
Apresentação

Notas para a UC de “Segurança Informática”
Inverno de 2020/21

José Simão (jsimao *em* cc.isel.ipl.pt)
Nuno Leite (nleite *em* cc.isel.ipl.pt)

Instituto Superior de Engenharia de
Lisboa

Objectivos

- Realizar uma introdução à teoria e prática da segurança informática
 - Teoria
 - ex. mecanismos criptográficos, modelos de controlo de acesso, ...
 - Prática
 - ex. utilização de API criptográficas, configuração de sistemas, ...
- Fornecer a base conceptual e prática necessária ao estudo dos aspectos de segurança em contextos específicos
 - Sistemas distribuídos
 - Sistemas de informação
 - Redes de comunicação de dados

Programa

- Parte I – Mecanismos e Protocolos Criptográficos
 - Esquemas criptográficos
 - Métodos para autenticação de chaves públicas
 - Protocolos de autenticação e estabelecimentos de chaves
- Parte II – Autenticação e Autorização
 - Autenticação baseada em *passwords*
 - Protocolos para gestão distribuída de identidade
 - OpenID Connect, OAuth 2.0
 - Modelos, políticas e mecanismos
 - Casos de estudo: ACLs, RBAC
- Parte III – Escrita de código seguro
 - Vulnerabilidades típicas em aplicações nativas e web
 - Técnicas de protecção

Componente prática e laboratorial

- Séries de exercícios
 - Exercícios teóricos
 - Exercícios práticos (de implementação)
- Ferramentas, plataformas e linguagens de programação utilizadas
 - OpenSSL
 - Labs for Security Education (SEED Lab)
 - Java / Node.JS
- Não existem aulas laboratoriais periódicas
 - A marcação de aulas laboratoriais será realizada no horário normal, em função das necessidades

Avaliação

- Teste final
 - 60% da nota final
 - Nota mínima de 9,5 valores
 - A realizar nas datas de exame
 - Duas datas, melhor das notas
 - Consulta limitada a 1 folha A4
- Três séries de exercícios
 - 40% da nota final
 - Apresentação/discussão em data a combinar
 - Datas previstas
 - Primeira série: publicação a 14/10/2020; entrega até 11/11/2020
 - Segunda série: publicação a 11/11/2020; entrega até 19/12/2020
 - Terceira série: publicação a 19/12/2020; entrega até 23/01/2021
 - Realizadas em grupos de 2 ou 3 elementos
 - Entregas no sistema Moodle

Suporte

- Páginas no sistema Moodle (<https://2021moodle.isel.pt/>)
 - Entradas LEIC, LEIM e LEIRT, com grupos em cada turma
- Suporte bibliográfico
 - Conjuntos de slides
 - Artigos e manuais
 - Livros recomendados
 - D. Gollmann, Computer Security, 2ª edição, Wiley, 2006
 - Wenliang Du, Computer & Internet Security: A Hands-on Approach, 2ª edição, 2019

Equipa docente

- Docentes
 - José Simão (jsimao *em* cc . isel . ipl . pt)
 - CCISEL, Sala 20
 - Nuno Leite (nleite *em* cc . isel . Ipl . pt)
 - Edifício do Departamento, sala F.2.2