Master in Computer Engineering (MEI)
Integrated Master in Informatics Engineering (MiEI)

Specialization Profile **CSI**: Cryptography and Information Security

Engenharia de Segurança

jose.miranda@devisefutures.com

Introductions

- Name: José Eduardo Pina Miranda
- Contacts:
  - E-mail: jose.miranda@devisefutures.com
  - Skype: pinamiranda
  - LinkedIn: pt.linkedin.com/in/josepinamiranda/

- Introduction of the students and expectations for the discipline.

Engenharia de Segurança

Engenharia de Segurança

The Security Engineering course focuses on **the methodologies and processes for developing secure software**. It aims to equip students with **skills** that include

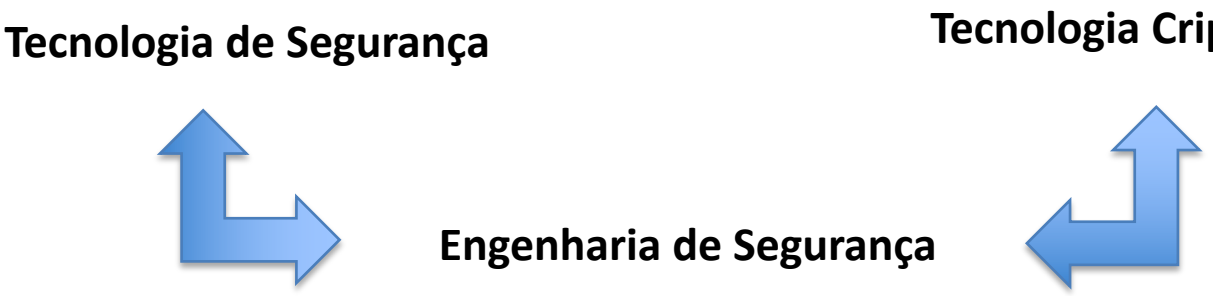
- Identification of risks and assessment of safety requirements of systems,
- Methodologies and tools to support development, and
- Experience with security standards and their implementations.

Goals

Primary Objectives

- Understand the types of vulnerabilities most common in applications, and know how to overcome them.
- Understand and apply software testing methodologies.
- Know the various components of a software development infrastructure.
- Adopt the best software and application security practices.
- Use of secure software development methodologies in the software development lifecycle.

Relation with the other CSI disciplines (first semester):



Goals

Secondary Objectives

- Use of cryptographic primitives in protocols, cryptographic applications and electronic identification documents;
- Understand the complexity in the development (and the security features imposed) of software platforms / applications, in relation to the EU Regulations, national laws and standards that must be followed. As a case study, the following will be used:
  - EU Regulation 910/2014 (eIDAS),
  - Law 32/2017 and respective regulatory ordinances,
  - DL 89/2017 and its regulatory ordinances,
  - Regulation EU 2016/679 (General Regulation on Data Protection - RGPD).

Relation with the other CSI disciplines (first semester):

Tecnologia de Segurança

Tecnologia Criptográfica

Engenharia de Segurança

Organization of the course

- Datas:
  - Every Monday from 14h00 – 17h00, from 04/Fev to 31/Mai – Edificio 7, room 0.04

- Doubts & Queries
  - Before or after classes, by prior appointment, during the class period.

- Copy of slides, exercises, notifications, ...
  - Github (**https://github.com/uminho-miei-engseg-18-19/EngSeg**)

Rating

- A. Theoretical (25%)
  - Written exam (minimum grade: 8 points) <date: students' suggestions accepted>
- B. Practical(75%)
  - Projects (minimum grade: 8 points) made by the working group, which will include:
    - B1 Worksheet in practical classes.
    - B2 Software development project **or** Research on a topic, with / without oral presentation

- Final Grade: 0,25 * A + 0,75 * (B1 * 2 + B2 * 3)/5
  - Successful completion of the course, if Final Grade >= 9,5 points

- The working group will have a maximum of 3 elements.

Program

- Software Vulnerabilities, Attacks and Intrusions:
  - Software Vulnerabilities;
  - Web Application Vulnerabilities (according to OWASP)
  - Vulnerability Classification Systems (CWE, CVE, CVSS, OVAL, CVRF)
- Software Testing:
  - Threat / attack models;
  - Blackbox testing;
  - Whitebox testing;
  - Static analysis (including Lint)
  - Dynamic analysis
  - Hybrid analysis
- Infrastructure for quality software development:
  - IDE;
  - Version control system;
  - Repository manager;
  - Source code quality manager;
  - Documentation generator;
  - Continuous integration tools.
- Secure Software Development Life Cycle (S-SDLC):
  - Life-cycle models of software development;
  - Risk analysis;
  - Standards and Methodologies for Safe Software Development;
  - (Rational) Unified Process applied to participants in the software development process of an SME;
  - Maturity Model.

Program

- Applied Cryptography:
  - Algorithms and key size - Legacy, Future;
  - Random / pseudo-random number generator
  - Secret sharing/splitting – Shamir
  - Authenticated encryption
- Cryptographic protocols / applications
  - SSL/TLS
  - SSH
  - TOR
  - Electronic Vote
- Electronic identification documents
  - Citizen Card
  - E-Passport
  - Dematerialized identification documents
- Steganography
- Regulation 910/2014 (eIDAS)
  - qualified providers
  - qualified trusted services
  - eIDs notification
- Law 32/2017 (Chave Móvel Digital - server-side signature)
- DL 89/2017 (SCAP - Sistema de certificação de atributos profissionais)
- Regulation 2016/679 (General Regulation of Data Protection)

Program

- Guests
  - Data Protection/RGPD (date to be set)
  - Citizen's Card and Electronic Passport (date to be set)
  - Security Considerations in Software Development (date to be set)
  - Innovation and security (date to be set)
  - … (to be set)

Bibliography

- Segurança no Software (2ª Edição Atualizada e Aumentada), Miguel Pupo Correia, Paulo Jorge Sousa, FCA – Editora Informática Lda, 2017
- Threat Modeling : Designing for Security, Adam Shostack, John Wiley&Sons Inc, 2014
- Hacking: The Art Of Exploitation, 2nd Edition, Jon Erickson, No Starch Press,US, 2008
- Software Security : Building Security In, Gary R. McGraw, Pearson Education (US), 2006
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard and Marcus Pinto, Wiley, 2011
- OWASP Testing Guide v4, https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents, OWASP, 2015
- OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, OWASP, 2017
- Software Assurance Maturity Model (SAMM) v. 1.5, https://www.owasp.org/index.php/OWASP_SAMM_Project, OWASP, 2017
- An Introduction to Information Security. Michael Nieles, Kelley Dempsey, Victoria Pillitteri. NIST-800-12 Revision 1, (https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final), 2017
- Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Ron Ross, Michael McEvilley, Janet Carrier Oren. NIST-SP-800-160 (https://csrc.nist.gov/publications/detail/sp/800-160/final), 2016.
- ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls, http://www.smartassessor.com/Uploaded/1/Documents/ISO-2017-standard.pdf, 2013.

Bibliography

- Regulamento UE 910/2014 (eIDAS) relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910&from=PT, 2014
- Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards v.1.1,https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport, ENISA, 2016
- Regulamento Geral de Proteção de Dados (RGPD) - Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT, 2016
- CEN/TS 419241-1:2017 Trustworthy Systems Supporting Server Signing - Part 1:General System Security Requirements, 2017
- CEN/TS 419241-2:2017 Trustworthy Systems Supporting Server Signing - Part 2:Protection profile for QSCD for Server Signing, 2017
- Cryptographic Mechanisms: Recommendations and Key Lengths, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf, BSI TR-02102-1, 2018
- NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management - Part 1: General, Elaine Barker, http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4, NIST, 2016
- Algorithms, key size and parameters report, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/at_download/fullReport, ENISA, 2014
- Data Hiding : Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols, Michael T. Raggo, Chet Hosmer, Syngress Media, 2013
- Information Hiding, Stefan Katzenbeisser, Fabien Peticolas, Artech House Publishers, 2016

Bibliography

- Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf, 2017
- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf, 2017
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf, 2017
- Common Methodology for Information Technology Security Evaluation - Evaluation methodology, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf, 2017
- Configuração do RUP com Vista à Simplificação dos Elencos Processuais em PMEs de Desenvolvimento de Software, Pedro Borges, Tese de Mestrado, Universidade do Minho, 2007
- Security Engineering 2nd Edition, Ross Anderson, http://www.cl.cam.ac.uk/~rja14/book.html, Wiley, 2008
- Secrets and Lies : Digital Security in a Networked World, Bruce Schneier, John Wiley&Sons Inc, 2004
- Sunshine on Secure Software: Baking Security into your SDLC Process, Sunny Wear, BookBabym 2013
- Secure Software Development: A Security Programmer's Guide, Jason Grembi, Cengage Learning, 2008
- Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 2008.

Tools

- WebGoat (Warning: Machine becomes vulnerable)
- PMD
- FindBugs
- FindSecurityBugs
- FlawFinder
- Atom
- Eclipse
- …

- Available in virtual machine
  - In this case, as it will be a virtual machine that will be changed during the course, students should store what they are doing in the (shared) directory of the host machine.

Software development project **or** Research on a topic, with / without oral presentation

- To be delivered by June 15.
- Proposals from students for projects or research are accepted, provided that they can be included in the scope of the subject taught in Engenharia de Segurança.
- Part of the practical classes should be used to discuss the project with the teacher of the course.
- Projects to be defined up to Feb / 15.