Distr.
GENERAL

CES/SEM.47/11
9 January 2002

Original: ENGLISH

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

Joint UNECE/Eurostat Seminar on Integrated Statistical Information Systems and Related Matters (ISIS 2002)
(17-19 April 2002, Geneva, Switzerland)

Topic II: Secure communications and data confidentiality

THE PRACTICE OF SAFE COMPUTING

Invited paper

Prepared and submitted by Eduardo Gelbstein[1]

I. INTRODUCTION

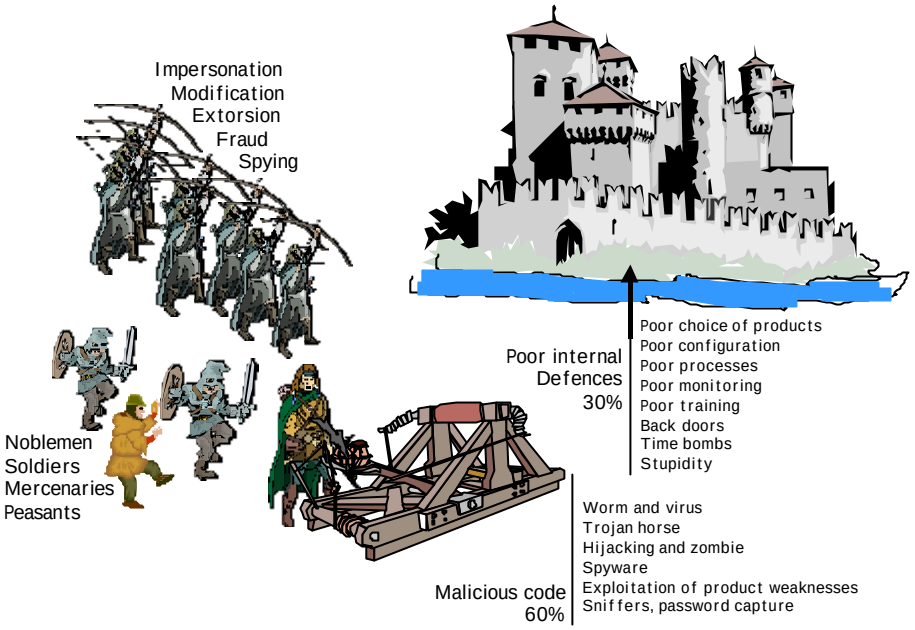
1. This paper consists of two parts, the first entitled "Players and Offences", describes the scope of information security today and explores both the "bad" and the "good" aspects of this subject. Whilst information security is often associated with the Internet and viruses, it is a much older discipline, as the need to protect information emerged almost at the same time as the invention of writing, about 5,000 years ago. The second part is a practical guide for individuals who wish to protect themselves and their information assets from the various players and offences described in part I. The paper also includes a substantial list of relevant publications and websites from which both further information and software tools can be obtained at zero or low cost.

II. PLAYERS AND OFFENCES

A. The medieval battleground

2. Medieval sieges and battles as described in history books appear to have many similarities with today's information security attacks. There are many different forms of attack – just as there were many forms of weapon – and today's weapons become more sophisticated very quickly.

[1] Independent consultant on the management of information systems and technologies (ed.gelbstein@wanadoo.fr).



3. There were many kinds of warriors – from the leader and the professional soldier to the mercenaries and peasants conscripted against their will.

4. Today's attackers also include professionals, including "reformed hackers" that become security advisors and consultants, mercenaries who hack for personal gain or satisfaction, others who copy the experts as well as, usually unknown to the owner, computers that have been hijacked and turned into zombies by malicious software planted by a knowledgeable hacker.

B. Today's "threatscape"

5. This differs from that of medieval times for two main reasons

- timeframe – everything happens in real time. In the middle ages, a good team could shoot two stones an hour with a catapult
- physical security has become less dominant than logical security – data thugs cybervandals and other players do not need physical contact with the victim

C. Today's information security players

C.1 Outsiders

Script kiddies

6. Usually young people who like to "play" with computers but are not particularly knowledgeable. However, by visiting websites of hacker clubs, chatrooms and exchanging readily available tools, they emulate the more knowledgeable players.

7. Some of these youngsters achieve "fame" as was the case in the mid 1990s of a 16 year old calling himself "Datastream" who, guided by more expert and yet to be found hackers, managed to penetrate the security of an U.S. Air Force Base and through this access point, reach a nuclear facility in Korea. At the

time of these exploits, the U.S. authorities became worried that this facility might be in the Democratic Republic of North Korea, as this intrusion could have been taken as hostile action. After a very elaborate set of traps and tracking of his activities, Datastream was finally identified, located and arrested. As a minor, no legal action could be taken against him. His mentor, code name Kuji, remains unidentified.

Manufacturers of malicious code

8. "Malicious code" is an umbrella term for any computer software designed to enter computers and making them perform unwanted actions. The forms of malicious code best known to the general public are Viruses and Worms. Viruses use software in the affected machine to replicate. Worms are self-replicating.

9. Other forms of malicious code in current use are

- Microsoft Word macros, usually written in Visual Basic (file extension .vbs) which was used in the Melissa virus attack
- Executable files (file extension .exe). A recent virus (the Anna Kournikova) was hidden in a picture using steganography
- Trojan Horse – software which performs legitimate functions but which has within it malicious code

10. The skills needed to write and/or modify Viruses and Worms are within the grasp of anyone with basic programming skills. Most viruses and worms are short programs. Many are variants of a previous one. Their characteristics, or "signature", like the DNA of a biological virus is used by the producers of Anti-Virus software to develop the tools to detect and eliminate such malicious code –always after the code has infected a large number of machines.

11. Other malicious code has been in existence since the beginning of the development of computer applications, in this case by expert programmers with malicious intent. Examples of such code include

- Back door and/or Superuser rights
- Logic bomb
- Fraudulent transactions

12. Back door and/or Superuser access rights are sometimes buried in a system by their designers as a means to bypass system security once the system is in full use in an organization i.e. to access data and the programs without being authorized to do so. Even with extensive auditing of computer systems, such back doors usually remain undiscovered.

13. A logical bomb is a piece of software hidden within an application which will be activated by its designer for example if they have a grudge against their employer or the company for whom the software has been produced or for the purpose of extortion or blackmail. The usual script is as follows:

- Your payroll system will grind to a halt on…
- I'm the only one who knows how to fix it
- If you wanted fixed, it will cost you….

Practitioners of this kind of malicious code rely on the fact that this kind of computer crime tends not to be reported because it can affect a company's reputation.

14. Fraudulent transactions are built into the software with the purpose of benefiting the person or persons who design such features (as in "deposit all the cents of every transaction into account

number…..”). These kinds of transactions are discovered mostly by chance.

15. Not all “extra code” is necessarily malicious. Many commercial software products include hidden in them what their programmers call “Easter Eggs” which range from undocumented games, the list of names of the software development team, etc. These are so well hidden that even after extensive pre-release testing and with millions of copies in use, few end-users are aware of their existence and it is only through technical magazines and chat rooms that, once discovered their existence is communicated to a wider audience.

Hackers, crackers and phreakers

16. Phreakers are individuals who have the knowledge and the tools needed to access a telephone network without being registered by the system. These techniques are used to, for example, make free long distance telephone calls – this was the technique used by Datastream and, once his presence was noted by the Security Administrator, allowed him to be traced back to his home through an elaborate trap.

17. The distinction between hackers (white hat hackers) and crackers (black hat hackers) is only one of intent. White hat hackers seem to be satisfied with being able to prove that they were able to overcome the security defences of an organization, often a government or military one. Black hat hackers or crackers do so with the intention of modifying data, deface a website, steal data or cause other forms of damage.

18. Many commercial companies have also been the subject of synchronized attacks by hackers through Distributed Denial of Service in which the webservers and e-mail servers of the target are accessed with such a large volume of transactions that they become saturated and unable to operate.

19. Hackers are technically knowledgeable people who are able to understand products in great detail and are able to identify weaknesses, particularly in security and therefore can make the products perform undesired functions. Some of them achieve considerable notoriety, as was the case of Steven Mitnick who was monitored, tracked and arrested, and is currently serving a prison sentence. Not everyone was in agreement with his imprisonment as an Internet search for his name will show that there are many websites demanding that he be released. Hackers are well organized and run conferences, good websites, exchange tools and information on product weaknesses (without reporting them to the product vendors).

Cyberhippies and hacktivists

20. The World Wide Web and Internet mail have given rise to a new form of political activism that manifests itself through, for example, organized Electronic Sit-Ins, the hijacking of legitimate websites by redirecting traffic to a spoof website pretending to be that of the organization or hijacking the personal computers of innocent users, turning them into a “zombie” and using these to launch coordinated Denial of Service attacks. Their targets tend to be the websites of governments, international organizations and world financial institutions. While these activists claim that this is merely a form of civil disobedience, the legal status of these actions is unclear as it is not covered by existing legislation.

Cyberterrorists

21. There appears to be no agreed definition of a Cyberterrorist – and the same is true for the definition of “Terrorist”. Here is a sample of definitions used in the United States of America:

- Terrorism is defined by the US State Department as “premeditated, politically motivated violence by subnational groups or clandestine agents, usually intended to influence an audience”.
- And by the U.S. Federal Bureau of Investigation (FBI) as “the unlawful use, or threatened use, of force of violence against persons or property in furtherance of political or social objectives”.

22. Furthermore, a terrorist seeks to change international events. Interestingly, there are no agreed definitions of what constitute "violence" in cyberspace (disabling the web and e-mail servers of an organization?) or what would be considered as an act of war in cyberspace.

23. There are concerns that some of the recent manifestations of worms such as CODE RED in the Summer of 2001, the NIMDA and GONER worms a little later may be tests or proof of concepts for software that could paralyze the Internet and be sponsored by a government or by independently funded groups.

24. The potential impact of a well conducted campaign of cyber-terrorism in which the targets are likely to be the utilities (electric power generation, water treatment and distribution, telephone and data networks) and important control functions (air traffic control, railway signaling, emergency services (ambulance, fire, police) could be as serious as the worst case scenario of the Year 2000 computer problem.

Organized crime and uncivil society

25. It would appear that technological innovations are quickly studied and exploited by people determined to misuse them for personal gain. Information and communication technologies are no different and ever since the introduction of the electric telegraph, new forms of fraudulent activities were developed, initially by individuals and later by organized crime.

26. Current examples of the misuse of such technologies include money laundering, credit card fraud, blackmail, extortion, pornography, pedophilia, off-shore gambling and many other. Internet technologies are also extensively used by what is generally described as the "Uncivil Society" for propaganda, disinformation and incitation to violence and hate.

Industrial (and other) spies

27. Espionage – obtaining confidential information about other parties without their consent – also has a long history. Ever since the industrial revolution, industrial espionage has been big business, particularly in industries where achieving and maintaining a position of leadership in a competitive market requires expensive and lengthy research. Given today's extensive reliance on computer systems and networks to document experiments and research and to exchange data with other researchers, it should not be surprising to note that industrial espionage is on the increase.

28. The gathering of military and other intelligence is usually identified with the work of governments, and although electronic surveillance is practiced worldwide, there are many instances where the existence of systems and facilities are reported in the press. In some cases these systems are acknowledged (as is the case of Carnivore) and in others, despite numerous rumors, there is no evidence that such systems actually exist, as for example Echelon – the name given to a surveillance network allegedly set up by a number of democratic governments to spy on their own citizens and those of other countries.

29. An e-mail message is today's equivalent to a machine readable postcard. While the use of foreign languages and/or encryption for such messages provides a measure of assurance of its confidentiality, it also signals to scanning systems (very likely to exist despite official denials) that the writer has something to keep secure. Throughout human history however, no code remains unbroken forever.

C.2 Insiders

Insiders with malicious intent

30. Until now, the most common source of fraud and abuse of computer systems has always been the knowledgeable insider – a trusted employee with legitimate access to systems and their data, a computer programmer working for the organization as an employee, contractor or as the employee of a supplier. Such malicious intent can arise for many different reasons: a wish to earn more money than through regular employment or a desire to "punish" the organization for actual or perceived misdeeds against the individual. Computer crime frequently remains unreported as it is generally believed that such reports would undermine public and stock market confidence

Unaware insiders

31. These are the employees, temporary staff, contractors, consultants and others working in an organization and granted various levels of system and network access rights who are unaware of the organization's security policies and practices and possibly genuinely not knowledgeable about information security issues. Under these circumstances, they may leave their passwords prominently displayed on a computer screen, open attachments containing malicious software which managed to get through the organization's defences, download shareware and freeware from websites, bring infected floppy disks or CDROMs into the organization.

Security managers and administrators

32. These are the individuals whose responsibility it is to define, maintain and monitor an organization's defences against malicious code and the misuse of computer systems and networks. By 2001 this has become a major job, with considerable responsibilities and requiring close contact with all parts of an organization.

Security consultants

33. The growing complexity of this field has led to the development of a major new service: consultancy in information systems security. Such consultancy services range from the development of security policies, conducting security awareness seminars, to highly detailed technical reviews of products and how these are configured and applied, the development of best practices in the monitoring and resolution of security incidents.

Security auditors

34. Two distinct types of security audits need to be considered: Compliance and Penetration audits. Compliance audits focus on the way in which security policies and practices are applied in an organization, how they are monitored, how incidents are dealt with and how effective they are. Penetration audits involve creating a controlled attack on the organization's security arrangements, with or without prior warning to the people responsible for information security. The purpose of these tests is to identify weaknesses in the defences and the reasons thereof and the subsequent development of recommendations for corrective action. Whenever an external company is used for such security audits, reliable references are essential as you will be revealing to them all the details of your security arrangements, technologies, organization.

D. Today's Information Security Offences

Computer network break-in (brute force access)

35. Using software tools that can be easily procured or, perhaps not so easily developed, hackers can break into computer systems. Once inside someone else's computer or network, they can steal data, including legitimate passwords, plant malicious code or simply cause chaos by modifying users' access names and passwords, corporate data, websites.

36. Network intrusions of this kind are, when carried out by a serious hacker, difficult to detect. Even when detected, identification of the culprit, who would normally be in another location and possibly in another country is very hard. If a successful identification is achieved, the current legal framework for seeking damages and other penalties is not particularly effective.

Industrial espionage

37. It would seem that many people just love to spy. The emergence of a global network of networks, like the Internet, has created a totally new environment where professional hackers-for-money search for, find and remove information about, for example, product development, commercial strategies, staff salaries, and other. Professional hackers can do this without leaving any evidence of theft and, as above, in the unlikely event of identifying the guilty party, legislation has not yet been written to cope with issues of electronic theft.

Software piracy and other copyright infringement

38. It is remarkably easy to make a copy of software and distribute it to others. This has been common since the early 1980s and the introduction of the personal computer, and continues to be practiced in many countries. The pirating of high value software (computer aided design, digital photography workshops and toolboxes, financial accounting packages) represents a substantial loss to the companies developing and marketing such applications. Software copied works as well as the original can be purchased for a fraction of the price and the chances of being found and prosecuted are relatively small.

Password sniffers

39. Password sniffers are programmes that monitor and record the name and password of a network user as they log in, thus weakening the security of the site, as the recipient of this information can then impersonate the legitimate user and obtain access restricted documents, perform transactions. Current legislation does not allow for the prosecution of a person for impersonating online someone else.

Spoofing and redirection of traffic

40. Spoofing consists of electronically making a computer look like another computer in order to either impersonate a legitimate user or to redirect traffic to another location which contains content that has been modified without the original owner of the site being aware of it. This modified content may be used to discredit the original owner or to provide disinformation or propaganda.

Malicious code

41. Malicious code is any software designed to interfere with the computer of those who receive it. This kind of code has been around for as long as computers and its various forms have already been discussed in the section dealing with the manufacture of such codes.

Hijacking of an end-user's personal computer

42. While the 1999 Cyberhippies that organized a Distributed Denial of Service attack on the website of the World Trade Organization relied on cooperation amongst like-minded individuals to share software that could launch such an attack, recent developments such as Code Red and Nimda, automated the process of taking over an end-user's computer and turn it, on demand, into a Zombie – i.e. a slave computer that will perform whatever tasks the worm was designed to perform. Such a Zombie could also be programmed to provide a back door to a corporate network thus bypassing all security measures designed to keep outsiders out.

Denial of Service and Distributed Denial of Service

43. The techniques used to overwhelm the corporate systems – until now websites and e-mail servers – by arranging to deliver massive pings, requests for web pages or thousands of e-mail messages in a very short period of time.

Monitoring of data traffic

44. There are many techniques that can be used to intercept data traveling between authorized origin and destination sources. These include:

- The theft of a physical medium in transit (for example backup tapes being taken to the location where they are stored off-site)
- Wiretapping – where an unauthorized entity monitors and records the data flowing between two points
- Intrusion – when access to the system or data flow is by circumventing a system's security features

45. Other forms of monitoring of data traffic include:

- The scanning and filtering of e-mail traffic by organizations other than those of the sender and recipient (such as Internet Service Providers, governments and/or their intelligence services)
- The tracking of the websites visited by an individual, the pages consulted, how much time spent on them. This could be done by an employer as well as by the owner of a website interested in learning about the usage patterns of individuals.

Tracking code

46. The World Wide Web Consortium defined a standard for "cookies", a mechanism that allows the server to store information about a user on the user's own computer. Cookies are simple text files stored on the end user's hard disk and they have many legitimate and beneficial uses such as customizing the content of a web page for an individual. A cookie tells the website that it's **you** who is looking at it. Undeleted cookies build a complete history of where you have been on the web – and many of these cookies are placed by companies who advertise on the web, keeping enormous databases of who looks at what.

47. Browsers can also be exploited as a surveillance tool: your browser can tell others where you are accessing the web from, what software and hardware you are using, details of the link you have clicked on and possibly even your e-mail address.

48. In addition to browsers and cookies, there is extensive use of software such as Web bugs (a one pixel by one pixel transparent graphic in GIF format) placed on a website or an e-mail.

49. This is invisible to the user because it is transparent and very small (it can only be detected by looking at the source version of a web page) and can be used to gather the following information:

- The IP address of the computer that fetched the bug
- The URL of the page that the We bug is located on
- The URL of the Web bug image
- The time the Web bug was viewed
- The type of browser that fetched the Web bug image
- A previously set cookie value

50. Proponents of privacy on the Internet object to the use of Web bugs. On the other hand, these bugs can also be used to track copyright violations on the Web.

e-mail related offences

Mail Spamming

51. It is relatively easy to write software that will instruct a computer – possibly other peoples' that have been turned into a Zombie (see below) – to repeatedly send e-mail to specified e-mail addresses with the objective of overwhelming the recipient's personal account or an organization's e-mail service causing it to shut down. It is not clear whether this is legal or not, but it is very disruptive.

Snooping of e-mail messages

52. An ordinary e-mail message is today's equivalent to a machine-readable postcard, and the machines to read them are either known to exist (Carnivore) or suspected (Echelon and similar in other parts of the world). The dividing line between the legality of a government owned machine and a privately owned one is an unclear one. It does not require much knowledge to identify from the e-mail header the IP address from which it originated and the route it took to reach the recipient.

Faked e-mail

53. The 'From" line in an e-mail message can be faked in several ways:

- *Spoofing* of e-mail messages consists of making a message appear to have come from somewhere or someone else. Spoofing is easy. The sender uses a software tool that is readily available on the Web to cut out the original IP address and replace it with someone else's address. The good news is that spoofing is relatively easy to deal with: the first server to receive the spoofed message records the real IP address of the sender, and this can be used to trace the original sender.

- A *remailer* is a computer that strips the sender's IP address and then remails the message with the IP address of the remailer. The only way to find out who sent the message is to get access to the logs of the remailer –designed to be anonymous, they don't log e-mail that has passed through it.

- *Relaying* consists of misusing someone else's e-mail server, something often done by spammers. A correctly configured e-mail server will not accept e-mail from IP addresses originating from outside its network. Unfortunately, not all e-mail servers are correctly configured to do so…

- *Stealing accounts* requires the offender to gain access to someone else's e-mail account and password details, either by looking over someone's shoulder, or more technically, by sniffing a network to intercept such details.

54. Once someone has a legitimate user ID and password, the whole e-mail system is compromised and all tracking will lead to the more than likely innocent victim whose account has been hijacked (unless the details were visible placed on a Post-It note, a practice which is still practiced).

55. Bogus e-mail accounts are opened from, for example, free e-mail services such as Hotmail by giving a false identity and address. As these accounts can be accessed from any computer with access to the World Wide Web, it is difficult to catch someone who has done this as the e-mail provider never knows who opened the false account.

Other activities of doubtful legality

56. There are numerous other activities that take place on the World Wide Web which do not appear to fall under the above categories and where the law is not always clear concerning what constitutes an offence or a crime and under what jurisdiction. The debate continues on all of the following activities:

- Distasteful and/or controversial content (hate, pornography)
- Arms and drugs trading
- Trading in antiquities and stolen goods
- Money laundering (including off-shore unregulated gambling)
- Political propaganda
- Disinformation

There is no doubt that human ingenuity will continue to create new offences.

III. GUIDELINES FOR THE INDIVIDUAL PRACTICE OF SAFE COMPUTING

57. The previous section describes a worrying scenario. What should an individual, at home, on the move and even at work do to be confident that one's personal information is not stolen and misused, that one's data is not compromised or corrupted and that one can use the resources of the Internet with reasonable confidence?

A. Privacy and the Internet

58. You would normally not give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. Life on the Internet is however, different. There are many parties who are interested in who you are and what you do on the Web, all with different intentions. It is because of this that initiatives such as the Electronic Privacy Information Centre (EPIC) and the World Wide Web Consortium (W3C) Platform for Privacy Preferences (P3P) were launched.

59. Amongst the many examples of potential intrusions on your personal privacy include:

- Details of your hardware and software configuration, the browser that you use, your assigned IP (Internet Protocol) address, the web pages you viewed and the referring page (the last one you visited) are readily available when you connect to the Web. Your ISP also knows your telephone number.
- Your IP address – dynamic or static, can be used to reveal at least some information about your Internet Service Provider and your geographical location. This, in turn, may be useful when trying to trace a suspect message received.
- The owner of a Website will want to know, for example, when you access the Website, what pages and documents you look at, whether you download items or not, whether you look at advertisements (those you click, specifically).

- To do this, they place cookies on your computer, they use spyware and other monitoring devices to track such use. The owner of a Website who specialises in advertising, wants to know your e-mail address and so does a spammer.
- Many Websites require individuals to register to provide access, usually free of charge to their content. Such registration requires details of name, address, and sometimes other personal information such as age and marital status and e-mail address.
- There is an issue of potential invasion of privacy when such information willingly provided by the visitor to the Website is subsequently matched against other commercially available sources of information such as demographic data, to build a more detailed profile of individuals which is stored in electronic databases and which may be made available to other parties.

60. The owner of a Website dealing with electronic commerce needs to know your name, address, e-mail address, credit card number and period of validity and other related information. There are other people whose interest may be somewhat less benign. Generally known under the name of "Pretexters" they may pose as representatives of survey firms, banks, Internet service providers and even government agencies to get you to reveal your Social Security Number or equivalent, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

61. Few websites provide their visitors with the ability to validate what information about them is held in the databases. In Europe this is in fact against the relevant Data Protection legislation which allows for (at least limited) access to such information (the European Union's Data Protection Act and other).

B. E-mail related privacy issues

Who is reading your e-mail?

62. Some of the tools that can be used to monitor the contents of e-mail messages (such as Carnivore and Echelon) have already been described. Similar systems may be used by an employer to monitor the content of messages for abusive or improper language, personal rather than business use.

63. Not all employers have clearly articulated policies about their rights and yours and without such policies, many problems can arise, largely influenced by the national legislation about the rights of individuals. Such matters become complex when, in the case of a teleworker, the employer's e-mail system was used by a family member for personal matters.

Is someone forwarding your e-mails without you knowing?

64. This is perhaps the most common source of trouble – and there have been many articles in the press – when an e-mail between two parties, intended to be a private exchange and essentially a confidential matter, is subsequently distributed by the recipient to third parties without the knowledge or consent of the sender.

Is someone sending e-mail on your behalf?

65. The first indication that you may have that someone is spoofing your mail or has stolen your account may be when you get into very serious trouble. If innocent, your only recourse is to ask for a full investigation which may or may not be conclusive.

Are you receiving fake e-mail?

66. As above, you may not know unless there is something suspicious about the content or it turns out to contain malicious software. Again, should this happen, it is advisable to arrange for an investigation.

C. Tools and measures

67. A word of caution: the tools and technologies described in this section are, at best, not perfect. However good they are, it is imperative that they should be

- installed correctly
- regularly maintained
- configured to operate at their maximum performance.

68. The best form of protection against malicious code is the use of quality and trusted anti-virus software. Such software is available commercially from a number of vendors as well as in the form of Freeware or Shareware.

69. In general terms, even the most expensive commercial antivirus software represents a fraction of the value of your computer, all of its software and, in particularly, your data. Several websites from which software can be downloaded are listed in the references.

70. The practice of implementing a personal Firewall is also spreading and it is worth considering if you access the Internet through a dial-up connection. For any form of permanent connection, the use of a personal firewall is strongly recommended.

71. A personal firewall consists of software that protects a single Internet-connected computer from intruders. Personal firewall protection is especially useful for users with "always-on" connections such as DSL or cable modem. As in the case of antivirus software, personal firewalls are available from several vendors and some of them can be downloaded from the Internet free-of-charge.

72. Software is not static, and both antivirus products and personal firewalls are frequently revised and improved by their vendors. These improvements come in three distinct shapes: patches, fixes and upgrades. Problems (bugs) are invariably found and a *patch* is the immediate solution provided to users; it can be usually down-loaded from the software maker's Web site. The patch is not necessarily the best solution for the problem and the product developers often find a better solution later. When the number of patches justifies it, a full edition of a software package incorporating proper fixes to bugs and other repairs, and, sometimes with additional functionality. This is rarely available free of charge.

73. The use of original, fully licensed software is essential in order to obtain such updates as well as technical support from commercial suppliers.

D. Protecting your privacy

Configure your personal computer features to avoid disclosure

74. You must configure your web browser to ensure that information you do not wish to share is not inadvertently made public: In your browser's configuration tool (which may be referred to as Options, Setup or Preferences, depending on which browser you use, you have the choice of using a pseudonym instead of your real name and of not entering an e-mail address or other personally identifiable information.

75. It is also a good practice to look a other "Internet-defaults" in your computer for example under Windows the "Internet Control Panel" and with an Apple "Configuration Manager" and "Internet Config" so that these can be made equally anonymous if they contain any fields for personal information.

76. For a higher level of protection there are products such as Window Washer, from anonymizer.com which perform many of these functions reliably and requiring the minimum amount of technical knowledge by the end user.

77. In a domestic environment where a computer is shared by several people, it is important to set out clear rules so that everyone knows NOT to reveal personal information other than on an approved, website by website basis.

Employers' policies concerning monitoring

78. What you do in your home, through your personal access to the Internet and the Internet Service Provider of your choice, is usually your own business, unless your employer has advised you otherwise. Using your employer's corporate network from your home or when travelling to surf the Web, download software and do your personal e-mail, may be in conflict with the employer's security policies and practices, which should normally be clearly disclosed to all staff

79. Privacy at work is a major topic in its own right, for which there are no fixed rules and no right and wrong. Legislation on this matter is either incomplete or ambiguous – except for criminal or civil investigations when there is "sufficient cause" and otherwise, it is a matter for clear communications between management and employees. It's wise to assume that there is NO privacy at work, and that this applies no only to computer systems, e-mail but also to the use of telephones and fax machines.

Cookie manager

80. Whilst cookies are well-defined and standard features of the Internet and when legitimately used, quite convenient, they can be abused, for example by disclosing information about your browsing habits to other interested parties, such as advertisers. Moreover, cookie files in your computer constitute a record of your usage of the Internet which you may wish to, at the very least, have some control over. The mechanism to do this is Cookie Management software. The latest versions of browsers (for example Internet Explorer V.6) include a cookie manager which allows you to decide which cookies you wish to accept as well as to view the cookies in your hard disk and delete those you wish to remove.

81. There are many other cookie managers that can be downloaded from the Internet, either free or requiring a modest registration fee, as well as commercial products such as Cookie Crusher obtainable from the limitsoft.com website.

User IDs and Passwords and/or physical devices

82. It is always a good idea to protect your computer, particularly notebooks and other small devices to prevent access to it by others. Such protection can take many forms ranging from a well-designed User ID and password to the use of physical devices such as Smart Cards or small pieces of hardware – commonly referred to as "dongles" that need to be physically pluged in (for example to a parallel port). A good password needs to meet two requirements: it should not require you to write it down and it should not be easily guessed (as first name, date or birth, name of a child) or broken (such as with a dictionary attack tool).

83. Generally accepted criteria are that a password should be at least six characters long and contain both characters and numbers. Some systems are case sensitive and will also differentiate between capitals and small case letters. Regrettably, these criteria are sometimes incompatible with that of not having to write it down. Memorising multiple passwords becomes a bigger headache unless you create a personal mnemonic system to assist in this.

Encryption and other privacy tools

84. Hiding your text or files with a password is a good practice but not necessarily a highly secure one. There are two important kinds of encryption: *Digital Signatures*, which are a mechanism to authenticate that a message was written by the person it claims to be from and that it has not been modified or damaged during transmission. Digital signatures use a pair of keys, a public one which you provide to everyone for example by posting it on your personal web page and a private or secret key, known only to one individual and kept in this person's personal computer in encrypted form requiring a "passphrase" to activate it. Anyone can send a private message encrypted with the public key. Only the genuine recipient of this message can read it with the private key. To send a personal digital signature to someone else, this is created using the private key. The recipient can confirm that it came from this individual by testing it with the public key.

85. It is essential that whatever software is used to create digital signatures it must be trusted to use secure techniques and be a robust well-supported and studied design. A product such as Pretty Good Privacy (PGP) is widely acknowledged to meet these requirements and is available free of charge for non-commercial use (please see the references). Tools are available to create a secure space in a hard disk to store sensitive information, often requiring a private key to provide access to it (PGP disk Encryption for example).

86. A Digital Certificate is an electronic file that uniquely links a person to a public key and is a device extensively used in electronic commerce.

87. *Cryptography* is the second mechanism and has been in used in many different forms since the invention of writing. Cryptography is usually reserved for the most highly confidential messages and it has a counterpart in Cryptanalysis, the process of braking ciphers – something that is not always possible (at present).

88. Sophisticated encryption devices and software are currently classified as weapons by several countries and require an export license which, in the U.S.A. is issued by the State Department – an authorization which appears difficult to obtain. In reality exporting software either on a floppy disk or by a file transfer is not that difficult and this is used to circumvent the authorization process.

89. The same criteria apply to the disclosure of confidential personal information such as credit card numbers. Encryption is used to protect the information about the credit card details in transmission to the website. However it does not ensure that the website stores the information securely. Many e-commerce websites have been broken into by crackers, and as a result thousands of credit card details have been stolen (World Economic Forum, Davos, 2001)

90. Credit card number details should NEVER be disclosed without making sure first that the connection is in fact encrypted – this is usually indicated by an icon such as a closed lock or padlock or an unbroken key as well as by a web address (URL which begins with https//: -- if the web address does not have this **s** at the end it is NOT a secure site).

E. Protecting your use of e-mail

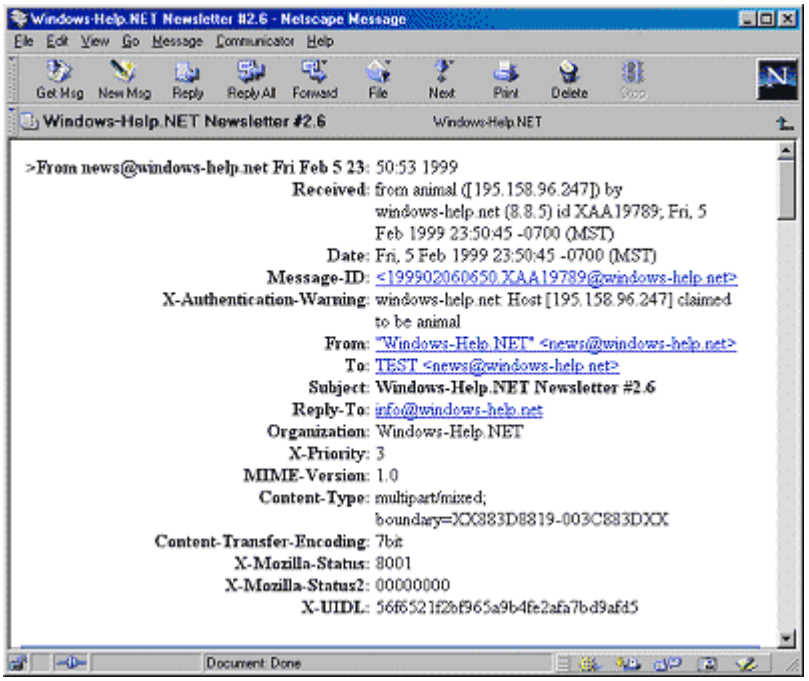
91. E-mail messages to unknown parties such as newsgroups, chat rooms and other public spaces need not be in your real name. In this situation, it is convenient to have one or more alternate accounts often but not necessarily using a pseudonym. Addresses that are widely posted become targets for on-line junk mailers, known as spammers. If you become their target, simply ditch the account and open a new one from one of the many free offerings available.

Understanding headers

92. E-mail headers can tell you a lot of things, the route a message took to get to your e-mail account, where the message originated, what e-mail program was used to send it, and more. But how do you get to know what the header contains?

93. Most e-mail programmes give you an option to "Show all headers", and in Microsoft's Outlook Express it's just a matter of pressing **Ctrl + F3** while selecting a message. This will open a separate window, where you can view all the header information. In Netscape Messenger, you can select the **View > Headers**, and make a selection from **Brief, Normal** or **All**. There are a wide variety of e-mail headers and some programs use/display different headers than others. The principles are the same. The example shown here shows which account received the message, and at which date/time.

94. The next header is the Received: header, which is the last *host* passed by the message before being placed in your mailbox. Here the message was from a machine with the name animal, with the I.P. address 195.158.96.247. It was received by windows-help.net, on Friday 5 February 1999, at 23:50:45 (MST), which is 7 hours (-0700) behind Greenwich mean time.



95. Message-ID: Each message is given a unique ID by the server, which can be used to search the logs of the server, for information about the message. The next headers (From**:**, To**:**, Subject, Reply-To**:** and Organization) are self evident. Now that you know the I.P. address where the e-mail originated, you can, if in doubt, crosscheck the originator's domain name to see if it is consistent with what it purports to be. At this point, you should be aware of the bad news: A good hacker or spammer will not find it difficult to forge the message headers by tampering with the SMTP server (**S**imple **M**ail **T**ransport **P**rotocol).

F. Good Safe Computing Practices

96. The following are some tips on good, safe computing practices:

- Consider not being “permanently connected” as is the case with DSL and cable modems because such connections use a static IP address that makes them especially vulnerable to potential hackers.

- Ensure your Internet browser is sufficiently recent to incorporate security features and that these are correctly configured in your computer (examples: Internet Explorer later than version 5.5 and Netscape Navigator later than version 6.0)

- Configure your Internet browser NOT to open attachments automatically

- Consider using an alternative e-mail package to Outlook (a Microsoft package included with the Windows operating system) for the simple reason that its popularity makes it a frequent target for virus and worm infections. Alternative software such as Eudora is largely immune from these attacks.

- Keep copies of all original and licensed software, together with appropriate ID codes and documentation needed to obtain updates and technical support

- Ensure that your freeware (software downloaded free of charge from the Internet) is from a reputable and recommended source and that your shareware (software downloaded free of charge from the Internet but for which a modest registration or usage fee is required) meets the same criteria as freeware AND it is registered with the provider

- Look for and install updates to virus definitions, personal firewalls, browsers and other software on which the security of your computer depends

- Monitor alerts and developments in malicious software from the Press or appropriate Websites. Take appropriate action immediately if a patch is required for your computer.

- Consider upgrading your software to a newer version or major new release if it contains features that

Will enhance your confidence in the security of your arrangements.

- Enable antivirus software and personal firewalls to operate in background all the time. Moreover, test for the presence of viruses, trojan horse and other malicious software on a regular basis that reflects the value of the software and data in your computer to your personal life.

- Remove all malicious software found – do NOT share it with anyone else

- Ensure that you have all the material necessary to rebuild your software and data should the worse happen. This requires systematic and comprehensive backups and there is commercial software available that facilitates this process.

97. There are of course other risks to consider, such as those of an electric power surge, hardware failure (loss of the hard disk), or worse, the loss or theft of your computer. Power supply protection devices come in a wide price range, from a simple surge arrestor to a uninterruptible power supply containing batteries that take over should the main electricity be turned off. Here, expenditure should match the need and the likelihood of such an event.

98. Should the hard disk fail and become unresponsive, should it contain highly valuable data which must be rescued before disposing of the disk or for which a complete backup is not available, there are specialised companies who can in most case do this even in the case of severely damaged disks, as is the case after a fire and the use of fire extinguishers.

99. Losing a notebook computer containing unprotected, unencrypted data is, regrettably a common occurrence due to distraction or theft. There is little that can be done to recover the computer and prevention is definitely better than cure.

G. Personal matters

100. Security is based on two very simple rules:

1. TRUST NO ONE

2. NO DISCLOSURE

101. The protection of personal information and privacy rely strongly on a little knowledge and a lot of common sense. The following are all simple to implement and quite effective:

- Beware of downloading and running programmes (games, screen savers) from sources that cannot be vouched for.

- Don’t give your credit card number unless the website URL is https AND the padlock is showing in the browser screen AND the website is trusted

- Beware of offers that appear too good to be true – they usually are, such as rewards or prizes in exchange for your contact or other information.

- NEVER reply to spammers: this confirms that your address is active and read – the result is that this will become known to more spammers. Clever spammers rely on e-mail software to tell them you have read the message.

- You should disable your e-mail package's automatic return receipt requests.

- If the problem becomes serious, contact your ISP with copies of the spam mail so that they can forward your complaint to the spammer's ISP.

- Use and maintain well-designed User Ids and passwords – cycling criteria

- Keep copies of your user ID and password in a secure and confidential place

- Disable your e-mail package's feature that automatically opens attachments. These may contain malicious code even when these appear to come from a trusted source.

- If there is the slightest doubt about the legitimacy of an attachment, ignore it until you can validate with the sender that it is OK to do so.

IV. REFERENCES AND USEFUL WEBSITES

Books and magazine articles

a. The art of information warfare: Insight into the knowledge warrior philosophy, by Richard Forne and Ronald Baklarz, 1999.
b. Cyberspace and the use of force, by Walter G. Sharp, 1999.
c. The happy hacker, by Carolyne Meinel.
d. Überhacker! How to break into computers, by Carolyne Meinel.
e. War in Cyberspace, by Carolyne Meinel (to be published).
f. The little black book of computer viruses, by Mark A. Ludwig.
g. The little black book of Internet viruses, by Mark A. Ludwig.
h. Secrets and Lies: Digital security in a networked world, by Bruce Schneider.
i. Cyberterrorism – American Programmer, May 1996, Vol 9 No. 5.
j. The Victorian Internet, by Tom Standage, 1988.
k. CODE RED for the Web, by Carolyn Meinel, Scientific American, October 2001.
l. Convention on Cybercrime (under discussion), Council of Europe (see also under websites below).

On the World Wide Web

Background and specialised information on Information Security for people who are not technical experts

http://whatis.com/
An excellent on-line encyclopædia specifically for IT-related definitions. It has a topic specific index for security, among other topics.

http://www.cert.org/contact_cert/certmaillist.html
A well-respected mailing list providing descriptions of serious security problems and their impact, along with instructions on how to obtain patches or details of work-arounds. In addition, the web site has excellent resources for improving security practices and implementations. Highly recommended.

http://ca.com/virusinfo/encyclopedia/

Website of Computer Associates for the provision of information on viruses

Websites specialising in security and related software (Commercial, shareware and freeware)

The listing below refers to well-known vendors and products. Inclusing in this list does not constitute an endorsment of the product by the author

http://www.zdnet.com/techupdate/filters/downloads
Website of major publishing and distribution house providing commercial software, shareware and freeware including antivirus, personal firewalls and encryption software

http://www.symantec.com/
Website of Symantec for antivirus software, personal firewalls and other utilities such as disk mirroring, backups
http://www.antivirus.com/vinfo/virusencyclo/
Website of Trend Micro on viruses

http://www.thelimitsoft.com/cookie.html
Example of a product for managing cookies (in this case Cookie Crusher, a product that distinguishes itself by advising you what the purpose of the cookie is when first encountered)

http://www.pgp.com
Suppliers of Pretty Good Privacy, software which can be downloaded free for non-commercial use.

http://www.networkice.com/products/blackice_defender.html
Network Ice was recently acquired by Internet Security Systems and provide personal firewall software for around 40 US dollars, roughly the same price as the Norton Personal Firewall distributed by Symantec

http://www.zonelabs.com
Another personal firewall software product which is currently available free of charge for personal use

http://www.fwnetwork.com
Website of the Freeware Network offering a wide variety of products

http://www.eudora.com
Free e-mail software, available in several languages

V. ABOUT THE AUTHOR

Eduardo Gelbstein is an advisor to executives and technical managers on the management of information systems and technology and collaborates with academic institutions on the practical aspects of managing complexity.

He was Director of the United Nations International Computing Centre, in Geneva. Prior to this he was Information Technology Strategy Manager for Network SouthEast, London (the largest business unit of British Rail prior to its privatization) and he has managed large I.T. projects for the International Union of Railways – the HERMES network linking eleven european railways and for the British Transport Police.

In the year 2000, he wrote the book “Preparing for the Information Age” for the Economic and Social Council of the United Nations and three sections for the Encyclopedia of Information Systems published in 2002 by Academic Press. He is currently finalizing a book on Information Security to be entitled “Trust No One”. He can be contacted at : ed.gelbstein@wanadoo.fr