Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística

Plano de Ensino

1) Identificação

Disciplina: INE5680 - Segurança da Informação e de Redes
Turma(s): 08238A, 08238B
Carga horária: 72 horas-aula Teóricas: 40 Práticas: 32
Período: 1º semestre de 2012

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- INE5625 - Computação Distribuída

4) Ementa

Introdução à Segurança. Conceitos básicos. Técnicas clássicas de criptografia. Criptografia Simétrica. Acordo de chave de Diffie-Hellman. Criptografia de Chave Pública. Gerenciamento de chaves públicas. Funções Hash. Assinaturas Digitais. Certificação Digital. Protocolos de Autenticação. Protocolos Criptográficos. Segurança de aplicações. Redes Privadas Virtuais. Tecnologias disponíveis para defesa. Gestão da Segurança da Informação.

5) Objetivos

Geral: Introduzir a área de segurança computacional, com relação as suas subáreas de: segurança da informação, segurança de redes, segurança de sistemas e segurança de aplicações.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos e protocolos criptográficos.
- Empregar ferramentas que servem de suporte à segurança computacional.
- Conhecer os fundamentos para Gestão de Segurança da Informação.
- Escrever artigo para desenvolver a linguagem escrita.
- Apresentar oralmente trabalho sobre tem escolhido.

6) Conteúdo Programático

6.1) Introdução à Segurança Computacional [2 horas-aula]
6.2) Conceitos básicos e técnicas clássicas de criptografia [2 horas-aula]
6.3) Criptografia Simétrica [4 horas-aula]
6.4) Gerenciamento de chaves simétricas [2 horas-aula]
6.5) Acordo Diffie-Hellman, Criptografia e Gerenciamento de Chave Pública [6 horas-aula]
6.6) Funções Hash, Assinatura Digitais [6 horas-aula]
6.7) Infraestrutura de Chaves Públicas e Certificação Digital [6 horas-aula]
6.8) Protocolos criptográficos [6 horas-aula]
6.9) Segurança de Aplicações [4 horas-aula]
6.10) Redes Privadas Virtuais [4 horas-aula]
6.11) Vulnerabilidades, Ameaças e Anatomia e Tipos de Ataques [2 horas-aula]
6.12) Políticas de Segurança [1 horas-aula]
6.13) Protocolos de autenticação, Segurança de acesso remoto [3 horas-aula]
6.14) Tecnologias disponíveis para defesa [6 horas-aula]
6.15) Conectando-se à Internet com segurança [2 horas-aula]
6.16) Modelos de segurança para ambientes cooperativos [2 horas-aula]

6.17) Avaliação escrita da aprendizagem [2 horas-aula]

6.18) Apresentação de tópicos selecionados por grupos [12 horas-aula]
- Gestão de Segurança da Informação
- Segurança de Aplicações e Protocolos Criptográficos
- Ferramentas de segurança
- Outros tópicos de interesse

7) Metodologia

AT-Aula Teórica, AP-Aula Prática, TT-Tarefa Teórica, TP-Tarefa Prática, APP-Apresentação Prática.

Tarefas teóricas: AT e TT
Tarefas práticas: AP e TP
Apresentações Orais: APP

8) Avaliação

A avaliação da disciplina se dará através de tarefas teóricas (questionários sobre partes da disciplina), tarefas práticas e apresentações orais e duas provas escritas considerando-se os seguintes percentuais máximos para as tarefas:

Tarefa 1a - Teórica: Questionário introdutório
Tarefa 1b – Teórica: Ambiente cooperativo
Tarefa 2a – Teórica: Técnicas clássicas de criptografia (5%)
Tarefa 2b - Prática: Algoritmo de criptografia simétrica (5%)
Tarefa 3 - Teórica: Protocolo de autenticação usando criptografia simétrica (5%);
Tarefa 4 – Prática: Especificar e fazer a validação do protocolo de segurança da questão (3) com a ferramenta Isabelle. (10%)
Tarefa 5a – Prática: Executar e responder questionário sobre uma ferramenta scanner de portas. (5%)
Tarefa 5b – Prática: Executar e responder questionário sobre uma ferramenta scanner de vulnerabilidades. (5%)
Tarefa 6 - Teórica : Criptografia baseada em senha (5%)
Tarefa 7 - Prática: GnuPG e a segurança de emails (5%);
Prova 1
Tarefa 8a - Teórica: Questionário Criptografia de Chave Pública (5%)
Tarefa 8b – Teórica: Questionário Funções Hash e Assinaturas (5%)
Tarefa 8c – Teórica: Acordo de Chave Diffie-Hellman (5%)
Tarefa 9 - Teórica: Funções Criptográficas de Hash, Código de Autenticação de Mensagens Baseado em Hash e Assinatura Digital (5%)
Tarefa 10 - Prática: Configurar a segurança de servidor web com certificação de
cliente e servidor. (10%)
Tarefa 11 - Prática: Montar uma rede privada virtual (VPN) (5%)
Prova 2
Tarefa 12 - Prática: Avaliação de uma ferramenta de segurança escolhida pelo aluno (5%);
Tarefa 13 - Teórica: Apresentação Oral de Tópicos Selecionados (15%);

Média das Provas MP: MP = (Prova 1 + Prova 2)/2 ;
Média das Tarefas (teóricas e práticas) MT:
MT = %T1 + %T2 + ... + %T(n-1)+ %Tn ; varia de 0%=0.00 à 100%=10.00

Média Final MF para aprovação:
MF = (MT + MP)/2; sendo que cada uma das médias deve ser maior ou igual a 6.0. Caso contrário, a média final MF será igual ao
valor mais baixo entre a média das tarefas teóricas e práticas e a média das provas.

Conforme parágrafo 2º do artigo 70 da Resolução 17/CUn/97, o aluno com frequência suficiente (FS) e média final no período (**MF**) entre 3,0 e 5,5 terá direito a uma nova avaliação ao final do semestre (**REC**), sendo a nota final (**NF**) calculada conforme parágrafo 3º do artigo 71 desta resolução, ou seja: **NF = (MF + REC) / 2**.

9) Cronograma

9/3 Introdução à Segurança Computacional (2), Conceitos básicos e técnicas clássicas de criptografia (2).
16/3 Vulnerabilidades, Ameaças e Anatomia e Tipos de Ataques (2), Criptografia Simétrica (2).
30/3 Scanner de Portas (2), Gerenciamento de chaves simétricas (2).
13/4 Scanner de Vulnerabilidades (2), Acordo Diffie-Hellman (1), Criptografia e Gerenciamento de Chave

Pública (1).
20/4 Protocolos de autenticação (2), Criptografia e Gerenciamento de Chave Pública (2).
27/4 Políticas de Segurança (2), Funções Hash (1), Assinaturas Digitais (1).
4/5 Segurança de emails (GnuPG) (2), Assinaturas Digitais (2).
11/5 Prova 1 (4).
18/5 Firewall, IDS, Conectando-se à Internet, Modelos de segurança para ambientes cooperativos (2), Infraestrutura de Chaves Públicas e Certificação Digital (2).
25/5 Segurança de servidor (2), Infraestrutura de Chaves Públicas e Certificação Digital (2).
1/6 Redes Privadas Virtuais (2), Protocolos Criptográficos (2)
15/6 Apresentação de Oral de Tópicos (2), Protocolos Criptográficos (2)
22/6 Apresentação de Oral de Tópicos (2), Protocolos Criptográficos (2)
29/6 Apresentação de Oral de Tópicos (2), Prova 2 (2)
06/7 Apresentação de Oral de Tópicos (2).

10) Bibliografia Básica

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Pearson.
- Segurança de Redes, Emílio T. Nakamura e Paulo L. de Geus, 4 Edição, Futura.
- Segurança de Dados, Routo Terada, 2 Edição, Editora Blucher, 2008.

11) Bibliografia Complementar

- Segurança e Auditoria em Sistemas de Informação, M. R. Lyra, C. Moderna.
- A Nova Escola de Segurança da Informação, A. Shostack et al. Alta Books.
- Redes de Computadores, Tanenbaum e Wetherall, 5 Edição, Pearson.
- Analysing Computer Security, H. Pfleeger e S. Pfleeger, Prent. Hall, 2012.
- Formal Correctness of Security Protocols, G. Bella, Springer, 2010.