**Learning outcome, core skills:**
After successful completion of the module students are able to

- describe and apply symmetric-key cryptosystems
- describe and apply public-key cryptosystems
- apply and compare mechanisms for authentication and access control
- explain attacks on different networks layers
- apply and compare defenses against network attacks
- identify vulnerabilities in software and use countermeasures
- describe types and mechanisms of malware
- apply and compare methods for intrusion and malware detection
- describe and use honeypot and sandbox systems

**Workload:**

- Attendance time: 56 h
- Self-study time: 94 h

**Course:** Introduction to Computer Security (Lecture, Exercise)

*Course frequency:* unregelmäßig

**Examination:** Klausur (120 Min.) oder mündliche Prüfung (ca. 20 Min.)

*Examination prerequisites:* Successful completion of 50% of the exercises

*Examination requirements:* Symmetric-key and public-key cryptosystems; mechanisms for authentication and access control; network attacks and defenses; software vulnerabilities and countermeasures; detection of intrusions and malicious software

**Admission requirements:** none

**Recommended previous knowledge:** B.Inf.1101, B.Inf.1802

**Language:** English

**Person responsible for module:** Prof. Dr. Konrad Rieck

**Course frequency:** unregelmäßig

**Duration:** 1 semester[s]

**Number of repeat examinations permitted:** twice

**Recommended semester:**

**Maximum number of students:** 50