

Programa de Ensino

1) Identificação

Disciplina: INE5429 - Segurança em Computação
Carga horária: 72 horas-aula Teóricas: 36 Práticas: 36
Período: 2º semestre de 2018 até a presente data

2) Cursos

- Ciências da Computação (208)

3) Requisitos

- Ciências da Computação (208)
 - INE5403 - Fundamentos de Matemática Discreta para Computação
 - INE5414 - Redes de Computadores I

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 aspectos 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) Noções básicas de segurança [8 horas-aula]

- Visão e definições gerais
 - Autenticidade, Integridade, Disponibilidade, Irretratabilidade
- Modelos e políticas de segurança

6.2) Criptografia básica e segurança de rede [16 horas-aula]

- Introdução à criptografia e criptossistema clássico
- Aleatoriedade e pseudo-aleatoriedade
- Protocolos de autenticação e gerenciamento de chaves
- IPSec, VPNs, TLS, problemas de comércio eletrônico

- 6.3) Identidade e Certificação Digital [10 horas-aula]
 - Certificados digitais, autoridades certificadoras e de registro
 - Assinatura digital de documentos eletrônicos
 - ICP-Brasil
 - Tipos de Certificados
 - Carimbos do Tempo
 - Padrão Brasileiro de Assinatura Digital
 - Gerenciamento de Identidades
 - Federação CAFe
 - Brasil Cidadão
- 6.4) Projeto de sistemas e garantia de segurança [12 horas-aula]
 - Princípios de projeto
 - Mecanismos de segurança
 - Auditoria de sistemas
 - Análise de risco
 - Verificação e avaliação da segurança de sistemas
- 6.5) Detecção de Intrusão e Resposta a Incidentes [12 horas-aula]
 - Classificação de Ataque e Análise de Vulnerabilidade
 - Detecção, Contenção e Resposta / Recuperação de desastres
- 6.6) Aspectos Legais e Éticos [2 horas-aula]
- 6.7) Tópicos emergentes em segurança [12 horas-aula]
 - Segurança em Dispositivos Móveis
 - Blockchain e moedas eletrônicas
 - Processamento com dados Cifrados
 - Processamento com dados autenticados

7) Bibliografia Básica

- Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1999.569p.

8) 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 Cryptographie. New York: McGraw Hill, 1998. 840p.
- Stinson, Douglas R. Cryptography: Theory and Practice. New York: CRC Press, 1995. 448p.