DATA SECURITY I

Oral task: Computer Crimes.

Preventions

Encryption /Decryption.

Prevention .

Reading: Anatomy of a virus.

How a virus infects a program

Grammar: Cause and effect 1

Specialist Reading: Safe Data Transfer

Class Discussion

1. What do we mean by Data security?
2. Is it technically possible for computer criminals to infiltrate into the Internet and steal sensitive information? Explain.
3. What's Cookies?
4. What's Encryption?
5. What's Decryption?
6. Explain the process "How a virus infects a program?
7. Make a list of computer crime.
8. What's a backup?
9. What is Firewall?

Reading

Read the text below to find answers to the 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. How does a Trojan differ from a virus?

The ANATOMY OF A VIRUS

A biological virus is 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.

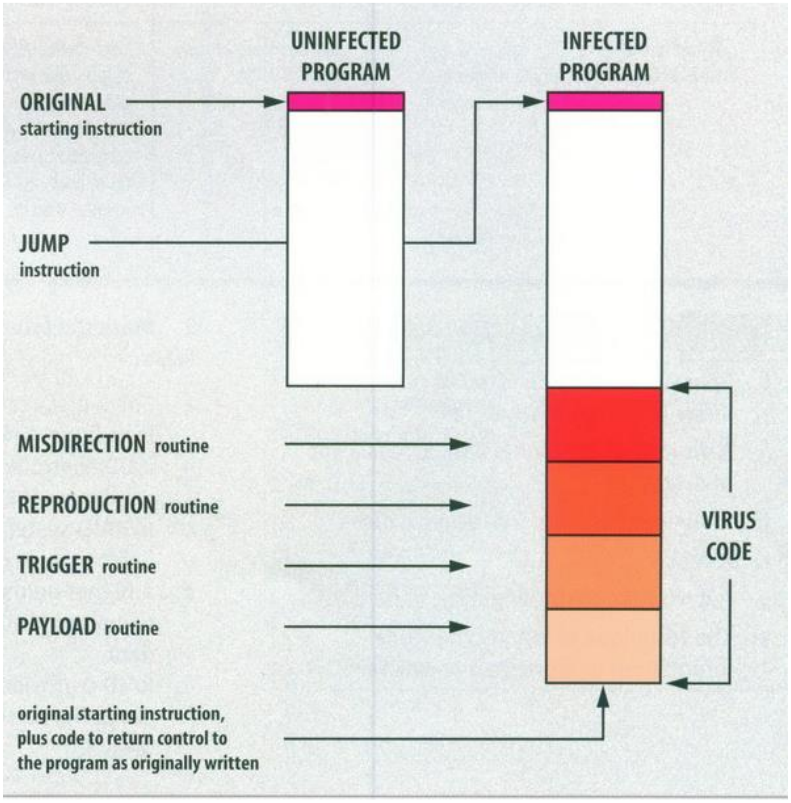
When it infects a file, the virus replaces the first instruction in the host program with a
command that changes the normal execution sequence. This type of command is known as a JUMP command and causes the virus instructions to be executed before the host program. The virus then returns control to the 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 doesn't have a reproduction routine is known as a Trojan.

From : PC magazine

How a virus infects a program.

The following diagram explains how one type of virus operates.



Vocabulary:

Trigger, routine, bug, patching, crack, web phone scam, payload, misdirection, reproduction.

Language work: Cause and effect (1)

Causative verbs are used when someone is causing someone else to do something by forcing, allowing and asking.

Also, the imperative verb form (no subject) is common with causative verbs, since both causatives and imperatives are used for giving orders.

Examples:

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.

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

Using a When clause.

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

Exercise1: Some verbs beginning or ending with 'en' have a causative meaning. Replace the words in *italics* with the appropriate form of 'en' verb from the 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.*

Exercise2: Describe the effects of these viruses and other destructive programs.

1. Anti EXE
   a. The infected program is run.
   b. The boot sector is corrupted.
   c. The disk content is overwritten.
   d. Data is lost.

2. Logic bomb
   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.

3. 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.

Specialist Reading

Safe Data Transfer

A **Find the answers to these questions in the following text.**

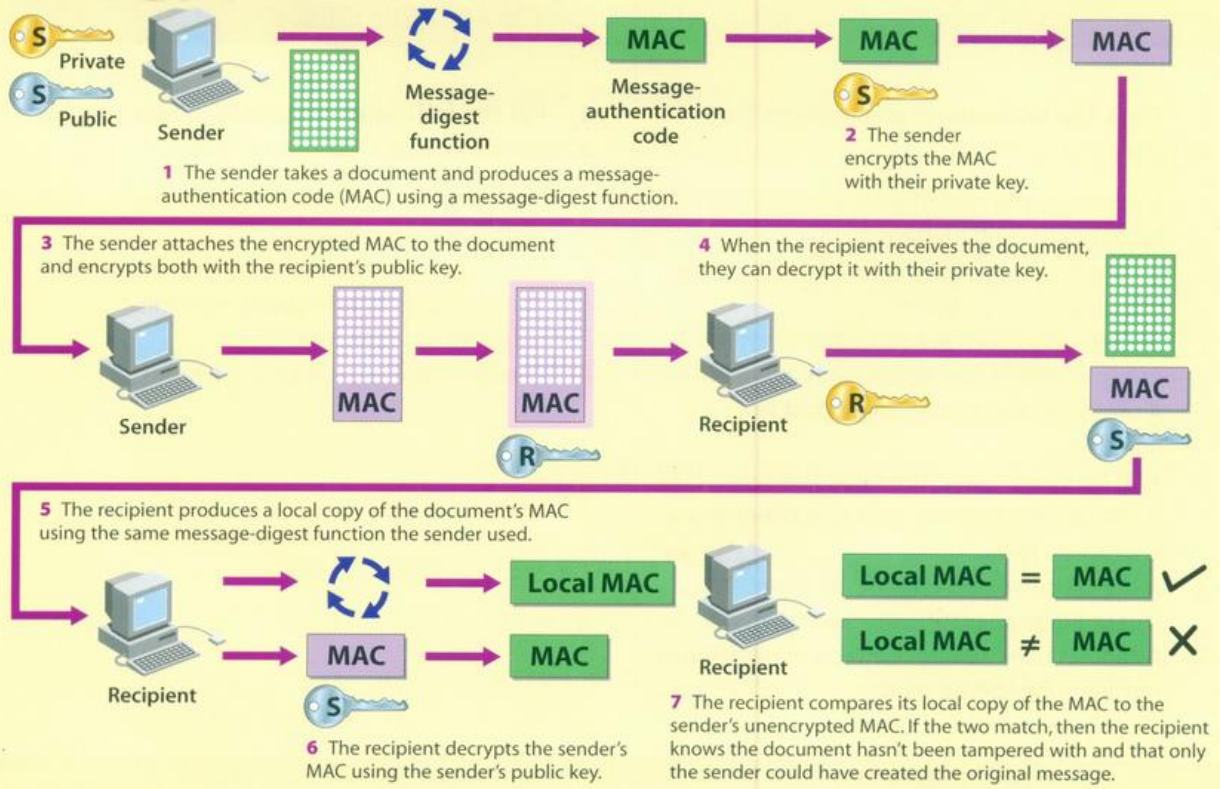
1 What does data encryption provide?
   a privacy
   b integrity
   c authentication
2 A message encrypted with the recipient's public key can only be decrypted with:
   a the sender's private key
   b the sender's public key
   c the recipient's private key
3 What system is commonly used for encryption?
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?

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.



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.

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

'Power User Tutor', PC magazine

Extracted from: ***Oxford English For Information Technology.***