CS-C3130 Information security, autumn 2020

Example exam questions

1. Security terminology

Give an example of each of the following in the context of a cloud-based medical database that stores critical patient data. The example should clearly demonstrate that you have understood the meaning of the concept. The answer should be an example; no points will be given for a definition.

1. no-write-up policy
2. de-anonymization
3. risk-based authentication

2. Security technology and concepts A

Acme Inc. has created a cloud-based online service where the users can register and set up a username and PIN code. So far, they have one million (1 000 000) registers users. The PIN codes are machine-generated random 10-digit numbers.

The passwords are stored as hash values that are truncated to 128 bits:

hash = truncate(SHA-256("acmeonline"+salt+password), 128)

The salt is a random value that is concatenated to the password before hashing. It is also stored in plaintext with the hash value.

Sadly, the password database has leaked to the deep web where Wile E., a notorious hacker, has found them, and he now plans do brute-force cracking.

Problem: *How much does it cost for the attacker to crack a specific user's PIN code / at least one PIN code / all PIN codes?*

In addition to the results, show the calculation steps.

3. Security technology and concepts B

In your role as a penetration tester, you have been asked to infiltrate the Euro Shopper factory and retrieve the secret energy drink formula from a computer in the factory control room. You have taken a job in the factory as cleaner. This allows you to roam the facility with relative freedom in the evenings, after the beverage engineers have gone home. You are not allowed to enter when they are at work. So far, you have discovered the location of the computer. It is a Windows PC.

You sneak into the control room in the evening and start examining the computer. You power up the computer and see the text: “Plug in the USB drive that has the BitLocker key”.

Problem: *What realistic ways do you have for getting access to the secret formula on the computer?*

(You can get some points by explaining why certain attacks will not work.)

4. Security technology and concepts C

National Land Survey of Finland (NLS) maintains a public register of land ownership and property transactions in Finland. All property transactions (i.e. sales and purchases of land) must be entered into the register to become official. Thus, the NLS database contains authoritative information about who owns each piece of land in the country. Obviously, the integrity of the property transaction register and the citizens' trust in its correctness are critical to the functioning of the society. The information in the NLS databases is public and available to anyone.

It has been suggested that the property transaction register maintained by NLS could be replaced by a distributed blockchain. There is, however, currently to consensus for making such changes. A public register maintained centrally by a government agency like NLS seems still the safest solution. Nevertheless, ideas from blockchains could be used for additional integrity protection and auditing on top of the centrally managed register.

Your task: Explain how ideas from blockchains could be used to protect and audit the integrity of the NLS property transaction register.

Using Word or Paint to draw a picture may help.

5. PKI and TLS

The attached certificate chain was received by a web browser from **https://www.yle.fi/.** The chain has been pretty-printed with the openssl tool. *Explain in detail how the web browser checks the certificate chain and uses it to authenticate the web site.*

Note 1: You do not need to write out the messages of the SSL/TLS handshake protocol.

Note 2: The answer must be specific to the attached chain. No points will be given for a generic answer that fails to match the attached certificate chain.

(See the lecture slides for how to pretty-print any certificate chain.)