available networks. What happens if you click the Connect button? Could you go to jail?

Recently a man was arrested in St. Petersburg, Florida, for connecting to someone else's wireless home network. He was charged with unauthorized access to a computer network. Legal opinions vary as to whether the US government has a case. Some lawyers argue that connecting to an unsecured wireless network is somewhat like walking across someone's garden when they haven't posted a "no trespassing" sign or otherwise given notice that you're not allowed. Could a defendant reasonably claim that by choosing not to use encryption or other security mechanisms, the network owner gave implicit consent for members of the public to use his signal?

Threat prevention (physical)

Although there may be a risk to office-bound computers from within an organisation or to a thief laptop computers (and the like) are even more vulnerable as they can be left on car, bus or train seat and lifted easily.

Possible security measures include –

Tether the computer to a desk or wall. Whilst it may remove the risk of a thief taking a computer easily, the tether may be pulled away from the computer rendering it useless to either the owner or the thief.

Apply a CMOS password. The advantage of this is that the computer will not boot up until the correct password is typed in. The disadvantage of this is that losing the password may render the computer unusable.

Ensure that wireless networking software is properly configured. This ensures other users in the proximity cannot use a wireless hot-spot to access your computer.

Apply a password for administrator rights of each computer. This ensures that Windows configuration may be accessed and changed only by the administrator.

Apply a password for each user rights of each computer. This ensures that user's configuration may be accessed and changed only by the appropriate user and the administrator.

Apply passwords to individual sensitive files. This ensures that the file will not open until the correct password is supplied. The disadvantage is that losing the password renders a file inaccessible.

Encrypt the hard disk. This may be done either by hardware or software. This encrypts everything on the hard disk. One disadvantage of this is it requires some computer resource. Another disadvantage is that should a physical fault develop with the hard disk everything on the hard disk may be lost.