Topic 3

Risks and Threats

Contents

Learning Objectives

- **Familiarity with the concept of a computer crime**
- **Appreciation of the possible forms of computer misuse**
- **Familiarity with the security measures which can be used to prevent crime**
- **Awareness of the privacy issues relating to computer crime prevention**

3.1 Introduction

In this topic we shall examine the various forms of computer crime and the security mechanisms which can be used to deter or prevent them. We shall also discuss the privacy issues which arise from the use of some of the security techniques.

It is important to keep the effects of computer crime in perspective. The most common breaches of system integrity result, not from criminal acts, but from computer crashes due to power failures and untested software. Some of the most expensive breaches to rectify are those caused by non-computer related events such as floods and fires.

You should note that surveys which attempt to quantify breaches of system integrity and estimate their costs are notoriously inaccurate. Organisations are very reluctant to publicise these breaches in case they lose the confidence of their customers or clients. Cases of fraud, in particular, are very rarely reported but a single incident of fraud can result in enormous losses.

3.2 Computer crime

We shall investigate five classes of computer crime ranging from the rather mundane theft of computer equipment to the electro-magnetic emissions technology used for eavesdropping and from piracy to the e-mail viruses which plague modern-day computing.

3.2.1 Theft

Computer theft can take a number of forms. The most obvious is the physical stealing and taking away of computer equipment. Physically depriving the owner of their property in the conventional sense of the term theft.

Theft in the computer world, however, can also occur without necessarily depriving the owner of their property. Depriving somebody of an exclusivity right is theft. Taking a copy of something, for instance. This doesn't necessarily involve infringing their intellectual property rights. It might simply be a case of violating their privacy.

3.2.2 Piracy

Piracy is the term used to describe that form of theft which deprives somebody of an intellectual property right. Infringing a copyright, patent, design right, trademark, etc. Intellectual property rights exist to reward the originators of an idea or work or brand for making their intellectual property public so that the rest of us can benefit from it.

Piracy is effectively stealing the originator's revenue. The copying of computer programs or files and the unscrambling or decrypting of protection mechanisms are generally held to be acts of piracy.

3.2.3 Espionage

Espionage is the stealing of secrets, the acquisition of confidential information. We shall briefly examine two ways in which this can be achieved – one software, one hardware.

Sniffers

Computer networks share communications channels so any node on a network can receive transmissions intended for other nodes. Normally a node would discard any packets not addressed to it but it is possible to configure nodes to be "promiscuous" and receive all packets. A sniffer program runs on a promiscuous node and inspects all of the packets on a network - particularly start of session packets which convey username and password details. Encryption can be used to prevent sniffers from making sense of the information sniffed but it incurs a network overhead, of course.

TEMPEST

Data can be captured from screens, keyboards, even disk accesses using TEMPEST - the Transient Electro- Magnetic Pulse Emission Standard. Obviously encryption can’t be used to protect the data sent to display screens. However a variety of techniques can be used to scramble the data in such a way that a human can still make sense of what appears on the screen whilst the eavesdropper cannot.

3.2.4 Fraud

Fraud is to gain a financial or other personal advantage by deceit. The key word here is “deceit”. It is impossible to estimate how much financial fraud occurs, with or without computer assistance. The only guarantee is that fraud will always be grossly under-reported by the victims. The scandal of large scale fraud can bring companies to their knees. Recall the case of Barings bank which was eventually sold for a song after a fraud scandal. A rule of thumb commonly used for estimating the true cost of fraud is to multiply the reported figures by ten.

One of the earliest forms of computer-based fraud was the “salami technique”. Most banks refuse to deal with amounts smaller than a certain limit, typically the smallest coin in use. Certain calculations, such as interest payments for instance, can result in account balances which violate that rule. For instance, in the UK at the present time the smallest denomination is a penny. A calculation which results in a balance of 10.3 pennies will be turned into a balance of 10 pennies. Where did the 0.3 of a penny go? Well, into the bank’s profit effectively because it certainly didn’t get credited to the customer. The salami technique involved picking up all those extra small bits of money, which you could argue really didn’t belong to anybody, and syphoning them off into another account where they could accrue into some very large sums indeed. Nowadays the salami technique refers to any process by which small amounts of money, sufficiently small to be unnoticed, are sliced off an account balance.

3.2.5 Sabotage

Sabotage can be thought of as reducing the effectiveness of a system through deliberate destruction or damage. Denial of service attacks, spam, viruses, worms, Trojan horses and bombs come into this category. We shall now clarify what all of these terms mean. Further details can be found in Grimes (2001).

Denial of service
Making multiple simultaneous accesses to a node on a network so that it becomes swamped with dealing with those accesses and can no longer do anything else, including serving further accesses. Web servers are a common target for such attacks but they are usually quite short-lived in duration.

Spam
Unsolicited, or unwanted, e-mail messages. In small quantities spam can be quite innocuous but few computer users remain untroubled by it these days. Spam filters, which score incoming e-mail messages against a number of well-known characteristics of spam, are the best defence at present since nobody seems prepared to take responsibility for tracking down the spammers and stopping their activities at source.

Virus
A virus is a self-replicating code segment which is embedded in a larger host program. A virus will typically be activated when the host program is executed and copy itself into other programs. It will then modify the new host to make sure it gets executed when the new host is accessed or run. As anti-virus software becomes more adept at identifying and dealing with viruses so more advanced viruses seem to be released. The latest stealth viruses go to great lengths to hide their existence and polymorphic viruses camouflage themselves so that the tell-tale signatures which the anti-virus software uses to identify them change on every new replication. The best defence against viruses remains anti-virus software but it is crucial to keep the virus definition files used by such software up to date. Anti-virus software is only as good as the data it uses and new viruses are being released all of the time.

Worm
A worm is a self-replicating program which spreads across a network by copying itself to connected hosts. Unlike a virus, no carrier program is needed. In recent years the term worm has come to be used to describe viruses which spread across networks using e-mail attachments. Viruses carried by e-mail messages, purportedly sent by somebody the recipient knows, have wreaked havoc by using people's address books to e-mail themselves from one victim to the next. Most anti-virus software can identify these forms of virus – as long as the virus definition files are maintained properly.

Trojan horse
This is a program which apparently performs a useful function but which includes hidden destructive code. Known Trojan horse programs can also be identified by most anti-virus software.

Bomb
A bomb is a trigger which can activate malicious code, such as a virus. There are two common types – the logic bomb and the time bomb. A logic bomb monitors system activity and detonates when a particular event occurs or when an event has occurred a given number of times. A time bomb monitors the system clock and detonates at a particular time or on a particular date.

3.3 Security and privacy

Security systems employ a variety of techniques ranging from the verification of identities, authentication of messages and encryption of data to the prescription of access controls, recording of audit trails and performance of risk analyses. We shall examine some of the methods used for verification and encryption in the following sub-sections. Further details can be found in Garfinkel and Spafford (2002).

Verification mechanisms are generally based on something possessed by the person whose identity is to be verified or something known only to them or some personal characteristic. Authentication systems can validate the originator of a message and confirm that its content hasn't been tampered with using certificates, digests or digital signatures. Finally, for confidential information which shouldn’t be read by unauthorised people, the content can be hidden from prying eyes with encryption algorithms.

3.3.1 Something possessed

Magnetic strip cards will probably be the most familiar example of this form of verification technique. The main problem with them is that they can be lost, stolen and forged. Mechanisms which have been employed to make the forger’s task more difficult, but not impossible, can include –

1. Watermarking the magnetic tape with an underlying non-erasable pattern and using an extra data track to check that it has not been tampered with.
2. Using a sandwich tape which has two layers of differing intensity such that any attempt to re-write the high intensity data would wipe out the low intensity background.
3. “Chip and pin” cards which have a much larger data storage capacity and can also perform some on-card processing. Typically the storage capacity will be 8K bytes as opposed to 250 bytes and the processing capability means that the card can be challenged to produce the correct response to many different verification requests.

3.3.2 Something known

Passwords can pose security risks if they are not chosen wisely, changed regularly or used sensibly. You will probably be familiar with a kind of password called a non-unique password. This kind of password enables a person to confirm a claimed identity – typically the identity associated with a username. There are, however, a number of other types of password system.

Group passwords are shared by many people and are used when a number of different people all need access to the same thing. Unique passwords are used to claim an identity. They are a username and password combined. Variable passwords can be used in more critical installations to ensure that the password changes on every use. Each time the password is used a new one is derived from the previous one. Finally, where the ultimate in security is required, there are single-use passwords which are changed after each access, not using a rule as in variable passwords, but by using the next password from a previously drawn up list. The banking system employs single-use passwords and the password lists are couriered out to the banks at the start of each working day.

Password selection is the weakest link in the security system chain. If users are given a free choice of passwords the results can be highly susceptible to guessing or cracking. In general people do not choose sensible passwords and it only takes one poor choice to undermine a system. Furthermore passwords may not be changed very often. Again, it only takes one lazy person to undermine a system.

Automatic system allocation of passwords using password generators is not necessarily more secure than freely chosen passwords. Unmemorable passwords can be generated in this way and these are bound to be written down. Smarter generators try to produce pronounceable words as passwords, with varying degrees of success.

3.3.3 Personal characteristics

If something possessed and something known are not practical or sufficient then we must turn to something "about" a person. Some personal characteristic which is unique to them. This is the field of biometrics.

There are two main types of biometric, physiological and behavioural. Physiological biometrics are physical characteristics which can usually be seen and measured in some way. Behavioural biometrics, on the other hand, are the result of some involuntary action such as a signature or a voice print.

We shall now look at the most common forms of both classes of biometric. We shall then briefly discuss some of the privacy concerns that have arisen as a result of the increasing likelihood of our being identified by biometrics in the future.

Physiological biometrics

DNA
Over 99% of our DNA is identical and so no use in identifying a given individual. DNA tests actually use the "junk DNA" which we all carry around but make no use of. DNA is not unique. Identical twins have identical DNA. Consider the following –

> 1 in 83 births in the USA is a twin
> 28% of twins are identical and so have identical DNA
> Therefore 1 million people in the USA do not have unique DNA

Face
There are two types of system used for face recognition. The first uses facial metrics. These measure specific features such as the distance between the inside corners of the eyes or the distance between the outside corners of the eyes and the mouth. These measures are then stored for comparison. The second method is based on "eigenfaces". An eigenface is a stereotypical face against which the face to be recognised is compared. Typically the degree of fit with forty carefully chosen eigenfaces might be recorded for each individual.

Fingerprint
Not even identical twins have the same fingerprints. Computer-based fingerprint checking does not use the loops, whorls, etc. that we do. Automated Fingerprint Identification Systems (AFIS) record the locations of around ninety minutiae - places where a ridge starts or forks. If this is done for each finger and thumb then about nine hundred minutiae are stored per person.

Hand geometry
Geometric techniques produce small data sets and do not discriminate well. The geometry can be ascertained in two ways – using a mechanical device or using edge detection from an image. Hand geometry uses estimates of finger lengths and thumb widths to identify an individual. A reduced form of the hand geometry approach uses the geometry of just two fingers.

Iris
Iris scanning seems to be the most robust and most accurate biometric discovered to date. Standard video cameras are sufficient to capture the images. The probability of two irises

having the same biometric value is 1 in 10^{78}. Even identical twins have different iris patterns. A typical iris recognition system stores just 256 bytes per person.

Retina
Blood vessel patterns in the retina are unique. To identify somebody from their retina they must look through an aperture and align their eye with the aid of target circles projected to help them. Infra-red light illuminates the retina to enhance the image of the blood vessels and a camera captures the image. Comparison can then be performed against previously captured images.

Vascular
As with retinal scanning, infra-red light is used to illuminate the blood vessels under the skin and a camera is used to capture an image. This technique can be used on readily accessible parts of the body such as the face, back of the hand or wrist.

Behavioural biometrics

Signature
The best systems do not treat this as a pattern recognition task because signature repeatability is generally quite poor. The dynamics of the pen motions are the key properties used – accelerations, directions, pressures and stroke lengths. Capturing these features is not easy and consistency is difficult to achieve.

Voice
Voice recognition is a pattern recognition task. A set phrase is used to create a voice print template. The phrase needs to be repeated several times during the creation of the template. Subsequent entry of the phrase can then be compared against a number of templates and the identity of the speaker retrieved. This technique attempts to be invariant to the physical characteristics of a voice but can become dangerously dependent on the behavioural characteristics of speech so somebody with a cold might not be recognised.

Privacy concerns

Biometrics, because they are so personal, have highlighted concerns about personal privacy and freedoms. Whilst nobody would object to being identified on those occasions when they choose to be, such as when accessing their bank account, surveillance techniques could take advantage of biometrics to identify us without us knowing about it. Some people find this very worrying (Garfinkel 2000). Developers and users of this technology need to be aware of and understand these concerns.

3.3.4 Cryptography

Cryptography is the art of hiding the content of a document or message from unauthorised people. The aim is to ensure that only those people who you wish to read the text can actually do so. Modern encryption techniques are not uncrackable, they just require an impractical amount of time to crack – many years, even with the fastest computers.

The algorithms used in modern cryptography are not secret. They are published for all to see and use. They rely for their power on keys which are large numbers known only to the sender and receiver of the message. In private key cryptography, such as the Data Encryption Standard (DES), the decryption algorithm is simply the inverse of the encryption algorithm and one key is used by both the sender and the receiver. This key must be kept secret. To crack the code one has to find the key.

One of the most effective and popular encryption algorithms is the Rivest, Shamir and Adleman, or RSA, algorithm (Garfinkel and Spafford 2002). This algorithm is actually two slightly different algorithms, one of which encrypts and the other of which decrypts. Two keys are required because each algorithm uses a different key. As long as the keys have been chosen carefully then knowledge of the algorithm and one of the keys will still leave the cracker requiring an enormous time to discover the other key.

Public key cryptography makes use of the fact that one key (the public key) can be released to everybody so that they can encrypt messages but not decrypt them. To decrypt a message a private key is needed and this is kept secret by the recipient of the messages. In this way anybody can send a secret message, such as the password for their bank account, but only the receiver, the bank, knows the other, private, key so only they can decrypt it and authorise access to the account.

3.4 Assigned task

You should write a 2000 word essay on one of the following two topics. This essay should be submitted at your third tutorial meeting.

1. Detailed Working of Biometrics

Research and describe the detailed working of one example from each of the two main categories of biometric; physiological and behavioural.

2. Reliability of Biometrics

Physiological biometrics identify bodies or, more specifically, parts of bodies. They do not identify people directly. Furthermore, all biometric data must be stored for subsequent comparison and it is a match between the presented and the stored data, which might not be the correct data, that is used for identification. Discuss the problems which these two levels of indirection might create.

3.5 End of topic test

<!-- IU
Please insert a multiple choice test here. The correct answers to each question are underlined.
-->

Q1. Which of the following was NOT suggested as a form of computer crime –
a). Debugging

b). Espionage
c). Fraud
d). Sabotage

Q2. Sniffer programs make use of what type of network node –
a). Client
b). Naked
c). Promiscuous
d). Server

Q3. Fraud is to gain personal advantage by –
a). Deceit
b). Hacking
c). Surveillance
d). Theft

Q4. Slicing small amounts of money off bank accounts is called the –
a). Bratwursting
b). Hot dogging
c). Salami technique
d). Sausage method

Q5. Which of the following were NOT cited as a form of sabotage –
a). Bombs
b). Explosives
c). Viruses
d). Worms

Q6. Authentication systems may employ –
a). Access controls
b). Digital signatures
c). Hall marks
d). Lie detectors

Q7. Which of the following was NOT suggested as a verification technique –
a). Letter of recommendation
b). Personal characteristic
c). Something known
d). Something possessed

Q8. A behavioural biometric results from what kind of action –
a). Aggressive
b). Involuntary
c). Physical
d). Voluntary

Q9. Which of the following was NOT cited as a type of biometric –
a). DNA

b). Fingerprint
c). Hair colour
d). Signature

Q10. How many keys must be kept secret in public key cryptography –
a). All
b). None
c). One
d). Two

References

Garfinkel, S., 2000, *Database Nation.* O'Reilly.

Garfinkel, S., and Spafford, G., 2002, *Web Security, Privacy & Commerce.* 2nd edition, O'Reilly.

Grimes, R.A., 2001, *Malicious Mobile Code.* O'Reilly.

Quinn, M.J., 2005, *Ethics for the Information Age*. Addison Wesley.