Data Security Exam 2019

Side 1

Suppose we build an App that patients can install on their smart phone to receive a sick note from their doctor electronically and send it to their employer.

Spørgsmål 1

First, we want to ensure that the transmissions are encrypted. We can assume that both the doctor and the employer have a webserver with https running. Do we need anything else?

- [ ] Nothing more needed, https is sufficient.
- [x] The patients need to authenticate themselves to the doctor's website, e.g. using nemID. It is NOT utterly necessary to authenticate to the employer's website.
- [ ] The patients need to authenticate themselves to the employer's website, e.g. using nemID. It is NOT utterly necessary to authenticate to the doctor's website.
- [ ] The doctor and the employer need to authenticate themselves to the patient.

Spørgsmål 2

Assume the sicknote from the doctor has the shape:

```
{sicknote,Timeperiod}inv(pk(D)), {isdoctor,pk(D)}inv(pk(idp))
```

where "sicknote" and "isdoctor" are just a fixed strings identifying the purpose of the signatures; "Timeperiod" are the days for which the sicknote holds; the first part is a signature of the doctor, using the doctor's private key "inv(pk(D))" and the second part is a signature from an identity provider that certifies that "pk(D)" is the public key of a doctor.

The goals are

- that the employer wants that a dishonest employee cannot falsely claim to be sick
- and that patients want to protect their privacy as far as possible.

Do these goals require any changes to the protocol?

- [x] The sicknote should contain the name of the patient.
- [ ] The sicknote should contain the name of the employer.
- [ ] The sicknote should contain the name of the doctor.
- [ ] The protocol is fine like this.

Spørgsmål 3

For this sicknote protocol, consider the following claims of problems and solutions. Which of them is both a correct claim of a problem and a valid solution for that problem?

- [ ] If an attacker gets hold of a doctor's private key, he can sign sicknotes himself. To prevent this, one does not need to change the sicknote protocol, but we must require that the doctor regularly generates a new key pair and has it certified by the idp.
- [ ] A dishonest doctor can replay old messages and send them to other employers. To mitigate this, the employer and the employee should first generate a fresh nonce that the doctor must include in the sick note.
- [x] The employer can see if several sick notes have been issued the same doctor. This can be prevented if the doctor each time generates a fresh key pair and has it certified by the idp.
- [ ] A man-in-the-middle attack on the https connection between patient and doctor allows an attacker to find out the name of the patient. This can be prevented by encrypting the sicknote with the employer's public key.

Side 2

Diffie-Hellman

Spørgsmål 4

Alice and Bob are using the Diffie-Hellman key exchange to generate a shared key. They are using the following values. Prime: p = 23, generator: g = 5, Alice's secret: x = 15 and Bob's secret: y = 7. What is the resulting shared key?

- [ ] 21
- [x] 15
- [ ] 18
- [ ] 1

Spørgsmål 5

Consider the following challenge for the above Diffie-Hellman exchange: Alice and Bob do not have a direct security relationship. However, suppos they have a mutual friend Charly who is honest and both Alice and Bob trust Charly. Moreover, Alice has a shared symmetric key with Charly, and also Bob has a shared symmetric key with Charly. So they decide to run the Diffie-Hellman key exchange with Charly as an intermediary -- so that all messages are encrypted either with the shared key of Alice and Charly or with the shared key of Bob and Charly, respectively.

What security guarantees does that give for the resulting Diffie-Hellman key that Alice and Bob establish?

- [ ] Charly is a man in the middle and can later read any messages that Alice and Bob encrypt with the new Diffie-Hellman key.
- [x] The new Diffie-Hellman key between Alice and Bob is secure, even if an intruder later learns the shared key of Bob and Charly.
- [ ] The forwarding via Charly does not improve the security at all.
- [ ] This can actually compromise security, if the shared key between Alice and Charly or between Bob and Charly was also established using Diffie-Hellman.

Side 3

Software Security

Spørgsmål 6

How can a cross-site request forgery (CSRF) attack be prevented?

- [ ] Sanitizing all requests before sending them.
- [ ] Sending requests only via https.
- [ ] Turning off Javascript.
- [x] Including a server-generated nonce in the request.

Spørgsmål 7

For an information flow analysis, way suppose a program has declared variables x,y,z as level "high" (or "secret") and variables a,b as level "low" (or "public"), and information flow from "high" to "low" is forbidden. Which line of the following statements is then a forbidden information flow?

- [ ] y=z−1+a/2;
- [x] if (y>x) b=0;
- [ ] c=(a+2)*(a−1);
- [ ] if (a==2) x=y;

Spørgsmål 8

Which of the following is true about the Spectre attack?

- [x] It exploits speculative execution to load data into the cache.
- [ ] It measures the power consumption of the processor to read the caches.
- [ ] It exploits how compilers arrange the statements in the code to optimize the pipeling in a processor.
- [ ] It exploits that the runtime of code often leaks information about which branches a program where taken.

Side 4

Cryptography

Spørgsmål 9

Which problems of primary security goals (CIA) can be solved by cryptography?

- [ ] Confidentiality and Availability
- [x] Confidentiality and Integrity
- [ ] Integrity and Availability
- [ ] Confidentiality, Integrity and Availability

Spørgsmål 10

You have intercepted an enemy agent who managed to send an encoded message just before you caught her.
In her waste paper basket you find a piece of paper with some numbers, which you suspect are part of a one time pad.
Cipher text fragment: 10 0d 06 17 16 11
One time pad fragment: 63 68 65 65 73 65

- [ ] answer
- [x] secret
- [ ] secure
- [ ] choice

Spørgsmål 11

Which of the following algorithms is not used in asymmetric-key cryptography?

- [ ] RSA algorithm
- [x] AES algorithm
- [ ] ElGamal algorithm
- [ ] None of the above

Spørgsmål 12

For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Cipher message=11 and thus find the plain text.

- [x] 88
- [ ] 122
- [ ] 144
- [ ] 112

Spørgsmål 13

What is Kerckoff's Principle?

- [ ] Keep both the algorithms and the keys secret
- [x] Do not rely on the secrecy of the algorithm
- [ ] Longer keys always give stronger encryption
- [ ] None of the above

Side 5

Secure Communications

Spørgsmål 14

What security property does a message authentication code ensure in the communication between two agents?

- [x] The agents message's integrity
- [ ] The agents messages availability
- [ ] The agents privacy when sending messages
- [ ] The agents message's confidentiality

Spørgsmål 15

Cryptographic protocols can be divided into three sub-types: arbitrated protocols, adjudicated protocols and self-enforcing protocols. Select the statement which is true about one of the protocol types:

- [ ] In self-enforcing protocols, disputes can arise between honest actors
- [ ] In an adjudicated protocol, one of the communicating actors can also act as the adjudicator
- [x] Self-enforcing protocols are preferred whenever possible
- [ ] In arbitrated protocols, the neutral arbitrator is only involved in case of disputes

Spørgsmål 16

The Kerberos service is built on:

- [x] Symmetric cryptography
- [ ] Asymmetric cryptography
- [ ] Hybrid cryptography
- [ ] All of the above

Spørgsmål 17

The Kerberos Ticket Granting Service generates a key for clients that are authorized to access a particular server. What kind of key is generated?

- [ ] Public key
- [x] Session key
- [ ] Complimentary key
- [ ] Private key

Side 6

Network Security

Spørgsmål 18

From a security perspective, why is it important to segment your network?

- [x] To prevent exploits in one subnet from spreading to the other subnets
- [ ] To ensure that one subnet can be maintained without shutting down the whole network
- [ ] To reduce the cost of purchasing network equipment
- [ ] All of the above

Spørgsmål 19

Which of the following categories best describes the systems that should be included in a demilitarized zone (DMZ)?

- [ ] Firewalls and intrusion detection systems
- [ ] Web-servers and Application servers
- [ ] All machines that host security critical services
- [x] All machines that host external facing services

Spørgsmål 20

Imagine an intruder breaks into a bank database, and changes the amount of money someone has stored in the bank. What security property has been violated for the database?

- [ ] Confidentiality
- [x] Integrity
- [ ] Availability
- [ ] Accountability

Side 7

Authentication

Spørgsmål 21

Consider the security of a password file, which includes a 10 bit salt and all passwords are hashed, but known to consist of exactly 8 characters from the following alphabet: lowercase letters ('a' to 'z'), uppercase letters ('A' to 'Z'), digits ('0' to '9') and the following special characters ('.', '-', '_', '+', '<', '>', '=', '@').
Assume that a password cracking system, which is able to check 12 billion (10^12) guesses per second and is able to run around the clock all year, is used to crack the password file. Which of the following worst case estimates for cracking the password file is most accurate?

- [ ] One year
- [x] Two years
- [ ] Three years
- [ ] Five years

Side 8

Access Control

Spørgsmål 22

In a system which employs an access control policy, when a user makes a request for a resource, which of the following components is the first to receive the user's request details?

- [ ] Policy Information Point
- [ ] Policy Decision Point
- [ ] Policy Administration Point
- [x] Policy Enforcement Point

Spørgsmål 23

The Quux Laundry Company employs Role-Based Access Control to manage access to data in different folders; the permissions for each role are shown in the table below.

	Folder 1	Folder 2	Folder 3	Folder 4
Management	R/W	R/W	R/W	R/W
Back-end office	R	R	W	R
Front office	R	R	R	R

Assuming a new receptionist is hired, he needs to get permissions as a front office employee. However the admin, who created the new employee in the system, was not paying attention, and added him to the role "Back-end office", which security goals are violated?

- [ ] Confidentiality and Integrity
- [ ] Confidentiality and Availability
- [x] Integrity and Availability
- [ ] Confidentiality and Integrity and Availability

Spørgsmål 24

A system employs Bell-LaPadula model for file protection where files are classified with different labels, and users are similarly divided into groups identified with clearance levels. The levels are Top Secret, Secret, and Unclassified. If Alice has a clearance of Secret, and file X's label is Unclassified, which one is correct about Alice's permissions on X?

- [ ] Alice can read and write to X
- [x] Alice can read X, but Alice CANNOT write to X
- [ ] Alice CANNOT read X, but Alice can write to X
- [ ] Alice CANNOT read or write to X

Spørgsmål 25

As the administrator in a news company you have to assign operations to 3 people.
Tina is employed in the HR division, and as such needs access to get the list of employees of the company, and access to update the information about a single employee.
Henrik is hired as a writer, so he needs to be able to send articles to approval and the access to get articles, to edit possible mistakes.
Lisa has been hired as an editor, and as such needs access to approve articles that are send for approval, and remove current live articles.
An overview of the operations and their operation number can be seen in the list of operations below.

[*Operation, Number*]
[Send article for approval, 1]
[Get employee list, 2]
[Approve articles, 3]
[Remove articles, 4]
[Update employee information, 5]
[Get articles, 6]

The model used is ACL, which of the following correctly reflects the users access to operations after the update?

- [x] Tina = {2, 5}, Henrik = {1, 6}, Lisa = {3, 4}
- [ ] Tina = {1, 2, 5}, Henrik = {1, 2, 6}, Lisa = {1, 3}
- [ ] Tina = {2, 5}, Henrik = {1, 4}, Lisa = {3, 6}
- [ ] Tina = {2, 5}, Henrik = {1, 4, 6}, Lisa = {3, 6}

Spørgsmål 26

You are managing a small security consultancy company with only five security consultants.
Henrik has recently done consultancy work for the National Roads Authority, Tesla Motors and Q8 Petroleum, but has earlier focused exclusively on security in the education sector. He is currently finishing a security architecture for Astralis Group (the company behind the Astralis Counter Strike team).
Peter is currently doing consultancy for the company that runs the Circle K petrol stations, but this assignment is low intensity and has a long deadline. In the past he has worked with Vestas and Siemens Wind-power.
Lotte has worked with you for 10 years, where she has developed security architectures for the financial sector. She is about to finish a security architecture for Korsbæk Bank Group.
Erik joined the company 5 years ago from a position at Saudi Aramco (the Saudi oil company). Since joining your company, he has primarily worked with micro breweries, but has also done some work for local municipalities.
Susan has recently graduated from DTU, where she worked as a teaching assistant on several security courses. She is is currently working on a small assignment for the Danish Defense Forces, which is about to end.

Your company is hired to develop a security architecture for the oil company Snake Oil Inc., which is concerned about possible conflicts of interests, so the Chinese Wall Model should be applied. On the other hand, they also want the architecture developed as quickly as possible.
Which team should you select for this assignment?

- [x] Lotte + Erik + Susan
- [ ] Peter + Lotte + Susan
- [ ] Henrik + Erik + Susan
- [ ] Henrik + Peter + Lotte

Side 9

Security Administration

Spørgsmål 27

A company has identified a risk in the system they use. They believe the risk has a likelihood of happening of 20%. If the event should occur, the company would lose 10,000,000$. They have therefore found 4 potential fixes:

Solution 1 would cost the company 5,000,000$ to implement, and reduce the likelihood of the event occurring to 10%.
Solution 2 would cost the company 500,000$ to implement, and reduce the likelihood to the event occurring to 15%.
Solution 3 would cost the company 150,000$ to implement, and reduce the likelihood to the event occurring to 18%.
Solution 4 would cost the company 6,000,000$ to implement, and reduce the likelihood to the event occurring to 8%.

Which of the four approaches provides the best value for money?

- [ ] Solution 1
- [ ] Solution 2
- [x] Solution 3
- [ ] Solution 4

Spørgsmål 28

Which of the following statements about GDPR is correct?

- [ ] The GDPR only applies to organizations based within the EU
- [ ] The GDPR only applies to personal data that is processed wholly by automated means
- [ ] The GDPR covers any processing of personal data of people in the EU, regardless of whether the organization concerned is based in the EU
- [x] The GDPR covers organizations outside the EU who offer goods and services to people in the EU

Spørgsmål 29

A subject requests that inaccurate/incomplete data be rectified. How long do you have to comply?

- [ ] 3 months
- [x] 1 month
- [ ] 1 week
- [ ] 2 months