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: 36 Práticas: 36
Período: 1º semestre de 2019

2) Cursos

- Ciências da Computação (208)

3) Requisitos

- 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) Metodologia

As aulas serão expositivas, intercaladas por aulas de laboratório, onde os alunos realizarão atividades práticas individuais ou em grupos. Algumas aulas teóricas, expositivas serão gravadas e disponibilizadas via Moodle aos alunos. Algumas aulas práticas serão feitas remotamente, mas com a entrega via Moodle de relatórios das atividade. Além disso, para cada tema relevante, será solicitado um trabalho individual, que terá uma parte teórica e outra prática a ser feita pelo aluno. Também haverá um trabalho a ser realizado em grupos de 2 ou 3 alunos sobre um tema atual de segurança em computação, procurando manter o grupo e a turma cientes do estado da arte da área.

A disciplina será acompanha pelo Estagiário de Docência Douglas Marcelin Beppler Martins, que é aluno de mestrado regularmente matriculado no PPGCC da UFSC

8) Avaliação

Serão aplicadas duas provas teóricas P1 e P2, um conjunto de até 10 trabalhos individuais cuja média forma a nota TI, e um trabalho em grupo TG. A média final será dada por MF = (P1 + P2 + TI + TG)/4. Os requisitos e critérios de avaliação dos trabalhos individuais serão postados no Moodle.

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

A primeira prova teórica será aplicada após a finalização do conteúdo de Identidade e Certificação Digital. A segunda prova após Aspectos Legais e Éticos. As datas para entregas dos trabalhos individuais e do trabalho em grupo serão postadas no Moodle. A prova de recuperação será na última semana de aula.

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.