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

2019-08-27

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 5

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.

If you get zero on one question, you will get Fx and the possibility for oral complementary assessment. If you get two or more zeroes, you must retake the exam.

Questions

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

(3p) 1. The security of common off-the-shelf devices, such as smartphones and home routers, can have severe implications on entire societies and even national security.

Discuss why this is the case and the responsibility of, *e.g.*, a smartphone-app developer.

(3p) 2. Review the following piece of code. Identify potential problems and explain why they are problems.

This is a shell script by the name of pwdauth, it runs with root priviledges.

```
#!/bin/bash
# pwdauth <user>

# get the username from command line
username = $1

echo "Please enter the password for $username:"
read passwd

real_passwd = $(cat /secure/passwds | grep $username)

if [ $passwd = $real_passwd ]; then
  sudo -u $username /bin/bash
  exit 0
else
  exit 1
fi
```

(3p) 3. You're having dinner with a few enthusiastic entrepreneurs, start-up starters and tech trendsters. They want to create a revolutionizing food ordering app: a user should be able to keep favourite orders (*e.g.*, custom pizzas) for easy reordering, easy but secure payments and delivery.

If the app doesn't have any security, it won't survive at all. (If someone can order pizza at the expense of someone else, this is not going to work.) You need great usability (to compete with the gazillion other food-ordering apps) and great privacy (also to compete with the gazillion other food-ordering apps). (Well, nowadays, maybe the app won't survice the GDPR fines if it doesn't have privacy.)

What properties do you need for the different functions, what user data do they require? (Remember: the principle of data minimization!)

Note: You don't have to rely on existing technologies, such as credit cards or Swish, you must specify the security and privacy properties you need for any function, *e.g.*, the payment system (that includes if you want to use Swish too). There can be separate food and delivery services, they don't have to be the same, whatever you see fit to maximize security, privacy and usability. Remember, you're working with some enthusiastic entrepreneurs who will not hesitate to create another trendy-tech start-up.

You're expected to use (*i.e.*, show) your knowledge and skills from the topics access control, authentication, accountability and usability. You will also use (*i.e.*, show) your knowledge of some high-level properties from cryptography. (Don't leave the exam room early, spend more time on this question instead, remember it's the size of 4–5 questions.)

(3p) 4. Browser fingerprinting attemtps to build a unique fingerprint for a web browser to track it across the web without making it store cookies. Whenever a browser connects to a web server it gives some information to it, *e.g.*, browser make and model (*e.g.*, Firefox v59.0) which fonts are available *etc.* Explain how this can be used to create a unique fingerprint to track browsers (*i.e.*, users) across the web. How much data is required? (You don't have to give any numbers, just how to calculate them.)

(3p) 5. Smartphones is a good example of where users a intentionally locked out. For example, a user is allowed to install a pay-for app to try and later change their mind to get their money back. This requires that the user can install the app on their phone, but that they cannot access the binary to make copies. This way, when they change their mind, then the phone can remove the binary and ensure the user has no copy remaining.

Explain what is technically needed to achieve this and discuss the limitations.