Modulbezeichnung:	**Security and Privacy in Pervasive Computing (SecPriPC)** (Security and Privacy in Pervasive Computing)	**5 ECTS**
Modulverantwortliche/r:	Zinaida Benenson	
Lehrende:	Zinaida Benenson	

Startsemester: WS 2018/2019	Dauer: 1 Semester	Turnus: jährlich (WS)
Präsenzzeit: 60 Std.	Eigenstudium: 90 Std.	Sprache: Deutsch

Lehrveranstaltungen:

Die erste Übung findet in der ersten Vorlesungswoche statt.
Die Modulsprache ist Deutsch, Folien sind auf Englisch.

This module will be held in German, slides are in English.

Security and Privacy in Pervasive Computing (WS 2018/2019, Vorlesung, 2 SWS, Zinaida Benenson)
Security and Privacy in Pervasive Computing - Übung (WS 2018/2019, Übung, 2 SWS, Zinaida Benenson et al.)

Empfohlene Voraussetzungen:

Basic knowledge in the area of IT security and privacy, such as security goals (CIA), symmetric and asymmetric cryptography principles, PKI, basic functionality of SSL is required. This knowledge can be acquired through the attendance of the module "Applied IT Security" (Angewandte IT Sicherheit) or similar modules.

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

Angewandte IT-Sicherheit

Inhalt:

Pervasive Computing, also called Ubiquitous Computing, is a computing paradigm that comprises billions computing devices integrated into everyday objects and connected into a global communication network that is orders of magnitude larger than the Internet today. These devices measure environmental characteristics, exchange information about their surroundings and interact with people in many different ways, such that sometimes people may be even unaware that they are using computers. The era of pervasive computing has already started and moves on rapidly, integrating the Internet, smartphones, wearable computing devices (such as Google glass or Apple Watch), smart grid, home automation, intelligent cars and smart cities.

In this course we look at the visions and current scenarios of Pervasive Computing from the security and privacy point of view. We consider security mechanisms and privacy concerns of the present-day technologies, such as smartphone operating systems, GSM/UMTS, WLAN, Bluetooth, ZigBee, RFID, and also of present and envisioned systems and services such vehicular networks, sensor networks, location-based services and augmented reality.

The **exercise** comprises (1) practical tasks on specific attacks, such as eavesdropping on WiFi or ZigBee communication, and (2) guest talks on selected topics, for example, NFC security. For practical exercises, students will be divided into groups, and each group will have to execute the tasks in our lab and write a report about their work for each task. Further details will be communicated in the first exercise.

Lernziele und Kompetenzen:

The students achieve the **main module goals** if they are able to:

- recognize existing and future computing systems as pervasive through analysis of their conceptual design and development, deployment and actual usage
- critically appraise pervasive computing systems for typical security- and privacy-related concerns and weaknesses in design, deployment and usage
- choose appropriate techniques and policies for securing pervasive computing systems
- choose appropriate techniques and policies for addressing privacy issues in pervasive computing systems

Literatur:

- Frank Stajano: Security for Ubiquitous Computing.
- John Krumm (Ed.): Ubiquitous Computing Fundamentals

- Adam Greenfield: Everyware

Other books and papers will be presented during the lecture.

Verwendbarkeit des Moduls / Einpassung in den Musterstudienplan:

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

[1] **Informatik (Bachelor of Science)**
(Po-Vers. 2009s | TechFak | Informatik (Bachelor of Science) | Wahlpflichtbereich (5. und 6. Semester) | Wahlpflichtmodule | Vertiefungsrichtung IT-Sicherheit)

[2] **Informatik (Bachelor of Science)**
(Po-Vers. 2009w | TechFak | Informatik (Bachelor of Science) | Wahlpflichtbereich (5. und 6. Semester) | Wahlpflichtmodule | Vertiefungsrichtung IT-Sicherheit)

[3] **Informatik (Master of Science)**
(Po-Vers. 2010 | TechFak | Informatik (Master of Science) | Wahlpflichtbereich | Säule der systemorientierten Vertiefungsrichtungen | Vertiefungsrichtung IT-Sicherheit)

[4] **Informations- und Kommunikationstechnik (Master of Science)**
(Po-Vers. 2016s | TechFak | Informations- und Kommunikationstechnik (Master of Science) | Schwerpunkte im Masterstudium | Schwerpunkt Kommunikationsnetze und Übertragungstechnik | Wahlpflichtmodule | Wahlpflichtmodul aus INF im Schwerpunkt Kommunikationsnetze)

[5] **Mathematik (Bachelor of Science)**
(Po-Vers. 2015w | NatFak | Mathematik (Bachelor of Science) | Module des Nebenfachs | Nebenfach Informatik | Vertiefungsmodule | Vertiefungsrichtung IT-Sicherheit)

Studien-/Prüfungsleistungen:

Security and Privacy in Pervasive Computing (Prüfungsnummer: 327615)
(englische Bezeichnung: Security and Privacy in Pervasive Computing)

Prüfungsleistung, mündliche Prüfung, Dauer (in Minuten): 30
Anteil an der Berechnung der Modulnote: 100%

Erstablegung: WS 2018/2019, 1. Wdh.: SS 2019
1. Prüfer: Zinaida Benenson
