JÖNKÖPING UNIVERSITY

CANDIDATE

19961127-5174

TEST

TIAN19 - Information Security - 1901 (5 hp) - 20191210

Subject code	TIAN19
Evaluation type	--
Test opening time	10.12.2019 09:00
End time	10.12.2019 13:00
Grade deadline	--
PDF created	07.12.2020 20:28

Automatic

Question	Question title	Status	Marks	Question type
1	Malicious code	Correct	2/2	Inline Gap Match
2	Digital signatures	Wrong	0/1	Multiple Choice
3	Infosec model	Correct	1/1	Multiple Choice
4	Passwords	Wrong	0/1	Multiple Choice
5	Security requirements	Partially Correct	1/2	Multiple Response
6	Assets	Correct	1/1	Multiple Choice
7	Security aspects	Correct	1/1	Multiple Choice
8	Access control	Partially Correct	0.5/2	Inline Gap Match
9	Security aspects	Wrong	0/1	Multiple Choice
10	Encryption	Correct	1/1	Multiple Choice
11	VPNs	Correct	1/1	Multiple Choice
12	Risk	Correct	1/1	Multiple Choice

Manual

Question	Question title	Status	Marks	Question type
13	Infosec definition	Answered	2/3	Essay
14	ISMS implementation	Answered	1.5/3	Essay
15	IDS, IPS	Answered	1/3	Essay
16	Encryption	Answered	3/3	Essay
17	MITM	Answered	1/2	Essay
18	Session hijacking	Answered	2/3	Essay
19	Penetration testing	Answered	0.5/2	Essay
20	Authentication	Answered	0/3	Essay

21	Infosec terms	Answered	2.5/5	Essay
22	Clickjacking	Answered	2/2	Essay
23	Temporal separation	Answered	0/2	Essay
24	OS security	Answered	0/2	Essay
25	OS security	Answered	0/2	Essay

1 Malicious code

Pfleeger, Pfleeger, and Margulies (2015) desribes a number of types of malicious code. Match the type of malicious code with the corresponding description.

Note that there are more types than descriptions.

Help

Rabbit | Trapdoor | Dropper | Scareware

Program that intercepts and covertly communicates data on the user or the user's activity. Spyware

Code that causes malicious behavior and propagates copies of itself to other programs. Virus

Code installed in the most privileged section of an operating system. Rootkit

2 Digital signatures

To create a digital signature, what is needed?
Select one alternative:

- Shared-key system
- Public-key system
- Private-key system
- All of them

3 Infosec model

Where in the information security model is the information security policy placed?
Select one alternative:

- External, informal, administrative security
- External, formal, administrative security
- Internal, informal, administrative security
- Internal, formal, administrative security

4 Passwords

Which alternative would provide the best countermeasure against an off-line brute-force attack on a password hash?
Select one alternative:

- The use of a long password
- To use of a firewall
- To use the Diffie-Hellman password exchange
- To use a strict limit on login failures

5 Security requirements

Select the security requirements below that are either not realistic or not verifiable.
Select one or more alternatives:

- A system without a loss of confidentiality.
- A firewall rule that can filter out all harmful traffic.
- A system with zero downtime.

6

Assets

Which of the following sentences describe the term asset best from an information security perspective?
Select one alternative:

- Anything that has a value to the organization.
- Anything that an organization sells.
- Anything that is situated within an organization's premises.
- Anything that an organization buys.

7

Security aspects

In an attack, the adversary changed the number 100,00 to 10000. This type of change can be considered an attack against what security aspect?
Select one alternative:

- Integrity
- Privacy
- Confidentiality
- Availability

8

Access control

Access control is an essential aspect of information security. An operating system often manages the access control. Access control is often described using the terms:

Note that there are more types than descriptions. Help

Identifications | Topics | Role-based | Subjects | Items | Secrecy-based | Accountability

Identities are the entities that can access objects (often the human user).

Objects are things on which an action can be performed such as, e.g., files, programs, and hardware devices.

There are many models for how to implement access control in practice, and one example is Access-based access control.

9 **Security aspects**

Which of the following is an established security aspect?
Select one alternative:

- Non-repudiation
- Administrative security
- Loss
- Granularity

10 **Encryption**

Which of the following standards could be considered the go-to encryption standard of today?
Select one alternative:

- DES
- SED
- AES
- WEP

11 **VPNs**

What is the benefit of using a Virtual Private Network?
Select one alternative:

- Protection against packet loss
- Decreased lag
- Protection against eavesdropping
- Increased lag

12 Risk

What is meant by residual risk?

Select one alternative:

- A risk that is mitigated by security controls.
- A risk that is avoided by circumventing the problem.
- A risk that is transferred to e.g. an insurance company.
- A risk that remains uncovered by security controls.

13 Infosec definition

How would you define information security? You could use existing definitions or your own definition, as long as it aligns with common definitions.

Fill in your answer here

Information security is a subject where you identify and protect breaches on data. It is both a study to model up a safe way of identifying security risks and what the information is that can be sensitive, and some ways on how to protect the information. Defining the risks and possibilites can help to establish a better and a more secure way to handle information. Information security can also be defined as an expanding area of security measuresments that is constantly evolving through new information threats.

14 ISMS implementation

Imagine that you have been appointed responsible for the implementation of information security in an organization. Provide three key factors you deem necessary in order to succeed with such a task. Motivate your answer.

Fill in your answer here

I would first want to identify all possible and relevant information threats, because with this information I could then know what to do and where to start looking on what is needed for the organization. After identifying the problems i would start modeling up what risks are there and what can be done to prevent them. This would enable a bigger overview of the problem and help with applying the countermeasurments. When this is done and prossesed through I would then apply some security standards (ex. CIA) that will help the organization to have a model of how to increase their information security.

15 IDS, IPS

Describe the concepts: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Also, differentiate the concepts.

Fill in your answer here

They are used for identifying incoming threats and to help us solve them. The main difference between IDS and IPS is the method used for the countermeasurements of the threats. While IDS help us identify the threat, IPS is helping us to solve the threat.

16 Encryption

Explain the difference between stream cipher and block cipher. Also, give an example when each type of cipher could be used.

Fill in your answer here

Stream ciphers use a constant flow of smaller information from A to B, while block ciphers use a bigger packed block of information that is sent from A to B. It is easier to read and hack the stream cipher then the block cipher, since it is sent more often and it is more likely to figure out the encryption.

Stream ciphers are used when you want a constant stream of information and is not bothered by small packet losses, while block ciphers have a less frequency with more information inside that could be bad if this get lost in a packet loss. Stream ciphers could be used for example when playing a video, and block ciphers could be used for example when sending a message to someone.

17 MITM

Man-in-the-Middle (MITM) is a common type of network attack. Give one applied example of a MITM.

Fill in your answer here

One example of this is when two people wants to write to eachother and another person intercepts the information sent between them, and it is either just listened to, or it could even be changed between the connections.

18 Session hijacking

Explain the concept of session hijacking by giving an example of such an attack.

Fill in your answer here

Session hijacking is when someone steals your session key on a website. This could be used when entering a site while having sensitive information stored directly on it. The hacker could then get access to all the information through having the same access as the user, and it could be used to send requests without the user knowing it.

19 Penetration testing

What are the disadvantages of penetration testing?

Fill in your answer here

It could weaken the system by breaking stuff that you might not see the first time and also give a way for someone to identify the security flaws so that they could use it for their advantage.

20 Authentication

Authentication mechanisms can be divided into three categories. Describe these three categories.

Fill in your answer here

Symetrical authentication, it is when both parties have a key that they use to identify theirselves when trying to communicate between eachother. This way is fast since you only need to check if the key is valid at the endpoint.

Assymetrical authentication, it is when both parties have a private key and a public key to identify theirselves when trying to communicate between eachother. This is quite slow since you need to first use the public key and then check if it is valid, and then use the private key.

21 Infosec terms

Define the terms: vulnerability, threat, and security controls. Also, relate the terms to each other by giving an applied example.

Fill in your answer here

Vulnerability is about what that could go wrong.

Threat is about what could cause something to go wrong.

Security controls is about how to fix or prevent something that could go wrong.

Security controls is used to fix and prevent vulnerabilities in a system so that there can be is no internal or external threats for a system.

22 Clickjacking

Suggest and describe a technique by which a browser could detect and block clickjacking attacks.

Fill in your answer here

It could be prevented if the website uses CORS, which is used for a browser to disable requests from a different source.

23 Temporal separation

Give an example of the use of temporal separation for security in a computing environment. Also discuss the advantages and disadvantages of such an approach.

Fill in your answer here

This could be used to increase the secrity of an internal database for example. The advantages of this is that the system will not be detected and manipulated from an external source, but could be from an internal source. A disadvatage could be that the system is much slower and it would need certain permissions to access this.

24 OS security

Why should the directory of one user not be generally accessible to other users (not even for read-only access)?

Fill in your answer here

Since when having a read-only access, a hacker could make a file that have the same access as whatever file on your system to then be able to read your data with ease, and this is why it is good to prevent this.

25 OS security

File access control relates largely to confidentiality. What is the relationship between an access control matrix and the integrity of the objects to which access is being controlled?

Fill in your answer here

The relationship between them is that different level of authority can access certain files, which would make someone with less authority unable to read highly confidential objects. This will still keep it at a high confidentiality for the access control.