Exam 2020

Side 1

Diffie-Hellman and friends

Filer: step.anb

Spørgsmål 1

What is the problem with the attached protocol StEp.anb?

- [ ] A cannot generate the h(...) term in the last step.
- [ ] B cannot generate the h(...) term in the last step and thus never obtain Msg.
- [x] A man-in-the-middle attack is possible.
- [ ] Diffie-Hellman forbids the re-use of exponents like the fixed sec(A) and sec(B).

Spørgsmål 2

It would be sufficient to break Diffie-Hellman, if one of the following four algorithms has a practical run time. Which one?

- [ ] Algorithm 1: given g, p, g^X mod p and Y, it computes (g^Y)^X mod p;
- [x] Algorithm 2: given g, p, g^X mod p, it computes X;
- [ ] Algorithm 3: given p, X, g^X mod p, it computes g;
- [ ] Algorithm 4: given p, X, (g^X)^Y mod p and X, it computes g^Y mod p;

Side 2

Protocol Security

Spørgsmål 3

Given a protocol that satisfies weak authentication, but suffers from a replay attack. Which of the following modifications eliminates the replay attack?

- [x] Add the following steps at the beginning of the protocol: every participant generates a fresh nonce and sends them to all other participants in clear text. Then add these nonces to every encrypted message of the protocols.
- [ ] Add the following steps at the beginning of the protocol: every participant generates a fresh public key and sends them to all other participants in clear text. Then every message is encrypted with the public key of the recipient.
- [ ] Add the following steps at the end of the protocol: every participant generates a fresh symmetric key and generates with that key a MAC of all messages they have sent or received, and sends it to all participants.
- [ ] None of the above methods for work every protocol.

Spørgsmål 4

Suppose Pw and M are two guessable secrets, while K is a non-guessable key, and Pk/inv(Pk) is a public/private key pair. Which of the following messages is NOT vulnerable to a guessing attack?

- [ ] {Pw,M}Pk
- [x] {M,K}Pk
- [ ] {|Pk,M|}Pw
- [ ] {{| K |}Pw}inv(Pk)

Spørgsmål 5

A Kerberos Key Distribution Center (KDC) server has a maximum ticket lifetime of 24 hours. What ensures that an expired Kerberos ticket can no longer be used?

- [ ] Whenever a client connects to a server with an expired ticket, the server sends a query to the KDC server to verify the ticket validity with respect to the KDC's clock, and fails to authenticate the client because the KDC reports that the ticket has expired.
- [ ] KDC server refuses to establish new connections between clients and servers for expired tickets.
- [x] When a client connects to a server, the server compares the ticket's expiration time to the server's current clock, and refuses to authenticate the user if the ticket expiration time is in the past.
- [ ] When a client connects to a server, the server sets a 24-hour timer to terminate the connection, which ensures a client cannot remain connected past the ticket’s maximum lifetime.

Side 3

Software Security

Spørgsmål 6

DTU has a website where professors can enter the exam grades of the students. Suppose a student sends a link to a professor leading to a malicious website that looks harmless and the professor clicks on this link while being logged in to the exam grading system. Now, somehow the student's grade in the exam database is set to grade 12. What attack could that have been, if we assume that there is no vulnerability in the professor's browser or email client?

- [x] XSS and/or CSRF
- [ ] Buffer Overflow
- [ ] SQL injection
- [ ] Side-channel

Spørgsmål 7

What is a correct way of mitigating a SQL Injection attack?

- [ ] Asking users to confirm dangerous operations.
- [x] Enforcing a separation between data and code.
- [ ] Merging the tables in the database.
- [ ] Using a firewall.

Spørgsmål 8

Which of the following statements is true about the Spectre attack discussed in the lecture?

- [ ] The attacker must know the exact location of the secret in memory.
- [x] The attacker must know the exact piece of code the victim is executing.
- [ ] The attacker must ensure all data needed by the code is in the cache.
- [ ] The attacker must ensure that the branch prediction is always correct.

Spørgsmål 9

Consider the information flows in the following piece of code:

```
while (z>10){
   b = x;
   if (c<20)
      y = y - 1;
}
a = (y/2) + 1;
z = x + 1;
```

From where to where flows information? (We omit flows that result from transitivity: if a->b and b->c then we may omit a->c.)

- [ ] x->b, y->a, x->z
- [x] x->b, y->a, x->z, z->b, c->y, z->y
- [ ] x->b, y->a, x->z, z->b, c->y, z->y, z->c
- [ ] x->b, y->a, x->z, z->b, c->y, z->y, z->c, b->x

Side 4

Privacy

Spørgsmål 10

Recall that many tracking apps for Covid19 generate a day pseudonym SK for every user, and the next day's pseudonym is obtained by applying a hash function: h(SK). Every 15 minutes a new ephemeral Identity is generated as prg(SK,i) where prg is a pseudo-random-number generator, SK is the day identity, and i is the i-th number generated (i.e., i is incremented every 15 minutes). The current ephemeral Identity is exchanged with devices in the proximity.

Recall also that when somebody declares sick, they essentially publish via a special server their SK's for the relevant days. Suppose they would instead publish the relevant ephemeral IDs instead, and moreover, they submit to the server each ephemeral ID in a separate message through an onion routing network.

What would be the consequence?

- [x] This would increase privacy, because the different ephemeral IDs cannot be linked to the same person.
- [ ] This would decrease privacy, because an intruder can see which ephemeral IDs correspond to a sick person.
- [ ] This would be equivalent in terms of privacy, it just increases the data volume that needs to be transmitted.
- [ ] This would increase privacy, because the onion routing protects the real identity of the sick person.

Side 5

Cryptography

Spørgsmål 11

Which of the following is not an encryption algorithm?

- [x] SHA
- [ ] DES
- [ ] AES
- [ ] RSA

Spørgsmål 12

The TCP handshake protocol starts by the initiator transmitting a SYN character (ASCII: 22) is encrypted using RSA. The following parameters are used for the RSA encryption and decryption: e = 7, d = 103 and n= 209. Which cipher-text corresponds to the encrypted SYN character?

- [x] 154
- [ ] 27
- [ ] 33
- [ ] 90

Spørgsmål 13

What statement best describes the concept of non-repudiation?

- [x] A party cannot later deny sending a message.
- [ ] Communication between two parties is secure.
- [ ] An attacker cannot interfere with a message in transit.
- [ ] An attacker cannot perform traffic analysis.

Spørgsmål 14

Which of the four general types of cryptanalysis requires the most powerful attacker?

- [x] Cipher-text only attack.
- [ ] Known plain-text attack.
- [ ] Chosen plain-text attack.
- [ ] Adaptive chosen-plaintext attack.

Spørgsmål 15

Which of the following is true for Self-Enforcing Protocols?

- [x] Disputes are not possible.
- [ ] A trusted third party is required.
- [ ] The protocol is always executed in its entirety.
- [ ] It should be avoided, since security is not sufficient.

Side 6

More Cryptography

Spørgsmål 16

Certificate revocation is a property of public key infrastructures (PKIs). Which of the following statements about certificate revocation is true?

- [x] Certificate revocation is necessary to ensure the validity of certificates in case the associated private key is compromised.
- [ ] Certificate revocation guarantees that all certificates provided by certificate authorities (CAs) are valid and never compromised.
- [ ] Certificate revocation can only be done manually by using Certificate Revocation Lists (CRL).
- [ ] Certificate revocation prevents certificate authorities from issuing certificates to unauthenticated users.

Spørgsmål 17

What is a Replay Attack?

- [x] Intercepting, and then delaying or retransmitting a legitimate message in order to misdirect or exploit the receiver's answer.
- [ ] Retransmitting fake data over and over to spam and misdirect the receiver.
- [ ] Sending the same or random messages to the receiver over a certain amount of time from many machines to overload the receiver.
- [ ] Receiving the response from the server and using it it to access sensitive information.

Spørgsmål 18

Which security property does a successful block replay attack violate?

- [x] Integrity.
- [ ] Confidentiality.
- [ ] Availability.
- [ ] Privacy.

Spørgsmål 19

You have been hired as an accountant to protect a door-lock system from Replay attacks. All messages sent and received are encrypted using public-key cryptography. What measure should be implemented to counteract this vulnerability?

- [x] Include a unique identifier in each message.
- [ ] Attach a signed hash of the message to each message.
- [ ] Encrypt each message with a shared symmetric key.
- [ ] Attach a HMAC to each message.

Side 7

Network Security

Spørgsmål 20

Which of the following types of Malware is most appropriate to use for an attacker, who wishes to infect as many systems as possible on a network

- [x] A Worm.
- [ ] A Rootkit.
- [ ] A Virus.
- [ ] A Trojan Horse.

Spørgsmål 21

How do Host Based Intrusion Detection Systems work?

- [x] By inspecting application log-files.
- [ ] By comparing network traffic with established patterns of malicious network traffic.
- [ ] By establishing base line for normal communication and detecting abnormal traffic pattern.
- [ ] By filtering traffic at each individual node of the network (personal firewalls).

Spørgsmål 22

The link-to-link encryption mode is one of the possibilities while choosing the method to encrypt network traffic. Its advantage over the End-to-End encryption is that it:

- [x] Encrypts some data-link headers as well as the body of the message.
- [ ] Allows the users to choose the encryption algorithm suiting their needs.
- [ ] Ensures that messages are protected through intermediate nodes.
- [ ] Provides the means to authenticate both of the users.

Spørgsmål 23

A retail grocery company, which ships groceries all around Zealand, has a single warehouse (named Warehouse1,) where they run a legacy warehousing software system, which allows them to keep track of the goods they have in the warehouse. Both in terms of warehouse location, amount, grocery to grocery store destination etc.
This is manged through a web browser on a machine connected to the system. As the system is old, it does not support modern software practices, including transit encryption, user login and proper logging of user activities.
As the company decides to expand with stores in Jutland, it intends to create a new warehouse (Warehouse2) to support this region of Denmark. There is also an interest to make grocery stores connect to the warehousing system.
It is found that the best value for money approach, as well as for simplicity, is for Warehouse2 to use the same software system as Warehouse1. Therefore, a secure site-to-site connection between Warehouse1 and Warehouse2 is needed. In addition, new legislation means that the company has to comply with accountability and auditing regulation.
All-in-all, there must be some confidentiality in place when connecting to the system from Warehouse1, user login capabilities, and some means to log user activity.
The supplier behind the legacy warehousing system does still exist, but has been bought up by a bigger consulting firm. They offer to change the warehousing system, but at a significant cost.
Given this scenario, what would be the best countermeasure solution?

- [x] Setup a circuit-level gateway between Warehouse1, Warehouse2 and setup an application proxy in front of the software system.
- [ ] Setup a circuit-level gateway between Warehouse1, Warehouse2. No other countermeasures are needed.
- [ ] Setup a stateful inspection firewall at Warehouse1 and allow only Warehouse2 IP and ports to connect. Then setup an application proxy in front of the software system.
- [ ] Setup a circuit-level gateway between Warehouse1, Warehouse2. For the software system, the only option is to have company pay the consulting firm to upgrade the system to support the company requirements.

Side 8

Authentication

Spørgsmål 24

Consider a read-only public password file stored in plain text. Each password entry in the file is stored in the format username:h(password,s):s, where username and password are strings indicating the username and the password of a user, h is some strong cryptographic hash function, and s is some fixed 32-byte string generated at random for each entry. Which of the following statements is true about s.

- [x] The inclusion of s helps in preventing an attacker from using a hash table or rainbow table to lookup hashed passwords.
- [ ] The inclusion of s helps in preventing an attacker from brute forcing the password of individual users.
- [ ] The inclusion of s allows the server to authenticate itself towards the user.
- [ ] The inclusion of s allows the server to authenticate the user on s if the user forgets his real password.

Spørgsmål 25

Assuming we are implementing Kerberos like authentication, in a setting where there are insecure "dumb" terminals, that users can access and a secure server. What is the use of synchronized clocks in this setting?

- [x] To ensure correct interpretation of timestamps and expiration dates.
- [ ] To generate the same random seed for the running key generator on all machines.
- [ ] To ensure proper connection setup and tear-down.
- [ ] To keep the system running on time.

Spørgsmål 26

Which is the best way to protect a password mechanism against a brute-force attack originating from outside the organization's network

- [x] Implement an exponential growing delay after each failed authentication attempt.
- [ ] Include a salt with the password.
- [ ] Only store hashed passwords in the password file.
- [ ] Enforce a policy where users must change password every 3 months.

Spørgsmål 27

Alice was given a task of monitoring the results of the hand geometry scanner used for the access granting to the very important laboratory. After a week, her boss asks her to report to him the accuracy (A) and the specificity (S) of the system.
Alice saved the monitored results in the following table:

	Person had access rights	Person did not have access rights
Test positive (authenticator did match)	16	1
Test negative (authenticator did not match)	2	12

Which two number should Alice report?

- [x] ~~A = 0.90; S = 0.86~~
- [ ] ~~A = 0.89; S = 0.58~~
- [ ] ~~A = 0.52; S = 0.86~~
- [ ] ~~A = 0.90; S = 0.80~~

Spørgsmål 28

An intelligent door-lock system for a smart home relies on an app on the user's smartphone. The app uses the phone's camera to perform facial recognition of the user and sends a message to unlock the door if a registered user is recognized. What authentication factors are used in this system?

- [x] Something he possesses and something he is.
- [ ] Something he possesses and something he knows.
- [ ] Something he knows and something he is.
- [ ] Something he knows and somewhere he is.

Side 9

Access Control

Spørgsmål 29

Which of the following statements are **NOT** a rule for Role Based Access Control (RBAC)?

- [x] A subject can only be assigned a single role.
- [ ] A subject's active role must be authorized for the subject.
- [ ] A subject can only execute a transaction if it is authorized for its active role.
- [ ] A subject can only execute a transaction if it has selected a role.

Spørgsmål 30

A company is using the Bell & LaPadula model for file protection. Files are classified into three different categories: Top Secret, Secret, and Unclassified. Every user's access to the files is defined from their clearance. Bob has clearance Unclassified. There exists a file X that is labeled secret.
What permissions does Bob have with regards to the secret file X?

- [x] Bob can write to X but cannot read X.
- [ ] Bob can both read and write to X.
- [ ] Bob can read X but cannot write to X.
- [ ] Bob cannot read nor write to X.

Spørgsmål 31

The company described in the previous question changes their protection system to one based on the Biba model; file labels and user clearances remain the same.
What permissions does Bob now have with regards to the secret file X?

- [x] Bob can read X but cannot write to X.
- [ ] Bob can both read and write to X.
- [ ] Bob can write to X but cannot read X.
- [ ] Bob cannot read nor write to X.

Spørgsmål 32

As the system administrator of the paper company Dunder Miflin, your boss Michael Scott has decided that you need to transform the current RBAC system into an ACL system and update the rights for the employee Dwight, from Salesman to Assistant Regional Manager.
An overview of the current roles and their operations can be seen below:
[Role, Operations]
[Secretary, {Email, Forward calls, Print/Copy, Schedule meetings}]
[Salesman, {Email, Print/Copy, Call, Register order}]
[Assistant Regional Manager, Salesman[{Forward to regional manager}]
[Regional Manager, Secretary [Assistant Regional Manager]

An overview of the current roles and the users can be seen below:
[Role, Users]
[Secretary, {Pam}]
[Salesman, {Jim, Dwight}]
[Assistant Regional Manager,{}]
[Regional Manager, {Michael}]

An overview of the current operations and their operation number can be seen in the table below:
[Operation, Number]
[Email, 1]
[Print/Copy, 2]
[Register order, 3]
[Forward calls, 4]
[Call, 5]
[Forward to regional manager, 6]
[Schedule meetings, 7]

Which of the following correctly reflects the users' access to operations after the changes has been applied?

- [x] Pam = {1, 4, 2, 7}, Jim = {1, 2, 5, 3}, Dwight = {1, 2, 5, 3, 6}, Michael = {1, 4, 2, 7, 5, 3, 6}
- [ ] Pam = {1, 4, 2, 7}, Jim = {1, 2, 5, 3, 6}, Dwight = {1, 2, 5, 3, 6}, Michael = {1, 4, 2, 7, 5, 3, 6}
- [ ] Pam = {1, 4, 2, 7}, Jim = {1, 2, 5, 3}, Dwight = {1, 2, 5, 3}, Michael = {1, 4, 2, 7, 5, 3, 6}
- [ ] Pam = {1, 4, 2, 7}, Jim = {1, 2, 5, 3}, Dwight = {1, 2, 5, 3, 6}, Michael = {1, 4, 2, 7, 5, 3}

Side 10

Security Management and Legal Issues

Spørgsmål 33

Which of the following statements are **NOT** true when planning a new security framework?

- [x] After creating a security plan from a set of given security requirements, the security policies of the company can be defined.
- [ ] To ensure the a new security plan is accepted and followed, there should be held periodic reviews of the security policies.
- [ ] Expected losses from potential risks to the organization have been calculated according to identified assets.
- [ ] It's important to ensure top level management support when defining security policies as they allocates funds and acts as the people with the power to settle conflicts between business and security goals.

Spørgsmål 34

A fashion shopping website uses a TLS protocol that requires both certificates from the server and the client issued by a trusted authority. The security architect assumes this is a sufficient and efficient way of establishing a secure channel for communication.
What is the problem with this assumption?

- [x] Most clients do not have a certificate of their own.
- [ ] Most web browsers do not support TLS protocols.
- [ ] Certificates can easily be forged by attackers, so they can impersonate the server or client.
- [ ] No certificates are necessary for the TLS.

Spørgsmål 35

The overall risk analysis of the ACME Company estimates an expected annual loss of 17 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 25 million kroner to implement, but will reduce the annual expected loss by 16 million kroner.
An Intrusion Detection System costs 10 million kroner to implement, but will reduce the annual expected loss by 12 million kroner.
A Security Operations Center costs 8 million kroner to implement, but will reduce the annual expected loss by 6 million kroner.
A Demilitarized Zone costs 6 million kroner to implement, but will reduce the annual expected loss by 5 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. Which technology do you recommend?

- [ ] Intrusion Detection System.
- [ ] Managed Security Service.
- [x] Demilitarized Zone.
- [ ] Security Operations Center.

Spørgsmål 36

You are working at a company based in the European Union (EU). Under which circumstances must you comply with the General Data Protection Regulation (GDPR)?

- [x] You must comply with GDPR whenever you are collecting data that is relating to an identified person.
- [ ] You must always comply with GDPR.
- [ ] You must comply with GDPR only if you are collecting medical data.
- [ ] You must comply with GDPR whenever you are collecting data about people that they might not want you to have, regardless of it being linked to an identified person.