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): 07238
Carga horária: 72 horas-aula Teóricas: 44 Práticas: 28
Período: 1º semestre de 2019

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- Sistemas de Informação (238) (currículo: 20001)
  - INE5625 - Computação Distribuída
- Sistemas de Informação (238) (currículo: 20111)
  - INE5615 - Redes de Computadores
  - INE5645 - Programação Paralela e 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: Apresentar os principais desafios, abordagens e técnicas para implementar, desenvolver e manter a segurança da informação nos sistemas e redes.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Conhecer os fundamentos para gestão de segurança da informação.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos de criptografia.
- Especificar protocolos criptográficos básicos.
- Empregar ferramentas que servem de suporte à segurança computacional.

6) Conteúdo Programático

6.1) Introdução [4 horas-aula]
- Conceitos Básicos
  - Propriedades Fundamentais
  - Vulnerabilidades, Ameaças, Riscos, Ataques
- Segurança nas Organizações
  - Políticas de Segurança
  - Normas de Segurança

6.2) Criptografia Simétrica [8 horas-aula]
- Princípios básicos
- Algoritmos de Fluxo
- Algoritmos de Bloco
  - Modos de Operação

6.3) Funções Hash, MAC, Criptografia Autenticada, Derivação de Chaves [6 horas-aula]
- Hash sem chave
- Hash com chave (MAC - Message Authentication Code)
  - Tipos de MAC
- Criptografia Autenticada
  - Modos e Padrões de Criptografia Autenticada

- Derivação de chaves

6.4) Criptografia Assimétrica [10 horas-aula]
- Princípios básicos
- Certificados digitais
  - Padrão X.509
- Algoritmos assimétricos
- Assinatura Digital
- Infra-estrutura de chaves públicas

6.5) Gerenciamento e Distribuição de Chaves [4 horas-aula]
- Protocolo Diffie-Hellman
- Distribuição de Chaves usando Criptografia Simétrica
  - Kerberos
- Distribuição de Chaves usando Criptografia Assimétrica

6.6) Protocolos criptográficos [4 horas-aula]
- Princípios básicos
- Protocolos básicos
  - Protocolos de troca de chaves
  - Protocolos de autenticação
- TLS (Transport Layer Security)/SSL (Secure Socket Layer)

6.7) Autenticação [4 horas-aula]
- Princípios
- Mecanismos de autenticação
- Protocolos com criptografia simétrica
- Protocolos com criptografia assimétrica
- Gerenciamento de identidades

6.8) Segurança da Rede e de Sistemas [4 horas-aula]
- Tipos de Ataques
- Varredura de Portas e Serviços
- Análise de Vulnerabilidades em Serviços
- Segurança de Servidor Web
- Segurança de Redes Sem Fio
- Segurança de Email
- Firewall
- Redes Privadas Virtuais

6.9) Atividades práticas [28 horas-aula]

7) Metodologia

Cada um dos tópicos teóricos do conteúdo programático será abordado de forma expositiva, através de projeção de transparências, ou discussão em grupo usando textos relacionados. Estão previstas demonstrações práticas através de exemplos e exercícios desenvolvidos durante as aulas. Tarefas práticas serão resolvidas pelos alunos em laboratório e também em horários extraclasse.

8) Avaliação

Os alunos serão avaliados através dos seguintes Instrumentos de Avaliação:
-Provas – 2 provas escritas individuais; e
-Tarefas – tarefas práticas com implementação e uso de bibliotecas criptográficas, tarefas práticas sem implementação e tarefas teóricas.

Os seguintes critérios serão observados para fins de avaliação:
-compreensão dos conteúdos discutidos, participação nas atividades, responsabilidade e pontualidade;
-prazos de entrega;
-freqüência suficiente (75%).

Cálculo da NF (Nota Final):

MPR (média das provas) = Nota Prova 1 * 0,5 + Nota Prova 2 * 0,5
MT (média das tarefas) = (Média de tarefas com implementação * 0,4 + Média de tarefas práticas sem implementação * 0,4 + Média de tarefas teóricas * 0,2)
MF (Média Final)= MPR * 0,65 + MT * 0,35

São previstas de 1 a 4 tarefas com implementação, de 1 a 5 tarefas sem implementação e pelo menos 1 tarefa teórica.

Para realização de avaliações em atraso, de acordo com a RESOLUÇÃO Nº 17/CUn/97, de 30 de setembro de 1997:

Art. 70 § 4o - Ao aluno que não comparecer às avaliações ou não apresentar trabalhos no prazo estabelecido será atribuída nota 0 (zero).

Art. 74 - O aluno, que por motivo de força maior e plenamente justificado, deixar de realizar avaliações previstas no plano de ensino, deverá formalizar pedido de avaliação à Chefia do Departamento de Ensino ao qual a disciplina pertence, dentro do prazo de 3 (três) dias úteis, recebendo provisoriamente a menção I.

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

As datas previstas dos principais eventos são listadas abaixo:
-Prova 1: 03/05/2019
-Prova 2: 27/06/2019
-Prova de Recuperação: 11/07/2019

As datas de entrega das tarefas serão definidas no decorrer do semestre.

10) Bibliografia Básica

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Prentice-Hall, 2008.
- Segurança de Redes em ambientes cooperativos, Emílio T. Nakamura e Paulo L. de Geus, Novatec, 2007.
- B. Preneel, C. Paar, and J. Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer, 2009. (Disponível com IP da UFSC no link: http://link.springer.com/book/10.1007%2F978-3-642-04101-3).

11) Bibliografia Complementar

- A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, October 1996. (Disponível online: http://cacr.uwaterloo.ca/hac/index.html).
- Ivo de Carvalho Peixinho; Francisco Marmo da Fonseca; Francisco Marcelo Lima. Segurança de Redes e Sistemas. RNP/ESR, 2013. (Disponível online: http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas).
- Diversos e-books da área da disciplina.