Exam 02239 Data security

Side 1

Vis rigtige svar
Skjul rigtige svar

Spørgsmål 1

TLS

Alice buys a train ticket online on the website of a trusted train company. She uses a standard web browser using an https connection with a certificate that Alice's browser can successfully validate. Neither Alice nor the website themselves have been hacked. Alice has no user account on the website. Alice selects her journey and pays by entering her credit card information. From the the website she obtains a QR code that she can show in the train as an electronic ticket.

Which of the following statements is correct?

- [ ] It is insecure that Alice enters her credit card, because an attacker can make a man-in-the-middle attack and obtain the credit card number
- [ ] It is insecure that Alice enters her credit card, because an attacker can make an offline guessing attack on the credit card number
- [ ] Because Alice is not authenticated, an attacker can obtain the QR code for a travel that Alice paid for
- [ ] None of the other statements is correct

Spørgsmål 2

Storing Passwords

When using password based authentication between users and a webserver for a login via TLS, which of the following is the most secure setup?

- [ ] The server stores the password in clear text, and at login, the webbrowser transmits the password over the TLS channel
- [ ] The server stores the password in clear text, and at login, the webbrowser transmits only a hash of the password over the TLS channel
- [ ] The server stores only a hash of the password, and at login, the webbrowser transmits the password over the TLS channel
- [ ] The server stores only a hash of the password, and at login, the webbrowser transmits only a hash of the password over the TLS channel

Side 2

Diffie-Hellman

For these questions, please consider the following attached AnB file:

DH.AnB

Please note there are several questions on this page!

Spørgsmål 3

The attached file has an attack. What's the problem?

- [ ] The half-keys exp(g,X) and exp(g,Y) must not be exchanged in plaintext
- [ ] B can never obtain the message Payload
- [ ] B is not authenticated
- [ ] a dishonest A can replay the Payload

Spørgsmål 4

There are several ways to fix the protocol DH.AnB by only changing the exchanged messages (i.e., not changing the initial knowledge or the goals). No matter how this fix looks like, one of the following statements is **wrong**. Which one?

- [ ] If the intruder learns sk(A,s) or sk(B,s), then he can find out any Payload exchanged before
- [ ] Also the goal "B authenticates A on exp(exp(g,X),Y)" holds
- [ ] Also the goal "B authenticates A on Payload" holds
- [ ] For the protocol to work, the server s must be honest

Side 3

Spørgsmål 5

Which of the following methods guarantee safety from a buffer overflow attack?

- [ ] Stack canaries: insert special values into the stack and abort a program that overwrites them
- [ ] Disallow that the processor jumps to a memory address within the area reserved for the stack
- [ ] Place each new stack frame at an unpredictable random address in memory
- [ ] None of the other answers

Spørgsmål 6

Information Flow

Consider the following program:

```
while(x>0){
  x=x-1;
  if(y>0) z=1;
  else z=z*x;
}
```

If we consider only two security classes H (High) and L (Low), which of the following declarations are "safe" in the sense that no information can flow from a high to low variable?

- [ ] x:H, y:H, z:L
- [ ] x:L, y:L, z:H
- [ ] x:L, y:H, z:L
- [ ] x:H, y:L, z:L

Spørgsmål 7

Consider an onion routing network with nodes N_1 to N_{10} and suppose Node N_1 wants to send a message M to Node N_8 via intermediate nodes N_2, N_5, and N_6. What does the intermediate message from node N_2 to N_5 look like?

- [ ] $N_5,\{N_6,\{N_8,\{M\}pk(N_8)\}pk(N_6)\}pk(N_5)$
- [ ] $N_5,\{N_6,\{N_8\}pk(N_6)\}pk(N_5),\{M\}pk(N_8)$
- [ ] $N_5,\{N_6\}pk(N_5),\{N_8\}pk(N_6),\{M\}pk(N_8)$
- [ ] $N_5,\{N_6,\{N_8,\{N_1,M\}pk(N_8)\}pk(N_6)\}pk(N_5)$

Spørgsmål 8

You have received a cleverly designed phishing email that looks like coming from your bank. Not noticing it was fake, you have clicked on a link in the email that leads you to a non-existing page in the domain of the bank. At this moment you notice the phishy nature of the email and contact the IT support of the bank who assure you (after inspection of the email) that the attack did not succeed. Which security mechanism was most likely preventing the attack?

- [ ] The same origin policy of your browser
- [ ] A challenge-response between your browser and the server
- [ ] The server is filtering all inputs from your browser
- [ ] The server checking the referrer tag of every http request

Side 4

Spørgsmål 9

A small Danish IT company has been the target for several attacks during this winter. They wish to hire an IT specialist to perform a risk analysis and decide which of risk mitigation strategy would give the company the most value of the cost.
What risk attribute is calculated to determine the solution with the most value for the company?

- ☐ Risk Impact
- ☐ Risk Exposure
- ☐ Risk Control
- ☐ Risk Leverage

Spørgsmål 10

Alice wants to send a message to Bob. She wants to be sure that the message can only be read by Bob, and that the message Bob receives, has not been tampered with.
What are the protection goals in this scenario ?

- ☐ Integrity and Non-Repudiation
- ☐ Confidentiality and Integrity
- ☐ Confidentiality and Authenticity
- ☐ Authenticity and Non-Repudiation

Spørgsmål 11

The overall risk analysis of the ACME Company estimates an expected annual loss of 42 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 24 million kroner each year for the next 5 years to operate. It is estimated to reduce the annual expected loss by 30 million kroner.
An Intrusion Detection System costs 60 million kroner to implement, and 10 million kroner each year to operate. It is estimated to reduce the annual expected loss by 27 million kroner.
An internal Security Operations Center costs 25 million kroner to implement, and 13 million kroner each year to operate. It is estimated to reduce the annual expected loss by 23 million kroner.
A Demilitarized Zone costs 25 million kroner to implement, and 3 million kroner each year to operate. It is estimated to reduce the annual expected loss by 10 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?

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

Side 5

Spørgsmål 12

You have been hired to set up a surveillance system, where a number of cameras installed in sensitive locations communicate with a single server. You wish to protect the communication with a cryptographic solution that achieves fast encryption/decryption of the video streams while still providing high security.
Which of the cryptographic primitives listed below is best for this scenario?

- [ ] Symmetric encryption
- [ ] Asymmetric encryption
- [ ] Cryptographic Hash functions
- [ ] Message Authentication Codes (MAC)

Spørgsmål 13

In the context of key exchange, what does a digital certificate associate?

- [ ] A public key and a user's identity
- [ ] A private key and a user's identity
- [ ] A public key and a digital signature
- [ ] A private key and a digital signature

Spørgsmål 14

Alice wants to hire Bob to work at her startup. She digitally signs a contract and sends it to Bob. Later that day, Bob receives the contract. He knows everything about digital signatures, so now he can be sure that (1) and (2). However, he cannot be sure that (3).
Each answer below provides 3 options to fill out the missing parts. Choose the one that offers the correct options:

- [ ] (1) nobody else (except for Alice and Bob) has seen the contract
(2) Alice will not be able to deny signing the contract
(3) the contract was signed by Alice
- [ ] (1) nobody else (except for Alice and Bob) has seen the contract
(2) the contract was signed by Alice
(3) Alice will not be able to deny signing the contract
- [ ] (1) the contract is signed by Alice
(2) Alice will not be able to deny signing the contract
(3) nobody has tampered with the contact after Alice has signed it
- [ ] None of the provided answers are correct

Spørgsmål 15

A company just set up a new server which is vulnerable to a replay attack.
Which of the following implementations would prevent such attack in the future?

- [ ] Encrypting all communication
- [ ] Adding sequencing numbers to the request
- [ ] Adding digital signature to the request using the clients private key, thus identifying of the client
- [ ] Adding a HMAC to the request

Side 6

Spørgsmål 16

Which of the following statements about Single Sign On systems (SSO) is false?

- [ ] When you switch websites, SSO perform operations in the background to authenticate you, freeing you of having to give your credentials again
- [ ] If you log out of a service, you will not be logged out of other servers in the same domain
- [ ] It is a trust agreement between organizations that permits a user to use the same identification across all applications part of that agreement
- [ ] It provides service from different web applications within the same identity domain using just one set of credentials

Spørgsmål 17

A system is designed with the following password policy:
The password must be 4, 5, or 6 characters. A character can be, a-z, A-Z, 0-9.
What would be the average time to crack a password, assuming we could test a password every nanosecond and the passwords are evenly distributed?

- [ ] 58 seconds
- [ ] 29 seconds
- [ ] 16 hours
- [ ] 8 hours

Side 7

Spørgsmål 18

A small company wants to implement an Access Control system and have been offered 4 different proposed solutions, where the security policies are managed by the supplier. Two of these solution use RBAC and the other two use ACLs, they are fine with either system, but want you to chose the solution that follow their specification which can be seen bellow:
These are the operation they want each of the 3 users to be able to perform: ([User, Operations])
[Alice, {Start server, Stop server, Check server status, Use server, Create user, Delete user}]
[Bob, {Create user, Delete user, Change user's permissions}]
[Charlie, {Check server status, Use server}]
Here are the operation each role have the right to perform in RBAC: ([Role, Operations])
[Server assistant, {Start server, Stop server}]
[Server administrator, {Start server, Stop server, Check server status, Use server}]
[Worker, {Check server status, Use server}]
[People supervisor, {Create user, Delete user}]
[People manager, {Create user, Delete user, Change user's permissions}]
Here are all possible operations with there corresponding number in ACL: ([Operation, Number])
[Start server, 1]
[Stop server, 2]
[Check server status, 3]
[Use server, 4]
[Create user, 5]
[Delete user, 6]
[Change user's permissions, 7]
Which one of the four Access Control System proposals correctly follows the specified users permissions listed above? (name [permissions])

- ☐ RBAC: Alice [Server assistant, Worker, People supervisor], Bob [People manager], Charlie [Worker]
- ☐ RBAC: Alice [Server administrator, People manager], Bob [People manager], Charlie [Worker]
- ☐ ACL: Alice [1, 2, 3, 4, 5, 6], Bob [5, 6, 7], Charlie [2, 3, 4]
- ☐ ACL: Alice [1, 2, 3, 4, 5 ,6], Bob [5, 6], Charlie [3, 4]

Spørgsmål 19

You are the system administrator of the British company Reynholm Industries and have been asked to assign privileges to three people that have just been hired in the IT department. The access control mechanism uses ACLs.
Jen is the department head, so in order to make sure that the day-to-day operations run smoothly she needs to be able to see the list of employees and assign tickets.
Moss is a computer programmer, so he needs to be able to access, solve and close tickets.
Roy is the IT technician and he should be able to access tickets and send them for review.
In the table below we can see an overview of the operations and the operation numbers.
[Operation, Number]
[See employee list, 1]
[Solve ticket, 2]
[Access ticket, 3]
[Send ticket for review, 4]
[Close ticket, 5]
[Assign ticket, 6]
Which of the following policy specifications reflects the access control policy defined informally above?

- ☐ Jen = [1, 5, 6], Moss = [2, 3, 5], Roy = [3, 4]
- ☐ Jen = [1, 6], Moss = [2, 4, 5], Roy = [3, 4]
- ☐ Jen = [1, 6}], Moss = [2, 3, 5], Roy = [3, 4]
- ☐ Jen = [1, 6], Moss = [2, 3, 5], Roy = [3, 4, 5]

Spørgsmål 20

You are the manager of a small firm (FM consulting) that provides consultancy services within cyber security.
Nina has recently done consultancy work for the DSB (Danish trains association) & ShareNow(car sharing company). She is currently finishing up a project with the Danish ministry of health.
Ahmed is a recent PHD graduate from DTU with a speciality in cyber security. He is is currently working
on smaller assignments for Ørsted (energy company), which is about to end.
Sara has worked with you for 10 years, where she has focused security on architectures for the food industry. She is about to finish a security architecture for Arla (food company).
Christian is currently doing consultancy for Ford and has in the past worked within security architecture for Nordea (Bank).
Peter joined the firm 6 years ago, before that he worked at Tesla (Electric car company). Since joining your firm, he mainly worked with providing services to financial institutions & banks.
Your firm is hired to develop a security architecture for the electric car company Bright Future. They want experienced consultants on the project. However the Chinese wall model should be applied to avoid, conflicts of interests.
Which team members will you choose for the project?

- [ ] Nina & Peter & Ahmed
- [ ] Ahmed & Christian & Sara
- [ ] Peter & Sara & Ahmed
- [ ] Nina & Sara & Christian

Side 8

Spørgsmål 21

Which of the following sentences is a characteristic of a Signature-based IDS detection method?

- ☐ Primarily introduced to detect and prevent unknown attacks and zero-day exploits
- ☐ May suffer from false-positives
- ☐ Effectiveness is highly dependent on having the latest updates
- ☐ Often incorporates statistical models or machine learning algorithms

Spørgsmål 22

Which of the following cryptographic protocols can the Kerberos protocol be classified into?

- ☐ Adjudicated protocol
- ☐ Arbitrated protocol
- ☐ Zero-knowledge protocol
- ☐ Self-enforcing protocol

Spørgsmål 23

The company Tycho Brahe Enterprises uses a private local area network, which uses a star topology; this means that all messages within this network are routed through the central router. All messages are protected by symmetric encryption (AES-128 in GCM mode) using a pre-shared key that was distributed when the network was originally configured and a HMAC using the same key.

After 2 years, an attacker is able to compromise the central router on the network, which of the following security goals are violated by this attack?

- ☐ Confidentiality – the attacker can read the contents of all messages
- ☐ Anonymity – the attacker can observe who communicates with whom
- ☐ Integrity – the attacker can swap the contents of messages without either party's knowledge
- ☐ None of the above – the described protocol guarantees all of these security goals

Spørgsmål 24

You're an IT-security expert working for a large company. You're in charge of designing a system to handle the private data of the company's customers and employees located in the EU. Some of the data is sent in through an online form, and some is input manually at several locations around the EU where the company operates. Typically paper forms filled out by customers, these are thrown into paper recycling afterwards. Given you're skilled at implementing the IT-system, the design and implementation of the system can be considered secure, i.e., it is not possible to break into the system or leak data during transport, and all clients and servers are located in the EU.
What other aspects must be considered before this setup is in compliance with GDPR?

- ☐ We must consider the physical security of our data sites, and not only the cybersecurity aspect of the data. It must also be considered how the physical data forms are handled as these also contain private information, and they should be dealt with properly. It is not sufficient to simply throw out these forms, there should be steps taken to ensure they are not legible after use
- ☐ We must consider the physical security of our data sites, and not only the cybersecurity aspect of the data. It is not sufficient to only build a secure IT-system, as data leaks can be caused by any number of factors. The issue related to physical data forms must be handled by other people as that is outside your responsibility
- ☐ We only need to consider the security of the IT-systems, including the physical locations where data is stored and processed, because GDPR only applies to data in electronic form
- ☐ Since you're hired only as an IT-security expert, implementing a secure IT-system is sufficient from our perspective, and the rest of the issues should be handled b other people

Spørgsmål 25

The Austrian privacy activist Max Schrems is currently ensued in a legal procedure with the social media company Facebook about the processing of user data and the permission necessary to do so. Therefore, let us consider the following scenario: Max is asking Facebook for a copy of his personal data according to data protection law. He does so by using the provided tool by Facebook.
Based on his legal rights, what data could Max expect to receive from Facebook?

- ☐ Any information relating to him as an identified or identifiable natural person.
  Furthermore, Facebook is required to prove the completeness of the data
- ☐ Facebook only needs to provide data it considers necessary, as it is stated in Art. 15 of the GDPR
- ☐
  As Max used the tool provided by Facebook for asking for a copy of his user data, he accepted an additional Term of Service and therefore Facebook is allowed to specify the range of data
- ☐ Since Facebook's Headquarter is situated outside an EU country, the GDPR does not apply in this case and is therefore not required to provide any data