Mestrado em Engenharia Informática (MEI)

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

Engenharia de Segurança

Apresentações

- Nome: José Eduardo Pina Miranda
- Contactos:
  - E-mail: jose.miranda@devisefutures.com

- Apresentação aos alunos e expectativas para a UC

Caderno de encargos

Engenharia de Segurança

A unidade curricular de Engenharia de Segurança foca-se nas **metodologias e processos que visam estabelecer a segurança dos sistemas de informação e de desenvolvimento de software seguro**.

- Visa dotar os 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.
- No **final** os alunos deverão:
  - Compreender os diferentes passos na implementação de um Sistema de Gestão da Segurança da Informação.
  - Realizar gestão de risco no âmbito do sistema de informação de uma organização.
  - Realizar modelos de ameaças em sistemas de “software”.
  - Utilizar metodologias de desenvolvimento de software seguro no ciclo de vida de desenvolvimento do software.

Caderno de encargos – adicional 2022/23

Engenharia de Segurança

Em 2021/22 entrou em vigor um novo plano curricular, significando que:

- No ano de 2022/23 não foi lecionada durante o primeiro semestre do Mestrado, a disciplina onde os alunos tinham o seu primeiro contacto com a criptografia.
- O novo plano curricular da licenciatura já estava em vigor no ano passado, pelo que eventualmente alguns/todos (??) alunos tiveram esse contacto com a criptografia durante o 3º ano da licenciatura.

Nessa perspetiva, a unidade curricular de Engenharia de Segurança vai começar pelos **conceitos de criptografia**, de modo a homogeneizar o conhecimento.

- Visa dotar os alunos de **competências** que incluem
  - Identificação dos *building blocks* da criptografia,
  - Experiência na utilização de APIs e bibliotecas de criptografia, e
  - Integração dos *building blocks* criptográficos em protocolos e aplicações.
- No **final** os alunos deverão:
  - Saber utilizar os *building blocks* da criptografia,
  - Identificar riscos associados à utilização de chaves e algoritmos criptográficos,
  - Compreender o modo de escolher e integrar algoritmos criptográficos em aplicações,
  - Conhecer aplicações avançadas da criptografia.

Conteúdos Programáticos

Inclui:

1. Gestão de Segurança de Informação:
   - Sistemas Gestão de Segurança de Informação [família ISO/IEC 27000): Controlos, métricas, gestão de risco, continuidade de negócio, gestão de incidentes, evidência digital.
   - Avaliação de segurança: níveis de conformidade (ITSEC e Common Criteria)
   - Potencial de Ataque: Cálculo e avaliação, de acordo com a metodologia de avaliação do Common Criteria
   - Esquemas de identificação eletrónica: nível de conformidade eIDAS.
   - Proteção de Dados e RGPD.
   - Métricas de segurança para Sistemas de informação (NIST SP800-55)
   - Trustworthy Secure Systems (NIST SP800-160)

2. Desenvolvimento de Software Seguro:
   - Modelação de Ameaças.
   - Boas práticas "SafeCODE"; utilização de componentes "third-party"; "*Secure Software Development LifeCycle* (S-SDLC)"
   - Avaliação de Garantias do "Software; "*Software Assurance Maturity Model* (SAMM)".
   - Qualidade do "Software": cobertura de código; interpretação abstracta; complexidade; compilação; "*coding standards*".
   - Teste de Segurança: guiões e "checklists"; "*Application Security Verification Standard*"

Conteúdos programáticos

Inclui

- Evolução da criptografia;
- Algoritmos e chaves criptográficas;
- Utilização de primitivas criptográficas em protocolos, aplicações criptográficas e documentos de identificação eletrónicos (mDL, ID.gov, EUDI Wallet, ...);
- 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), e DL 12/2021,
  - 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),
  - Revisão do Regulamento UE 910/2014 (Regulamento eIDAS 2).

Avaliação

- A. Avaliação prática 1 (10%)
  - Ficha de trabalho sobre tema da aula teórica (em média, uma ficha de trabalho por semana) - (nota mínima: 8 valores) efetuada pelo grupo de trabalho.
- B. Avaliação prática 2 (85%)
  - PA – Projeto de análise de um tema, com elaboração de relatório, assim como exposição do trabalho;
  - PD1 – Projeto para consolidação dos conceitos básicos de criptografia;
  - PD2 – Projeto de desenvolvimento que poderá incluir várias componentes para além do desenvolvimento em si (e.g., identificação do "*Software Assurance Maturity Model* (SAMM)" da equipa, RGPD PIA, *compliance* com boas práticas de desenvolvimento).
- C. Participação individual (5%)
  - Participação individual nos projetos e no acompanhamento presencial.

- Classificação final: 0,1 * A + 0,85 * (0,25 * PA + 0,3 * PD1 + 0,45 * PD2) + 0,05 * C
  - Condição para aproveitamento nesta disciplina: Classificação final >= 9,5 valores

- O grupo de trabalho poderá ter entre 3 e 5 elementos, sendo recomendado que seja constituído por 3 elementos.
  - Note que se o grupo tiver mais do que 3 elementos, a avaliação prática 1 e a avaliação prática 2 terão componentes suplementares de trabalho.

Modo de funcionamento

- Cópia dos slides, exercícios, avisos, fichas de trabalho, projetos, ...
  - Github (https://github.com/uminho-mei-engseg-22-23/EngSeg),

- Grupos de trabalho
  - **Cada grupo enviará o nome dos seus elementos, nº de aluno, endereço de e-mail e utilizador no github, por e-mail para o docente**;
  - A numeração do Grupo de Trabalho será efetuada por ordem de chegada do mail;
  - O docente criará um repositório para cada Grupo, por baixo de https://github.com/uminho-mei-engseg-22-23, para onde convidará os elementos do Grupo, sendo esse repositório o local que cada Grupo utilizará para os trabalhos práticos.

- Mattermost
  - O canal de mattermost "Engenharia de Segurança" é utilizado para deixar avisos, assim como para apoio aos alunos;
  - Para se juntarem ao canal, sigam https://chat.devisefutures.com/signup_user_complete/?id=hj4j9qob9idy8ktboot5o53xca&sbr=fa .

Modo de funcionamento

A UC de Engenharia de Segurança foi pensada para ser efetuada em modo híbrido durante todo o semestre (i.e., poderão existir aulas presenciais, aulas pré-gravadas e aulas remotas), tendo sido colocado o focus no acompanhamento presencial da progressão dos alunos.

Desse modo,

- Aulas teóricas e fichas de trabalho (avaliação prática 1) – serão disponibilizadas semanalmente antes do dia da aula no Github da disciplina.

- Enunciados dos projetos da avaliação prática 2 - disponibilizados no Github durante esta semana (PA), e até início do mês de Março (PD1 e PD2).

- Acompanhamento presencial:
  - Todas as terças-feiras das 09h00 – 12h00, durante o 2º semestre
  - Estas aulas poderão ser presenciais, pré-gravadas ou remotas – caso não sejam presenciais, a informação será disponibilizada no Github da UC ou no canal mattermost da UC .

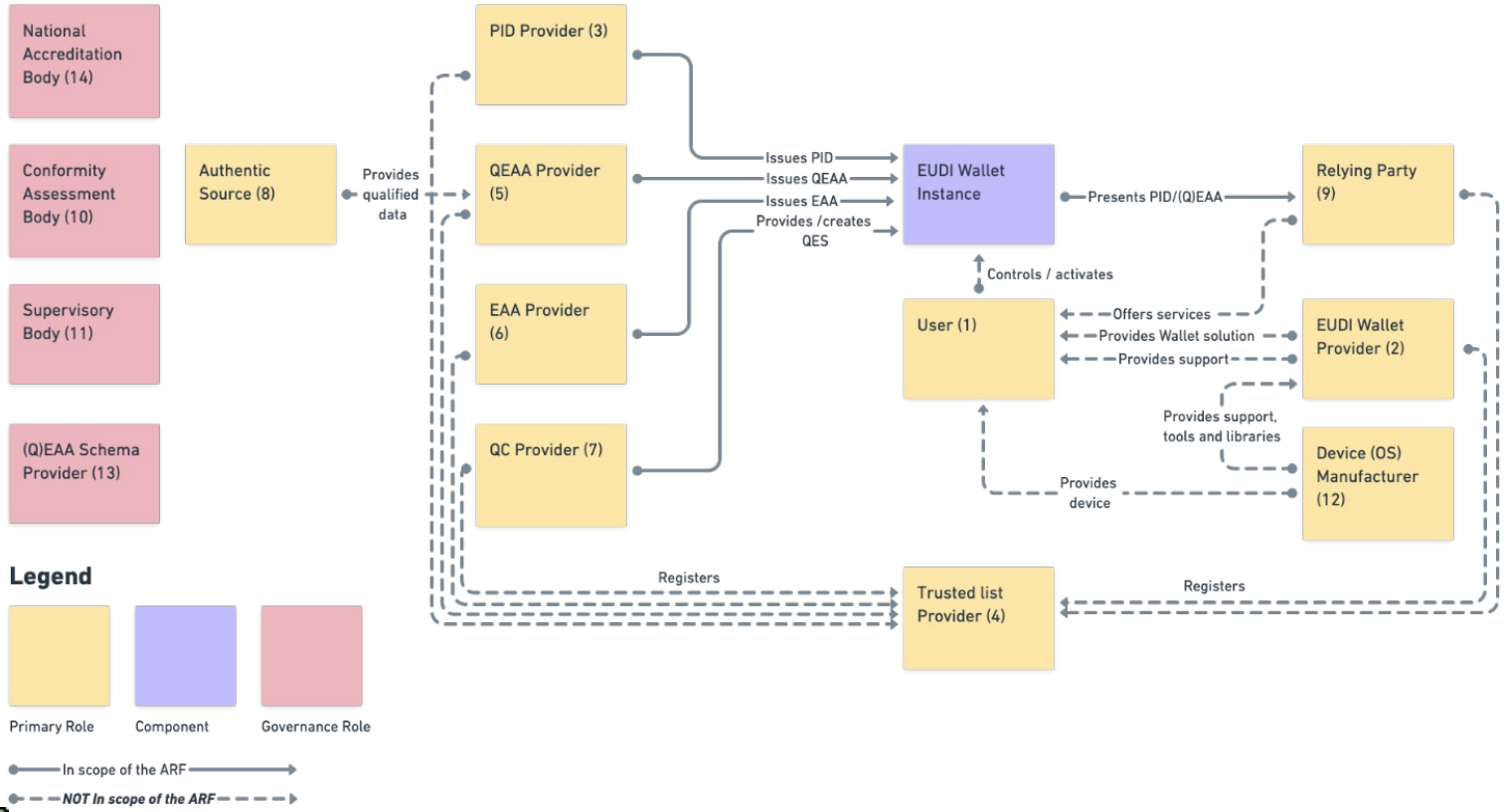
Projetos de avaliação prática 2

- 3 projetos:
  - PA – Projeto análise de um tema, com elaboração de relatório, assim como exposição do trabalho, com entrega de relatório até 13/03/2023.
    - Disponibilizado no Github durante esta semana.
  - PD1 – Projeto para consolidação dos conceitos básicos de criptografia, com entrega final até 24/04/2023.
    - Disponibilizado no Github até início do próximo mês.
  - PD2 – Projeto de desenvolvimento, com entrega final até 15/06/2022.
    - Note que este projeto pode ter componentes que são entregues anteriormente, em data a indicar.
    - Disponibilizado no Github até início do próximo mês.

- Nota: Toda a documentação e relatórios deverão ser feitos em **português de Portugal**.

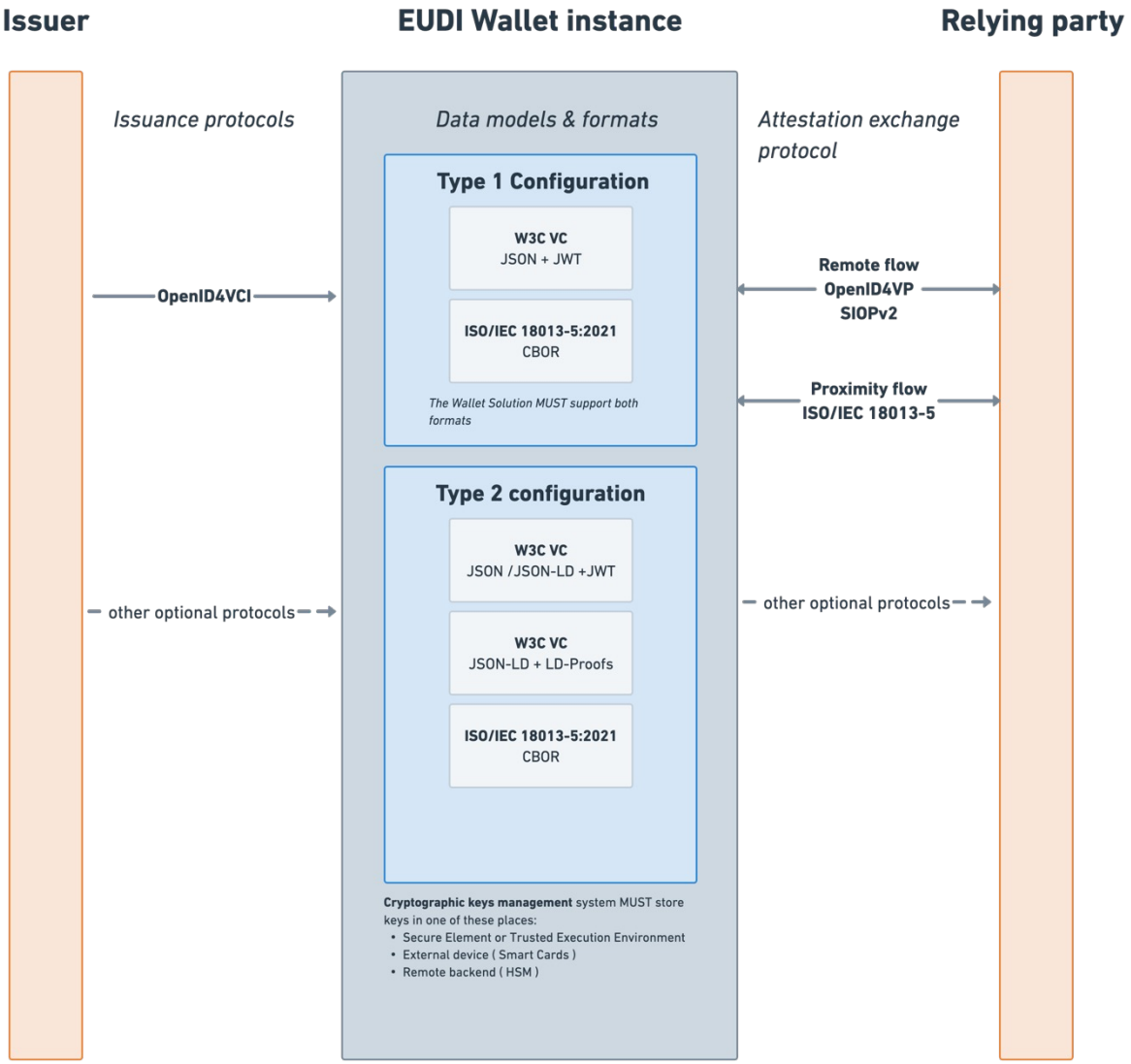
UC Engenharia de Segurança – Motivação

- Novo Regulamento (UE) eIDAS 2.0
  - European Identity Digital Wallet (EUDIW)
  - EUDIW Architecture and Reference Framework (ARF)



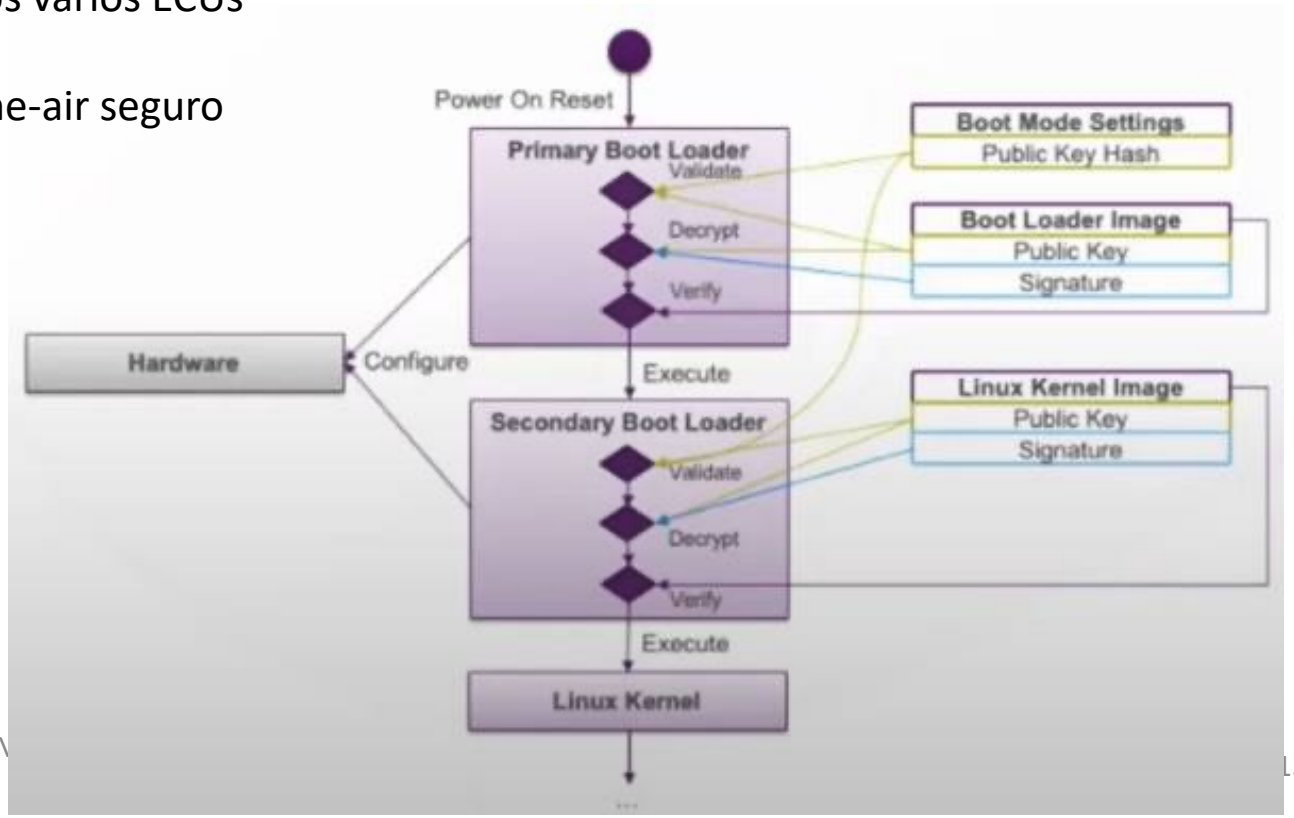
UC Engenharia de Segurança – Motivação

- Novo Regulamento (UE) eIDAS 2.0
  - European Identity Digital Wallet (EUDIW)
  - EUDIW Architecture and Reference Framework (ARF)



UC Engenharia de Segurança – Motivação

- Automotive ECUs (Electronic control unit)
  - Controlam diferentes processos e funcionalidades dos veículos (incluindo, condução (semi)-autónoma)
  - Vulnerabilidade: acesso remoto e ativação de funcionalidades em automóveis Tesla (https://www.helpnetsecurity.com/2016/09/28/tesla-code-signing/)
  - Assinatura de código
  - Autenticação dos vários ECUs
  - Boot seguro
  - Upgrade over-the-air seguro



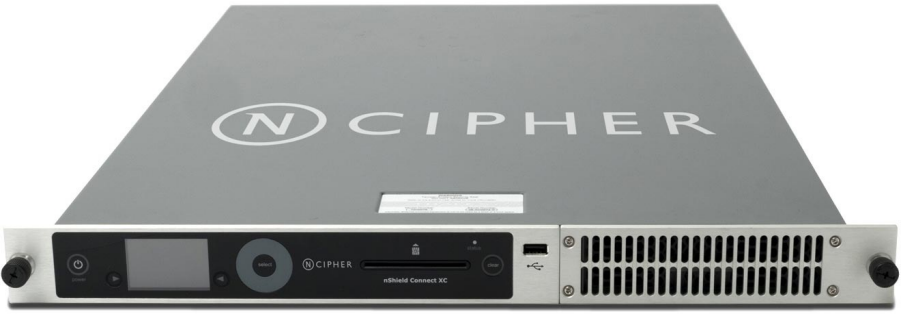
UC Engenharia de Segurança – Motivação

- HSM (*Hardware Security Module*)

  "*It is a physical hardware security device that provides protection for cryptographic keys and other sensitive data. The HSM is designed to ensure that cryptographic keys cannot be accessed or disclosed, even if the device is compromised by malware or a breach.*

  HSMs are commonly used in cryptographic security applications, such as the protection of financial transactions, the storage of two-factor authentication keys, and the generation of digital signatures. They can be implemented as a standalone physical unit or embedded within other devices such as servers, mobile devices, or network gateways.

  The HSM provides several security features such as strong authentication, secure storage, random key generation, encryption of sensitive data, and digital signature. By protecting cryptographic keys and sensitive data, the HSM ensures the confidentiality and integrity of transactions and information is preserved." (in ChatGPT)



Programa

- Criptografia:
  - Resenha história
  - Criptografia de chave simétrica
  - Criptografia de chave pública
  - Hashing
  - Timestamping
- 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 (MDL, EUDI Wallet)
- Esteganografia
- Regulamento 910/2014 (eIDAS) e DL 12/2021
  - 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

- 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.

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/images/1/19/OTGv4.pdf, OWASP, 2015
- OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, https://owasp.org/www-project-top-ten/, OWASP,
- Software Assurance Maturity Model (SAMM) v. 1.5, https://www.owasp.org/images/6/6f/SAMM_Core_V1-5_FINAL.pdf, 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.