
Apresentação

Notas para a UC de “Segurança Informática”
Inverno de 2011/12

José Simão (jsimao@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, gestão de identidade, ...
 - Prática
 - ex. utilização de API criptográficas, protecção contra vulnerabilidades típicas das aplicações web, ...
- 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

- Mecanismos criptográficos
 - Esquemas criptográficos
 - Métodos para autenticação de chaves públicas
 - Protocolos de autenticação e estabelecimentos de chaves
 - Casos de estudo: Java Cryptography Architecture (JCA), Kerberos, SSL
- Gestão de identidade e controlo de acessos
 - Autenticação baseada em *passwords*
 - Modelos clássicos, políticas e mecanismos para controlo de acessos
 - Protocolos para gestão de identidade em ambientes distribuídos
 - Casos de estudo: ACL, RBAC, OpenID, OAuth
- Escrita de código seguro
 - Vulnerabilidades típicas
 - Técnicas de protecção
 - Casos de estudo: Buffer overflow, SQL injection, XSS, CSRF

Dependências com temas de outras UCs

- Plataforma e linguagem Java
- Plataforma .NET e linguagem C#
- HTTP, HTML, MVC.NET

Componente prática e laboratorial

- Não existem aulas laboratoriais periódicas
 - A marcação de aulas laboratoriais será realizada no horário normal, em função das necessidades
- Séries de exercícios
 - Exercícios teóricos
 - Exercícios práticos (de implementação)

- Teste final
 - 50% da nota final
 - Nota mínima de 9,5 valores
 - A realizar nas datas de exame
 - Duas datas, melhor das notas
 - Consulta limitada a uma folha A4
- Três séries de exercícios
 - 50% da nota final
 - Discussão final
 - Primeira série: publicação a 27/09/2011; entrega a 25/10/2011
 - Segunda série: publicação a 25/10/2011; entrega a 29/11/2011
 - Terceira série: publicação a 29/11/2011; entrega a 10/01/2012
 - Realizadas em grupos de 2 ou 3 elementos

- Sumários e material de apoio no Moodle (<http://moodle.isel.ipl.pt/deetc/>)
 - SI-1011SI (meta-disciplina)
 - SI-LI51D-1112SI
 - SI-LI51N-1112SI
- Suporte bibliográfico
 - Conjuntos de slides
 - Artigos e manuais
 - Livros recomendados
 - D. Gollmann, Computer Security, 2ª edição, Wiley
 - M. Bishop, Introduction to Computer Security, Addison-Wesley

Equipa docente

- Docentes
 - José Simão (jsimao *em cc isel ipl pt*)
 - CCISEL, Sala 20
 - Pedro Félix (pedrofelix *em cc isel ipl pt*)
 - Responsável da disciplina
 - CCISEL, Sala 20