Course Objectives

• Identify causes and consequences of (lack of) system and software security

• Master essential techniques to reduce and avoid system and software security problems, to introduce and reason on security requirements and controls

• Apply advanced modelling techniques (notations, tools, and processes) to build secure systems and software
Course Structure

Security Risk Management
- Security risk management
- Security threats, errors and their types
- Security requirements
- Dependability
- Social engineering

Security modelling
- Security goals and business activities
- Secure system functions and behaviour
- Alignment between different modelling perspectives

Security controls
- Introduction to cryptography
- Role-based access control

Examples of secure software solutions
- Estonian X-Road
- Internet voting
- Analysing Cyber Security

Development processes of secure software
- Traditional secure software development processes
- Security pattern-oriented development

Lecture 1: Security Risk Management
Lecture 2
Security Modelling

- Understanding security goals and business activities
  - BPMN
  - Secure Tropos

Lecture 3:
Security Modelling

- Designing secure system functions and behaviour
  - Misuse cases
  - Mal activities
Lecture 4
Security Modelling

• Aligning between different modelling perspectives
  – Functional
  – Behavioural
  – Goal and Rule
  – Topological

Lecture 5:
Security Risk Analysis

• Malware types
• Seven pernicious kingdoms
• Security threats
• Attack trees
Lecture 6: Security Requirements

- Security criterion
- Security requirement

**Criteria for writing good security requirements**
- What, not how (external observability)
- Understandability, clarity (not ambiguous)
- Cohesiveness (one thing per requirement)
- Testability
  - Possible to test or validate whether the requirement has been met, clear acceptance criteria

Lectures 7 and 8: Role-based Access Control
Lecture 9:
Cryptography

κρυπτός γράφειν

hidden writing

Lecture 10:
X-Road
Lecture 11: 
I-Voting

Lecture 12: 
Related (to Security) Requirements

Defensibility — Safety — Security — Survivability

Privacy

Data Protection — Anonymity — Unlinkability — Undetectability — Unobservability — Pseudonymity

Trustor — Trustum — Trustee
Lecture 13:
So You Want to Start a Cyber War

Lecture 14:
Social Engineering
Lecture 14:
Security Patterns

Context – Problem – Solution

Lecture 15:
Development Process for Secure Software

Microsoft SSDL
OWASP CLASP
Seven Touchpoints
Practicals
Exercises and Workshops

• Exercises
  – Security Risk Management
  – Security Modelling (2)
  – Security Risk
  – Security Requirements
  – Security Metrics
  – Role-Based Access Control
  – Privacy Preserving Data Publishing
  – Modelling of Social Engineering Problem
  – Secure Software Processes

• Workshops
  – Security Model Transformation
  – Model-driven Security
  – Security Pattern Application

Exam

1. June – first time
8. June – second time
15. June – re-sit exam