Modulbezeichnung:	**Human Factors in Security and Privacy (HumSecPri)** (Human Factors in Security and Privacy)	**5 ECTS**
Modulverantwortliche/r:	Zinaida Benenson	
Lehrende:	Zinaida Benenson	

Startsemester: SS 2020	Dauer: 1 Semester	Turnus: jährlich (SS)
Präsenzzeit: 60 Std.	Eigenstudium: 90 Std.	Sprache: Deutsch

Lehrveranstaltungen:

Human Factors in Security and Privacy (SS 2020, Vorlesung, 2 SWS, Zinaida Benenson)
Human Factors in Security and Privacy - Übung (SS 2020, Übung, 2 SWS, Zinaida Benenson)

Empfohlene Voraussetzungen:

REQUIRED: basic knowledge in the area of IT security and privacy, such as security goals (CIA), basic protection mechanisms (symmetric and asymmetric cryptography principles), cryptographic hash functions, digital certificates, PKI, basics of SSL/TLS. This knowledge can be acquired through the attendance of the module "Applied IT Security" or similar modules.

Es wird empfohlen, folgende Module zu absolvieren, bevor dieses Modul belegt wird:

Angewandte IT-Sicherheit

Inhalt:

Das Modul findet online statt, solange die Corona-Maßnahmen bestehen. Termine werden voraussichtlich wie geplant stattfinden: erste Vorlesung am Do 23.4., erste Übung am Mi 29.4.20. Vorlesungen und Übungen werden aufgezeichnet und ins StudOn gestellt. Links zu entsprechenden virtuellen Räumen werden über StudoOn E-Mails kurz vor dem Vorlesungsbeginn mitgeteilt.

People are often said to be "the weakest link" in the chain of IT security measures. This course provides insight into the ways in which IT security is affected by people and why it happens. Special attention will be paid to complex environments such as companies, governmental organizations or hospitals. A number of guest talks from practitioners and researchers highlight some of the issues in greater depth. 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)
- Risk perception and decision making in security and privacy context (usage of security software, reaction to security warnings, divulging 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 exercises aim at deepening the understanding of the topics and are highly relevant for oral examinations. We plan to conduct approximately eight exercises per semester; the rest of the exercises is reserved for the guest talks. A typical exercise consist of two parts:
(1) For each topic, the students receive a homework assignment consisting of practical exercises.
(2) For each topic, the students receive 1-3 papers to read for the next exercise. The papers will be discussed in the class with the teaching assistant.

Lernziele und Kompetenzen:

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. In particular, when developing or evaluating security- and privacy-enhancing technologies or policies, the students are able to:

- critically appraise technological solutions or policies for likely “human factors" weaknesses in design and usage
- choose appropriate techniques for testing and evaluation of the design and usage
- develop and test improvements

More precisely, after the successful completion of the course the students are able to:

- discuss the meanings of the terms “security" and “privacy"
- identify main research questions in the area of human factors in security and privacy
- demonstrate specific difficulties in developing and testing of usable security mechanisms
- compare different approaches to the development of usable security features
- apply elements of the mental models approach and of user-centered design to development and evaluation of security- and privacy-enhancing techniques
- contrast the approaches of traditional and behavioral economics to the explanation of security- and privacy-related behavior
- illustrate the influence of the psychological risk perception principles (especially under- and overestimation of risk) on security and privacy decision making
- argue advantages and disadvantages of mass surveillance and other kinds of mass data collection for security and privacy of citizens
- explain main psychological principles behind the cyber fraud
- illustrate specific difficulties in awareness campaigns and user training in the realms of security and privacy
- critically appraise design and results of published user studies
- plan and conduct small user studies
- scan research papers and other materials for important points that clarify and deepen course contents
- prepare and conduct a discussion in the class on a given topic, using research papers and other materials
- develop well-founded personal opinions on the course topics and defend them in the class discussions

Literatur:

- L. F. Cranor, S. Garfinkel. Security and usability: designing secure systems that people can use. O’Reilly Media, Inc., 2005.
- Schneier, Bruce. "Beyond fear." Copernicus Book, 2003.
- Anderson, Ross. Security engineering. 2nd edition, John Wiley & Sons, 2008. http://www.cl.cam.ac.uk/ rja14/book.h

---

Verwendbarkeit des Moduls / Einpassung in den Musterstudienplan:

Das Modul ist im Kontext der folgenden Studienfächer/Vertiefungsrichtungen verwendbar:

[1] **Medizintechnik (Master of Science)**

(Po-Vers. 2019w | TechFak | Medizintechnik (Master of Science) | Modulgruppen M1, M2, M3, M5, M7 nach Studienrichtungen | Studienrichtung Medizinische Bild- und Datenverarbeitung | M5 Medizintechnische Vertiefungsmodule (BDV) | Human Factors in Security and Privacy)

Dieses Modul ist daneben auch in den Studienfächern "Informatik (Bachelor of Arts (2 Fächer))", "Informatik (Bachelor of Science)", "Informatik (Master of Science)", "International Information Systems (IIS) (Master of Science)", "Mechatronik (Master of Science)", "Medizintechnik (Bachelor of Science)" verwendbar.

Studien-/Prüfungsleistungen:

Human Factors in Security and Privacy (Prüfungsnummer: 658644)
(englische Bezeichnung: Human Factors in Security and Privacy)

Prüfungsleistung, Klausur, Dauer (in Minuten): 90
Anteil an der Berechnung der Modulnote: 100%
weitere Erläuterungen:
Gemäß Corona-Satzung wird als alternative Prüfungsform festgelegt: Klausur, Dauer (in Minuten): 90, benotet Klausuraufgaben werden auf Deutsch gestellt Klausuraufgaben können sowohl auf Deutsch als auch auf Englisch beantwortet werden
Prüfungssprache: Deutsch und Englisch

Erstablegung: SS 2020, 1. Wdh.: WS 2020/2021
1. Prüfer: Zinaida Benenson

Organisatorisches:

Die Modulsprache ist Deutsch, Folien sind auf Englisch. Übungen sind auf Deutsch formuliert, und können in Englisch beantwortet werden. Klausuraufgaben werden auf Deutsch gestellt. Klausuraufgaben können sowohl auf Deutsch als auch auf Englisch beantwortet werden.

This module will be held in German, slides are in English. Assignments will be formulated in German, and can be answered in German or English. Written exams will be formulated in German and can be answered in German or English.