Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

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

2019-03-22

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.

Questions 6

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. "Well, every respectable website requires at least eight characters, with lower and upper case, numbers and special characters", your boss says, "so we can have it too".

What would you like to say in this conversation? (First, consider the alternatives to passwords. Second, how would you do passwords properly?)

> **Suggested solution** There are better alternatives to passwords. E.g. we can use cryptographic techniques instead, BankID is a good example. Then we would reduce the problem of breaches as well, no problem leaking public keys since they're public.
>
> If we are to use passwords: 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) 2. (a) Give an example of a covert channel and

> **Suggested solution** A server is anonymous (e.g. a Tor hidden service), i.e. you may access the server but not know its location. Part of the server's service is giving the time. It has been shown that the variations in the system clock depend on the ambient temperature. This means that by studying how the time on the server varies over day and night and over the seasons, we can eventually figure out the ambient temperature. From the ambient temperature we can later deduce the geographical location of the server.

(b) what we can do about it.

> **Suggested solution** We can lower the resolution in the time-stamps the server gives, e.g. by not giving seconds. This lowers the bandwidth of the covert channel, perhaps so that the attack is infeasible. We could also sync the servers clock more often, e.g. by using the Network Time Protocol. However, the only way to prevent it is by not revealing the time of the server's system clock.

(3p) 3. What is the purpose of separation of duty? Explain and illustrate your explanation with an example.

> **Suggested solution** The purpose of separation of duty is to make it more difficult for a malicious entity to subvert the system. E.g. a systems developer at the bank should not be able to add a back-door for himself so that he later can steal money without anyone noticing. If he is only allowed to write the code, but not to certify its correct function — then there is a higher chance that he is caught before the system is launched. So to subvert the system a malicious actor must act together with others.

(3p) 4. There are numerous alternatives available today for end-to-end secure communication[1], e.g. the apps Signal, WhatsApp and Telegram for instant messaging, media messaging and video calls; PGP and S/MIME for email. They are all based on a combination of public-key and shared-key cryptography.

Discuss the security and usability challenges facing end-to-end secure communication.

[1] Normally this is referred to as end-to-end *encrypted* communication, but we have integrity in addition to confidentiality.

Suggested solution The challenge for these systems is to provide a design which aligns the security with how users work.

The easy part is to provide a tool for securing the communication, i.e. encrypting and providing integrity checks.

The hard part is to do proper key management, specifically to authenticate the owners of the other keys. The currently most used approach is that of Signal, WhatsApp and Telegram. They authenticate phone numbers by sending text messages to the phone number. Thus they can be sure that the owner of the phone number is also the owner of the private key. (Well, the phone operator can of course impersonate the owner of the phone number.) Then another user has identified another user by his or her phone number, then the app will ensure the verified key is used.

(3p) 5. What problems do you see for web services to replace passwords with biometrics? What would you say is needed for that to work?

Suggested solution A web service cannot have its own fingerprint reader. Thus is cannot know from there whether the fingerprint is fresh. This makes the fingerprint equivalent to a password. This password being a fingerprint means that is will be the same everywhere, i.e. a bad password.

The web service must be able to ensure freshness. This could be done by the web service trusting a particular brand of fingerprint readers. Then it can send a challenge to the fingerprint reader which includes the challenge in a digital signature which also signs the fingerprint.

It could also be implemented such that the user's device is fingerprint protected and then the device simply uses a public-private keypair with the web service.

(3p) 6. Would you classify buffer overruns in software as a violation of confidentiality, integrity or availability? The answer is yes, all three. Why?

Suggested solution Confidentiality, because you can read out memory you shouldn't. Integrity, because you can make the system do things it shouldn't. Availability, because you can make the program crash.