Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DV026G Information Security

Daniel Bosk

Department of Information and Communication Systems,
Mid Sweden University, SE-851 70 Sundsvall
Email: daniel.bosk@miun.se
Phone: 010-142 8709

2017-11-07

Instructions

Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet. Do not forget to *motivate your answers.*

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points—even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary, course material and notes, calculator.

Questions 7

Preliminary grades

Each question can be awarded up to three points: one point for E, two points for C and three points for A. To get an E, you must get at least one point on each question — i.e. no question must be awarded zero points. For a C, you must get two points on at least half of the questions. For an A, you must get three points on at least half of the questions.

Questions

The questions are given below. They are not given in any particular order.

(3p) 1. There is a strong relation between accountability and identity (why?). There is also a strong relation between identity and authentication (why?). Finally, there is a strong relation between authentication and usability (why?). Discuss the various requirements and possible trade-offs needed to get proper accountability. (Also answer the why-questions above.)

> **Suggested solution** Accountability needs the identity of the subject to hold the subject accountable for its actions. To ensure that the identity of the subject is correct, we need authentication to authenticate the subject's identity. Authenticating the subject of course affects the usability.
>
> Accountability is long term, concerning many events over maybe days, weeks or years. This means that we need to authenticate every (critical) action of the subject. This affects usability even more (than just authenticate at login, for instance).

(3p) 2. What is mandatory access control? Discuss its advantages and disadvantages and its suitability in different situations.

> **Suggested solution** Mandatory access control sets the access policy for created objects based on fixed rules in the system.
>
> This helps enforcing the policy and avoid mistakes. On the other hand, it will prevent communication downwards, which might be necessary sometimes (this is usaully solved by special procedures for declassification).
>
> However, whether it is good or bad depends on the situation. Sometimes it's good to have a combination of mandatory and discretionary access control.

(3p) 3. Discuss the overall goal of the security field and its role in society.

> **Suggested solution** The goal of the security field is to provide means to prevent, detect or recover from failures. This includes all kinds of systems, from buildings to smartphones.
>
> Security must take a more central role in society as society becomes more and more dependent on digital systems whose interfaces are available to everyone, e.g. through the Internet — for example, a web portal to the company network or the interface of a web-connected surveillance camera or "Internet of Things" in general.
>
> It must be everyone's responsibility to improve security — no one must neglect it! This was clearly illustrated by the Mirai botnet, where vulnerabilities in ordinary peoples' IoT products (webcams, video recorders, etc.) were used to take down large parts of the core Internet infrastructure. Although a vulnerability in a webcam intuitively is only bad for the person having the webcam — some remote person can spy on them, record secret videos etc. — this is not the case, it can be bad for everyone as that webcam can be used to execute attacks against others. Thus one insecurity "here" might actually result in insecurities "there", "there" and "there". It is very hard to predict.

(3p) 4. You've just landed a job at an IT department somewhere and now you're having one of your first few days. There is a discussion in the "fika room", the topic is the IT department's password policy.

"Well, every respectable website requires at least eight characters, with lower and upper case, numbers and special characters", the head of department says, "so we have it too".

What would you like to say in this conversation?

Suggested solution The last decades' research in user authentication says that such a policy yields bad security. It forces users to select easy to guess passwords and incentivizes password reuse while more secure passwords are disqualified according to the policy.

A better policy is to have at least 12 characters as the only requirement. Also, no requirement of updating the password at regular intervals — only if a breach has occurred.

(3p) 5. Alice wants to provide confidentiality to a file.

(a) She can accomplish this through mechanisms provided in the operating system. Explain how this works and what the limits are.

(b) She can also accomplish this through purely cryptographic mechanisms. Explain how this works and what the limits are.

Suggested solution The first way she's securing her file is by using access control mechanisms in the operating system (OS).

Assuming we have physical access to the computer, then we can just read the raw data from the disk. This can be accomplished by either booting our own OS on her computer, or by removing the disk.

If we don't have physical access we can always try to bypass the access control mechanisms in other ways, e.g. by gaining privileges in the system or seeing if the OS has failed to protect reading from the raw disk (i.e. not using the file system).

The main point here is that the operating system must be working correctly for its mechanisms to be effective. The *running* operating system will provide confidentiality by not allowing other users' requests to open the file.

The most obvious way to have system independent security for this file is to encrypt it, i.e. using cryptographic mechanisms. This way no one can read it unless they have access to the key, and this is true no matter if you change the environment. (Of course, if the system is untrusted someone can get to the key that way, but that's outside the scope of this question.)

(3p) 6. We have talked about how the users' mental models of how a program (and computer) works can endanger the users' security when the mental model and reality are not aligned. This is true also for developers (we mentioned this when we talked about software security), give an example of how the developers' mental models are relevant for software security.

Suggested solution Gollmann talked about broken abstractions. One example is characters: usually we abstract away the encoding and decoding parts, we see them as characters and not bytes. So encodings like UTF-8 can cause problems since the same character can be represented by several byte sequences.

Another is the finite precision arithmetic that we work with in computers, usually congruences modulo 2^{32} or 2^{64}.

(3p) 7. Give an example of a side-channel attack and motivate why it is a side channel. Explain whether your side-channel requires an active or passive adversary and discuss how difficult this side-channel will be to exploit.

Suggested solution A side channel is an unintended channel emitting information which is due to physical implementation flaws and not theoretical weaknesses or forcing attempts.

Extracting the secret key from a device by measuring energy consumption or electromagnetic emissions while the device performs computations using the secret key.

This is a side channel since it relies on a weakness in the hardware implementation of the crypto system. It is further an active attack since we might need the device to perform operations on certain ciphertexts (or plaintexts).

The example from the lecture of reading the electromagnetic emissions from a screen display is a passive attack.