

Deutscher Titel: Usable Security

Englischer Titel: Usable Security

Kürzel: USEC

Workload: 180 h

Leistungspunkte: 6

Semester: 5

Dauer: 1 Semester

Häufigkeit: Regelmäßig im Wintersemester

Lehrveranstaltung:

Vorlesung: 30h Präsenzzeit, 60h Selbststudium

Seminar & Projekt: 30h Präsenzzeit, 60h Selbststudium

Gruppengröße: -

Qualifikationsziele:

Sie verstehen die Rolle des Faktors „Mensch“ in der IT-Sicherheit und denken Informationssicherheit als Prozess und nicht als Zustand. Sie sind in der Lage menschenzentrierte Design- und Entwicklungsmethoden anzuwenden, um Sicherheitsmechanismen sowohl technisch robust als auch intuitiv bedienbar zu gestalten und diese auch implementieren. Sie können Usability-Probleme in bestehenden Systemen identifizieren, evaluieren und durch benutzerzentrierte Ansätze minimieren, um ein hohes Schutzniveau aufrecht zu erhalten. Sie haben ein umfassendes Verständnis der Rahmenbedingungen für IT-Systeme, welche durch die Kontextfaktoren Sicherheit, Datenschutz und Ethik geprägt sind.

Inhalte:

- *Grundlagen menschlichen Verhaltens:* Untersuchung von menschenzentrierten Aspekten, um zu verstehen, wie und warum Anwender bei der Nutzung von IT-Systemen sicherheitskritische Entscheidungen treffen.
- *Sichere Authentifizierungssysteme:* Bewertung und Implementierung etablierter Verfahren wie Passwörter, Hardware-Tokens und der Zwei-Faktor-Authentifizierung (2FA) im Spannungsfeld zwischen technischer Sicherheit und Usability.
- *Biometrische Authentifizierungssysteme:* Detaillierte Betrachtung biometrischer Verfahren (physiologische- und verhaltensbiometrische Methoden) mit Fokus auf Nutzerakzeptanz, systembedingte Fehleranfälligkeit und Herausforderungen bei der Implementierung.
- *Verschlüsselte Kommunikation:* Praktische Herausforderungen in der Nutzbarkeit von verschlüsselter Kommunikation und Ansätze um diese zu überwinden.

- *Nutzerzentrierte Angriffe*: Analyse von Bedrohungen wie Phishing und Social-Engineering sowie der psychologischen Mechanismen, mit denen Angreifer den Faktor Mensch gezielt als Schwachstelle ausnutzen.
- *Nutzerzentrierte Evaluationsmethoden*: Anwendung qualitativer und quantitativer Methoden (z. B. empirische Usability-Testing), um die Bedienbarkeit von Sicherheitssystemen systematisch und empirisch zu überprüfen und zu optimieren.
- *Privatsphäre und Ethik*: Sensibilisierung für den Umgang mit sensiblen Nutzerdaten, Prinzipien des datenschutzkonformen Systemdesigns (Privacy-by-Design) sowie ethische Fragestellungen bei der Überwachung und Steuerung von Nutzerverhalten.

Verwendbarkeit des Moduls: Wahlpflichtmodul im Studiengang Informatik-Softwaresysteme, Wahlpflichtkatalog B

Empfohlene Voraussetzungen/Vorkenntnisse:

- Empfohlen: Programmierkenntnisse in Python (z. B. GIP1, GIP2, PIP)
- Empfohlen: Machine Learning Kenntnisse (z. B. MLDS1)

Prüfungsformen: Klausur, Vortrag, schriftliche Ausarbeitung

Voraussetzung für die Vergabe von Leistungspunkten: Bestandene Modulprüfung

Stellenwert der Note in der Endnote: Einfaches Leistungspunkte-Gewicht

Hauptamtlich Lehrende(r): Prof. Dr. Jonathan Liebers

Modulbeauftragte(r): Prof. Dr. Jonathan Liebers

Sonstige Informationen:

Garfinkel, S., & Lipford, H. R. (2014). Usable security: history, themes, and challenges (1st ed.). Morgan & Claypool Publishers. <https://doi.org/10.1007/978-3-031-02343-9>

Jain, A. K., Ross, A. A., Nandakumar, K., & Swearingen, T. (2024). Introduction to Biometrics. In Texts in computer science (2nd ed.). Springer International Publishing AG. <https://doi.org/10.1007/978-3-031-61675-4>

Gerber, N., Stöver, A., & Marky, K. (2023). Human Factors in Privacy Research (1st ed. 2023). Springer International Publishing. <https://doi.org/10.1007/978-3-031-28643-8>