| **Module title**<br>Secure Programming | | | | |
|---|---|---|---|---|
| **Module code**<br>SPG | **Level**<br>Master (M.Sc.) | **Hours per week**<br>4 | **ECTS credits**<br>5 | **Duration**<br>1 semester |
| **Module instructor**<br>Prof. Dr. Skornia | **Lecture type**<br>Interactive seminar with integrated exercises | **Prerequisite(s)**<br>n/a | **Grading**<br>Final exam | |

**Objectives**

- Students understand the root causes of vulnerabilities in C, C ++ and Java code and how insecure programs can be exploited.
- They can identify and analyse insecurities in code and apply general principles of security audits.
- They are able to follow proscriptive rules for secure coding and increase the security level of their code.
- They know how to apply avoidance strategies in software engineering.

**Content**

- Main security flaws in C, C ++ and Java programs
- In depth analysis of data types and memory management
- Overflows on several levels
- Risks in data-type-conversions
- Counting and loops
- Secure Input and Output (including pre-processor inputs)
- Concept of least privilege and its application
- Encrypted temporary data (File and RAM)
- Principles of Code Audit and Secure Software Engineering

**Textbook/teaching material**

- Jason Grembi, Secure Software Development: A Security Programmer's Guide
  Delmar Cengage Learning; 1 edition (May 8, 2008)
- Robert C. Seacord, The CERT C Secure Coding Standard
  Addison-Wesley Professional; 1 edition (October 24, 2008)
- Robert Seacord, Secure Coding in C and C++
  Addison-Wesley Professional; 1 edition (September 9, 2005)
- Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda, The CERT Oracle Secure Coding Standard for Java
  Addison-Wesley Professional; 1 edition (September 18, 2011)

Note: this is not the official course description according to the "Studien- und Prüfungsordnung" (SPO)