8 Security and ethics

Key objectives

Objectives of this chapter are to revise:

- security and data integrity
- cookies
- loss of data and data corruption
- firewalls
- security protocols
- encryption techniques
- denial of service attacks
- computer ethics
- free software, freeware and shareware

Key definitions

Term	Definition
Hacking	A way of gaining illegal access to a computer system
Cracking	The editing of program source code so that it can be exploited or changed for a specific purpose
Viruses	Program code that can replicate/copy itself with the intention of deleting/corrupting data/files or causing the computer to malfunction
Phishing	Sending legitimate-looking emails to encourage users to give out personal data
Pharming	Malicious code installed to redirect users to a fake website
Spyware/ key logging software	Gathers data by monitoring key presses on user's keyboards
Cookies	Pieces of data which allow detection of web pages viewed by a user and store their preferences
Accidental or malicious loss of data	This could be due to accidentally deleting a file or to malicious attack from viruses or hacking
Firewalls	Examines traffic between user's computer and a public network. They can help to prevent viruses or hackers entering a user's computer
Security Sockets Layer (SSL)	Allows data to be sent and received securely across a network
Transport Layer Security (TLS)	A protocol that is designed to ensure that no third party may eavesdrop or tamper with any message
Symmetric encryption	A secret key which makes a message unreadable unless the recipient also has the decryption key
Asymmetric encryption	A form of encryption requiring both a public and a private key
Authentication	Used to verify that data comes from a trusted source
Denial of Service attacks	an attempt at preventing users from accessing part of a network, notably internet servers
Ethics	A set of principles set out to regulate use of computers
Free software	Users have the freedom to run, copy, change or adopt free software
Freeware	Software that a user can download free of charge
Shareware	Users are allowed to try out shareware free for a trial period

Security and data integrity

Hacking

- Hacking is a way of gaining illegal access to a computer system.
- This can lead to identity theft and loss or corruption of data.
- The risk of hacking can be minimised by using strong passwords and firewalls.

Cracking

- Cracking is the editing of program source code so that it can be exploited or changed for a specific purpose (mostly an illegal act).
- It is often done for malicious purposes, e.g. modifying legitimate software to do something like redirect a user to a fake website.
- It is difficult to guard against; software engineers need to make the act of breaking into the software nearly impossible (i.e. make it difficult to identify ‘back doors’).

Viruses

- A virus is program code that can replicate/copy itself with the intention of deleting/corrupting data/files or causing the computer to malfunction.
- They can cause the computer to run slow (due to the hard disk filling up with data, for example) or crash (e.g. due to deletion of some key .exe files); they can also cause some software to run abnormally (due to loss or corruption of files/data).
- The risk of viruses can be minimised by running anti-virus software or not opening emails or software from unknown sources.

Phishing

- Legitimate-looking emails are sent to users; on opening the email, the user could be asked to supply personal or financial details or they may be asked to click on a link which sends them to a fake/bogus website where the user could be asked to supply personal data.
- Once the user is sent to the fake/bogus website, they may be asked to give out personal or financial data.
- Many ISPs filter out phishing emails; the user should also be very cautious about opening emails from unknown sources.

There are a number of signs to look out for in phishing emails:

- messages containing poor spelling and grammar
- a message that asks for personal information or where you didn't initiate the action
- a message that makes unrealistic threats or promises, or financial rewards, for example, cash prizes, lottery winnings, investment or pensions advice.

Pharming

- Malicious code is installed on a user's computer or web server; the code redirects the user to a fake or bogus website without their knowledge.
- Once the user is sent to the fake/bogus website, they may be asked to give out personal or financial data.
- Some anti-spyware software can identify and remove pharming code on the hard drive; the user should also look out for clues that they are being redirected (websites which are safe can usually be identified by https or by the green padlock 🔒 sign in the status bar).

Wardriving

- This is the act of locating and using wireless internet connections illegally.
- Could lead to stealing of internet time and bandwidth; also user's passwords and other data may be intercepted.
- Prevented by use of WEP (wired equivalent privacy) encryption; use of complex passwords before accessing the internet and use of firewalls to prevent outsiders gaining access.

Spyware/ key logging software

- Gathers data by monitoring key presses on user's keyboards and sending the data back to the person who sent the spyware.
- Sends important data, such as passwords, back to the originator of the spyware; it can also allow the originator to change settings on the user's computer.
- Prevented by use of anti-spyware; use of mouse to select characters from a drop down box to enter passwords rather than using a keyboard.

Cookies

- Pieces of data which allow detection of web pages viewed by a user and store their preferences.
- Create an anonymous user profile (e.g. user's preferences).
- Cookies can be deleted from the user's desktop, although this can remove some of the features of certain websites.

Data integrity

Data can be lost on a computer due to:

- accidental or malicious mal-operation
- hardware malfunction
- software malfunction.

Accidental or malicious loss of data

- This could be due to accidentally deleting a file or to malicious attack from viruses or hacking.
- This can be guarded against by doing regular back-ups of data (although this won’t allow recovery following virus attack); also use of passwords and user ids to protect the data (see above for virus and hacking safeguards).

Hardware faults (e.g. head crash)

These can be guarded against by regular back-ups of data, use of UPS to prevent ‘power glitches/loss’ and use of parallel hardware.

Software faults (e.g. two pieces of incompatible software)

These can be guarded against by regular back-ups of data and the saving of data every 30 mins, for example, in case the computer becomes unresponsive.

Firewalls

- Examines traffic between user’s computer and a public network.
- Checks whether incoming/outgoing data meets certain criteria.
- If data fails criteria, the firewall blocks the traffic and issues a warning.
- Logs all incoming/outgoing traffic.
- Criteria can be set to prevent access to certain websites; this can be done by the firewall keeping a list of all undesirable IP addresses.
- Firewalls CAN help to prevent viruses or hackers entering a user’s computer.
- Warns the user if some software on their system tries to access an external data source (e.g. automatic software upgrade).

Firewalls cannot prevent certain harmful traffic if an individual by-passes the firewall or if employees are careless and divulge passwords etc.

Common errors

- Many students confuse phishing and pharming and assume phishing scams automatically link a user to a fake/bogus website.
- Many students believe backing up data guards against viruses; this is not the case, since the backed-up data may also be infected.
- Students often say ‘viruses damage the computer’ with no mention of the nature of the damage or how it can be caused.

Security protocols

Secure Sockets Layer (SSL)

- Type of protocol (set of rules) used by computers to communicate with each other across a network.
- Allows data to be sent and received securely across a network.
- When a user logs on, SSL encrypts the data.
- User knows if SSL is being applied when they see https or the green padlock 🔒 sign in the status bar.
- When a user wants to access a website, the web browser asks the web server to identify itself; the web server sends a copy of the SSL certificate which the web browser authenticates; if this is OK then SSL-encrypted two-way data transfer begins between user's computer and web server.

Transport Layer Security (TLS)

- TLS is similar to SSL but is more recent and a more effective system.
- TLS is formed of a *record protocol* (contains data being transferred over the internet) and a *handshake protocol* (which permits website and client to authenticate each other and make use of encryption algorithms).
- Only recent web browsers support TLS.
- Makes use of *session caching* which improves the overall performance (here TLS can either start a new session each time a user accesses a website, or it can attempt to resume an earlier/existing session which improves systemperformance).

Encryption

Symmetric encryption

- Utilises a secret key; when the key is applied, the *plain text* (original text) goes through an *encryption algorithm* , to produce *cypher text* (encrypted message).
- The recipient needs a key to then decrypt the message back into plain text.
- The main risk is that both sender and recipient need the same key which could be hacked or intercepted allowing a third party to decrypt the sent encrypted message.

Asymmetric encryption

- Asymmetric encryption uses *public keys* and *private keys*.
- Public key is available to everybody; private key is known only to computer user; both are needed to encrypt and decrypt messages.
- Encryption keys are generated by a *hashing algorithm* – this translates the message or key into a string of characters often shown in hex notation; an example is MD4 which generates a 128-bit string (the greater the number of bits, the harder it is to 'crack' the encryption).

Authentication

- Used to verify that data comes from a trusted source.
- Makes use of passwords, digital signatures and/or biometrics.

Denial of service attacks

- Denial of service is an attempt at preventing users from accessing part of a network, notably internet servers.
- Can prevent users from accessing their emails, accessing certain websites or accessing online services.
- This is achieved by the attacker flooding the network with useless traffic; for example, sending out thousands of requests to a website or sending out thousands of spam emails to users, ‘clogging it up’.
- Can be mitigated against by:
  - using an up-to-date virus checker
  - using a firewall to restrict traffic
  - using email filters
  - looking out for signs (e.g. slow network performance, increase in spam or inabilityto access certain websites).

Ethics

- Ethics is a set of principles set out to regulate use of computers; three factors are considered:
  - intellectual property rights (e.g. copying software without permission)
  - privacy issues (e.g. hacking or any illegal access to a computer)
  - effect of computers on society (e.g. job losses, social impacts, and so on).
- A code of ethics is published by the ACM and IEEEC (see the Student’s Book for a list of theten codes).

Free software

Users have the freedom to run, copy, change or adopt *free software* . There are rules, however, that need to be obeyed:

- Cannot add source code except fromsoftware which is also free software.
- Cannot produce any software which copies existing software that is subject to copyrightlaws.
- Cannot alter the source code so that it infringes any copyright that protects other software.
- May not produce software that is possibly offensive.

Freeware

Software that a user can download free of charge. There are no fees associated with the software (e.g. Adobe or Skype) but they are subject to copyright laws and the user is often asked to tick a box to say they understand and agree to the terms and conditions governing the software.

Shareware

Users are allowed to try out shareware free for a trial period. At the end of this period, the user will be requested to pay a fee. Very often, the trial version doesn’t have all the features of the full version
– all the features become available once the fee is paid.

Common errors

- Many students don’t realise loss of data doesn’t have to be a malicious act, it can be due to an error or not following correct procedure.
- Students often claim that firewalls ALWAYS protect against viruses and hackers – this is not the case.
- Students often confuse free software, freeware and shareware.