Tutorial Letter 202/0/2018

INFORMATION SECURITY

INF4831

Year course

School of Computing

IMPORTANT INFORMATION

Please register on myUnisa, activate your myLife e-mail addresses and make sure that you have regular access to the myUnisa module website, INF4831-18-Y1.

Note: This is an online module and therefore it is available on myUnisa. However, in order to support you in your learning process, we will also send you some study material in printed format.

Define tomorrow.

UNISA university of south africa

CONTENTS

Page

1 Memorandum Assignment 05

2 Assignment 05: Chapters 1 - 13

Long questions – Chapters 1-13

Question 1

1.1 Company A, wants to send a protected tender document to, Company B. Company A wants to ensure that only Company B can open the protected tender and no one else, thus ensuring confidentiality through the use of PKI. Which key would Company A use to send the protected tender document to Company B? (1)

1.2 Company A wants to ensure authenticity when sending the protected tender document to Company B. Which key would Company A use? (1)

1.3 Discuss the five components of a digital signature. (5)

1.4 Explain how a digital signature is created by making use of drawings and describe the process.(6)

[13]

ANSWER

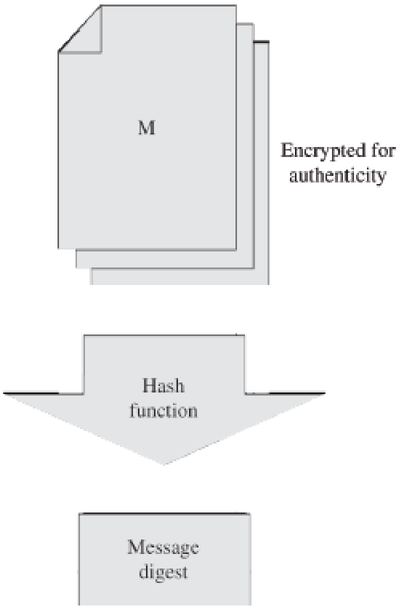
1.1 . Company B's public key (1)

1.2 Company A's private key (1)

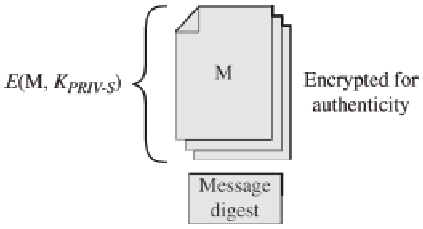
1.3.

- A file,
- demonstration that the file has not been altered,
- indication of who applied the signature,
- validation that the signature is authentic,
- that it belongs to the signer, and
- connection of the signature to the file.

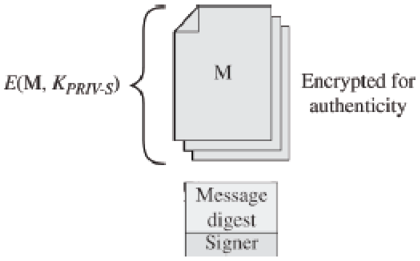
1.4. Start with the file.
If we use a secure hash code of the file to compute a message digest and include that hash code in the signature, the code demonstrates that the file has not been changed. A recipient of the signed file can recomputed the hash function and, if the hash values match, conclude with reasonable trust that the received file is the same one that was signed.



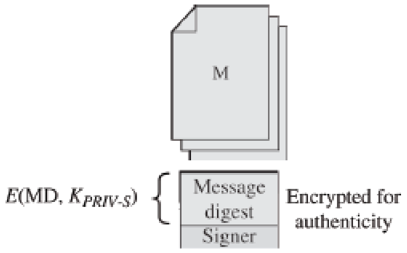
Next, we apply the signer's private encryption key to encrypt the message digest. Because only the signer knows that key, the signer is the only one who could have applied it.



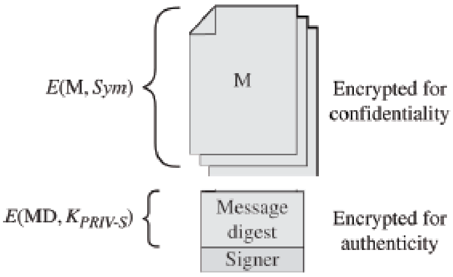
The only other piece to add is an indication of who the signer was, so that the receiver knows which public key to use to unlock the encryption. The signer's identify has to be outside the encryption because if it were inside, the identity could not be extracted.



The secure hash code is also encrypted with the signer's private key to ensure authenticity.



To ensure confidentiality the signer encrypts the message with this symmetric key and stores the key under the receiver's asymmetric public key.
(p.124-126)


$E(M, Sym)$
M
Encrypted for confidentiality
$E(MD, K_{PRIV\text{-}S})$
Message digest
Signer
Encrypted for authenticity

Question 2

THIS IS A SECRET

Encrypt the plain text message above using the two techniques as required by (a) and (b) respectively, one after the other:
a) Use a Caesar Cipher with a shift of TWO, and then,
b) encrypt the resulting ciphertext using a FOUR-column columnar transposition cipher.

Note that you must perform the *Caesar Cipher* on the message, then the *columnar transposition* on the cipher text that is produced from the operation of the Caesar Cipher.

Failure to perform the operations as specified in the correct order, and failure to show your method will result in lower or no marks being awarded.

ANSWER

a) Shift of 2

Plain	a	b	c	d	e	f	g	h	i	j	K	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher	c	d	e	f	g	h	i	j	k	l	M	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b

(2 marks) (If the student made a mistake here, minus the mark here and then give marks for the rest of the steps if the approach is applied correct in the next steps – thus carry the mistake over and only penalise once)

Plain	t	h	i	s	i	s	a	s	e	c	r	e	t
Cipher	v	j	k	u	k	u	c	u	g	e	t	g	V

(2 marks) (If the student made a mistake here, minus the mark here and then give marks for the rest of the steps if the approach is applied correct in the next steps – thus carry the mistake over and only penalise once)

b) Four column columnar transposition

v	j	k	u
k	u	c	u
g	e	t	g
v	x	x	x

(2 marks)

Final answer:

VKGVJUEXKCTXUUGX (1 mark)

[7]

Question 3

There are many ways in which programming can fail and many ways to turn the underlying flaws into security failures. You need to advise the software engineering team to incorporate modularity, coupling, encapsulation, information hiding and mutual suspicion in the design of a new financial system.

Describe to the team what modularity, coupling, encapsulation, information hiding and mutual suspicion respectively are and how they can incorporate it in the design of the new financial system. (2 marks for each concept.)

[10]

ANSWER

1 mark for the concept and 1 mark for defining concept

Modularity: The process of dividing a task into subtasks (1). It is done on a logical or functional basis (1). Each component performs a separate, independent part of the task (1). Each component must meet 4 conditions – single purpose, small, simple, and independent.(1) (Max 2 marks)

Coupling: The degree to which a component depends on other components in the system (1). Thus low or loose coupling is better than high or tight coupling because they loosely coupled components are free from unwitting interference from other components.(1)

Encapsulation: Hides a component's implementation details (1), but it does not necessary mean complete isolation. Many components must share information with other components (1). This sharing is carefully documented so that a component is affected only in know ways by others in the system (1). Sharing is minimised so that the fewest interfaces possible are used (1). Limited interfaces reduce the number of covert channels that can be introduced. (1) (Max 2 marks).

Information hiding: Concealment of information (1). It is desirable because developers can note easily and maliciously alter the components of other if they do not know how the components work.(1)

Mutual suspicion: Describe the relationship between two programs. Mutually suspicious programs operate as if other routines in the system were malicious or incorrect.(1) A calling program cannot trust that its called subroutines are correct. (1)Each protects it interface data so that the other has only limited access. (1)

(p. 203-207)

Question 4

Discuss seven manners in which end users can protect themselves against malicious code. **[7]**

ANSWER

Example answers (consider student's answer)

- Software from reliable, well established vendors
- Test software on an isolated computer
- Only open attachments if you know it is safe
- Install software and other executable files only when you really know them to be safe
- Recognise that any website can potentially be harmful
- Make a recoverable system image and store is safely
- Make and retain backup copies of executable program files

(p. 197-198)

Question 5

5.1 Discuss how each of the following is used to implement operating system security:

a. Virtual machine (2)
b. Honeypot (2)
c. Separation and sharing (2)
d. Hardware protection of memory (2)

ANSWER

a. **Virtual machine** –presenting user just the resources that the user should have. Use of a virtual machine enhances security by preventing a user from accessing resources that they are not authorized to use. (p. 293)

b. **Honeypot** a system designed to lure an attacker into an environment that can be controlled and monitored. Usually deployed in a network, with a limited set of resources, while the administrator can monitor the activities of an attacker in real time to learn more about the attacker's objectives, methods, tools and techniques. The knowledge gained can be used defend systems effectively.
(pp. 295)

c. **Separation and sharing** – Keeping objects separate. d e.g. physical separation, temporal separation, logical separation, and cryptographic separation

d. **Hardware protection of memory** - using both separation and sharing can be achieved in several ways e.g. fence register, base / bounds registers, tagged architecture, segmentation, paging.
(pp. 279-306)

5.2 The principles of secure program design also apply to operating systems. Discuss three principles that must be considered for the secure design of operating systems. (3)

ANSWER

Simplicity of design
Layered design
Layered trust
(p. 309-311)

Or

Least privilege
Economy of mechanism
Open design
Complete mediation
Permission based
Separation of privilege
Least common mechanism
Ease of use
(p. 315-316)

[11]

Question 6

6.1 Inference is a way to infer or derive sensitive data from non-sensitive data. The inference problem is a subtle vulnerability in database security. The indirect attack seeks to infer a final result based on one or more intermediate statistical results.

a) Name three indirect attacks on databases that report statistics. (3)

b) Explain each by giving a relevant example. (3)

ANSWER

Sum: To infer a value from a reported sum. Eg sum student aid by M and F – report show that now female living in is receiving financial aid.

Count: Can be combined with sum to produce some even more revealing results. Table with financial aid can when combined with a count table show that what amount a student is receiving as support – see table 7-8 and 7-9 p 523

Mean: Can show exact disclosure if the attacker can manipulate the subject population. Eg. obtain the mean for all salaries of all employees, then exclude the president salary and compute the mean again – one can the compute the president's salary.

Median: Obtaining a midpoint of an ordered list of values. Using two lists and finding the middle name e.g. Major one might be able to identify the race of the person – fee page 523.

Tracker attack: Using additional queries to produce small results. p. 524.

(p.522-526)

examples
sum - sum student aid by M and F - show that F living in is receiving financial aid
count - combine tables financial aid and count to show what amount student is receiving as aid
mean - obtain mean for all salaries of all employees, excl president salary compute mean again, you can compute president salary
median - use two lists and find middle name eg Major - you can identify race
tracker attack - p524

6.2 Discuss seven security requirements for databases (7)

ANSWER

1. Physical database integrity: Data of a database are immune to physical problems such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.
2. Logical database integrity: The structure of the database is preserved. A modification to the value of one field does not affect other fields.
3. Element integrity: Data contained in each element are accurate.
4. Auditability: Possible to track who or what has accessed elements in a database.
5. Access control: User is allowed to access only authorised data and different users can be restricted to different modes of access.
6. User authentication: Users are positively identified, both for audit trail and for permission to access certain data.
7. Availability: Users can access the database in general and all the data for which they are authorised.

(p. 507)

[13]

Question 7

7.1 Explain what a man-in-the-browser attack is and why it poses a risk to the user. (2)

ANSWER

A man in the browser attack is a Trojan horse that intercepts data passing through the browser.
Code inserted into the browser can read, copy and redistribute anything the user enters in a browser.
The threat is that the hacker can intercept and reuse credentials to access financial systems and other sensitive data.
(p.234-235)

7.2 Banking and other financial transactions are normally protected in transit by an encrypted session, using a protocol named SSL or HTTPS. Explain if SSL or HTTPS can mitigate the risk of a man-in-the-browser attack. (2)

ANSWER

No (1), SSL encryption does not mitigate this risk as the Trojan horse acts as part of the browser where the characters are passed to the browser prior to encryption – thus a timing vulnerability. (1)

(p.235)

7.3 Discuss each of the following security defences against malicious network traffic:

a. Link encryption (1)

b. End to end encryption (1)

c. Browser encryption (1)

d. SSH encryption (1)

e. SSL encryption (1)

f. IPsec (1)

g. VPN (1)

h. firewall (1)

i. Intrusion detection and prevention systems (1)

ANSWER

Does not have to be exact words – consider student's own wording.

a. Link encryption: data are encrypted just before the system places them on the physical communication link. Occur on layer 1 and 2 in OSI. Protects message in transit.

b. End to end encryption: Applied from one end of transmission to next. Between user and host by a hardware device. Can also be done by software running on host computer. Usually at level 7 in OSI, sometimes on 5 or 6.

c. Browser encryption: Browser and server negotiate a common encryption key, during transmission.

d. SSH encryption: Secure shell, pair of protocols providing an authenticated and encrypted path to the shell of operating system command interpreter. (p. 438)

e. SSL encryption: Secure Sockets Layer and upgrade names Transport Layer Security (TLS). Operates between applications and TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communication channel between client and server. (p.438)

f. IPsec: Provides standard means for handling encrypted data. Implements encryption and authentication in Internet protocols. Similar to SSL. (p.444)

g. VPN: Using link encryption, simulates the security of a dedicated, protected communication line on a shared network. (p.447)

h. Firewall: Most important security device for networks. Filters all traffic between a protected or inside network and less trustworthy or outside network. Permits and blocks data flow between two parts of a network architecture. (p.452)

i. Intrusion detection and prevention systems: A device that monitors activity to identify malicious or suspicious events. It monitors users and system activity, provides auditing etc. (p. 476)

[13]

Question 8

8.1 Contrast the packet filtering gateway, application proxy firewall and circuit gateway firewall (3 marks each.) Thus, explain the differences between the three firewalls.(9)

ANSWER

Packet filter gateway	Application proxy firewall	Circuit gateway firewall
Simplest decision-making rules – packet by packet.	Simulates the effect of an application program.	Joins two sub-networks.
Sees only addresses and service protocol type.	Sees and analyses full data portion of pack.	Sees address and data.
Auditing limited because of speed limitations.	Auditing likely.	Auditing likely.
Screens based on connection rules.	Screens based on behaviour of application.	Screens based on address.
Complex addressing rules can make configuration tricky.	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behaviour.	Relatively simple addressing rules; make configuration straightforward

(p. 468)

8.2 Explain how malicious code gains control as part of a compromise by demonstrating it with a figure and including an explanation. (5)

ANSWER

(If students explained the other methods on page 182-183 it can also be marked as correct)

Malicious code such as a virus (V) has to be invoked instead of the target (T).

- The virus can assume the target (T), by replacing T's code in a file structure, Figure A. (The virus can also overwrite T in storage by replacing the copy of T)

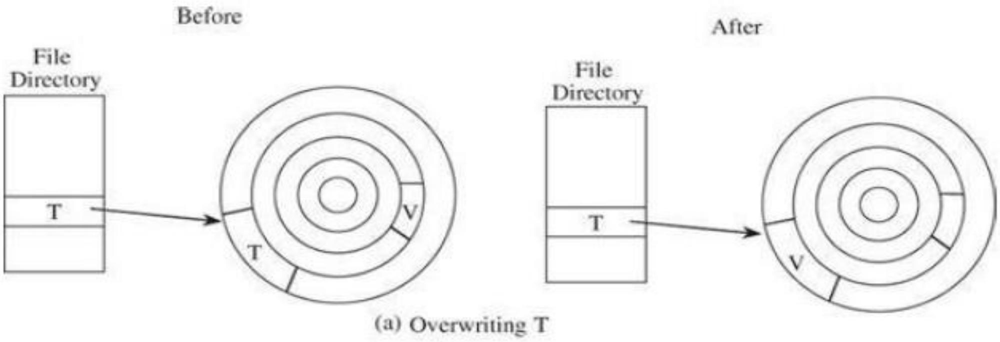


Figure A: Overwriting T (p. 186)

- The virus can also change the pointers in a file table so that the virus is located instead of T when T is accessed through the file system, figure b.

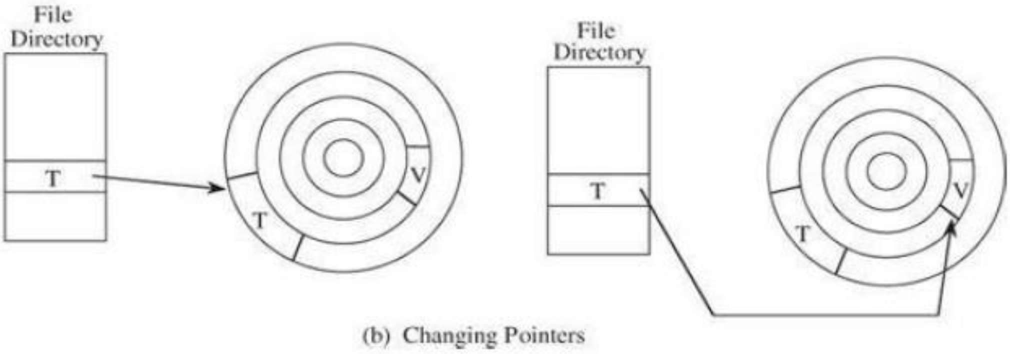


Figure B - Changing Pointers (p. 186)

[14]

Question 9

9.1 While moving data and functionality to the cloud does have its risks. Cloud services can be valuable security tools in a number of ways. You need to motivate/argue to management in your organisation what security benefits there are in moving the organisation's data to a cloud environment. Explain two benefits. (2 marks each.) (4 marks total.)

ANSWER

Example answers – consider student's answers

Geographic diversity: Cloud computing is a cost effective way to diversify geographically to mitigates risks such as natural disasters, fires, internet outages, etc – eliminate single point of failures.

Platform diversity: The cloud provider would probably run different operating systems, applications, and protocols than the organisation. Thus, different vulnerabilities.

Infrastructure diversity: The infrastructure could differ between the client and the service provider e.g. the hardware, network configuration, security controls, quality of security staff, addresses and suppliers.

(p. 557-558)

9.2 Secondly, you need to ensure that management is aware of the security-related issues when considering the cloud environment for the organisation's data storage. Explain to management three security-related issues that they must be aware of when making use of a cloud environment. (2 marks each) (6 marks total.)

ANSWER

- How sensitive is the data that will be stored in the cloud.
- Will data need to be shared with anyone and if so what kinds of access control will be required.
- Are the data subject to export controls or other regulatory requirements
- Discussion of back ups
- Encryption in a public cloud
  (p. 561-562)

[10]

Question 10

10.1 You need to advise management on how to design a business system and supporting processes that will protect the privacy and security of customer data. You decide to use the Fair Information Practice principles as guidance and to enhance it with additional security controls that are used as standard techniques for protecting the privacy of data.

Name and explain each of the Fair Information Practice principles that should be considered when designing the new business system and processes. (Half mark for each principle and half mark for each explanation.) (8 marks total.)

ANSWER

1. Collection limitation (0.5): Data should be obtained lawfully and fairly. (0.5)
2. Data quality (0.5): Data should be relevant to their purposes, accurate, complete and up to date. (0.5)
3. Purpose specification (0.5): The purpose for which data will be used should be identified and that data destroyed if no longer necessary to serve that purpose. (0.5)
4. Use limitation (0.5): Use for purposes other than those specified is authorised only with consent of the data subject or the authority or law. (0.5)
5. Security safeguards (0.5): Procedures to guard against loss, corruption, destruction, or misuse of data should be established. (0.5)
6. Openness (0.5): It should be possible to acquire information about the collection, storage, and use of personal data systems(0.5)
7. Individual participation (0.5): The data subjects normally have a right to access and challenge data relating to them. (0.5)
8. Accountability (0.5): A data controller should be designated and accountable for complying with the measures to effect the principles. (0.5)

(p. 596-597)

[8]

Question 11

A security plan identifies and organises the security activities for a computing system. The plan is both a description of the current situation and a map for improvement. Every security plan should address seven issues. Discuss the content of a good security plan in one sentence for each issue. (7 marks.)

ANSWER

Policy – Indicating the goals of computer security effort and the willingness of the people involved to work to achieve those goals
Current state – Describing the status of security at the time of the plan
Requirements – Recommending ways to meet the security goals.
Recommended controls – Mapping controls to the vulnerabilities identified in the policy and requirements
Accountability – Documenting who is responsible for reach security activity
Timetable – Identifying when different security functions are to be done
Maintenance – Specifying a structure for periodically updating the security plan
(p. 649)

(Half mark for issues, half mark for discussion)

[7]

Question 12

12.1 Give three reasons why a company should invest in cyber security. (3)

ANSWER

Consider student's answer. Should include aspects such as:
Cyber crime attacks are on the increase
Organised groups – advanced persistent attacks
Cyberwarfare
Internet of Things – all devices connected via Internet
Cloud computing – organisational data collected via Internet, etc.

12.2 Discuss two techniques in which privacy of patients can be protected in a scenario where patient data from a database is analysed through a data mining exercise. (4)

ANSWER

Correlation – Joining databases on common fields. Swopping data fields to prevent linking of records. Value swopping. Affects accuracy of results. (2)

Aggregation – Mid sized subsets preserve privacy - maintain with the rule of n items over k per cent. Add a small positive or negative error term to each data value. Helps to protect privacy without sacrificing the accuracy of results. (2)

Anonymization: Removing identifying information from records. (p.613).

Granular access: Fine grained access – only having access to authorised objects, not the entire database table or file (p. 545).

Other possible answers: adding noise

[7]

Total: 120