Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative
Istituto sistemi informativi e networking

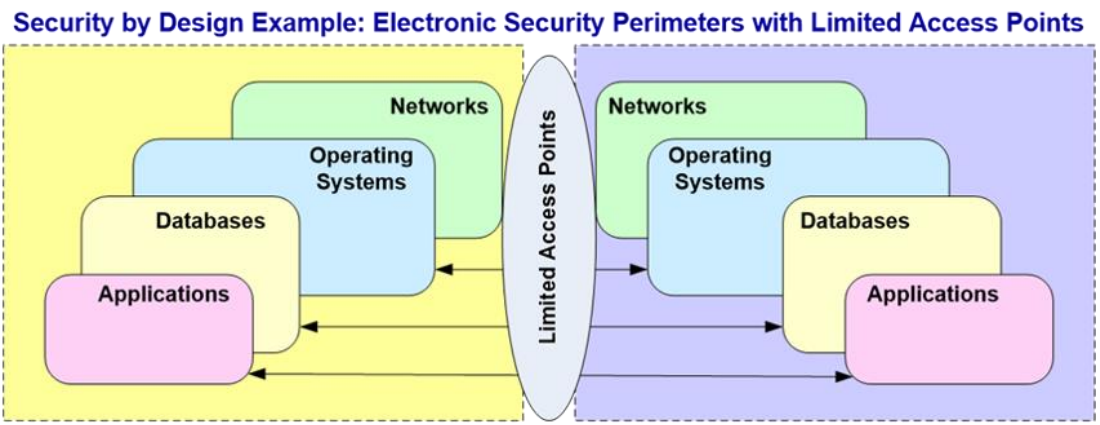
SUPSI

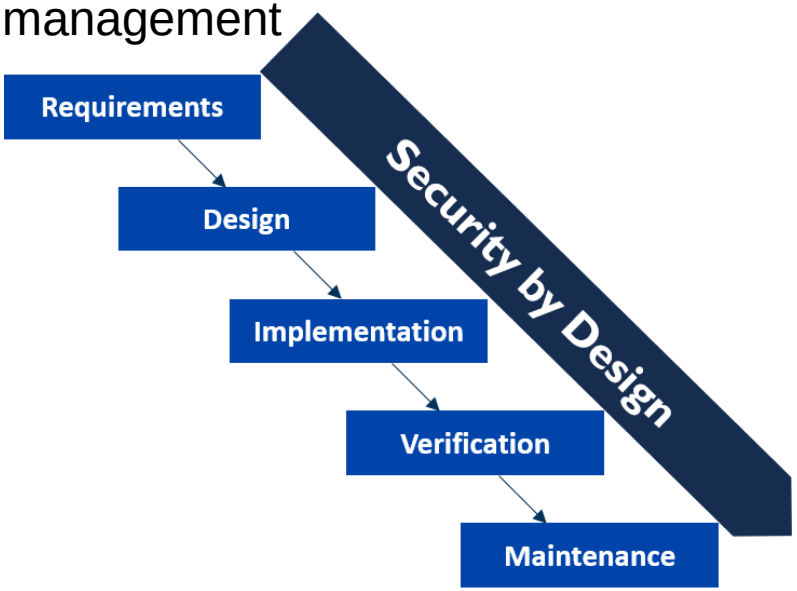
Security and Privacy by Design

Angelo Consoli
SUPSI-DTI , Lugano-Viganello
2024/25

Learning Objectives

- Know the fundamentals of developing secure by design projects and solutions
- Know the technical concepts applicable to the development of secure systems by design
- Know the main techniques for hardening hardware and software systems
- Know how to design secure communication, processing and data storage solutions
- Fundamental concepts of software security and technology systems in general
- Standards for designing secure hardware and software solutions
- Gain practical experience identifying and mitigating security pitfalls
- Rules and methodologies for designing privacy-friendly systems
- Privacy basics: Swiss Data Protection Act DPA
- The main rules of the EU GDPR standard for privacy management
- (…)





Learning Objectives

- (…)
- Security development lifecycle (SDL)
- Techniques for attacking hardware and software systems.
- Open systems and security.
- Advanced software security guidelines and concepts.
- Testing techniques of hardware and software solutions
- Principles of anti-tampering systems
- Knowledge of testing techniques for web solutions
- Impact of securitye privacy by design on technology project phases
- Standards for testing and vulnerability assessment of hardware and software solution

Course outline

- The principles of security and for setting up networked systems
- How to assess vulnerabilities of IT solutions
- Solutions for vulnerability testing of systems and networks.
- National Institute of Standards and Technology (NIST) pentest procedures
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP: web application security, the Open Web Application Security Project.
- Framework for security assessment of hardware and software systems
- Principles of the ISO/IEC27001:2013 standard: Lead Auditor and Information Security Manager
- Recommendations and best practices for auditing secure systems

Course outline

- Reverse code engineering: understanding code
- Software testing: fuzzing and sanitization
- The security of mobile systems
- Sandboxing techniques
- The security of IoT systems
- Production cycle and change management in technology projects
- Impact of redesign activities on security and privacy management in software and hardware projects.
- Most common weaknesses in software security.
- How to avoid such problems in software and at the system level.
- Methodologies for assessing the security of a given device, source code, or entire applications
- Bug bounting
- Security policies: memory security and operating environment management Anti-forensics techniques.

Course evaluation

The written exam will be held in January 2025. Students are allowed to use a personal resume of 12 pages (6 sheets).

The 3 lab projects assigments will be evaluated and their weight on the final evaluation is 35%

Weight of the written exam: 65%