



Romel Cabling ▾



[Home](#)

[Home](#) > [My courses](#) > [Social And Professional Issues](#) > [05 Aspect Of Computer Crime \(Cont.\)](#) > [Lesson Proper for Week 5](#)

Lesson Proper for Week 5

ASPECTS OF COMPUTER CRIME (CONT.)

Computer Security Measures

In this section we briefly discuss various measures that may be taken in order to enhance computer security. The topics covered are indicated in Figure 3.3.

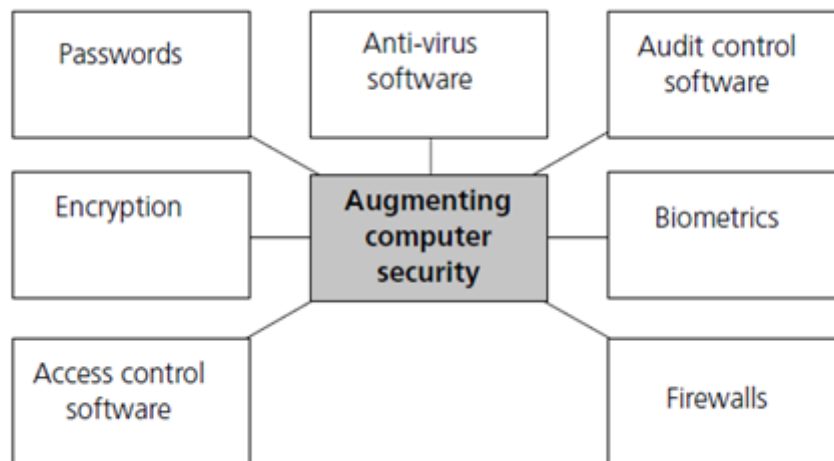


Figure 3.3: Various security measures that are discussed in this section *Passwords*

One of the simplest and most widely used computer security measures involves the use of passwords which authenticate authorized users and allow access to a system or network. Passwords represent the first line of defense in network security. However, they have a number of inherent weaknesses. Perhaps the most serious of



these is that passwords are often too obvious and easy to guess. People tend to choose the names of their partners, spouses or family pets, or a favorite hobby. If a password cannot be guessed, then password-cracking software is relatively easy to obtain.

To counteract these weaknesses, rigorously enforced password policies need to be adhered to. Passwords can be made less obvious and memorable by avoiding the use of partner's names. They should include at least eight characters, with a mixture of numbers and lower- and uppercase letters, and should not be words found in any conventional dictionary. Passwords should be issued only to the minimum number of people requiring access. Passwords, moreover, must be kept confidential at all times and should not be disclosed to anyone else. They must be changed on a regular basis (every two to four weeks). A password policy should also include the monitoring of logins (to see the date and time of recent logins, and all unsuccessful login attempts since the previous successful login). This is in order to see whether an unauthorized user has been attempting to gain access to an authorized user's account. Another important measure in any password policy is to secure the password database – a crucial area of vulnerability in a computer network.

Encryption

In computer networks, whether local area networks or the wider Internet, one of the more complicated problems is to secure information in transit between the server and the end user, and between sender and receiver. This is important in the transmission of any kind of sensitive or confidential information which must be protected adequately from the risk of being intercepted. It applies to e-commerce transactions and submission of credit card numbers, private e-mails, or any kind of security, military or business communication. One way to secure this data is through encryption.

Encryption is the conversion of data into a form (called a cipher) that cannot be easily understood by unauthorized receivers. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the 'scrambling' of voice signals. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

When a message or piece of data is encrypted, it is effectively 'locked' and can only be decrypted (or deciphered) by someone with the correct password or key. In order to easily recover the contents of an encrypted signal, the correct decryption 'key' is required. This key is an algorithm that 'undoes' the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to 'break' the cipher. The more complex the encryption algorithm, the more difficult it becomes to infiltrate communications without access to the key.



Encryption/decryption is used when carrying out any kind of sensitive transaction, such as a credit card purchase online, or confidential communication, such as the discussion of a company secret between different departments of an organization.

In the US banking system, for obvious security reasons, the Treasury Department already requires that all electronic fund transfers be encrypted. For those of us doing commerce at a somewhat smaller level (!), or simply e-mail or information transfers, security is equally important.

There are many different protocols, or standards, used in encryption. The SET (Secure Electronic Transactions) standard is used to encrypt credit card information being transmitted over the Internet. An alternative protocol is a Secure Socket Layer (SSL) which automatically encrypts information sent to websites and then decrypts it before the recipient reads it. Websites that request credit card details carry a padlock sign denoting a secure socket layer, which means the link between the user and the web server is encrypted. Encryption devices in the form of DSPs (Digital Signal Processors) are also used to scramble voice and data messages over telephone networks. Voice encryption is especially important in military and security communication, but is also used in many other fields.

Other encryption technologies include digital signatures which are used to verify the identities of both the senders and the recipients of a message, or the authenticity of electronic documents. This technology also relies on the use of encryption keys to encode and decode a message. In this case, a private key is used to sign one's signature to a message or file, and a public key is used to verify the signature after it has been sent. The public key might be published in a directory or made available to other users. Spinello [2000] presents a scenario to best describe the functioning of digital signatures:

Assume that John and Mary are exchanging e-mail, and Mary wants to verify John's identity. Mary can send John a letter with a random number, requesting that he digitally sign that number and send it back. John receives the letter, and digitally signs the random number with his private key. When the letter is sent back to Mary, she verifies that signature with her copy of John's public key. If the signature matches, she knows that she is communicating with John, assuming that John has been careful with his private key.

The drawbacks of encryption, however, are the security of the keys or ciphers themselves, which can be stolen or hacked

The level of encryption is another major issue. In general, the stronger the cipher (that is, the harder it is for unauthorized people to break) the better. However, as the strength of encryption/decryption increases, so does the cost. The strength of encryption is measured by the number of bits used in the key to encode the message or data.



It is generally recognized within the computer security field that the default 40-bit encryption used by web browsers is inadequate. The SSL used by browsers when purchasing goods online, for example, can easily be hacked into. For adequate levels of protection, 128-bit encryption, at least, is needed.

Access Control Software

Access control software assigns access rights and privileges in a computer network to different users. It restricts users, individually identified by password, to only those files they are authorized to use. Even then, the software permits the users to perform only authorized functions, such as appending or deleting information, and prevents them from accessing parts of the system which they are not entitled to enter.

However, one obvious limitation with access control software, is that it does not protect an organization against frauds committed by employees while going about their legitimate tasks; as we mentioned earlier, a high proportion of computer crimes occurs this way. Most networks provide system administrators with 'super user status', enabling them to access and modify virtually any file on the network. A further problem with access control software is that if intruders are able to obtain this status, they can obtain access to all parts of the system.

Another technology used to authenticate user access to a network, and to protect an organization's assets, is dial back or black box systems. When a user dials into a computer, a black box intercepts the call and demands a password. The unit then disconnects the call, looks up the password in the directory and calls the user back at their listed telephone number. Fraudsters dialing from another telephone number will be screened out. A server may have hundreds of ports of entry from remote stations and each one has to be protected.

Firewalls

A firewall consists of hardware and/or software that is designed to insulate an organization's internal network (or 'intranet') from the wider Internet, by putting a boundary around it (a 'firewall'). Firewall software gives access only to trusted Internet (IP) addresses and scrutinizes data for irregularities or signs of danger. Ideally, firewalls are configured so that all connections to an internal network go through relatively few, well-monitored locations. A firewall cannot only serve to protect against hacking from outside, but also to restrict access to the Internet from inside a network, for example by blocking access to certain websites. The main shortcoming of firewalls, however, is that they provide no protection against crimes by insiders.

Firewalls are used to achieve a basic level of security for commercial websites, by firstly, securing the web server and the files that it contains, and secondly, guaranteeing the integrity of the information that travels between web server and the end user. This includes user names, passwords and credit card numbers. Securing the web server itself can also be accomplished by using standard computer security techniques, such as authentication



mechanisms and intrusion protection devices. Gatekeepers and digital locks can also secure networks on which these servers reside. Although firewalls can be used to protect web servers, most companies set up public websites outside their firewalls to make them more easily accessible to those trying to buy their products.

Biometrics

Another weapon in the fight against computer crime is biometrics, or the digitizing of biological characteristics. These technologies work by sampling 'unique' biological features, such as the voice, the pattern of blood vessels in the retina, or fingerprints. They then extract and convert these features into a mathematical code and store them as a biometric template. To confirm a user's identity, the user interacts with the system, for example by an iris or fingerprint scan. The sample is then compared to the template for a match, and access is accordingly granted or denied. Some computer systems, for example, require a thumbprint match to log onto to a computer, either physically or over the Internet. The main applications of biometrics are in security and fraud prevention. Biometric scanning devices can control access to computer rooms, bank vaults and military bases.

To reduce the risks of terrorism, several US airports now use fingerprint identification systems to ensure that only authorized employees enter restricted areas. Following trials at Heathrow Airport, it was reported in 2004 that the UK Home Office was planning to introduce an iris recognition system at five UK airports to verify identities of selected overseas travelers. These were part of wider plans to roll out biometric technology in the use of visas, passports and eventually ID cards (*Computer Weekly*, 22 June, 2004).

Whereas the use of biometrics seems set to increase dramatically, there are some serious practical, social and political problems with this technology. When a credit card number is stolen, we can get a new account with a new number, but if a hacker gets a copy of the file with our digitized thumbprint or retina scan, we cannot get a new one. Given the weak security of the Internet, it is likely that hackers will be able to steal biometric files as easily as they now steal files of credit cards. Another problem is reliability. The two most developed forms of biometric identification, fingerprints and iris scanning, can produce false results, especially when used for mass identification purposes. This could mean that someone who was a legitimate owner of a passport or a credit card, or someone with authorized access, could be rejected by the identification system. Biometric systems have to be completely robust and carefully tested before being introduced – and at present this is certainly not the case.

A third area of concern is that the increased use of biometrics can also lead to increased surveillance and tracking of our activities by government agencies. The potential for loss of privacy and civil liberties is considerable.

Audit Control Software



Audit control software is used to closely monitor the use of a computer. This enables auditors to trace and identify any operator who gains access to a system, and the exact time that this occurred – such as after working hours. This type of software can also be used specifically to browse through vast amounts of financial transactions, looking for signs of any abnormal activity, such as a high number of ‘correction entries’, which often indicates the trial-and-error approach of fraud. Such systems are often used in the financial sector, to identify insider trading and stock or foreign exchange fraud.

Anti-Virus Software

In the previous lesson, we explained that computer viruses are malicious programs with enormous destructive potential. Anti-virus programs are therefore an essential aspect of computer security. Anti-virus software works by searching the computer’s hard disk and storage media for virus patterns and signatures, and matching them against its own database of virus definitions. If a match is found, and an existing virus is detected, an appropriate course of action is suggested to remove the virus. Anti-virus programs also prevent infected files from being downloaded (whether from a disk or an e-mail attachment) and prevent viruses from inserting themselves into a computer system.

However, since new viruses are appearing all the time, the application’s database has to be constantly updated. Some viruses also change their pattern as they replicate, so the software must also scan for suspicious code as well as known virus patterns.

The market for this kind of software has expanded rapidly with the increasing use of the Internet by organizations and individuals, and the increasingly destructive potential of computer viruses. Some forms of virus protection include isolation of the infected system(s), or the use of non-writable system disks so that viruses cannot copy themselves there. Other antivirus measures include testing of unknown software (particularly public domain software downloaded from bulletin boards) on a minimal, isolated system.

Management Issues

Security is not only a technical issue, it is also a management issue that involves educating staff and increasing employee awareness of security issues. As IT security consultant, Gary Hinson (2004) argues:

‘Computers alone don’t implement information security policies and standards – human beings purchase and configure the systems, switch on the control functions, monitor the alarms and run them. Whatever way you look at the problems, it is just as important to invest in your people as your technology.’



Security policies also need to include management policies for checking employees – for example, undertaking thorough reference and background checks when recruiting staff. This is especially important in the case of personnel whose jobs involve access to confidential or sensitive data. Security policies also involve decisions about appropriate levels of network access and authority, and the implementation of password systems, disaster recovery plans and other security procedures.

The Computer Misuse Act, 1990

Computer crime in the form of unauthorized access to computer systems, in any of the three main categories discussed in Module 3, is covered by the Computer Misuse Act, as amended by the Police and Justice Act 2006. We saw how an individual can be prosecuted in the UK under the Computer Misuse Act as long as there is at least one 'significant link' with the UK. This is especially important with new kinds of cybercrime which are committed across national borders. International jurisdiction of the law, however, also represents a problem in the apprehension and prosecution of computer criminals. The individual suspected of writing and releasing the ILOVEYOU computer virus in 2000, for example, which jammed computers and destroyed files worldwide, was not prosecuted because he lived in the Philippines, which had no law that applied to his actions.

There are a number of additional legal problems when prosecuting suspected computer criminals. One general area of concern about the current legislation on computer misuse is that the law is out of step with the rapidly changing nature of computer crime. Legal experts, security consultants, and law enforcement agencies have argued that the Computer Misuse Act needs urgently updating to take into account the growth of the Internet and the emergence of new kinds of offences. The Police Justice Act 2006 moves towards this, with its amendments to the Computer Misuse Act; the Fraud Act 2006 (introduced in January 2007) covers areas of technology-related crime, such as phishing and spoofing.

Another problem is that there are no statutory provisions relating specifically to computer evidence in trials involving computer crimes. Evidence from computers that have been attacked may not be admissible in court proceedings, because, under common law, it has been taken from mechanical instruments which are not in 'working order' (Hill, Shelley, Dec 2003/ Jan 2004, Computer Misuse, C & L, www.scl.org).

The question of intention has been another sticking point. Section 3 of the Computer Misuse Act, 1990 states that an offender is guilty of an offence only if 'he has requisite intent and requisite knowledge'. The problem is then how to show and prove this intent, with evidence of responsibility. A key defense in many cases has been that 'the accused did not intend to cause any harm,' or that 'material had been placed on the computer of the accused without their knowledge'. In the case of Aaron Caffrey, the accused had allegedly launched a denial of- service attack against the Port of Houston's (US) computer system which prevented access to the port's information by shipping, mooring and support services. The port is one of the busiest in the world. Caffrey alleged that a Trojan horse was responsible and that it installed itself on his computer without his knowledge. There was no trace of the Trojan



found on his machine, but he argued that it deleted itself after committing the acts of which he was accused. Despite the prosecution arguing that this technology did not exist, the jury acquitted Caffrey. (Hill, Shelley, Dec 2003/Jan 2004, Computer Misuse, C & L, www.scl.org).

In another case in 2002, computer experts found 11 Trojan horse programs on the computer of Julian Green which had been downloaded as a result of his opening unsolicited e-mails. After receiving this expert evidence, prosecutors dropped charges against Green for possession of 172 indecent images of children.

Commentators suggested that one of the key reasons for these acquittals was that the juries were confused by the technical evidence put before them – a further key problem in the prosecution of computer crime cases. In both cases, the defense argued that Trojan horses could delete themselves after they had infected a machine, and that this was the reason for the absence of infection when the machine was inspected. The prosecution on the other hand argued that this technology did not exist. Some reports suggest that one juror developed a migraine after hearing the technical evidence! (Hill, Shelley, Dec 2003/Jan 2004, Computer Misuse, C & L, www.scl.org).

Another concern voiced by law enforcement agencies, and victims of computer crime, is that the sentences for computer crimes are simply too lenient. All too often, such criminal activities attract light sentences or avoid prosecution altogether as the Crown Prosecution Service and the judiciary fail to recognize their damaging nature. Computer theft, fraud and vandalism, it is argued, deserve to be treated as seriously as more traditional areas of law and order such as crimes against the person, crimes against property and the maintenance of public order.

Professional Duties and Obligations

Other legislation relevant to the field of computer security is the Data Protection Act, 1998. We will be exploring this Act in greater detail in next lesson in relation to privacy issues. However, one of the Act's key principles has a direct bearing on the issue of computer security. This principle requires that companies and organizations take 'appropriate security measures ... against unauthorized access to, or alteration, disclosure or destruction of, personal data, and against accidental loss or destruction of personal data'. This means that organizations have a legal obligation to protect any personal data that they may hold, and to take appropriate security measures against the destruction, alteration or disclosure of that data.

This also raises issues of professional responsibility. It can be argued that computer professionals, individually, and organizations, collectively, have ethical and professional duties to implement adequate security measures. While security techniques and practices have improved dramatically in the past few decades, there are still gaping holes. Attitudes to security in many businesses, organizations and government agencies have not caught up with the new risks. New technologies and applications are introduced – new vulnerabilities ensue.



Professional duty can also be taken to include responsibility to incorporate security features when designing new software. In the rush to get products online, to develop the potential of the Web, and to use the newest technologies, security issues are repeatedly ignored until systems are vandalized, robbed or shut down. Many computer viruses, worms and intrusions use well-known security flaws that have not been fixed on the victim's systems. Known corrections for loopholes are not implemented, out of carelessness, lack of management support, or lack of knowledge (of the problem, the risks or the solution). Many computer system administrators, particularly in small businesses and organizations, do not have adequate security training or knowledge of the systems they administer.

Economic considerations also come into play here. To implement extra security measures and features costs organizations' time and money, and many companies have other spending priorities. However, this short-sighted view may backfire on businesses. Customers may punish companies who have a cavalier attitude about their personal data and credit card numbers by shunning their websites. By damaging customer confidence and trust, and denting a company's public image, security breaches can also damage business. The longer-term view is that sound security measures are an important investment – one that will repay itself by bolstering consumer confidence that the Internet is a safe place to do business.

Many of these professional duties and obligations, with regard to security, crime and the law, are stated in the codes of conduct of bodies like the British Computer Society (BCS). There are a number of clauses in the BCS Code of Conduct, and in the codes of professional computing bodies in other countries, that allude to such responsibilities. Some of these we have noted already in the previous lesson. In particular, they are that 'members shall have due regard to the legitimate rights of third parties' and that they '... have knowledge and understanding of relevant legislation, regulations and standards ... and ... comply with such requirements' (British Computer Society, *Code of Conduct* 2006).

◀ Preliminary Activity for Week 5

Jump to...



Analysis, Application, and Exploration for Week 5 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1



Multimedia

Network Attacks: Detection, Analysis & Counter...

Ojt/Practicum 1

Social And Professional Issues

Participants

General


03 Computer Hacking

04 Aspect Of Computer Crime

05 Aspect Of Computer Crime (Cont.)

 Preliminary Activity for Week 5

 **Lesson Proper for Week 5**

 Analysis, Application, and Exploration for Week 5

 Generalization for Week 5

 Evaluation for Week 5

 Assignment for Week 5

System Integration And Architecture 2

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

 Assignments

 Forums

 Quizzes



Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)

