INE5429-07208 Segurança em Computação Apresentação da Disciplina

Prof. Jean Everson Martina
Prof. Ricardo Felipe Custódio

Descrição da Disciplina

Disciplina: INE5429 - Segurança em Computação

Turma(s): 07208

Carga horária: 72 horas-aula Teóricas: 36 Práticas: 36

- Requisitos:
  - INE5403 - Fundamentos de Matemática Discreta para Computação
  - INE5414 - Redes de Computadores I

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).

Objetivo Geral

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

Objetivos 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.

Conteúdo Programático

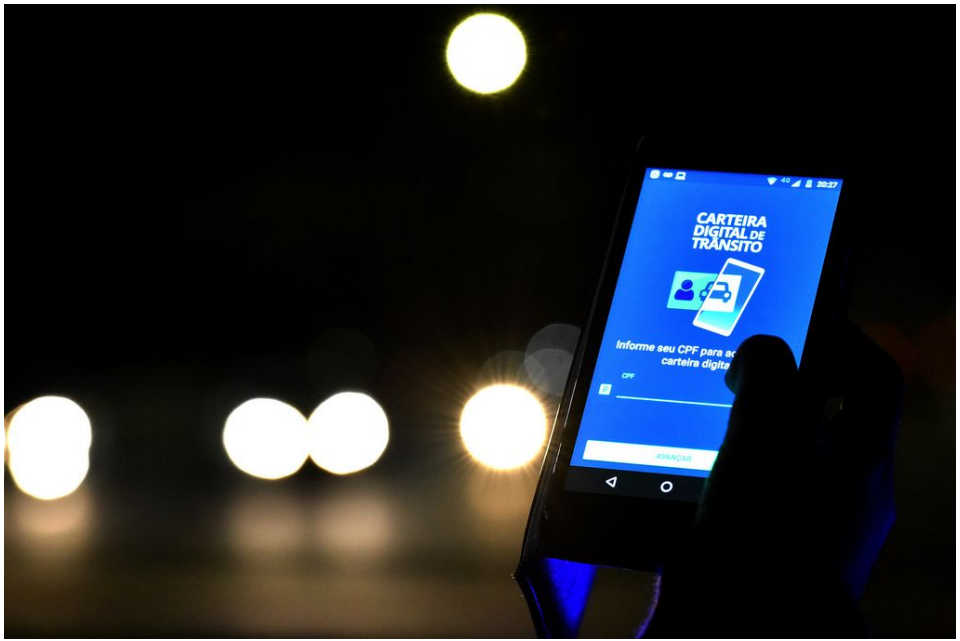
- Noções básicas de segurança [8 horas-aula]
  - Visão e definições gerais
  - Autenticidade, Integridade, Disponibilidade, Irretratabilidade
  - Modelos e políticas de segurança

Conteúdo Programático

- 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

Conteúdo Programático

- 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

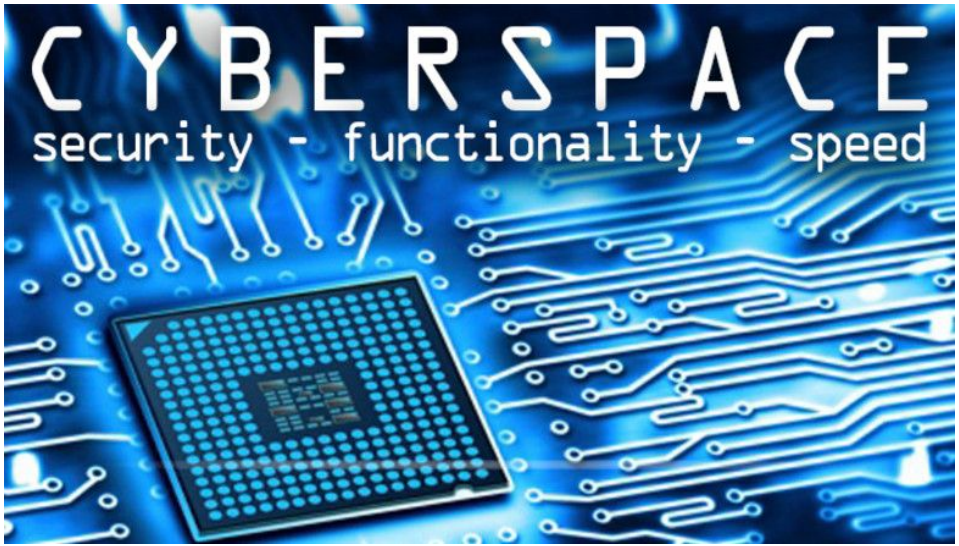


Conteúdo Programático

- 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

Conteúdo Programático

- Detecção de Intrusão e Resposta a Incidentes [12 horas-aula]
  - Classificação de Ataque e Análise de Vulnerabilidade
  - Detecção, Contenção e Resposta / Recuperação de desastres



Conteúdo Programático

- Aspectos Legais e Éticos [2 horas-aula]
- Tópicos emergentes em segurança [12 horas-aula]
  - Criptomoedas
  - Eleições Eletrônicas

Metodologia

- As aulas serão expositivas, **intercaladas** por aulas de cunho prático
- Para cada tema relevante, será solicitado um **trabalho individual**.
- Também haverá um trabalho a ser realizado em **grupos de 2 ou 3 alunos** sobre um tema atual de segurança em computação.
- A disciplina será acompanhada por um **Estagiário de Docência** que é aluno de mestrado regularmente matriculado no PPGCC da UFSC
- As **aulas intercalam entre sincronos e assincronos**, dando prioridade para o conteúdo teórico sempre de forma assíncrona.

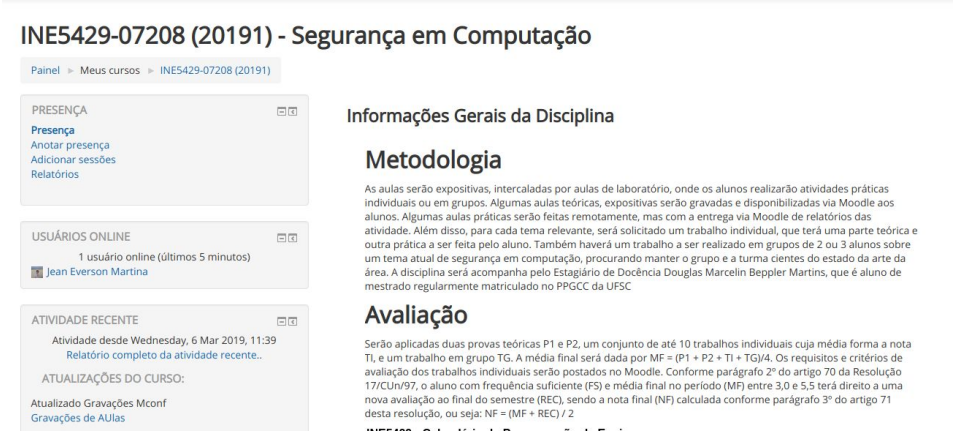
Avaliação

- Serão aplicadas **duas provas teóricas** P1 e P2.
- Um conjunto de até **5 trabalhos individuais** cuja média forma a nota TI.
- 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**.

Cronograma

- Valem as datas no Moodle
- O calendário já permite ver todas as aulas sincronas e assincronas.
- O calendário também inclui as datas das provas
- As datas de entrega dos trabalhos serão decididos durante o semestres
- As temáticas vão ser definidas durante o semestre.

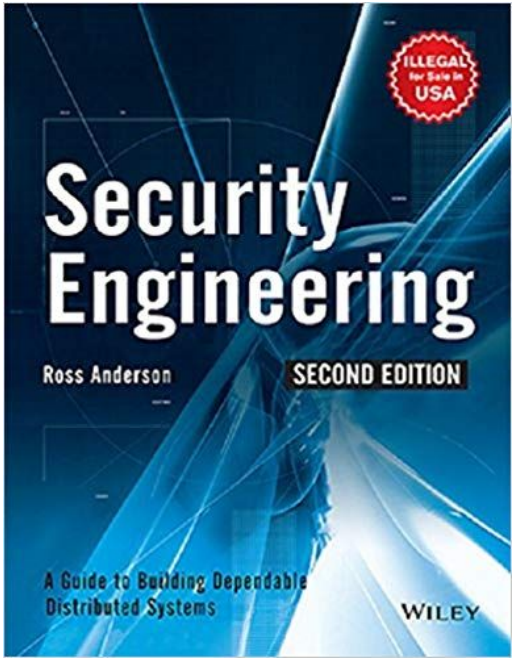
Moodle

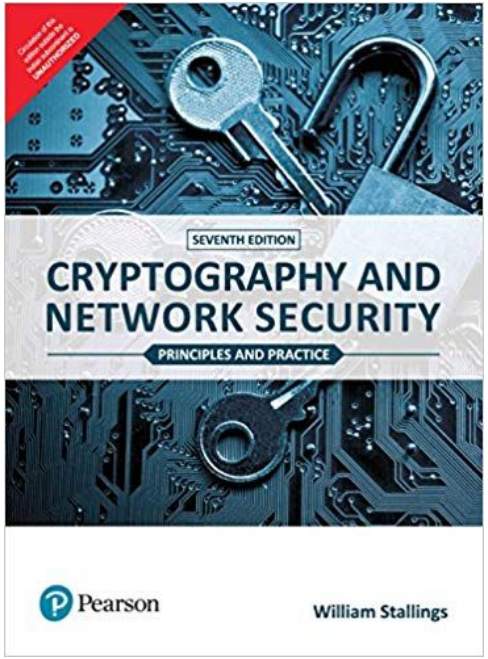


- Tem todo o planejamento dinâmico da disciplina
- Tem todo o material de apoio
- Tem as descrições dos trabalhos
- É a plataforma de acompanhamento da disciplina

Bibliografia Básica

- Stallings, William - Cryptography and Network Security: Principles and Practice, Sixth Edition
- Anderson, Ross - Security Engineering - The Book - 2nd Edition





Perguntas?

jean.martina@ufsc.br
ricardo.custodio@ufsc.br