

INSTITUTO POLITÉCNICO DE TOMAR
Escola Superior de Tecnologia de Tomar
Departamento de Engenharia Informática
Curso de Engenharia Informática

DISCIPLINA DE
Telecomunicações e Redes Integradas II

4º Ano

Regime: Semestral (8º)

Ano Lectivo:2005/2006

Carga Horária:2T+3P

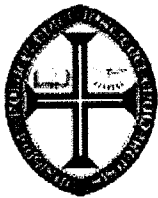
Docente: Luís Miguel Lopes de Oliveira

OBJECTIVOS

Dotar os alunos de conhecimentos teóricos e de experiências práticas que lhes permita projectar e concretizar redes e sistemas informáticos seguros.

PROGRAMA

1. Conceitos fundamentais e terminologia.
 - Necessidade de proteger as redes e os sistemas informáticos.
 - Definição de segurança Propriedades e serviços de segurança
 - Estruturação do estudo dos suportes de segurança.
2. Princípios e Fundamentos dos métodos criptográficos.
 - Princípios de criptografia computacional
 - Princípios do funcionamento dos métodos criptográficos
 - Métodos e algoritmos de criptografia simétrica
 - Métodos e algoritmos de criptografia de chave pública
 - Infra-estruturas de Chave Pública.
 - Funções de Hashing e Message Digests.
 - Assinaturas digitais e sua utilização.
 - Certificados digitais.
 - Caso de estudo – Pretty Good Privacy (PGP).
3. Sistemas de autenticação, certificação e controlo de acessos.
 - Kerberos V4/V5
 - Serviços de autenticação com certificação X.509



INSTITUTO POLITÉCNICO DE TOMAR
Escola Superior de Tecnologia de Tomar

Departamento de Engenharia Informática

Curso de Engenharia Informática

Sistemas de autenticação centralizada (Sistemas SingleSignOn).

Sistemas e infra-estruturas de gestão de chaves públicas (PKIs).

4º Firewalls e sistemas de detecção de intrusão

Tipos de Firewalls.

Sistemas de detecção de intrusão (IDS).

5. Planeamento de redes Wireless 802.11.

O Protocolo 802.11

Segurança em redes Wireless 802.11.

Projecto de redes Wireless 802.11

6. Redes Seguras

Principais características das redes seguras.

Planeamento de redes seguras.

Mecanismos e protocolos usados nas redes seguras.

Métodos de Avaliação:

A avaliação é composta pela avaliação contínua com o peso total de 40% e uma frequência ou exame individual com o peso de 60%. O aluno obtém aprovação se a média pesada (60% T e 40% P) for superior a 9,5 (nove valores e cinco décimas) e se a nota da teórica for maior que 6,5 (seis valores e cinco décimas)

Avaliação contínua:

A avaliação da componente contínua incide sobre o desempenho dos alunos nas aulas prática e na avaliação dos relatórios laboratoriais. Os relatórios laboratoriais são realizados individualmente ou em grupos de dois alunos. Todos os trabalhos são sujeitos a discussão.

É obrigatória a presença nas aulas práticas de acordo com o art. 12 do Regulamento de Académico

Avaliação teórica:

Só são admitidos à prova escrita os alunos que tenham obtido 10 (dez valores) na componente prática. A prova escrita é composta por uma frequência ou exame escrito sem consulta.

Bibliografia:

Stallings Willian, "Network Security Essentials, Prentice Hall, 2000.



INSTITUTO POLITÉCNICO DE TOMAR
Escola Superior de Tecnologia de Tomar

Departamento de Engenharia Informática

Curso de Engenharia Informática

Stallings William, "Cryptography and Network Security: Principles and Practice",
Prentice Hall, Second Edition, 1998.

Gast S. Mathew, "802.11 Wireless Networks", O'Reilly, 2002.

O Docente responsável.

(Luís Miguel Lopes de Oliveira)

Assistente do 2º Triénio