Mestrado em Engenharia Informática (MEI)
Mestrado Integrado em Engenharia Informática (MiEI)

Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança

jose.miranda@devisefutures.com

Apresentações

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

- Apresentação dos alunos e expectativas para a disciplina

Caderno de encargos

Engenharia de Segurança

A unidade curricular de Engenharia de Segurança foca-se nas **metodologias e processos de desenvolvimento de software seguro**. Visa dotar o alunos de **competências** que incluem

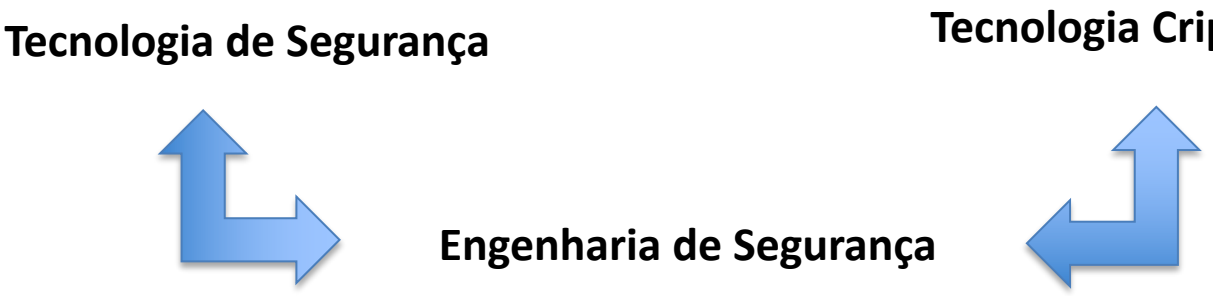
- Identificação dos riscos e levantamento de requisitos de segurança dos sistemas,
- Metodologias e ferramentas de apoio ao desenvolvimento, e
- Experiência com os "standards" de segurança e suas implementações.

Objetivos

Objetivos Primários

- Conhecer os tipos de vulnerabilidades mais comuns nas aplicações, e saber como as ultrapassar.
- Compreender e aplicar metodologias de teste de software.
- Conhecer as várias componentes de uma infraestrutura de desenvolvimento de software.
- Adotar as melhores práticas de segurança do software e aplicacional.
- Utilização de metodologias de desenvolvimento de software seguro no ciclo de vida de desenvolvimento do software.

Relação com outras disciplinas do CSI (do primeiro semestre):

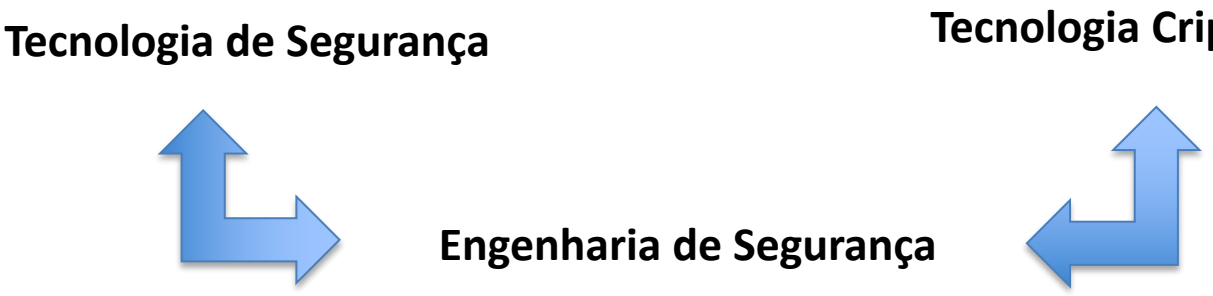


Objetivos

Objetivos Secundários

- Utilização de primitivas criptográficas em protocolos, aplicações criptográficas e documentos de identificação eletrónicos;
- Perceber a complexidade no desenvolvimento (e nas características de segurança impostas) de plataformas/aplicações de software, face aos Regulamentos UE, Leis nacionais e standards que têm de ser seguidos. Como caso de estudo, serão utilizados:
  - Regulamento UE 910/2014 (eIDAS),
  - Lei 32/2017 e respetivas portarias regulamentares,
  - DL 89/2017 e respetivas portarias regulamentares,
  - Regulamento EU 2016/679 (Regulamento Geral de Proteção de Dados – RGPD).

Relação com outras disciplinas do CSI (do primeiro semestre):



Organização da Disciplina

- Datas:
  - Todas as segunda-feira das 14h00 – 17h00, de 05/Fev a 25/Jun.
- Horário de dúvidas
  - Antes ou após as aulas, mediante marcação prévia, durante o período de aulas.
- Cópia dos slides, exercícios, ...
  - Através do Blackboard quando tiver acesso ao mesmo, e
  - Github

Avaliação

- A. Avaliação teórica (30%)
  - Exame escrito (nota mínima: 8 valores) a 25/Jun
- B. Avaliação prática (70%)
  - Trabalhos (nota mínima: 8 valores) efetuados pelo grupo de trabalho, que incluirão:
    - Dissertação/Pesquisa/Investigação sobre um tópico, com/sem apresentação oral.
    - Ficha de trabalho nas aulas práticas.
    - Projeto de desenvolvimento de software.

- Classificação final: 0,3 * A + 0,7 * média B
  - Condição para aproveitamento nesta disciplina: Classificação final >= 9,5 valores

- O grupo de trabalho terá no máximo 3 elementos.

Programa

- Vulnerabilidades de software, ataques e intrusões:
  - Vulnerabilidades de Software;
  - Vulnerabilidades de Aplicações Web (de acordo com OWASP)
  - Sistemas de Classificação de Vulnerabilidades (CWE, CVE, CVSS, OVAL, CVRF)
- Testes de software:
  - Modelos de ameaças/ataques;
  - Blackbox testing;
  - Whitebox testing;
  - Análise estática (incluindo Lint)
  - Análise dinâmica
  - Análise híbrida
- Infraestrutura para desenvolvimento de software de qualidade:
  - IDE;
  - Sistema de controlo de versões;
  - Gestor de repositórios;
  - Gestor de qualidade de código fonte;
  - Gerador de documentação;
  - Ferramentas de integração contínua.
- Ciclo de vida de desenvolvimento de software seguro - Secure Software Development Life Cycle (S-SDLC) -:
  - Modelos de ciclo de vida de desenvolvimento de software;
  - Análise de Riscos;
  - Standards e Metodologias de desenvolvimento de software seguro;
  - (Rational) Unified Process aplicado aos participantes no processo de desenvolvimento de software de uma PME;
  - Modelo de Maturidade.

Programa

- Criptografia Aplicada:
  - Algoritmos e tamanho de chaves - Legacy, Futuro;
  - Gerador de número aleatórios / pseudo-aleatórios
  - Secret sharing/splitting – Shamir
  - Authenticated encryption
- Protocolos/aplicações criptográficas
  - SSL/TLS
  - SSH
  - TOR
  - Voto eletrónico
- Documentos de identificação eletrónicos
  - Cartão de Cidadão
  - Passaporte Eletrónico
  - Documentos de identificação desmaterializados
- Esteganografia
- Regulamento 910/2014 (eIDAS)
  - prestadores qualificados
  - serviços qualificados de confiança
  - notificação eIDs
- Lei 32/2017 e respetivas portarias regulamentares (Chave Móvel Digital - assinatura server-side)
- DL 89/2017 e respetivas portarias regulamentares (SCAP - Sistema de certificação de atributos profissionais)
- Regulamento 2016/679 (Regulamento Geral de Proteção de Dados)

Programa

- Participação de convidados
  - CISO (data a indicar)
  - Auditor de segurança (19/Março)
  - CEO de PME, que desenvolve plataforma software industrial (data a indicar)
  - … (a indicar)

Bibliografia

- 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.

Bibliografia

- 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

Bibliografia

- 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.

Ferramentas

- WebGoat (Atenção: Máquina fica vulnerável)
- PMD
- FindBugs
- FindSecurityBugs
- FlawFinder
- Atom
- Eclipse
- …

- Disponibilizadas em máquina virtual
  - Nesse caso, como será uma máquina virtual que irá sendo alterada, alunos devem guardar aquilo que forem fazendo na diretoria (partilhada) da máquina principal.

Projeto de desenvolvimento de software

- 2 projetos para serem feitos até final de Junho.
- Cada projeto é feito por um conjunto alargado de alunos, divididos nos grupos que decidirem, com as funções que decidirem e com as fases e timings que decidirem.
- Parte das aulas práticas deverão ser utilizadas para discussão do projeto com o docente da disciplina.

Projeto 1 – Leilões online

- Leilões online, com entrega de propostas em "carta fechada";
- Pode ser uma extensão para software *open source* de leilões online.

Projeto 2 – Gestor de passwords com base em QrCodes

- Gestor de passwords, em que com base em QrCode apresentado pelo site, o telemóvel lê o QrCode e envia o user + password para desbloquear o acesso;
- Pode ser uma extensão para software *open source* de gestão de passwords.