

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

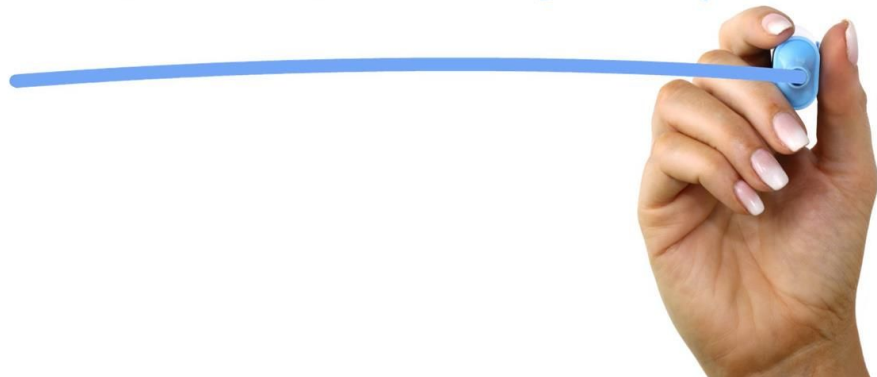


- Prover uma **visão geral da Criptografia** Convencional: técnicas clássicas e modernas;
- Mostrar os **conceitos básicos de Criptografia** por Chave Pública e Funções em Hash;
- Descrever **aspectos de Segurança em redes de computadores**: Assinatura Digital e Protocolos de Autenticação;
- Apresentar 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

COMPUTER
SECURITY



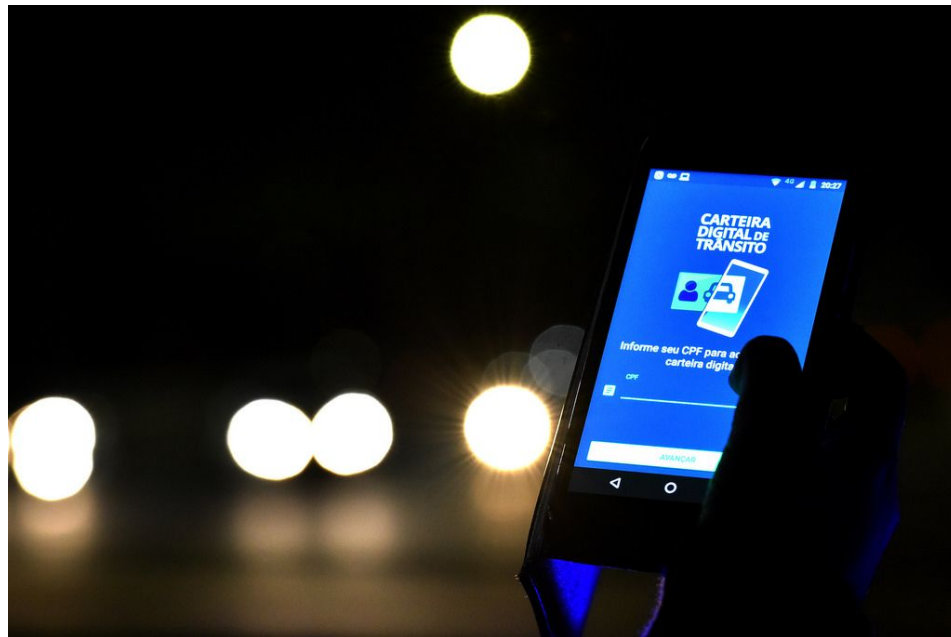
Conteúdo Programático



- 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



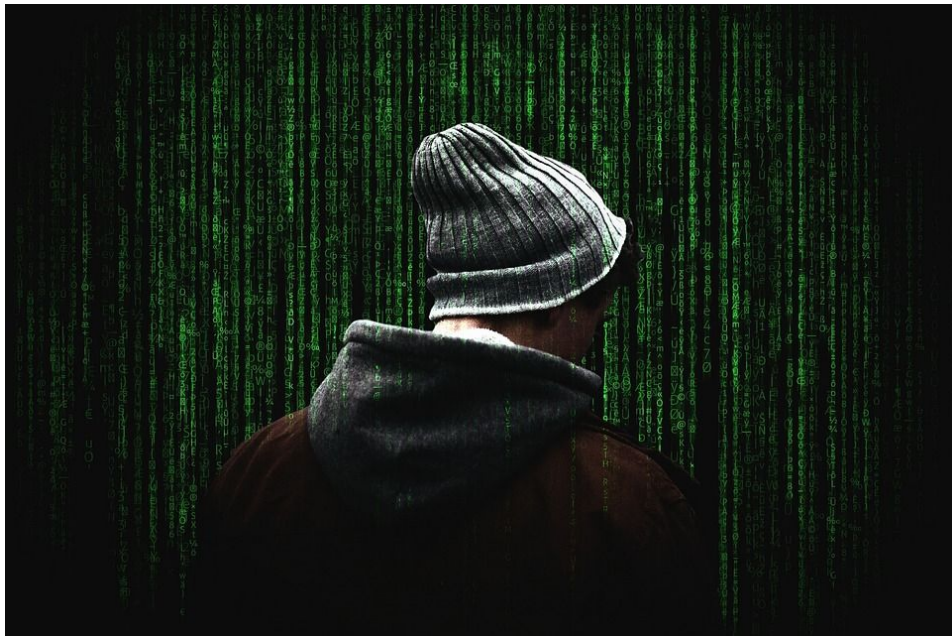
- Projeto de sistemas e garantia de segurança [12 horas-aula]
 - Princípios de projeto
 - Mecanismos de segurança
 - Auditoria de sistemas
 - Análise de risco
 - Verificação e avaliação da segurança de sistemas

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 síncronos e assíncronos**, 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 síncronas e assíncronas.
- 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

INE5429-07208 (20191) - Segurança em Computação

Painel » Meus cursos » INE5429-07208 (20191)

PRESENÇA



Presença

Anotar presença
Adicionar sessões
Relatórios

USUÁRIOS ONLINE



1 usuário online (últimos 5 minutos)

 Jean Everson Martina

ATIVIDADE RECENTE



Atividade desde Wednesday, 6 Mar 2019, 11:39
[Relatório completo da atividade recente...](#)

ATUALIZAÇÕES DO CURSO:

Atualizado Gravações Mconf
Gravações de Aulas

Informações Gerais da Disciplina

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 atividades. 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 acompanhada pelo Estagiário de Docência Douglas Marcelin Beppler Martins, que é aluno de mestrado regularmente matriculado no PPGCC da UFSC.

Avaliação

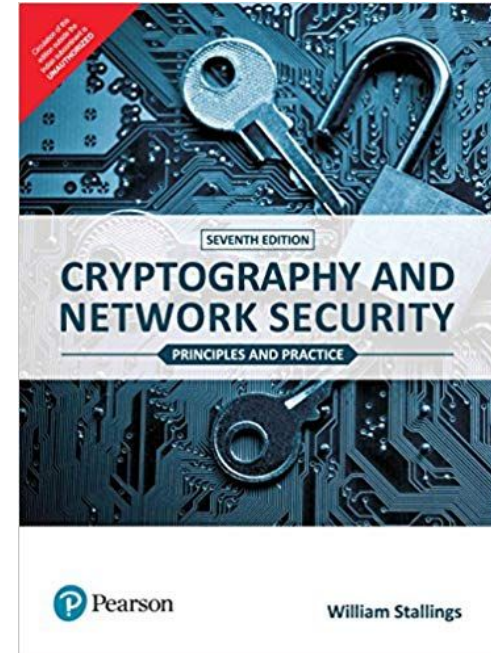
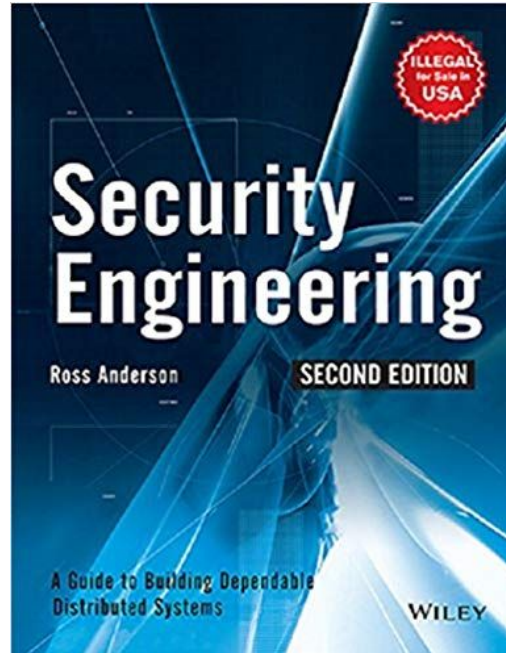
Serão aplicadas duas provas teóricas P1 e P2, um conjunto de até 10 trabalhos individuais cuja média forma a nota Ti, e um trabalho em grupo TG. A média final será dada por $MF = (P1 + P2 + Ti + TG) / 4$. Os requisitos e critérios de avaliação dos trabalhos individuais serão postados no Moodle. Conforme 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: $NF = (MF + REC) / 2$

INFORMAÇÕES GERAIS DA DISCIPLINA

- 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



QUESTIONS



Perguntas?

jean.martina@ufsc.br

ricardo.custodio@ufsc.br