Name …...ID …............................... Section …........Seat No..........

Sirindhorn International Institute of Technology
Thammasat University

Final Examination Answers: Semester 2/2008

Course Title : CSS322 Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Thursday 5 March 2009, 9:00 to 12:00

Instructions:

- This examination paper has 19 pages (including this page).
- Condition of Examination
  Closed book
  No dictionary
  Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.

Multiple Choice Questions [18 marks]

Select the most accurate answer. Select only one answer. Each question is worth 1.5 marks. You will receive 0 marks for a wrong answer.

1. What function can be used to convert a hash function into a MAC function?

   a) MD5

   b) SHA1

   c) HMAC

   d) Triple DES

   e) RSA

   f) None of the above

2. Assume a user had a 10-character password. Which would you consider the strongest against a dictionary attack?

   a) Random characters

   b) Combination of two English words

   c) Pronounceable string (without dictionary words)

   d) Combination of names of people

   e) Words with a mixture of upper and lower case characters

   f) Words combined with numbers and special characters

3. If Transport Layer Security is used to secure data (e.g. web pages) between a client and server, TLS uses:

   a) Public key algorithms for data confidentiality and MD5 or SHA1 for data integrity

   b) Symmetric key algorithms for key exchange and message authentication codes for authentication

   c) Message authentication codes for data integrity and symmetric key algorithms for data confidentiality

   d) Public key algorithms for key exchange and Diffie-Hellman for data integrity

   e) None of the above

4. Which technology is most appropriate to create a VPN?

   a) TLS

   b) IPsec

   c) DDoS

   d) SSH

   e) RSA

   f) None of the above

5. A computer virus:

   a) Is host independent

   b) Is non-replicating

   c) **Goes through the phases of being dormant, propagating, triggering and execution.**

   d) Is a program that searches for other systems to infect, connects to a remote system and copies itself to that remote system and executes.

   e) Is a program modification that contains unauthorized access to functionality

   f) Is none of the above.

6. Software the replicates itself and sends the copies to other computers is best described as a:

   a) Logic bomb

   b) Trojan horse

   c) Rootkit

   d) Exploit

   e) Worm

   f) Backdoor

7. A malicious user in a buffer overflow attack aims to:

   a) Overwrite the existing instruction pointer with malicious code

   b) Overwrite the existing instruction pointer with NOP instructions

   c) Overwrite the existing instruction pointer with a new instruction pointer

   d) Overwrite the program stack with the malicious code

   e) Overwrite the program stack with NOP instructions

   f) Overwrite the program stack with a new instruction pointer

8. Consider a passwords file on a computer system:

   a) The entire file must be encrypted

   b) The individual passwords in the file must be in plaintext

   c) No two users can have the same password

   d) The file must not be readable by administrator users

   e) The number of attempts to read the file must be limited

   f) **None of the above**

9. What standard is used to describe digital certificates?

   a) X.509

   b) IPsec

   c) TLS

   d) IETF

   e) MD5

   f) RSA

10. Which of the following cannot be used to provide authentication?

   a) DES

b) RSA

c) MD5

d) SHA-1

e) AES

f) None of the above

11. To allow confidential access to web sites using HTTPS, web browsers most often use:

a) IPsec

b) TLS

c) MD5

d) SSH

e) SHA-1

f) None of the above

12. Using symmetric key encryption to successfully provide authentication relies upon:

a) The sender encrypting with a private key

b) The sender encrypting with a public key

c) The sender sending an encrypted copy of the shared secret key

d) The recipient being able to identify messages encrypted with the wrong key

e) The recipient being able to make their shared secret key public

f) The recipient being able to perform a hash operation on the received ciphertext

General Questions [82 marks]

Question 1 [14 marks]

Consider the diagram below where a packet filtering firewall (FW1) is running on router R2. The "internal" networks are on the left of the firewall (that is, connected to interface 1 of router R2). Each IP network is identified by a letter (e.g. "Network A"), and each host on a particular network is identified by a number (e.g. "Host A.4"). You can refer to "any" value using * (e.g. "A.*" meaning all hosts on network A). Note that although only several hosts are shown in the figure, you must assume there may be more hosts than shown in each network.

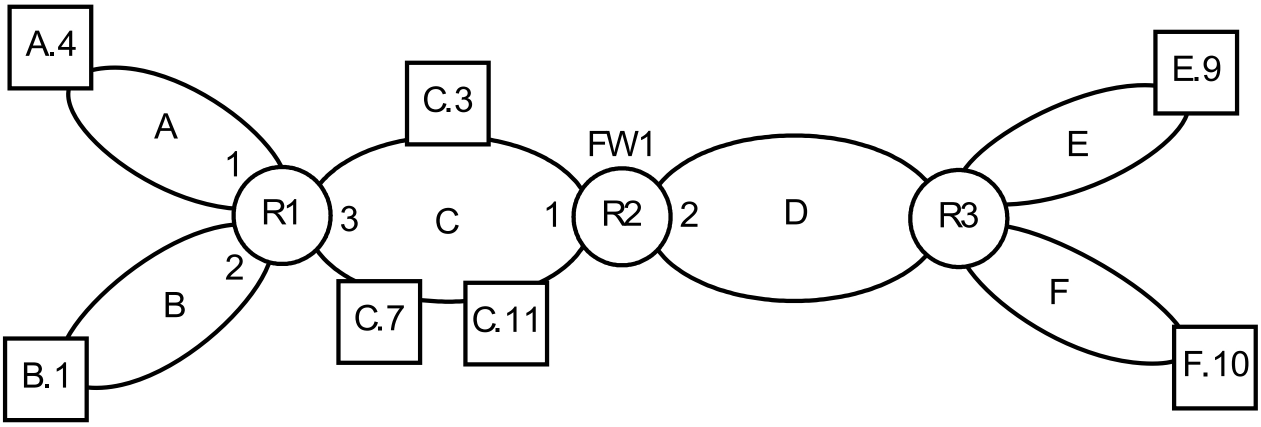


Figure 1: Firewall Network

For the following scenarios, complete the necessary firewall rules in the table provided. You do not have to use all table rows, and you can add more rows if necessary. You must use the correct values in the table (e.g. "*" or "A.4" or "A.*" are valid addresses; a written description is not valid). The default policy in all cases is DROP. Treat each part independent of other parts. All application protocols in this question use TCP. The interface numbers are written next to the router in the above figure. Assume Stateful Packet Inspection (SPI) is used.

a) Allow all internal hosts to connect to all web servers. [2 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	*	*	*	80	TCP	Allow

b) Allow all hosts on network F to connect to the secure shell (SSH) server on C.7. [2 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
2	F.*	*	C.7	22	TCP	Allow

c) Allow all hosts on network C, except the two servers (C.3 and C.7), to connect to all email servers. [3 marks]

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Answer

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	C.3	*	*	25	TCP	Drop
1	C.7	*	*	25	TCP	Drop
1	C.*	*	*	25	TCP	Allow

Assume the firewall table contains all rules as you created in the previous parts and the SPI table is initially empty.

d) Complete the SPI table after the following connections have been established or blocked. [2 marks]

- Web browser with port 4031 on Host A.4 has initiated a connection to the web server on E.9.
- Client with port 5506 on Host F.10 has initiated a connection to the SSH server on C.7.

Initiator IP	Initiator Port	Responder IP	Responder Port

Answer

Initiator IP	Initiator Port	Responder IP	Responder Port

A.4	4031	E.9	80
F.10	5506	C.7	22

Assume a second packet filtering firewall (FW2) is installed on router R1 to create a Demilitiarised Zone (DMZ) in network C. An application-level firewall that acts as a proxy for web and email traffic is installed on C.11. Other traffic (that is not web or email) is not allowed. Assume the firewall entries from the previous parts are deleted (that is, the firewall and SPI tables are empty).

e) Complete the firewall tables for both firewalls so that the traffic cannot bypass the application-level firewall. [5 marks]

Firewall FW1:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Firewall FW2:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action

Answer

Firewall FW1:

Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	C.11	*	*	80	TCP	Allow
1	C.11	*	*	25	TCP	Allow
2	*	80	C.11	*	TCP	Allow
2	*	25	C.11	*	TCP	Allow

Firewall FW2:

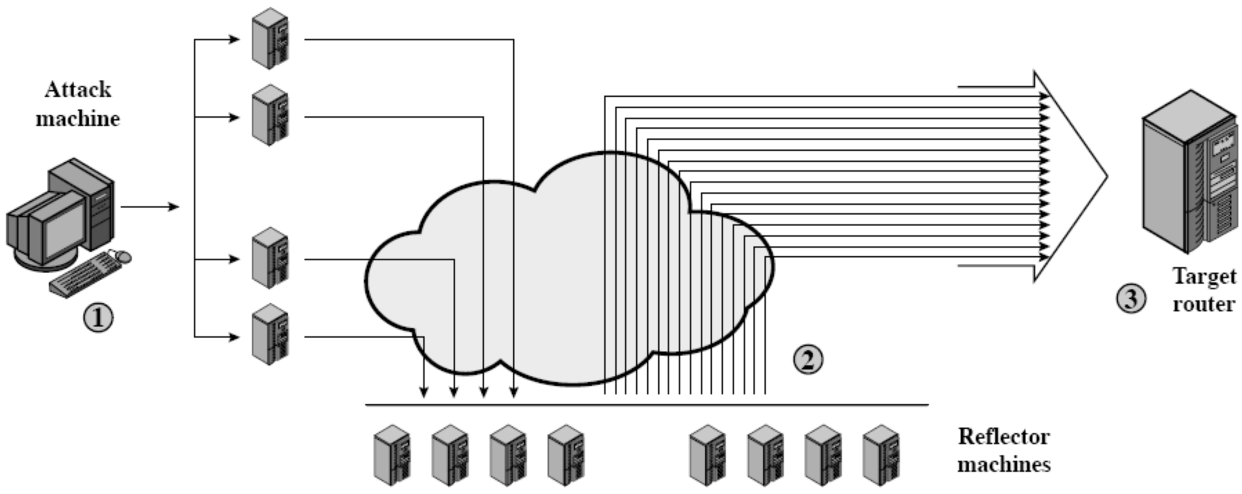
Interface	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	*	*	C.11	80	TCP	Allow
1	*	*	C.11	25	TCP	Allow
2	*	*	C.11	80	TCP	Allow
2	*	*	C.11	25	TCP	Allow
3	C.11	80	*	*	TCP	Allow
3	C.11	25	*	*	TCP	Allow

Alternatively, you could rely on SPI to create the last two rows of each table.

Question 2 [13 marks]

a) Draw a diagram that illustrates an ICMP Ping distributed denial of service attack. Show (and label) the nodes involved (including Attacker, Slaves, Reflectors and Target), the direction of messages and the types of messages. [4 marks]

Answer



b) Of the nodes involved in the ICMP attack, which nodes are controlled (or infected) by the malicious user? [1 mark]

Answer

Attack machine and Slave nodes.

c) In the ICMP attack, what will the values of the IP source and destination addresses be for ECHO Request and ECHO Reply messages? (Do not give specific IP address, instead refer to the types of nodes in the network) [2 marks]

ECHO Request - Source IP Address

ECHO Request - Destination IP Address

ECHO Reply - Source IP Address

ECHO Reply - Destination IP Address

Answer

Request Source: Target

Request Dest.: Reflectors

Reply Source: Reflectors

Reply Dest.: Target

d) A DoS makes a system (network and/or computers) unavailable for normal users to use. Explain how the ICMP attack achieves this, including what does it make "unavailable". [2 marks]

Answer

The ICMP attack uses up network capacity leading up to the Target (or the network of the Target), thereby making that network capacity unavailable. In addition, the processing of ICMP ECHO replies may use up processing (CPU) capacity of the Target, making that host unavailable.

e) Explain the difference between a *direct* DDoS attack and a *reflector* DDoS attack. [2 marks]

Answer

A direct DDoS attack involves hosts under the control of the attacker directly performing an attack (by sending messages) on a target. A reflector DDoS attack involves hosts under control sending messages to uncontrolled (normal) hosts in the network, that then perform an attack on the target.

f) State two advantages of a reflector DDoS attack (compared to direct DDoS attack). [2 marks]

Answer

1. Potential of many more nodes participating in the attack, since the attacker can use uninfected nodes.

2. Harder for target to identify the attacker because traffic comes from many random uninfected nodes.

Question 3 [10 marks]

a) Describe the one-way property of hash functions. [2 marks]

Answer

Computationally hard to compute the inverse of a hash function, i.e. to determine the original emssage, given only the hash value. If H(X) = A, then hard to compute $H^{-1}(A)$ to obtain X.

b) Describe the weak collision resistance property of hash functions. [2 marks]

Answer

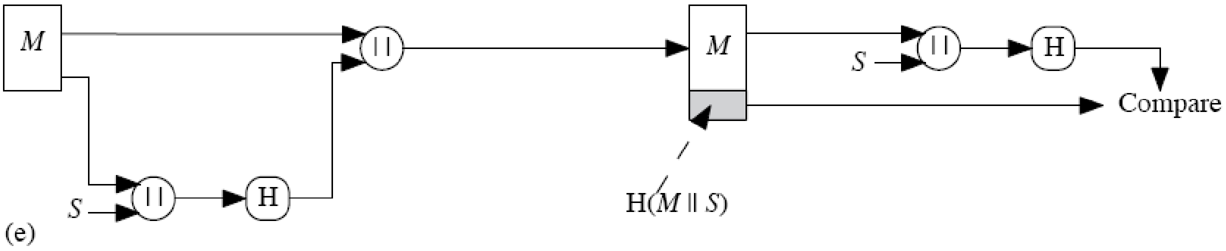
Given a message X and its hash value A (H(X) = A), computationally hard to find another message Y such that H(X) = H(Y) = A.

c) Describe the strong collision resistance property of hash functions. [2 marks]

Answer

Computationally hard to find two messages, X and Y, such that their hash values are the same, i.e. H(X) = H(Y).

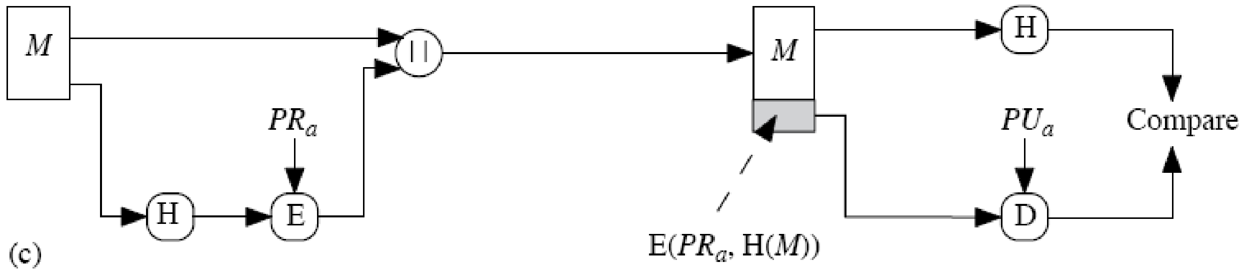
d) The following figure shows a technique for authentication. M is a message and S is a shared secret. Explain the problem in this scheme if the hash function does not have the one-way property (that is, what could a malicious user do and how could they do it?) [2 marks]



Answer

If the one way property does not hold then an attacker that intercepts the message and hash value can determine the value of M || S. Given also M, the attacker can determine S, which is supposed to be a secret (not known to the attacker).

e) The following figure shows a technique for authentication. M is a message sent by node a. Explain the problem in this scheme if the hash function does not have the weak collision resistance property (that is, what could a malicious user do and how could they do it?) . [2 marks]



(c)

Answer

An attacker could intercept the message and signature, find another message Y and forward the modified message Y with the original signature (unmodified bits). The receiver would compare the H(Y) and the received H(M), find they are the same and not detect the modification.

Question 4 [8 marks]

a) User A wants to digitally sign a document M and send it to B. Give a function that describes how the signing is performed (you must also describe all variables used) and explain what is sent from A to B. [3 marks]

Answer

Signature = E(PR_A,M) where PR_A is the private key of A

The signature and M are sent to B (e.g. concatenated together).

b) User A wants to send a MAC authenticated message M to B. Give a function that describes how the authentication data is generated (you must also describe all variables used) and explain what is sent from A to B. [3 marks]

Answer

MACdata = MAC(S,M) where S is a shared secret key with B.

The MAC data and M are sent to B (e.g. concatenated together).

c) Explain why MAC-based authentication cannot be used as a digital signature. [2 marks]

Answer

A MAC function uses a shared secret key. A message authenticated with a MAC function confirms that the message was generated by either the of the parties that has the secret. It does not confirm which of the two parties generated the message (which is the purpose of a digital signature).

Question 5 [7 marks]

Three important parts of a digital certificate for a user are the identity of that user (ID_{user}), the public key of the user (PU_{user}) and the signature of the authority (S_{auth}). Together, a digital certificate may be shown as $C_{user} = <ID_{user}, PU_{user}, S_{auth}>$. Note that a certificate authority may sign its own certificate (C_{auth}) and whenever a user obtains their certificate (C_{user}) from the authority, the user also obtains the authorities certificate (C_{auth}). All public keys are stored/transmitted in certificates.

Consider a hierarchical scheme where user A obtains its certificate from authority X, user B obtains its certificate from authority Y, and both X and Y obtain their certificates from authority Z.

a) Assuming every node has its own certificate, in the initial state, complete the list of *other* certificates that each node has. (The list already contains each nodes own certificate) [2.5 marks]:

User A:	C_A,
User B:	C_B,
Authority X:	C_X,
Authority Y:	C_Y,
Authority Z:	C_Z,

Answer

Each user has the certificate of its authority, and each authority has the certificates of its users.

User A:	C_A, C_X
User B:	C_B, C_Y
Authority X:	C_X, C_Z, C_A
Authority Y:	C_Y, C_Z, C_B
Authority Z:	C_Z, C_X, C_Y

User A has sent its certificate, C_A, to user B.

b) Explain why user B cannot immediately validate the certificate of A. [1.5 marks]

Answer

C_A is signed by authority X. B does not have the public key (certificate) of X to validate the signature.

c) Explain the steps taken for the certificate to be validated by user B, including the exchange of any additional certificates between nodes. [3 marks]

Answer

B sends a request to its authority, Y, requesting the certificate of X. Y sends a request to its authority Z, requesting the certificate X. Z sends the certificate of X to Y, which then sends it on to B. B can then validate the signature of X.

Question 6 [15 marks]

Figure 2 shows an IP network with 3 hosts in a subnet connected to router R1 and two hosts in a subnet connected to router R7. Refer to IP addresses of nodes by their name, e.g. H1 or R1 (note that although in practice a router will have at least two IP addresses, you can use its name to refer to either address).

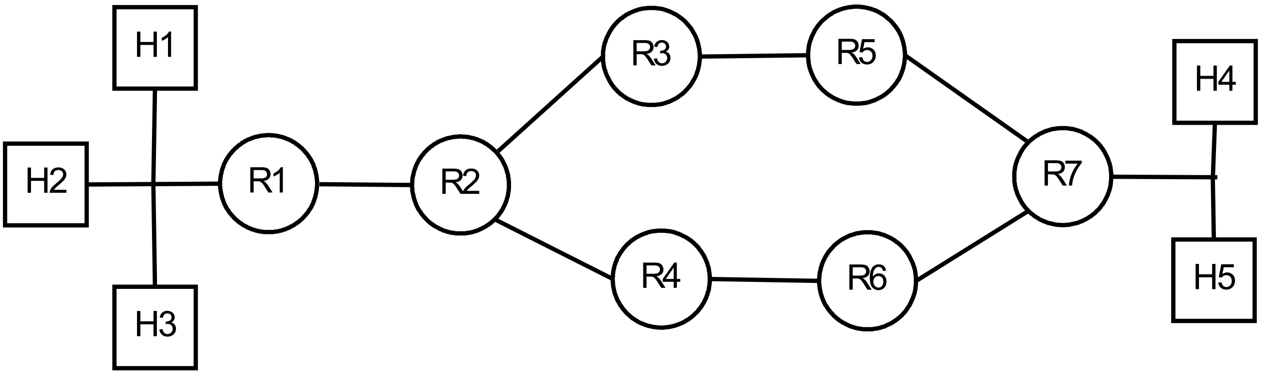


Figure 2: Network Topology

In parts (a) to (d), assume IPsec in transport mode (with Encapsulating Security Payload) is used by all hosts for any data transfer. Host H1 is sending data, using IPsec, to H5. The application protocol is called APP, which uses TCP as a transport protocol. Packets are routed via R4 and R6.

a) Draw the structure of the packet sent by H1. Show all headers/trailers, and for any IP headers, indicate the source and destination addresses. [3 marks]

Answer

IP IPsec TCP APP IPsec

IP Source = H1

IP Destination = H5

b) If a malicious user with access to router R4 intercepts the packet, can the malicious user determine the destination host? Explain your answer [1 mark]

Answer

Yes. The IP header is sent in the clear (unencrypted) and hence the malicious user can identify the IP address of the host H5.

c) Can the malicious user determine the application protocol in use? Explain your answer [1 mark]

Answer

No. The Application layer header and data is encrypted, as is TCP header, so the malicious user cannot identify what is inside the IP datagram.

d) If the malicious user modifies the IP source address in the packet, will host H5 detect the modification? Explain your answer. [1 mark]

Answer

Yes. The authentication is applied across the static fields of the IP header, and hence any changes can be detected.

In parts (e) to (h), assume IPsec in tunnelling mode (with Encapsulating Security Payload) is used, where the tunnel end points are routers R2 and R7. Host H1 is sending data to H5. The application protocol is called APP, which uses TCP as a transport protocol. Packets are routed via R4 and R6.

e) Draw the structure of the packet sent by H1. Show all headers/trailers, and for any IP headers, indicate the source and destination addresses. [2 marks]

Answer

IP TCP APP

IP Source = H1

IP Destination = H5

f) Draw the packet structure of the packet received by router R4. Show all headers/trailers, and for any IP headers, indicate the source and destination addresses. [3 marks]

Answer

IPnew IPsec IPold TCP APP IPsec

IPnew Source = R2

IPnew Destination = R7

IP Source = H1

IP Destination = H5

g) Can the malicious user determine the destination host? Explain your answer [1 mark]

Answer

No. The inner (original) IP header is encrypted, hiding the IP address of the destination host.

h) Can the malicious user determine the IP subnet from where the packet originated from? Explain your answer. [1 mark]

Answer

No. The malicious user can determine the packet came from router R2, but cannot identify the IP subnet attached to router R1.

i) Describe two advantages of using tunneling mode (versus transport mode) of IPsec. [2 marks]

Answer

IPsec only needs to be configured on routers, not on all PCs; hide the IP addresses of the originating and destination nodes.

Question 7 [15 marks]

Below is the pseudo code of a simple virus.

```
1. program V :=
2. {goto main;
3.       1234567;
4.       subroutine infect-executable :=
5.                {loop:
6.                file := get-random-executable-file;
7.                if (first-line-of-file = 1234567)
8.                         then goto loop
9.                         else prepend V to file; }
10.      subroutine do-damage :=
11.               {whatever damage is to be done}
12.
13.      subroutine trigger-pulled :=
14.               {return true if some condition holds}
15. main: main-program :=
16.      {infect-executable;
17.      if trigger-pulled then do-damage;
18.      goto next;}
19. next:
20.      <original program>
21. }
```

a) If this virus was also a logic bomb, give two examples of conditions for the logic bomb. [2 marks]

Answer

Date/time is a specific value

File exists (or does not exist)

b) Explain the line(s) of code that would implement the logic bomb. [2 marks]

Answer

The subroutine "trigger-pulled" would return true if the the logic bomb conditions were true.

c) How many other files does this virus infect? Explain your answer. [2 marks]

Answer

1. It gets a random executable file (line 6), and if it is not already infected then it infects it. Once it has infected one file, the infect-executable subroutine returns.

2.

d) Will this virus infect a file that is already infected with the virus? Explain your answer. [1 mark]

Answer

No. Each infected file is marked with 1234567, and the virus only infects files without such a marking.

e) Explain why it is relatively easy for anti-virus software to detect such a virus. [2 marks]

Answer

The size of the original program is modified. Therefore, anti-virus software can simply compare the file size of files against the expected file size – if they differ, then potentially they are infected with a virus.

f) Ignoring techniques such as polymorphic and metamorphic viruses, explain how this virus can be improved to avoid detection by anti-virus software. [2 marks]

Answer

The virus can compress the program so that the total size (virus plus program) is the same as the original program size. Then, before executing the original program, the virus can decompress the program.

g) Explain the difference between a worm and a virus. [2 marks]

Answer

A virus involves user interaction (e.g. opening a file) whereas a worm does not. A worm will automatically distribute itself.

h) Explain the difference between a polymorphic virus and a metamorphic virus. [2 marks]

Answer

When a polymorphic virus copies the original virus to create a new virus, the new virus appears different than the original, but functions the same. For a metamorphic virus, the new virus both appears different and functions differently.