Homework 2

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only one homework per email. Please also submit only ASCII text or PDFs (no .docs etc). Every solution should be preceded by the corresponding question, like:

Qn:	**…a difficult question from me…**
A:	**…an answer from you …**
Q$n+1$	**…another difficult question…**
A:	**…another brilliant answer from you…**

Solutions will only be accepted until 20th December! Submit with your partner a single solution!

1. Another question for thinking like an attacker: Imagine you have at home a broadband contract with TalkTalk. You do not like their service and want to switch to Virgin, say. The procedure between the Internet providers is that you contact Virgin and set up a new contract and they will automatically inform TalkTalk to terminate the old contract. TalkTalk will then send you a letter to confirm that you want to terminate. If they do not hear from you, they will proceed with terminating the contract and will request any outstanding cancellation fees. Virgin on the other hand sends you a new router and paperwork about the new contract. Obviously this way of doing things is meant to make switching as convenient as possible. Still can you imagine situations in which this way of switching providers can cause you a lot of headaches? For this consider that TalkTalk needs approximately 14 days to reconnect you and might ask for reconnection fees.

2. Often problems in e-voting are due to difficulties with authentication. Keep this in mind for what could go wrong with the following discount offered by an insurance company: John Hancock Insurance is partnering with Vitality, which you might know as one of those work-related wellness programmes. The programme is available in 30 US states. If you sign up for this, John Hancock will send you a free Fitbit monitor. That's a tiny, pill-shaped device that some people wear in sleek-looking bracelets to track how far they walk/run, the calories burned, and the quality of sleep. That means the insurance company would know exactly when a customer does a sit-up, how far she runs – or when he or she has skipped the gym for a few days. For 'good' customers there will be a discount in their premiums. Why is this a problem?

3. Voice voting is the method of casting a vote in the 'open air' for everyone present to hear. Which of the following security requirements do paper ballots satisfy **better** than voice voting? Check all that apply and give a brief explanation for your decision in each case.

- ☐ Integrity
- ☐ Enfranchisement
- ☐ Ballot secrecy
- ☐ Voter authentication
- ☐ Availability

4. Explain how an attacker can use chain voting in order to influence the outcome of a poll using paper ballots.

5. Which of the following mechanisms help with defending against chain voting? Check all that apply. Give a brief reason for each defence that mitigates chain voting attacks.

   - ☐ Using a glass ballot box to make it clear there are no ballots in the box before the start of the election.
   - ☐ Distributing ballots publicly before the election.
   - ☐ Checking that a voter's ID (drivers license, passport) matches the voter.
   - ☐ Each ballot has a unique ID. When a voter is given a ballot, the ID is recorded. When the voter submits his or her ballot, this ID is checked against the record.

6. In the Estonian general election, votes can be cast via Internet some time before the election day. These votes cast via Internet can be changed an unlimited amount of times, the last vote is tabulated. You can even change your vote on the polling day in person. Which security requirement does this procedure address?

7. Paper ballots boxes need to be guarded on the voting day, but can be unguarded the rest of the year. Why do pure electronic voting machines need to be guarded the whole year?

8. What is the main difference between online banking and e-voting? (Hint: Why is the latter so hard to get secure?)

9. Imagine, hypothetically, you have a perfectly secure Internet voting system, by which I mean nobody can tamper with or steal votes between your browser and the central server responsible for vote tallying. What can still go wrong with such a perfectly secure voting system, which is prevented in traditional elections with paper-based ballots?

10. **(Optional)** This question is for you to provide regular feedback to me, for example what were the most interesting, least interesting, or confusing parts in this lecture? Is there anything you like to have improved or explained in the handouts? Please feel free to share any other questions or concerns.