



DISCIPLINA DE
Telecomunicações e Redes Integradas II

4º Ano

Regime: Semestral (8º)

Ano Lectivo:2004/2005

Carga Horária:2T+3P

Docente: Luís Miguel Lopes de Oliveira

OBJECTIVOS

Aprendizagem de conceitos fundamentais sobre:

- Segurança Informática;
- Segurança em Redes;
- Segurança de Sistemas.
- Conhecer os principais mecanismos e tecnologias de segurança.
- Conhecer as principais ferramentas de segurança.
- Conhecer os aspectos relacionados com a segurança de Sistemas Informáticos.
- Capacidade de resolver problemas de segurança em Sistemas Informáticos.
- Capacidade de definição e implementação de Políticas de Segurança de organizações.
- Capacidade de realizar tarefas de monitorização e auditoria de segurança.
- Capacidade de conceber e instalar soluções de segurança em Redes Informáticas

PROGRAMA

1 . Conceitos fundamentais e terminologia.

Necessidade de proteger as redes e os sistemas informáticos.

Propriedades e serviços de segurança

Estruturação do estudo dos suportes de segurança.

2. Princípios e Fundamentos dos métodos criptográficos.

Princípios de criptografia computacional



INSTITUTO POLITÉCNICO DE TOMAR
Escola Superior de Tecnologia de Tomar

Departamento de Engenharia Informática

Curso de Engenharia Informática

Princípio de 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

Serviço de autenticação com certificação X.509

Sistemas de autenticação centralizada (Sistemas SingleSignOn).

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

Firewalls

Sistemas de detecção de intrusão (IDS).

4. Planeamento de redes Wireless 802.11.

O Protocolo 802.11

Segurança em redes Wireless 802.11.

Projecto de redes Wireless 802.11

5. Redes Seguras

Principais características.

Planeamento de redes seguras.

Protocolos usados nas redes seguras.

Métodos de Avaliação:

A avaliação é composta por dois trabalhos com o peso total de 40% e uma frequência ou exame individual com o peso de 60%.

Avaliação prática:

Os trabalhos práticos 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:



INSTITUTO POLITÉCNICO DE TOMAR
Escola Superior de Tecnologia de Tomar

Departamento de Engenharia Informática

Curso de Engenharia Informática

Só são admitidos à prova escrita os alunos que tenham obtido 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.

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