Human Factors in Security and Privacy

Zinaida Benenson
Friedrich-Alexander-University Erlangen-Nuremberg, Germany
zinaida.benenson@cs.fau.de

Since 2012, I have been teaching a course called "Human Factors in Security and Privacy" at the University of Erlangen-Nuremberg, Germany, every summer term. The course consists of a lecture (two contact hours per week) and an exercise (also two contact hours per week). Although usability of security and privacy measures constitutes a sizable part of the course, the goal of the course is to give a broad overview of issues that arise when people have to make security- and privacy-related decisions.

The core idea is to communicate to the students that people do not make these decisions fully rationally, but also based on intuition, emotions and social influence. The goal is to teach the students, as future security professionals, to take into account these factors and to expect this kind of behavior from the users, and to make informed, rational decisions about development and evaluation of security- and privacy-preserving mechanisms and policies (Fig. 1). The goals of the course are formulated as follows in the course description:

> The main goal of this course is for the students to develop a mindset that naturally takes into account typical psychological and physical characteristics of the users.
>
> When developing or evaluating security- and privacy-enhancing technologies and policies, the students are able to:
>
> - critically appraise technologies and policies for likely human factors weaknesses in design and usage
> - choose appropriate techniques for development, testing and evaluation of security- and privacy-enhancing technologies and policies

The course covers the following topics:

- Terminology of security and privacy, technical and non-technical protection measures
- Development and testing of usable security mechanisms (encryption and authentication tools, security policies, security warnings)

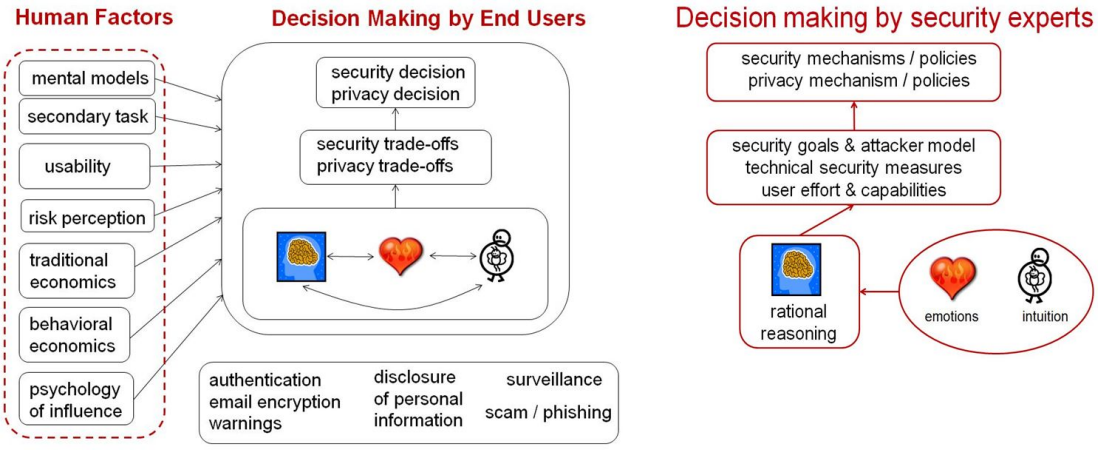

Figure 1: Decision making by the users vs. by security professionals

- Risk perception and decision making in security and privacy context (usage of security software, reaction to security warnings, sharing information in social media)
- Economics approach to security and privacy decision making (traditional and behavioral economics)
- Trade-offs between the national security and surveillance (psychology behind the EU data retention directive and NSA programs)
- Psychological principles of cyber fraud (scams, phishing, social engineering)
- Security awareness and user education
- Interplay of safety and security in complex systems
- Research methods in human factors (qualitative vs. quantitative research, usability testing, experimental design, survey design, interviews)

The exercise is divided in two parts:

(1) After each lecture, the students receive a homework assignment consisting of practical exercises, such as conducting a short survey or interviews with 2-3 users of their choice on the topic of the next lecture, e.g. password management strategies, or designing a usability test for a small part of a an existing system, e.g. a browser security warning.

(2) The students are divided into groups, and each group prepares a 30-minutes long presentation with the following discussion for the class on a given topic, for example social authentication or the privacy paradox. Materials such as papers and key discussion questions are provided.