Ciências ULisboa

Segurança Aplicada

Código: 425175
Ano Letivo: 2015/16
Departamento: Informática
ECTS: 6
Carga horária: T: 2:00 h; TP: 1:30 h; OT: 2:00 h;
Área Científica: Informática;

Objetivos da Unidade Curricular

Esta cadeira aborda um conjunto de tópicos avançados relacionados com o desenvolvimento de sistemas distribuídos seguros.

Hoje em dia, num mercado globalizado, as organizações e indivíduos necessitam de estar interligados pela Internet, de maneira a que seja possível fornecer informação e serviços aos utilizadores, criar relações entre parceiros e fazer negócios. Neste ambiente aberto, vários tipos de ameaças existem, executadas por diversos tipos de indíviudos.

A disciplina vai focar tecnologias e soluções actuais para a concretização de sistemas distribuídos capazes de conduzir operações seguras neste ambiente potencialmente adverso.

Pré-requisitos

- Segurança Informática (26714)

Conteúdos

Algoritmos e protocolos criptográficos avançados para autenticação, comunicação segura e transacções eletrónicas seguras.

Descrição detalhada dos conteúdos programáticos

Componente Teórica

Algoritmos de criptografia simétrica e assimétrica & algoritmos de hashing (ex., AES, DES, RSA, DH, SHA, HMAC, RC4)

Mecanismos e formas de autenticação (ex., Kerberos, RADIUS)

Comunicação segura em sistemas abertos (ex., IPsec, SSL/TLS, IEEE 802.11 e Bluetooth);

RFID

Correio electrónico seguro (Secure MIME, PGP)

Transacções eletrónicas seguras (bitcoin, cartões, E-Cash, Millicent)

Componente Teórica-Prática

As aulas teórico-práticas têm o objectivo de complementar os tópicos tratados nas aulas teóricas, através do tratamento de temas mais específicos, a realização de trabalhos no laboratório, e de suporte aos projectos.

Bibliografia

Recomendada

W. Stallings, Cryptography and Network Security, Principles and Practice (Six Edition) , Prentice Hall, 2014

Outros elementos de estudo

Selected papers

C. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communication in a Public World (Second Edition), Prentice Hall, April, 2002.

D. O´Mahony, M. Peirce, H. Tewari, Electronic Payment Systems for E-Commerce (Second Edition), Artech House Computer Security Series, 2001

Madjid Nakhjiri, Mahsa Nakhjiri, AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility, 2005

Frank Thornton, Chris Lanthem, RFID Security, 2005

Métodos de Avaliação

* (40%) Dois projectos, e pelas impressões do professor nas aulas teórico-práticas;
* (10%) Apresentação e discussão de artigo científico em temas da cadeira
* (50%) Exame final.

Língua de ensino

Português ou Inglês