Handout 1 (Security Engineering)

Much of the material and inspiration in this module is taken from the works of Bruce Schneier, Ross Anderson and Alex Halderman. I think they are the world experts in the area of security engineering. I especially like that they argue that a security engineer requires a certain *security mindset*. Bruce Schneier for example writes:

> *"Security engineers — at least the good ones — see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it."*

> *"Security engineering…requires you to think differently. You need to figure out not how something works, but how something can be made to not work. You have to imagine an intelligent and malicious adversary inside your system …, constantly trying new ways to subvert it. You have to consider all the ways your system can fail, most of them having nothing to do with the design itself. You have to look at everything backwards, upside down, and sideways. You have to think like an alien."*

In this module I like to teach you this security mindset. This might be a mindset that you think is very foreign to you (after all we are all good citizens and not ahck into things). I beg to differ: You have this mindset already when in school you were thinking, at least hypothetically, about in which ways you can cheat in an exam (whether it is about hiding notes or looking over the shoulders of your fellow pupils). Right? To defend a system, you need to have this kind mindset and be able to think like an attacker. This will include understanding techniques that can be used to compromise security and privacy in systems. This will many times result in insights where well-intended security mechanisms made a system actually less secure.

Warning! However, don't be evil! Using those techniques in the real world may violate the law or King's rules, and it may be unethical. Under some circumstances, even probing for weaknesses of a system may result in severe penalties, up to and including expulsion, fines and jail time. Acting lawfully and ethically is your responsibility. Ethics requires you to refrain from doing harm. Always respect privacy and rights of others. Do not tamper with any of King's systems. If you try out a technique, always make doubly sure you are working in a safe environment so that you cannot cause any harm, not even accidentally. Don't be evil. Be an ethical hacker.

In this lecture I want to make you familiar with the security mindset and dispel the myth that encryption is the answer to all security problems (it is certainly often part of an answer, but almost always never a sufficient one). This is actually an important thread going through the whole course: We will assume that encryption works perfectly, but still attack "things". By "works perfectly"

we mean that we will assume encryption is a black box and, for example, will not look at the underlying mathematics and break the algorithms.[1]

For a secure system it seems four requirements need to come together: First a security policy (what is supposed to be achieved?); second a mechanism (cipher, access controls, tamper resistance etc); third the assurance we obtain from the mechanism (the amount of reliance we can put on the mechanism) and finally the incentives (the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy).

[1] Though fascinating it might be.