Ciências ULisboa

Introdução à Segurança Informática

Código: 425173
ECTS: 6
Ano Letivo: 2015/16
Carga horária: T: 2:00 h; TP: 1:30 h; OT: 2:00 h;
Departamento: Informática
Área Científica: Informática;

Objetivos da Unidade Curricular

A disciplina pretende abordar a problemática da segurança nos sistemas computacionais abertos, incluindo computadores e redes de comunicação, isto é, numa óptica de sistemas distribuídos. As competências adquiridas com a cadeira podem ser equacionadas pelo conhecimento dos fundamentos da segurança em sistemas de computadores numa óptica abrangente.

Os estudantes conseguirão também compreender as principais estratégias e decisões presentes no projecto de sistemas de computadores seguros e serão expostos ao exemplos mais relevantes de sistemas e tecnologias actuais. Os estudantes serão capazes de estender este conhecimento com estudos de pós-graduação subsequentes, ou de aplicá-lo directamente nas suas vidas profissionais, com vantagem em relação a investigadores ou profissionais com uma formação superficial ou ocasional em segurança.

Pré-requisitos

- Redes de Computadores (26704)
- Sistemas Distribuídos (26730)

Conteúdos

Conceitos Fundamentais de Segurança.

Paradigmas de segurança.

Modelos de Computação Distribuída Segura.

Sistemas e plataformas seguros.

Descrição detalhada dos conteúdos programáticos

Componente Teórica

Conceitos Fundamentais de Segurança

* Conceitos Fundamentais de Segurança
* Definição de Segurança, o que motiva o Intruso,
* Redes Seguras, Arquitecturas Distribuídas Seguras

Paradigmas de segurança

* Trusted Computing Base,
* Criptografia simétrica e assimétrica,
* Hashes seguros e sínteses de mensagens,
* Assinatura Digital, Dinheiro Digital,
* Outros paradigmas e algoritmos criptográficos,
* Autenticação, Controle de Acesso,
* Comunicação Segura

Modelos de Computação Distribuída Segura

* Classes de ataques, vulnerabilidades e intrusões,
* Frameworks de segurança e estratégias para operação segura,
* Utilizando protocolos criptográficos,
* Modelos de autenticação, distribuição de chaves,
* Modelos de protecção, modelos de segurança formal,
* Proteção de arquitectura: topologia e Firewalls,
* Comunicação e processamento distribuído seguros,
* Modelos de transacções electrónicas

Sistemas e plataformas seguros

* Operações remoto e mensagens,
* Intranets e Firewalls,
* Extranets e redes privadas virtuais,
* Serviços de autenticação e autorização,
* Comércio electrónico seguro e Sistemas de Pagamento,
* Gestão de Segurança na Internet

Componente Teórica-Prática

* Apresentação de ferramentas de segurança para detetar vulnerabilidades, firewalls e deteção de intrusões.

* Apresentação de trabalhos recentes da área da segurança tais como segurança em IoT, segurança em cloud, segurança em firewall.

* Apresentação de casos de estudo.

Componente Prática

Trabalhos com diversas ferramentas de segurança, tais como as ferramentas disponibilizadas pelo kali linux e o nessus.

Bibliografia

Recomendada

Computer Security: Principles and Practice, William Stallings and Lawrie Brown, 3rd edition, 2015, Pearson

Outros elementos de estudo

P. Veríssimo e L. Rodrigues, Distributed Systems for System Architects, Kluwer Academic Publishers, 2001, 650pp., Part IV -- Security.

Introduction to Computer Security, Matt Bishop. Addison Wesley Professional, 2004. ISBN-10: 0-321-24744-2.

Network Security: Private Communication in a Public World, 2nd Ed. C. Kaufman, R. Perlman, M. Speciner. Prentice Hall, 2002.

Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition. William R. Cheswick, Steven M. Bellovin, and Aviel Rubin. Addison-Wesley Professional, 2003. ISBN: 0-201-63466-X.

Network Intrusion Detection 3rd Ed., Stephen Northcutt, Judy Novak. New Riders Publishing, 2002, 490 pages. ISBN 0735712654.

Applied Cryptography (2nd Ed), B. Schneier, John Wiley & Sons, 1996.

Hack Attacks Revealed, 2nd Ed., John Chirillo, Wiley Publishing, 2002.

Hack attacks denied: a complete guide to network lockdown for unix, windows and linux, 2nd Ed., John Chirillo, Wiley Publishing, 2002.

Java Security, 2nd edition, Scott Oaks, O'Reilly 2001.

Several research and design papers, available on the Web.

Métodos de Avaliação

Regras de classificação: 40% - Projecto e Trabalhos, 60% - Exame final (cada uma das componentes tem nota mínima)

Língua de ensino

Português ou Inglês