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

Plano de Ensino

1) Identificação

Disciplina: INE5429 - Segurança em Computação
Turma(s): 07208
Carga horária: 72 horas-aula Teóricas: 72 Práticas: 0
Período: 1º semestre de 2013

2) Cursos

- Ciências da Computação (208)

3) Requisitos

- INE5403 - Fundamentos de Matemática Discreta para Computação
- INE5414 - Redes de Computadores I
- INE5415 - Teoria da Computação

4) Ementa

Segurança em aplicações: programação segura, detecção de falhas, códigos maliciosos (malware). Segurança em sistemas operacionais: princípios de controle de acesso, sistemas confiáveis. Segurança em redes de computadores: ataques e defesas. Princípios de criptografia: criptografia simétrica e assimétrica, integridade de dados. Protocolos de autenticação: princípios, infra-estrutura de chaves públicas e aplicações (X.509, OpenPGP, SPKI, IBE), protocolos criptográficos (S/Mime, IPSec, SSL, OpenSSH, Kerberos, VPNs).

5) Objetivos

Geral: Prover ao aluno conhecimentos teóricos e práticos dos princípios da criptografia, segurança em redes de computadores e segurança em computação.

Específicos:

- Prover uma visão geral da Criptografia Convencional: técnicas clássicas e modernas;
- Mostrar os conceitos básicos de Criptografia por Chave Pública e Funções em Hash;
- Descrever apectos de Segurança em redes de computadores: Assinatura Digital e Protocolos de Autenticação;
- Apresentar a Infra-estrutura de Chaves Públicas;
- Mostrar como utilizar as técnicas de criptografia e protocolos para propiciar a Segurança de Sistemas: E-mail, IP e Web seguros. Intrusos, vírus e vermes. Firewalls.

6) Conteúdo Programático

6.1) Exame detalhado da criptografia convencional e princípios de projeto, incluindo o uso desta para confidencialidade [20 horas-aula]
- Introdução a criptografia clássica e moderna
- Introdução a criptografia assimétrica e infra-estrutura de chaves públicas

6.2) Criptografia por chaves públicas [10 horas-aula]
- Teoria de Números
- Autenticação
- Funções Hash

6.3) Protocolos de Autenticação [5 horas-aula]

6.4) Assinatura Digital [5 horas-aula]

6.5) Autenticação de Aplicações [12 horas-aula]
- Kerberos
- X.509

6.6) E-mail seguro [12 horas-aula]
- PGP
- S/MIME)
- IP seguro

- Web seguro (SSL e SET)

6.7) Intrusão e programas maliciosos [4 horas-aula]

6.8) Filtros de Pacotes [4 horas-aula]

7) Metodologia

As aulas serão expositivas, intercaladas com aulas práticas em laboratório. Além disso, para cada tópico importante, será solicitado um trabalho individual ao aluno. E para o fechamento da disciplina, cada grupo de dois alunos farão um trabalho sobre um tema de segurança em computação, procurando manter o grupo e a turma cientes do estado da arte da área.

8) Avaliação

Serão feitas duas provas teóricas (P1 e P2), um conjunto de até dez trabalhos individuais cuja média simples desses formará uma terceira avaliação (TI) e um trabalho em grupo (TG). A média final será dada por MF = (P1 + P2 + TI + 2*TG) / 5.

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 aulas iniciam na terceira semana de Março de 2013 e finalizam na segunda semana de Julho. A primeira avaliação (P1) será aplicada ao final do primeiro mês de aulas. A segunda avaliação (P2) ao final do segundo mês de aulas. As datas de entrega dos trabalhos individuais e do trabalho em grupo serão acordadas com os alunos e postadas no sistema Moodle. A prova de recuperação será na segunda semana de Julho.

10) Bibliografia Básica

- Stallings, William. Cryptografhy and Network Security: Priciples and Practice. Prentice Hall, 1999.569p.

11) Bibliografia Complementar

- Tanenbaum, Andrew S. Computers Networks. 3rd. Edition, New Jersey: Prentice Hall, 1996. 813p. Cap. 7: The Application Layer, p.577-766.
- RSA Data Security, Inc. “Frequently Asked Questions about Today’s Cryptography”.1998. http://www.rsa.com
- Soares, Luiz F. G.; Lemos, Guido; Colcher, Sérgio. Redes de Computadores: Das LANs MANs e WanS às Redes ATM. 2ª Edição, Rio de Janeiro: Ed. Campus, 1995.740p. Cap.17: Segurança em Redes de Computadores, p.447-488.
- Oaks, Scotr. Segurança de dados em Java. Rio de Janeiro: Ed. Ciência Moderna, 1999. 433p.
- Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2ª Edition, New York: John Wiley & Sons, 1995. 784p.
- Smith, Richard E. Internet Cryptography. New York: Addison-Weslwy, 1997. 356p.
- Menezes, Alfred J.; Oorschot, Paul C.; Vanstone, Scott A. Handbook of Applied Cryptography. New York: CRC Press, 1996. 816p.
- Schneier, Bruce. E-mail Security: How to Keep Your Electronic Messages Private. New York: John Wiley & Sons, 1995. 384p.
- Grant, Gail L. Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks. New York: Computing McGraw-Hill, 1997. 304p.
- Feghhi, Jalal; Williams, Peter; Feghhi, Jalil. Digital Certificates: Applied Internet Security. New York: Addison-Weslwy, 1998. 453p.
- Pfleeger, Charles P. Security in Computing. New Jersey: Prentice Hall, 1996. 574p.
- Nichols, Randall K. ICSA Guide to Cryptographe. New York: McGraw Hill, 1998. 840p.
- Stinson, Douglas R. Cryptography: Theory and Practice. New York: CRC Press, 1995. 448p.