Mittuniversitetet
MID SWEDEN UNIVERSITY

DT145G Computer Security

Final exam:
A small case

Daniel Bosk

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

2020-03-20

Instructions

You will be given a small assignment. You should solve this assignment in groups, with no limit on resources. The group will write up the solution in *one report per group* and hand it in before the deadline.

To provide a "proof of knowledge", everyone will book a timeslot for a 15-minute individual meeting in Zoom. During this meeting I will ask you

1. if there's anything you'd like to change in the solution (you might not agree fully with the group);
2. about some selected details of the solution.

Note that during this meeting you *must have a working webcam and microphone and a valid ID*.

I strongly advice you to ensure that everyone is involved in every part of the report. For instance, write the report in a joint Google Docs or Overleaf document while everyone participates over Zoom (or similar). (To make it easier for everyone to navigate the editing, it might be good to name someone secretary and that person shares the screen. The secretary position doesn't have to be fixed, it can rotate every now and then.)

Also, write your own notes about various design decisions during the work in the group, particularly those that you disagree with.

Grading criteria

The relevant intended learning outcomes (ILOs) are: that you are able to

- *apply* different cryptographic primitives and *explain* how these work (on a high level);
- *analyse* problems of authentication, access control, accountability and different solutions;
- *explain* how some common attacks on software works and *analyse* code for security vulnerabilities;
- *evaluate* strengths and weaknesses of hardware-based security such as full-disk encryption.

The grades will be based on the following grading criteria.

Grade E You fulfil all the ILOs above. You should have identified a relevant problem, and given a solution to it. It must be a viable solution, however gaps and mistakes are allowed, if they don't render your solution unusable.

Grade C You fulfil the criteria for E. Additionally, your evaluations and designs are *good* with *some base* in theory and, where applicable, the research literature. Gaps and errors are allowed if they only render your solution less optimal.

Grade A You fulfil the criteria for C. However, your evaluations and designs must be *extensive* (in detail) and *well-founded* in theory and, where applicable, the research literature. Gaps and errors are not allowed in the solution unless they have been properly addressed and you have given a suggestion for an approach to how to start resolve the issue.

The grades B and D are intermediary grades.

The assignment

You should design the architecture for an online banking app. This means the design of the app internals and the server-side API.

The app should provide the following features:

1. Create an account. For money-laundering purposes, the account must be tied to a real identity.
2. See the account balance and transaction history. Only the account holder should be able to do this.
3. Transfer money from one account to another.
4. Anonymous payments (think Swish, but better). The money should be untraceable: the recipient will not learn who paid (*e.g.*, the account), the bank will not learn who paid to whom (*e.g.*, from which account to which account), the sender will not learn the account of the recipient.

You can see the last one as optional for a higher grade than E.

Solving this assignment will touch upon almost every topic in the course. Make sure to base your designs on the theory of the course, add references, that will help you (remember that's a part of the grading criteria). "This feels secure" is not a convincing argument. Likewise, "all connections should use TLS" will not cut it either; why do you want TLS, what properties do you need and which of those will TLS provide and why?