BKKBCL

Anonymkod/Anonymous code: BKKBCL

TENTAMEN/EXAMINATION

INTROSEC HT2023

Introduktion till informationssäker

Tentamen/Written exam 6 hp/hec

ML470C (SU) 470A AF

Torsdag/Thursday 2024-01-04
09:00-13:00

Poäng Points	Betyg Grade

Markera besvarade frågor med 'X' / Mark answered questions with 'X'													Antal blad
1	2	3	4	5	6	7	8	9	10	11	12		# sheets

Vakt kontrollerat antal blad:	

Obs! Denna sida måste ligga överst - This page should be placed in front
Avlägsna tomma blad före inlämningen
Remove empty sheets before handing in the exam
Fyll i samtliga uppgifter på sidhuvudet på varje blad
Please fill in all information in the header on each sheet

[Quiz] Introsec written exam January 4, 2024

Attempt 09:00:54 - 12:57:30

Question 1

Problem 1

General structured advice for dealing with ethically complex scenarios can be summarised with steps:

- **Understand the situation**
- **Know several theories of ethical reasoning**
- **List the ethical principles involved**
- **Determine which principles outweigh others**

a) Discuss what the step "Know several theories of ethical reasoning" involves, and show how differing theories of ethical reasoning can suggest different courses of action for a specific scenario.

Rather than following such steps for each and every scenario it is common to follow codes of ethical conduct that are stipulated for organisations that one belongs to and keep to those, such as:

"Members and ISACA certification holders shall:

1. **Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.**
2. **Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.**
3. **Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.**
4. **Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.**
5. **Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.**
6. **Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.**
7. **Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.**

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures."(ISACA, no date[1])

[1] ISACA (no date), *Code of Professional Ethics*, available at: https://www.isaca.org/code-of-professional-ethics, (Accessed: 3 January 2024).

b) Describe a realistic and illustrative information security scenario where such a code of conduct might inform a course of action in the face of an ethical dilemma.

a)An important step in the process of dealing with ethically complex scenarios is to know several theories of ethical reasoning.
This step involves having the knowledge about ethics and ethical reasoning to apply it to the current scenario being faced and reasoning about outcomes and consequences of taking an action to deal with the issue.
Consider a specific scenario where a senior company employee is being asked to reveal certain information about the company he
is working for by the government.The government requires this information for military security of the country.
Since the employee has signed non-disclosure aggreement with the company from a certain viewpoint of ethical reasoning he should not reveal the information.
But considering that the government requires the information and he is also a citizen of the country it could be his moral obligation that the
non-disclosure agreement can be broken here.

One theory of ethical reasoning is that the employee should follow the agreement he has signed whereas based on a differing theory of ethical reasoning morally he might feel obligated to provide the information to the government.

b) Consider a specific scenario where a person is the CEO of an Artifical Intelligence company OpenAI.
The CEO is answerable to the board members of the company and also the board and CEO of a Social Media Company Microsoft ,the employees of his company OpenAI and some other stakeholders.
An external company New York Times files a case in the court against OpenAI claiming their product ChatBPT is using their news articles to create
the product and it produces very similiar articles and the general public can view these articles.
Thus the company OpenAI is being asked to reveal the working of their product ChatBPT to see if their product really uses the news articles of New York Times
for the creation of their product. However if the company reveals this information other companies and entities could copy their product ChatBPT
and this would violate the interests of many stakeholders of OpenAI.
The CEO of the company thus needs to find a way to prove that their product does not use articles of New York Times while also making sure that
he does not reveal too much information about the working of the product ChatBPT.
In this scenario the ISACA code of professional ethics can help the CEO to design a specific course of action.
He needs to serve the stakeholders but also disclose certain information about the product as required by legal authority.
He needs to perform his duties with dilligence and care in accordance with a professional standard.
Thus the ISACA code of professional ethics can help him to face this dilemma and provide him a course of action.

Question 2

Problem 2

Explain why a *certificate signature chain* can be necessary when one wishes to use public key cryptography to send an encrypted message to some party one may never have met personally, and yet be confident that only the intended recipient will be able to decrypt that message. Summarise the two approaches commonly used to establish certificate signature chains.

Certificate is necessary in order to prove that a person's identity is associated with a cryptographic key.
A certificate is used to bind identity to a cryptographic key.
Before a sender sends a message to a recipient ,it is important to verify the public key associated with the recipient as the public key is used to encrypt messages .
If the association is wrong,someone other than the intended recipient could decrypt and read the messages.

Suppose Alice wants to send a message to Bob.

If the 2 parties have never met they can take help of a trusted third party to verify their public keys.
But there is no one single party who trusts both Alice and Bob.
Consider a scenario where there are 2 other parties Carol and Mark.
Carol trusts Alice. The party Mark trusts Carol .
Mark also trusts Bob.

There can be a chain of signatures where Carol can sign Alice's public key and Mark can sign Carol's public key and so on.
This leads to creation of a certificate signature chain involving all the parties and Alice can verify Bob's public key.
In this situation certificate signature chain is necessary in order to prove that the recipient's identity is associated with his public key,
due to the absence of a single third party trusted by both Alice and Bob.
In this way ,Alice can verify Bob's public key and can send a message to Bob without the risk of it being decrypted and read by someone else.

There are 2 approaches to establish certificate signature chains
PGP is one method to establish a certificate signature chain.
The full form of PGP is Pretty Good Privacy.

PKI is another method to establish a certificate signature chain.
The full form of PKI is Public Key Infrastructure.

Question 3

Problem 3

An access control matrix is a general model for describing a secure system by mapping the rights or privileges of subjects over objects. It is common to use such a model as a basis for implementing access control in file systems, where we may assume for the purposes of this problem that the subjects are normally users of the system, and the objects are normally computer files. Sets of such rights will commonly include *read*, *write*, and *execute*.
a) With reference to Saltzer and Schroeder's principles of secure design, give as broad a motivation as possible as to why we may assume it to be sound practice to keep the set of possible rights small.
b) Suggest, explain and exemplify an additional kind of right beyond *read*, *write* and *execute* that can be motivated in order to improve the expressive power, and thereby the control and security over a file system's access control. Good answers will also illustrate how adding this specific kind of right to the system can introduce new security problems, thereby illustrating a security trade-off in the design of this set of rights.

a)
Salter and Schroeder's principles of secure design emphasize on simplicity of design.
Simple design helps the system to be secure.
According to principle of least privilege a subject should only have the privileges necessary to complete its task.
In case it needs any additional privileges to do a specific task ,the privileges should be given and immediately removed after completion of the action.
It is a good practice to keep the subset of possible rights small.
If more rights are given to the subject than necessary, it increases the chances of violation of security policy, one reason could be due to the execution of

a process with malware by a user unknowingly.
Giving only the necessary rights would reduce the potential of the malware to cause harm to the system.

According to principle of least authority the subject should be given only the authority needed to complete its tasks.
This principle also emphasizes the importance of keeping the set of rights small.

The principle of fail safe defaults states if a subject tries to access an object for which it is not explicitly given access for the access should be denied.
According to this principle, the default access control for an object should be None.
It helps to prevent unauthorized access to an object.
Keeping the set of possible rights small also supports this principle.

b)
An additional right beyond read, write and execute is the own right.
Persons with the own right have power and control over the file system's access control.
Suppose the system has three types of users owner,group and other user.

Persons with the own right have the ability to define the rights of the group users and other regular users of the computer system over the file.
Adding this right could cause new security problems .
One problem occurs if the system of the person with own right is usurped by an attacker,
the attacker has the complete ability to redefine the access control policy of the file for all users and can make it unaccessible for
any group or other users.
Another issue is since the person with own right has complete ability to define the access control for all users if any malware is executed by a person with own right,
it would be more dangerous as the access control of the owner is not restricted unlike the group and other users who only have some rights .
Hence the malware has more potential to cause harm to the system.

Question 4

Problem 4

Explain each of the following IT security related terms. Also, for each of these terms give an example of an application/situation/distinctive trait (whichever is most appropriate) that further helps to elucidate the concept. Give concrete examples wherever possible. Furthermore, for each of these terms further illustrate the concept by choosing a closely connected information security concept and by explaining the relationship between the concepts. The relationship may suitably illustrate in what ways your chosen concept is like - and conversely unlike - the given term.
Structure each of your answers with headings *explanation, example,* and *relationship to [your chosen related concept].* Your answers should be designed to help an uninformed reader to greater

understanding of the concept, thereby contributing to evidence of your own deep understanding. Examples and related concepts should be chosen and explained to maximise the depth of your answers.
Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- **Security Policy**
- **Multifactor Authentication**
- **Discretionary Access Control (DAC)**
- **Privacy by Design**

Security Policy

Explanation

It is a statement of what is and what is not allowed .A security policy
divides a system into a set of authorized or secure states and a set of unauthorized or non-secure states.

Example

Company employees of an IT company can only login to their company email account and access their company emails once they are connected to the company's secure Virtual Private Network.

Relationship to Security Mechanism

A mechanism is a sequence of steps or procedure required to enforce a security policy.
A policy needs a mechanism so that the policy can be enforced.

Multifactor authentication

Explanation

It is a type of authentication that requires a user to pass 2 different types of authentication to be authenticated by a system and gain access to the system.

Example

When a user logs into their email account,once they enter their password ,they are also sent a code to their mobile phone
which they must enter to login into their account.
Password is something the entity knows and the code sent to their mobile is something the entity has.
These are the 2 different types of authentication.

Relationship to Challenge Response Protocol

Multifactor authentication is an example of the challenge response protocol.
The challenge response protocol is when the system gives a specific challenge to the user which the user must complete to
perform authentication.
The challenge in the example given is the code being asked by the system which is sent to user and the user enters the code as a response.

Discretionary access control

Explanation

It is identity-based access control.
It is a form of access control where the owner of the object can define the rights of the object for the other users.
There is no restriction placed by the system on the kind of rights that can be given by the owner on the object.

Example
An owner of a word document can specify rights of other users detailing which users can read,edit or delete the word document.

Relationship to Mandatory access Control
Mandatory access control is unlike discretionary access control.
The computer system places restrictions on what rights can be allowed on the specified object and the owner does not have complete control to define the rights. These rights could be enforced by the Operating System.

Privacy by Design
Explanation
Privacy by Design is when a system is designed to be private and the information in the system cannot be accessed
unless the person allows other entities and users access to the information.

Example
A person has some private file with confidential information.
This file is not shared with other entities unless the person gives access to other persons.

Relationship to Spatial privacy
Spatial privacy is right to be let alone and it is unlike privacy by design.

Question 5

Problem 5

Identify and describe a kind of malware that one can reasonably assume can be particularly difficult for an automated malware detection system to discover, also explaining what makes it hard to discover.

A rootkit is a kind of malware that is particularly difficult for an automated malware detection system to discover.
A rootkit is a pernicious trojan horse and it is highly harmful and destructive .
Once it is inside a system, a rootkit installs various traps and backdoors in the system. It alters the functioning of various system programs that could reveal the presence of the rootkit.
For example a program to list contents of a directory is altered to not show presence

of certain files.
A program to list the network connections could be altered to not show specific hosts.

An approach to discover rootkits could be to run non-standard programs that obtain the same information as the system programs.
These programs bypass the system programs and use system calls to the kernel to obtain required information.
However , rootkits have become more sophisticated . They modify parts of the kernel and make it difficult even for non-standard programs to obtain
information that could reveal the presence of the rootkit.
Hence the rootkit is a type of malware that is very difficult to discover by an automated malware detection system and
it requires lot of effort to detect a rootkit.