2022 Exam 02239 Data Security

Der anvendes en scoringsalgoritme, som er baseret på "One best answer"

Dette betyder følgende:
Der er altid netop ét svar som er mere rigtigt end de andre
Studerende kan kun vælge ét svar per spørgsmål
Hvert rigtigt svar giver 1 point
Hvert forkert svar giver 0 point (der benyttes IKKE negative point)

The following approach to scoring responses is implemented and is based on "One best answer"
There is always only one correct answer – a response that is more correct than the rest
Students are only able to select one answer per question
Every correct answer corresponds to 1 point
Every incorrect answer corresponds to 0 points (incorrect answers do not result in subtraction of points)

A Protocol for the Superbif Company

The company *Superbif* wants to develop a mobile App for movie theater tickets, namely for purchasing a ticket for a movie and for showing the ticket at the theater entrance.

For the purchase, we assume that there is a central trusted server for all the movie theatres called "cms" (central movie server) that stores which seats in which shows are currently free, and will also handle the connection to payment solutions. It must of course be prevented that an intruder who may have also installed the App on their own phone can for instance obtain the movie tickets purchased by another user. Thus, to establish a secure connection between each phone/App and the cms, the Superbif company considers using TLS. Which of the following statements is correct?

Choose one answer

- TLS is not secure for this, because an attacker who sits somewhere between App and cms can launch a man-in-the-middle attack.
- Using TLS requires that each device has its own public key certificate, which is not very practical.
- The use of TLS is adequate, as it can ensure that the movie ticket is sent to exactly the App from which the purchase was made.
- Since the attacker can analyze the App's machine code and extract every secret that is embedded into the App, the attacker can impersonate the App and "hijack" every TLS session of an honest App user.

The Superbif company decides to not use TLS and implement their own protocol instead. They have combined the purchasing protocol with the protocol for showing a ticket at the movie theater. This protocol between App, cms, and theater is attached as an AnB file:
Superbif.AnB (https://resources.mcq.eksamen.dtu.dk/v1/48fe4f6e-14bd-4d96-9643-d9a922a90b12)
Here "theater" can be a simple near field communication device at the movie theater that does not memorize which tickets have been shown, but rather confirms every ticket show with cms. "Seat" and "DesiredSeat" are here random numbers but should model a particular seat in a particular show (room, date and time) at the theater.
Unfortunately, this protocol has an attack -- OFMC's output is also attached:
Superbif - OFMC attack output (https://resources.mcq.eksamen.dtu.dk/v1/a1096ae0-cec5-45b9-849b-8e8418d61260)
What does this attack mean and how can it be fixed?

Choose one answer

- The intruder replays the accepting message from the cms and thus gets a ticket accepted a second time. A simple fix is that the theatre device generates a fresh nonce that is included in the encrypted/signed messages between theatre and cms.
- The intruder replays the accepting message from the cms and thus gets a ticket accepted a second time. A simple fix is that the cms generates a fresh nonce that is included in all messages except the first one.
- The intruder uses the accepting message from the cms for an honest app user to get a forged ticket accepted. A simple fix is to include the name of the App in the signed message from cms.
- The intruder uses the accepting message from the cms for an honest app user to get a forged ticket accepted. A simple fix is to let cms rather sign the encrypted message for theater.

Superbif guarantees to delete all information about a purchase 30 days after watching the movie, in order to protect the customers' privacy. They want to offer loyal customers however the opportunity to watch every 10th movie for free. Is it possible to make an electronic solution that does not reduce the privacy at all and that is also secure against fraud?

Choose one answer

- Yes, the cms at each purchase additionally generates a digital voucher that contains a fresh nonce and is signed by the cms. After collecting 9 such vouchers, one can use them to purchase a new ticket.
- Yes, one can use the Schnorr protocol to make a zero-knowledge prove of possession of 9 old movie tickets without revealing them. The server as verifier would then issue a new ticket for free.
- Yes, if the all tickets can be stored in a blockchain: the distributed nature of a blockchain makes a privacy breach extremely unlikely.
- No, either the purchase information is stored until the customer has gotten the free movie, or it is possible for dishonest customers to lie about the number of movies they have seen.

Diffie-Hellman: Only one of the following statements is true about Diffie-Hellman with half keys exp(g,X) of A and exp(g,Y) of B, and with resulting key exp(exp(g,X),Y). Which one?

Choose one answer

- ○ The half-keys must be kept secret between A and B, otherwise the resulting key may be known to a third party.
- ○ The half-keys must be authenticated by A and B, respectively, otherwise the resulting key may be known to a third party.
- ○ Neither A nor B must not use their half key in another Diffie-Hellman exchange, otherwise the resulting key may be known to a third party.
- ○ When encrypting a low-entropy message (like a poorly chosen password) with the resulting key, an intruder can launch an offline guessing attack.

An Poor Online Bookstore

An online bookstore is running a website where shoppers can select books they like to purchase and put them into their shopping basket. The website has some backend program written in C for handling the purchases. It uses the following data structure for an item in the shopping basket:

```
struct basket_item{
  char ISBN[14];    // a null-terminated string identifying the book
  int16_t priceDKK; // the price of the item in Danish Kroner (16 bit signed integer)
};
```

Here the ISBN number is a 13-character international serial book number.

When a customer selects to enter a book into the shopping cart, the following function is called that creates the new item:

```
basket_item * create_item(char *ISBN){
  basket_item *new_item = new basket_item;
  new_item->priceDKK = lookup_price(ISBN);
  strcpy(new_item->ISBN, ISBN);
  return new_item;
}
```

where lookup_price is a function to look up a price of a book - we do not care how lookup_price is implemented, but it will return the largest 16 bit signed integer value if the item is not found.

Let us assume that a dishonest shopper found a way to control what string is used as argument **ISBN** to the **create_item** function. Is it then possible that a dishonest shopper might be able to get a "bargain" on their purchase?

Choose one answer

- ○ No, because the **ISBN** number has the sufficient size, including space for terminating zero-byte.
- ○ No, because the memory address where the new item is created cannot be guessed by the shopper.
- ○ Yes: using a buffer overflow attack they can ensure that **priceDKK** is zero.
- ○ Yes: using a buffer overflow attack they can ensure that **priceDKK** is negative.

We have assumed that a dishonest shopper can determine the precise string that is sent to the **create_item** function in the previous question. Which of the following scenarios is realistic?

Choose one answer

- If adding an item to the shopping basket generates a URL that contains the **ISBN** number, the attacker can manipulate the URL to insert the desired **ISBN**.
- If the price for the desired book is not in the bookstore server's cache, one can use a SPECTRE attack to overwrite the memory address that contains the **ISBN**.
- If one can use social engineering to get a bookstore employee to click on an attacker-chosen link that contains the manipulated **ISBN**, one can use an XSS attack to run the C code with chosen parameters.
- If the price lookup function uses an SQL database without sanitizing inputs, the attacker can run an SQL injection attack to manipulate which **ISBN** is returned.

Information Flow.

Consider the following code snippet:

```
k = 1;
z = b + 1;
if (x > 2) {
    z = n - 1;
    if (y < 8) {
        a = 4;
    }
}
n = (y + 5) * 2;
```

What is the complete set of information flows in this piece of code?

Choose one answer

- b->z, n->z, y->n
- b->z, n->z, y->n, x->z, y->a
- b->z, n->z, y->n, x->z, y->a, x->a
- b->z, n->z, y->n, x->z, y->a, x->a, x->n

Which of the following statements is **not** true about onion routing?

Choose one answer

- Each node in a routing sequence knows the final destination, but not the source.
- Each node knows the previous and the following node in a routing sequence.
- As long as one node in a routing sequence is not controlled by the attacker, the security is maintained.
- The sender knows the public key of every node in the routing chain.

You are performing a security analysis for a company whose product is a Social Media platform.
Which of the following risks compromises the Integrity property of the primary security goals?

Choose one answer

- A lightening strike which results in the destruction of the company's Internet gateways
- A data leak which results in user data being exposed
- A man-in-the-middle intruder intercepting a communication between users and performing a modification attack
- A corrupt employee who accepts money to disclose some company's private information

An intruder has gained access to an electronic patient health record system of a hospital. A doctor prescribes medication to a patient and enters all relevant information in the health record system. The intruder alters the entered information and doubles the prescribed medication dosage. The modification on medication dosage is now available in the health record system.
Which of the following security principles were violated?

Choose one answer

- Integrity & Confidentiality
- Confidentiality & Availability
- Authenticity & Integrity
- Availability & Authenticity

According to Deloitte, "91% of all cyber attacks begin with a phishing email to an unexpected victim." Considering this information, what makes a good enterprise security plan?

Choose one answer

- A security plan where the risk of incidents is minimized
- A security plan that ensures the worst case scenario is survivable
- A security plan that renders malicious usage infeasible
- A security plan made in collaboration with the relevant users

Don Omar, an IT security administrator gets notified about a possible port scan attack from IP
address X. He wants to set up a firewall to protect the network from the possible attackers. What
type of firewall would be the most effective to defend against the attacker with IP address X but
also from similar attackers with different IP addresses in the future?

Choose one answer

- The Onion Routing (TOR)
- Packet filtering gateway / Screening router
- Stateful inspection firewall
- Application Proxy

Sally is working at Social Security A/S, and has gotten the job of adding a mail server that connects to the internet. The current implementation at Social Security A/S is strictly running on a Local Area Network (LAN). This is done as important information such as social security numbers are stored locally in a database.
How should Sally go about expanding the current network architecture with a mail server such that the important information remains as safe as possible from intruders?

Choose one answer

- Adding firewalls to the workstations in the network
- Encrypting the databases containing sensitive information
- Connect the LAN to a DMZ in which the mail server is contained
- Ensure that all workers are well-versed in cyber security

Bob is working as a security engineer in a large Danish corporation. Because of COVID-19, his company started using a Remote Desktop software, allowing the employees to connect to the company's servers using their personal laptops.
What does the company need to do, in order to ensure that it stays protected in a remote working environment?

Choose one answer

- ○ Nothing, all of the employees attended online cyber security awareness training courses last year and we can trust their computers are secure
- ○ Set the session tokens/cookies' expiration time to 5 days, preventing hackers from stealing and using them to authenticate into corporate machines
- ○ Make sure all employees use 2-factor authentication to access the corporate VPN and all incoming traffic is assumed to be untrusted and potentially malicious
- ○ The company shouldn't allow remote work for its employees as it is not secure and all of the employees have to return back to the office

How does segmentation help address the problem of network attack prevention?

Choose one answer

- Segmentation filter incoming and outgoing network traffic based on predetermined security rules
- Segmentation divides the network into isolated zones and prevents random network traffic between zones
- Segmentation encrypts the data sent on the network
- Segmentation monitors the network to detect intrusions in the system

The main goal of a honeypot in security is to occupy an attacker with a fake application while learning how they attack your system. You as the security expert with limited information on honeypots is ordered to examine the limitations of a honeypot.
Which alternative is _not_ a limitation of a honeypot?

Choose one answer

- If we do not isolate and secure the honeypot from the real system, the attacker may manage to successfully breach the honeypot and attack other systems through it
- By noticing that the honeypot contains fake data, the attacker may attack the honeypot with multiple attempts and draw the attention from the real system to the honeypot
- The idea behind a honeypot is to lure the attacker, therefore a honeypot does not detect any attacks on the system, and breaches may go unnoticed
- Since the idea behind a honeypot is to log all the information, there exists a potential risk to overflow the logging system with useless information

The table below shows the access control matrix for a system.

	secret.txt	Program.exe	script.sh	public.txt	printer
Alice	ORW	X	X	RW	W
Bob		R	R	R	W
Charlie	R	ORWX	ORWX	R	
Dan			R	RW	
Erin	R	RW	X	ORW	OW

The following list of security goals have been identified for the system:
A. Only Charlie can write to the script.sh file
B. Every user who can read the secret.txt file can also execute the script.sh file
C. Only Alice can print the content of the secret.txt file
D. Every user who can read the secret.txt file can also execute the Program.exe file
E. Only Alice can write to the secret.txt file
F. Every user who can read the secret.txt file can write to the public.txt file
G. Every user can read the public.txt file

Given the access control matrix for a shared system presented above, which of the stated security goals are met?

Choose one answer

- A, B, F, G
- A, C, E, G
- A, B, D, G
- A, B, E, G

Alice works at a software company. The project management system of the company manages the workflow of a project and uses Role-based Control Access as the authorization mechanism.
There are totally five roles divided due to the positions: project manager, senior engineer, junior engineer, hiring manager and intern.
The access control policy is stored in a file, which stores permissions of the roles; the policy file looks like the following
list.

Project manager : read project , read tasks , add tasks , read time plan , change time plan
Senior engineer : read project , read tasks , read time plan
Junior engineer : read project , read tasks , read time plan
Hiring manager : add or delete members of the project
Intern : read project , read tasks

Alice is able to directly make changes to the contents of the project in the system. What is the role of Alice in the company?

Choose one answer

- Project manager
- Senior engineer
- Junior engineer
- Intern

An intruder was able to crack all encrypted passwords by comparing known password hashes with
the stored hashes (also known as rainbow table attack). How could this method of attack have been
prevented?

Choose one answer

- Use block chain cryptography to store the passwords
- Use modern hashing algorithms like SHA-3
- Use salting in combination with your hashing algorithm
- Require the passwords to include non alphanumeric characters

You work as a security consultant and are invited to offer support to a small size sports equipment company (50 employees), whose technical management decided to make some changes, for making the organization more secure. Currently, users are logging in their sales app, based on their credentials, using passwords having only alphabetic characters(letters) and minimum 6 characters, and their passwords are hashed with a Sha256 key, and stored on a reliable Database. Moreover, the system will permanently block users' access, if they have more than 3 wrong login attempts in a row on the server. To get back the lost access, employees have to make a formal request to their manager, which is approved in 10 working days. Moreover, the company's authentication system currently also uses a token-based mechanism, with digital tokens sent to the user's phone which works fine, but some users complain this makes it more inconvenient to login.

Which of the following options would be most secure strategy for establishing the company's authentication mechanism?

Choose one answer

- Increase password length to minimum 10 characters, including digits & special characters. Store the password using different random generated salts for every user and block users for 30 min when inputting more than 3 wrong passwords in a row. Keep the Token mechanism
- Increase password length to minimum 10 characters, including digits & special characters. Store the password using the same random generated salts for every user, and block users for 30 min when inputting more than 3 wrong passwords in a row. Keep the Token mechanism
- Increase password length to minimum 12 characters, including digits & special characters. Store the passwords using different random generated salts for every user, and permanently block users when inputting more than 4 wrong passwords in a row. Keep the Token Mechanism
- Increase password length to minimum 12 characters including special characters, store the passwords using the same random generated salts for every user and block users for 72 hours when inputting a wrong password more than 5 wrong passwords in a row. Drop the Token Mechanism

The company Lightfinger Enterprises Ltd. is developing an optical sensor for biometric verification.
Test of the sensor shows the following results.

	user is correct	user is imposter
Test is positive	50	30
Test is negative	10	900

What are the values of sensitivity, specificity, accuracy and prevalence respectively?

Choose one answer

- 0.83, 0.97, 0.96, 0.06
- 0.97, 0.96, 0.06, 0.83
- 0.96, 0.06, 0.83, 0.97
- 0.06, 0.83, 0.97, 0.96

Alice is building a website for her family of 5 where each family member can make posts. Every family member should be able to authenticate that a given post has been created by someone within this family. What would be best to achieve this? Assume that keys can be distributed safely.

Choose one answer

- ○ Message authentication codes
- ○ Cryptographic hash functions
- ○ Encryption using CBC
- ○ Digital signatures

The company Total Surveillance Corporation (TSC) uses AES-256 on dedicated hardware to encrypt video streams from their cameras to the back-end server. The video resolution has recently improved, but the encryption/decryption chip that TSC has currently licensed cannot encrypt the video stream at the high resolution, so the company has decided to install two chips in each camera, so that encryption can be carried out in parallel. They now want to know which cipher mode may be used when encryption and decryption is managed by two chips in parallel.
One of the following block cipher encryption method has the ability to encrypt video frames so that they can be decrypted again while running in parallel.

Witch of the following cipher modes satisfy those requirements?

Choose one answer

- ○ Electronic codebook mode (ECB)
- ○ Cipher block chaining mode (CBC)
- ○ Counter mode (CTR)
- ○ Cipher feedback mode (CFB)

Which of the following statement about cryptography is wrong?

Choose one answer

- In symmetric cryptography, all involved agents share the same secret key and use it for both encryption and decryption of a message
- The signing and checking of a digital signature correspond to the encryption and decryption process in cryptography and they both use a private key
- In asymmetric cryptography, the encryption of a message uses a public key which everyone knows but the decryption of the message uses a private key which only involved agents know.
- Hash-based Message Authentication Codes (MAC) can be understood as keyed hash because a shared secret key is prepended to the message before applying hash function

The overall risk assessment of the ACME company estimates an expected annual loss of 66 million Kroner from identified security vulnerabilities. A survey of different security technologies identify four different technologies that mitigate one or more vulnerability, these are summarized below:

- A Managed Security Service costs 5 million kroner to implement, and 33 million kroner each year for the next 5 years to operate. It is estimated to reduce the annual expected loss by 37 million kroner.
- An Intrusion Detection System costs 80 million kroner to implement, and 15 million kroner each year to operate. It is estimated to reduce the annual expected loss by 35 million kroner.
- An internal Security Operations Center costs 45 million kroner to implement, and 23 million kroner each year to operate. It is estimated to reduce the annual expected loss by 38 million kroner.
- A Demilitarized Zone costs 25 million kroner to implement, and 8 million kroner each year to operate. It is estimated to reduce the annual expected loss by 15 million kroner.

The company wishes to optimize its investment in computer security, so it will only invest in the single technology that provides the best value for money over the next 5 years. Which technology do you recommend?

Choose one answer

- ○ The Managed Security Service
- ○ The Intrusion Detection System
- ○ The internal Security Operations Center
- ○ The Demilitarized Zone

Implementing the Kerberos protocol in the Andrew File System (AFS) requires synchronized clocks on all work stations.

Why is this required?

Choose one answer

- To generate the same random seed in the running key generator on all workstations
- To ensure proposer connection setup and tear-down
- To ensure proper ordering of events in the file system logs
- To ensure correct interpretation of timestamps and ticket expiration times