1 Motivation and Goals

Most commercial transactions involve two or more parties with different objectives, including taking advantage of others. For most “real-world” applications, many possible dishonest strategies are evident, and the transactions are designed with these in mind. Imagine, for example, a teller machine where you swipe your ATM card, enter the amount to withdraw, and then take the corresponding amount of money from a stack of bills. Imagine further anonymous credentials in the shape of drivers licenses that do not divulge any identifying information, but where the right to drive a vehicle would be associated with the ownership of such a licence. It is clear that while both of these “implementations” work well in an environment where nobody cheats, it would also be highly questionable to employ them in an imperfect society. Cryptographic protocol design strives to identify and protect against abusive strategies in applications where standard “real-world” defenses fail.

To properly defend against attacks, we must first become aware of the nature of potential threats. These may be unauthorized access to resources or rights, as in the examples involving teller machines and drivers licenses.
Examples of other types of unauthorized access are piracy (namely dishonest access to a service or product); unauthorized sharing of information; unauthorized attempts at forging or modifying contracts, and similar. Another type of threat is the violation of other users’ privacy, whether this relates to their actions, location, memberships and associations, and more. Yet another type threat is inappropriate use of system features – such as the use of encryption by drug dealers and the use of steganographically hidden communication by terrorists. (In these examples, the user may simply use available applications in a way that corresponds to their intended use, but for purposes that are not endorsed by society.)

Thus, the design of a system requires not only an understanding of its wanted behavior (e.g., to allow people to withdraw money resp. give evidence that they belong to a certain group of people, such as ”people who may drive a car”). It is also crucial to understand the unwanted types of behavior, whether these constitute attacks on the system itself, or simply stray from the intended use. Moreover, it is important to understand the available tools and how these can be employed to reach a set of goals. This course will address these issues by the discussion of various applications, abuses, and cryptographic techniques.

The intention of the course is to provide a broad understanding of potential threats, and an improved intuition on how to deal with these. Given the large quantity of material to be covered, some material will not be covered in great depth in the lectures. Instead, each student will select one topic of interest for a brief presentation, and one for a final project. The latter may be performed in groups.

The course will have one technical component, and one component relating to understanding and removing protocol flaws. To understand the nature of the second component, consider the following non-technical example: Most realtors do not request identification from apartment owners picking up or replacing keys of apartments they are listing. How could this be abused?
2 Mechanics

YOU MUST BE ENROLLED IN THE COURSE TO ATTEND THE LECTURES.

2.1 Notes and Papers

The course is based on research papers and lectures. A detailed syllabus, along with pointers to useful sources of information, will be made available during the first lecture. A partial list of topics is as follows:

- **Signatures.** How to construct a digital signature. Existing signature schemes. Certificates and Public Key Infrastructure (PKI). Use of signatures in payment schemes, and more generally, in e-commerce. Contracts, fair exchange (namely, and exchange in which both parties are guaranteed to get the other’s signature if he gets their’s.)

- **Authentication.** Techniques for authentication by both computers and humans. Passwords and ways to recover when passwords are forgotten.

- **Privacy.** Privacy of data; of location; or purchase patterns. Traffic analysis. Perfect vs. revokable privacy. Anonymizers and crowds. Polling and voting.

- **Payments.** Various attacks on the monetary system and ways to recover from these. How to get fair and transactions in a setting where people can disconnect their computers after they get what they want (and before they send what they promised.)

- **Wireless Security.** Ad hoc networking and routing security; providing incentives for peer-to-peer collaboration; denial of service attacks; key establishment and pairing. RFID tags, Bluetooth, 802.1. Privacy concerns.

- **Digital Rights Management.** Defining who the adversary is and how to be secure against such an adversary. Existing techniques, trends, impossibility results.
2.2 Books.

There is no required textbook. Instead, lecture notes will be provided online, and will contain hyperlink pointers to references. However, depending on the choice of project, one of the following books may be very helpful:

- "Handbook of Cryptography" by Menezes, Vanstone and van Oorschot for a careful description of cryptographic techniques.
- “Security Engineering” by Ross Andersson for a good technical overview of applications and known problems in such.

2.3 Prerequisites

The only formal prerequisite is Fundamental Algorithms I. Depending on the project you choose, you may also benefit from knowledge about programming languages or an exposure to discrete math.

2.4 Requirements

Two problem sets (worth 30%), one brief presentation (worth 10%), and a major project or paper (worth 60%). There will be no final exam.

LATE ASSIGNMENTS WILL NOT BE ACCEPTED without a note from your physician or from your employer. (We will discuss the solutions on the day you hand in the assignment. That’s why I don’t want any late homeworks. As for the project, this is a question of fairness.)

On the other hand, collaboration on the problem sets IS allowed. You may work together with one other partner and sign both of your names to a single submitted homework. Both of you will receive the grade that the homework merits. There is no penalty for working on problem sets in teams of two (more than two is not allowed).
3 Project

3.1 Programming Project (Individual or Group)

Select an application that interests you, and implement a corresponding protocol (whether one that is already known, or one that you develop yourselves.) Below are two example projects meant to illustrate the type of projects allowed. Other examples will be discussed in class.

Project Example 1. Implement a scheme for secure synchronization of a hand-held computer to a home computer via a public and untrusted machine. The project will be graded on its security, ease of use, and code quality.

Project Example 2. Implement a test of “being human”, which is a test that is easy for humans to pass but hard for computers. Such a method can be used to control access to resources, verify that a person is paying attention, for advertising, gaming, and more. The test may be based on one of many computational problems, with examples from computer vision, voice analysis, and more. The code will be graded based on its ease of use, integration with existing software, and its likely security against attacks.

3.2 Paper Project (Individual Only)

Survey. Each student wanting to write a survey paper will read several research papers and then describe the results in a paper (7-10 single-spaced pages), containing four non-trivial problems based on the studied material, along with the student’s solutions. Generally, the quality should be publishable and on par with articles in publications such as Byte, Wired, or Dr. Dobbs. The paper will be graded based on how much value it adds, and on how easily understood it is. If you are interested in honing your presentation skills, you may choose to present what you read to the class. An example survey could be to review different methods to improve anonymity in existing systems; methods of piracy and how to provide disincentives for these; or methods for password-based login authentication schemes (such as EKE, SPEKE and PAK).
Business idea. Propose an application, develop and analyse the required protocols, prepare a demo, and write up a (very brief) business plan. The project will be graded based on its novelty and degree of usefulness. Alternatively, survey a given market with special attention to technology claims of vendors; such a project would be graded based on the importance of the findings and the depth of the analysis.

Research paper or patent application. Develop a novel technique and write it up, either as a research paper (of quality publishable in a high-quality scientific conference) or as a provisional patent application (which you may choose whether you wish to file or not – a provisional application costs $75 to file.) The project will be based on its judged quality.