Handout 1 (Security Engeneering)

Much of the material and inspiration in this module is taken from the works of Bruce Schneier, Ross Anderson and Alex Halderman. According to them, a security engineer requires a certain 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 mindset. To defend a system, you need to have this mindset and think like an attacker. This will include understanding techniques that can be used to compromise security and privacy of others.

Warning! However, don't be evil! Using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Acting lawfully and ethically is your responsibility.

Don't be evil! - Ethics requires you to refrain from doing harm - Always respect privacy and property rights - Otherwise you will fail the course - Federal and state laws criminalise computer intrusion and wiretapping - e.g. Computer Fraud and Abuse Act (CFAA) - You can be sued or go to jail - University policies prohibit tampering with campus systems - You can be disciplined, even expelled

To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in EECS 588 is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what the law prohibits — you don't want to end up like this guy. The EFF provides helpful advice on vulnerability reporting and other legal matters. If in doubt, we can refer you to an attorney.