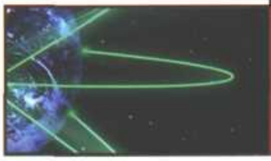
UNIT 18



Data Security 1

STARTER

1 What stories do you think followed these headlines? Compare answers within your group.

1 Love bug creates worldwide chaos.
2 Hackers crack Microsoft software codes.
3 Web phone scam.

2 What other types of computer crime are there? Make a list within your group.

READING

3 Study this diagram which explains how one type of virus operates. Try to answer these questions.

1 What is the function of the Jump instruction?
2 What are the main parts of the virus code?
3 What is the last act of the virus?

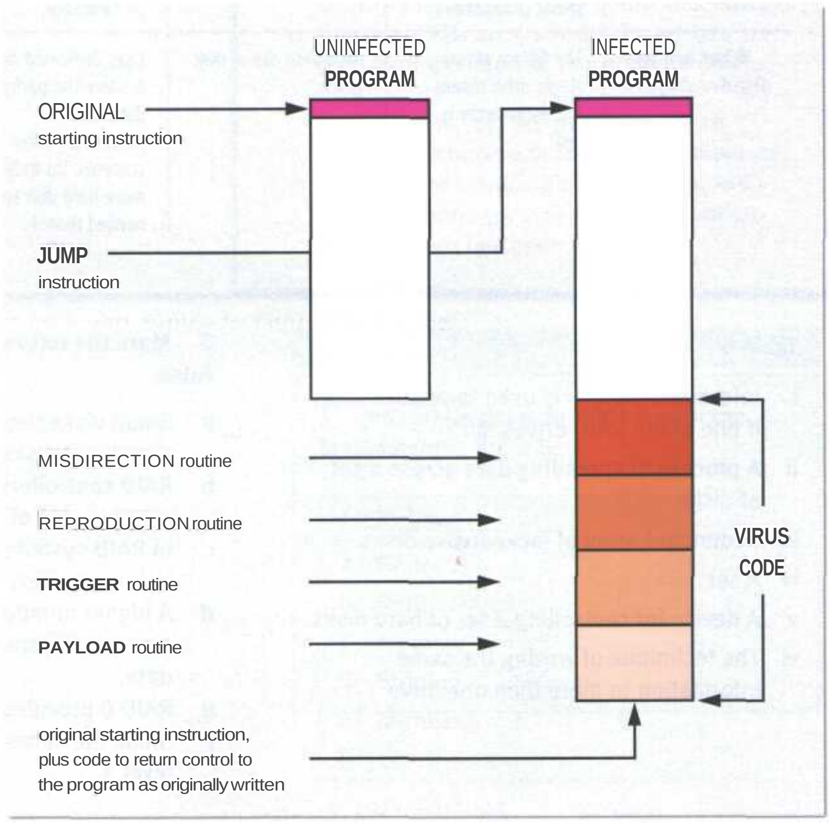


Fig 1
How a virus infects a program

4 Scan this text to check your answers to Task 3. Ignore any parts which do not help you with this task.

THE ANATOMY *OF* A VIRUS

A biological virus is a very small, simple organism that infects living cells, known as the host, by attaching itself to them and using them to reproduce itself. This often causes harm to the host cells.

Similarly, a computer virus is a very small program routine that infects a computer system and uses its resources to reproduce itself. It often does this by patching the operating system to enable it to detect program files, such as COM or EXE files. It then copies itself into those files. This sometimes causes harm to the host computer system.

When the user runs an infected program, it is loaded into memory carrying the virus. The virus uses a common programming technique to stay resident in memory. It can then use a reproduction routine to infect other programs. This process continues until the computer is switched off.

The virus may also contain a payload that remains dormant until a trigger event activates it, such as the user pressing a particular key. The payload can have a variety of forms. It might do something relatively harmless such as displaying a message on the monitor screen or it might do something more destructive such as deleting files on the hard disk.

When it infects a file, the virus replaces the first instruction in the host program with a command that changes the normal execution sequence. This type of command is known as a JUMP command and causes the virus instructions to be executed before the host program. The virus then returns control to the host program which then continues with its normal sequence of instructions and is executed in the normal way.

To be a virus, a program only needs to have a reproduction routine that enables it to infect other programs. Viruses can, however, have four main parts. A misdirection routine that enables it to hide itself; a reproduction routine that allows it to copy itself to other programs; a trigger that causes the payload to be activated at a particular time or when a particular event takes place; and a payload that may be a fairly harmless joke or may be very destructive. A program that has a payload but does not have a reproduction routine is known as a Trojan.

5 Now read the whole text to find the answers to these questions.

1 How are computer viruses like biological viruses?

2 What is the effect of a virus patching the operating system?

3 Why are some viruses designed to be loaded into memory?

4 What examples of payload does the writer provide?

5 What kind of programs do viruses often attach to?

6 Match each virus routine to its function.

Routine	Function
1 misdirection	a does the damage
2 reproduction	b attaches a copy of itself to another program
3 trigger	c hides the presence of the code
4 payload	d decides when and how to activate the payload

7 How does a Trojan differ from a virus?

LANGUAGE WORK Cause and effect (1)

What is the relationship between these actions?

1 A date or event occurs.
2 The trigger routine runs.
3 The payload routine activates.
4 The hard disk is wiped.

These events form part of a cause and effect chain. We can describe the links between each event in a number of ways:

Using *cause* + *to* V or *make* + V.

1 A date or event occurs which *causes* the trigger routine to *run.*

2 A date or event occurs which *makes* the trigger routine *run.*

Putting the events in sequence and using a causative verb.

3 The trigger routine runs, which *activates* the payload routine.

Using a *when* clause.

4 *When the trigger routine runs,* the payload routine activates.

6 Describe the effects of these viruses and other destructive programs.

1 logic bomb-example
a A dismissed employee's name is deleted from the company's payroll.
b A logic bomb is activated.
c All payroll records are destroyed.

2 *Form* (Boot sector virus)
a A certain date occurs.
b A trigger routine is activated.
c Keys beep when pressed and floppies are corrupted.

3 *Beijing* (Boot sector virus)
a The operator starts up the computer for the one hundred and twenty-ninth time.
b A trigger routine is activated.
c The screen displays, 'Bloody! June 4,1989'.

4 *AntiEXE*
a The infected program is run.
b The boot sector is corrupted.
c The disk content is overwritten.
d Data is lost.

5 *Cascade* (File virus - COM files only)

a A particular date occurs.
b The payload is triggered.
c Characters on a text mode screen slide down to the bottom.

6 macro virus-example

a An infected document is opened in the word processor.
b The virus macro is executed.
c The virus code is attached to the default template.
d The user saves another document.
e The virus code attaches to the saved document.
f The saved document is opened in the wordprocessor.
g The virus destroys data, displays a message or plays music.

7 Some verbs beginning or ending with *en* have a causative meaning. Replace the words in italics in these sentences with the appropriate form *of en* verb from this list.

enable
encode
encourage
encrypt
enhance
enlarge
ensure
brighten
widen

1 A MIDI message *makes* sound *into code* as 8-bit bytes of digital information.

2 The teacher is using a new program to *give courage to* children to write stories.

3 The new version of SimCity has been *made better* in many ways.

4 A gateway *makes it possible for* dissimilar networks to communicate.

5 You can *convert* data *to secret code* to make it secure.

6 *Make sure* the machine is disconnected before you remove the case.

7 Designers can offer good ideas for *making* your website *brighter.*

8 Electronic readers allow you to *make* the print size *larger.*

9 Programmers write software which *makes* the computer *able* to carry out particular tasks.

10 You can *make* the picture on your monitor *wider.*

PROBLEM-SOLVING 8

Decide in your group what these kinds of computer crime are. Then match the crimes to the short descriptions which follow.

1 Salami Shaving
2 Denial of Service attack
3 Trojan Horse
4 Trapdoors
5 Mail bombing
6 Software Piracy
7 Piggybacking
8 Spoofing
9 Defacing
10 Hijacking

a Leaving, within a completed program, an illicit program that allows unauthorised - and unknown - entry.

b Using another person's identification code or using that person's files before he or she has logged off.

c Adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. In other words, it appears to do something useful but actually does something destructive in the background.

d Tricking a user into revealing confidential information such as an access code or a credit-card number.

e Inundating an email address with thousands of messages, thereby slowing or even crashing the server.

f Manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere. The victims are often unaware of the crime because the amount taken from any individual is so small.

g Unauthorised copying of a program for sale or distributing to other users.

h Swamping a server with large numbers of requests.

i Redirecting anyone trying to visit a certain site elsewhere.

j Changing the information shown on another person's website.

SPEAKING 9

Work in pairs, A and B. You both have details of a recent computer crime. Find out from your partner how his/her crime operated and its effects. Take notes of each stage in the process.

Student A Your computer crime is on page 187.
Student B Your computer crime is on page 193.

WRITING 10

Using your notes from Task 9, write an explanation of the computer crime described by your partner. When you have finished, compare your explanation with your partner's details on page 187 or 193.

WHEN YOU HAVE FINISHED THE READING SECTION ON THE FOLLOWING PAGES, COME BACK TO THESE ADDITIONAL EXERCISES

3 Mark each of the following statements with True or False:

a A message encrypted with a public key can be decrypted by anyone.
b To send a secure message you must know the recipient's public key.
c Secure messages are normally encrypted using a private key before they are sent.
d A message can be reconstructed from its MAC.
e Two message can often have the same MAC.
f A digital certificate is sent to a client in an encrypted form.
g A digital certificate should be signed by a trusted digital-certificate issuer.
h A MAC is used to check that a message has not been tampered with.

4 Put the following sentences, about sending a secure email, in the correct order:

a The message is decrypted with the recipient's private key.
b The message is received by the recipient.
c The message is encrypted with the recipient's public key.
d The message is sent by the sender.

SPECIALIST READING

A Flnd the answers to these questions in the following text.

1 What does data encryption provide?
  a privacy
  b integrity
  c authentication
2 A message encrypted with the recipient's public key can only be decrypted with
  a the sender's private key
  b the sender's public key
  c the recipient's private key
3 What system is commonly used for encryption?
4 What is the opposite of 'encrypt'?
5 A message-digest function is used to:
  a authenticate a user
  b create a MAC
  c encrypt a message
6 What information does a digital certificate give to a client?

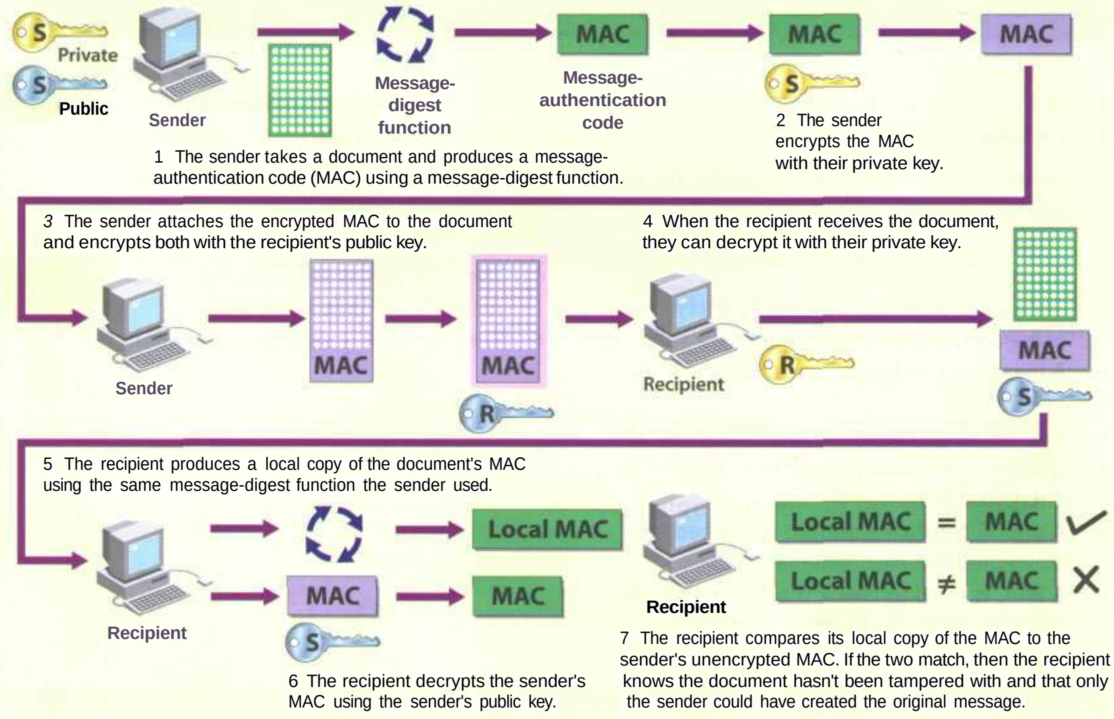
Safe Data Transfer

Secure transactions across the Internet have three goals. First, the two parties engaging in a transaction (say, an email or a business purchase) don't want a third party to be able to read their transmission. Some form of data encryption is necessary to prevent this. Second, the receiver of the message should be able to detect whether someone has tampered with it in transit. This calls for a message-integrity scheme. Finally, both parties must know that they're communicating with each other, not an impostor. This is done with user authentication.

Today's data encryption methods rely on a technique called public-key cryptography. Everyone using a public-key system has a public key and a private key. Messages are encrypted and decrypted with these keys. A message encrypted with your public key can only be decrypted by a system that knows your private key.

For the system to work, two parties engaging in a secure transaction must know each other's public keys. Private keys, however, are closely guarded secrets known only to their owners. When I want to send you an encrypted message,

This shows the complex process that's required to send data securely across open communication lines while satisfying the three basic tenets of secure transfer: data encryption, interference prevention, and user authentification.



1 The sender takes a document and produces a message-authentication code (MAC) using a message-digest function.

2 The sender encrypts the MAC with their private key.

3 The sender attaches the encrypted MAC to the document and encrypts both with the recipient's public key.

4 When the recipient receives the document, they can decrypt it with their private key.

5 The recipient produces a local copy of the document's MAC using the same message-digest function the sender used.

6 The recipient decrypts the sender's MAC using the sender's public key.

7 The recipient compares its local copy of the MAC to the sender's unencrypted MAC. If the two match, then the recipient knows the document hasn't been tampered with and that only the sender could have created the original message.

I use your public key to turn my message into gibberish. I know that only you can turn the gibberish back into the original message, because only you know your private key. Public-key cryptography also works in reverse - that is, only your public key can decipher your private key's encryption.

To make a message tamper-proof (providing message integrity), the sender runs each message through a message-digest function. This function within an application produces a number called a message-authentication code (MAC). The system works because it's almost impossible for an altered message to have the same MAC as another message. Also, you can't take a MAC and turn it back into the original message.

The software being used for a given exchange produces a MAC for a message before it's encrypted. Next, it encrypts the MAC with the sender's private key. It then encrypts both the message and the encrypted MAC with the recipient's public key and sends the message.

When the recipient gets the message and decrypts it, they also get an encrypted MAC. The software takes the message and runs it through the same message-digest function that the sender used and creates its own MAC. Then it decrypts the sender's MAC. If the two are the same, then the message hasn't been tampered with.

The dynamics of the Web dictate that a user-authentication system must exist. This can be done using digital certificates.

A server authenticates itself to a client by sending an unencrypted ASCII-based digital certificate. A digital certificate contains information about the company operating the server, including the server's public key. The digital certificate is 'signed' by a trusted digital-certificate issuer, which means that the issuer has investigated the company operating the server and believes it to be legitimate. If the client trusts the issuer, then it can trust the server. The issuer 'signs' the certificate by generating a MAC for it, then encrypts the MAC with the issuer's private key. If the client trusts the issuer, then it already knows the issuer's public key.

The dynamics and standards of secure transactions will change, but the three basic tenets of secure transactions will remain the same. If you understand the basics, then you're already three steps ahead of everyone else.

[Jeff Downey, 'Power User Tutor', PC Magazine, August 1998]

B Re-read the text to find the answers to these questions.

1 Match the functions in Table 1 with the keys in Table 2.

Table 1	
a	to encrypt a message for sending
b	to decrypt a received message
c	to encrypt the MAC of a message
d	to encrypt the MAC of a digital signature

Table 2	
i	sender's private key
ii	trusted issuer's private key
iii	the recipient's private key
iv	the recipient's public key

2 Match the terms in Table A with the statements in Table B.

Table A	
a	Gibberish
b	Impostor
c	Decipher
d	MAC
e	Tenets
f	Tamper

Table B	
i	Message-authentication code
ii	Principal features
iii	Meaningless data
iv	Person pretending to be someone else
v	Make unauthorised changes
vi	Convert to meaningful data

▶ Additional exercises on page 129