CI1007: Segurança Computacional

- **Disciplina**: CI1007: Segurança Computacional
- **Carga Horária** (horas): teoria 60h, prática 00h, total 60h
- **Pré-requisito**: Sistemas Operacionais (CI215), Redes de Computadores 2 (CI061)
- **Professor**: Carlos A. Maziero

- Cronograma 2019-2
- Notas 2019-2

Objetivos

Esta disciplina visa estudar os conceitos básicos associados à segurança de sistemas computacionais, bem como as técnicas e mecanismos usados para assegurar as propriedades de segurança de um sistema.

Ementa

Conceitos básicos. Introdução à criptografia. Autenticação e controle de acesso. Segurança de sistemas e aplicações. Segurança em redes e na Internet. Auditoria. Gestão da segurança. Ética na computação. Computação e a sociedade. Politicas nacionais de segurança da informação.

Conteúdo

1. Conceitos básicos: princípios e propriedades fundamentais para segurança computacional; ameaças, vulnerabilidades e ataques; base de computação confiável;
2. Criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas;
3. Autenticação: local; em rede; distribuída;
4. Controle de acesso: políticas; modelos; mecanismos;
5. Segurança de sistemas e aplicações: ataques contra sistemas e mecanismos de defesa; segurança de sistemas; segurança em aplicações Web; desenvolvimento seguro;
6. Segurança em redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; protocolos de segurança;
7. Auditoria: logs; testes de invasão; detecção de intrusão; antivírus; análise de malware;
8. Gestão da segurança: normas e padrões; gerenciamento de vulnerabilidades; ética em segurança.

Metodologia

- **Teoria**: aulas expositivas, com análise e discussão dos temas abordados e textos de apoio.
- **Prática**: atividades referentes aos temas abordados nas aulas teóricas (regras das atividades de laboratório).

Textos e slides

Este material possivelmente será completado e transformado em livro-texto, um dia…

Capítulo	Texto	Slides
1: Conceitos básicos	seg-texto-01.pdf	seg-slides-01.pdf
2: Criptografia simétrica	seg-texto-02.pdf	seg-slides-02.pdf
3: Criptografia assimétrica	seg-texto-03.pdf	seg-slides-03.pdf
4: Assinaturas e certificados	seg-texto-04.pdf	seg-slides-04.pdf
5: Autenticação	seg-texto-05.pdf	seg-slides-05.pdf
6: Modelos de controle de acesso	seg-texto-06.pdf	seg-slides-06.pdf
7: Mecanismos de controle de acesso	seg-texto-07.pdf	seg-slides-07.pdf
8: Princípios de auditoria	seg-texto-08.pdf	seg-slides-08.pdf
a completar ...		

Avaliação

A média final da disciplina é composta pelas médias das provas e do conjunto de trabalhos desenvolvidos em cada bimestre:

```
M = (P1 + P2 + T1 + T2) / 4

P1: prova do 1º bimestre (parcial)
P2: prova do 2º bimestre (parcial)
T1: média dos trabalhos do 1º bimestre
T2: média dos trabalhos do 2º bimestre
```

Bibliografia

Básica:

- Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2a. edição. Wiley Publishing, 2008 (disponível online).
- Willian Stallings. *Criptografia e segurança de redes: princípios e práticas*, 6a. edição. Pearson, 2015.
- Emilio Nakamura e Paulo Lício de Geus. *Segurança de redes em ambientes cooperativos*. Novatec, 2010.

Complementar:

- Michael T. Goodrich e Roberto Tamassia. *Introdução à Segurança de Computadores*. Bookman, 2013.
- David Kim e Michael G. Solomon. *Fundamentos de segurança de sistemas de informação*. LTC, 2014.
- Mark Stamp e N. J. Hoboken. *Information Security: Principles and Practice*. Wiley-Interscience, 2006.
- Matt Bishop. *Computer Security: Art and Science*. Addison-Wesley Professional, 2005.
- A. Menezes, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001.

Outros recursos:

- Sites interessantes em segurança de sistemas
- Projeto SEED

Podem ocorrer mudanças nesta página, com a devida divulgação prévia aos alunos.

From:
https://wiki.inf.ufpr.br/maziero/ - **Prof. Carlos Maziero**

Permanent link:
https://wiki.inf.ufpr.br/maziero/doku.php?id=sc:start

Last update: **2020/07/08 15:44**