DRIEI
PhD Program in Electronic and Computer Engineering
University of Cagliari, Italy

Course:	Software Security and Protection
Instructors:	Leonardo Regano
SSD:	ING-INF/05 INFORMATION PROCESSING SYSTEMS
Credits / hours:	3 credits / 24 h
Language:	English
Scheduling:	Spring Semester, yearly (July)
Final Exam:	Written

Goal of the Course

The importance of software security cannot be underestimated in the Digital Age when software underpins all aspects of our daily lives. The urgent need for strong security measures has been highlighted recently in the context of real-world examples such as ransomware attacks leveraging software vulnerabilities. Indeed, risk should be managed in all the phases of the software lifecycle, from application design to continuous monitoring after deployment to manage newly discovered vulnerabilities and threats.

This course encompasses multiple aspects in the broad field of software security, covering threat modeling techniques to ensure sound choices during application design, secure software development techniques, software testing techniques to ease vulnerability discovery, and software protection techniques to safeguard the application’s assets against reverse engineering attacks. Practical classes will be included to present real-world examples of common software vulnerabilities and valuable hands-on experience with automated software testing and protection tools.

Requirements

The student must have appropriate knowledge of the C programming language. A basic knowledge of the x86 Assembly language is not mandatory but recommended.

Intersection with other courses at the University of Cagliari

There is no significant intersection with other courses offered in the PhD programme DRIEI and in the Master Degrees at UniCa.

Course Outline

1. Secure programming: principles and guidelines (4 hours)

2. Security evaluation of software (4 hours)
3. Lab: software vulnerabilities (2 hours)
4. Lab: software testing with automatic tools (2 hours)
5. Techniques for protection of software and Intellectual Property (6 hours)
6. Lab: static analysis of software (2 hours)
7. Lab: software obfuscation (4 hours)