

CI301 - Cronograma 2017/1

Local das aulas: Sala CT-03



- As atividades indicadas com  serão avaliadas;
- Os projetos devem ser entregues usando o [Moodle](#).
- Leia com atenção as [Regras das Atividades de Laboratório](#).

21/2: Aula 1

- Apresentação da disciplina
- Conceitos básicos
- **Leitura complementar:**
 - [Computer security](#), C. Landwehr, 2001.
 - [Basic Concepts and Taxonomy of Dependable and Secure Computing](#). A. Avizienis et al, 2004.
 - [A Review of Information Security Principles](#), 1997

23/2: Aula 2

- Conceitos básicos (cont.)
- Sorteio de temas de [Aspectos de Governança da Segurança](#)
-  **Atividade 1:** [Base de Vulnerabilidades](#) (prazo: aula 4)

2/3: Aula 3

- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- **Leitura complementar:**
 - [Algoritmo de troca de chaves de Diffie-Hellman](#)
 - Vídeo: [Diffie-Hellman Key exchange \(a\)](#)
 - Vídeo: [Diffie-Hellman Key exchange \(b\)](#)
 - [How RSA Works with Examples](#)
 - Vídeo: [Public Key Cryptography: RSA Encryption Algorithm](#)
 - Vídeo: [How RSA works](#)
 - Vídeo: [Elliptic Curves Cryptography](#)

7/3: Aula 4

- **Atividade 2:** [cifradores simétricos](#)

9/3: Aula 5

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.

14/3: Aula 6

- Criptografia: (cont)
- Autenticação: usuários e grupos; técnicas de autenticação; senhas;
-  **Atividade 3: Certificados digitais** (prazo: aula 10)
- **Leitura complementar:**
 - [Modelos de criptografia de chave pública alternativos](#). Goya et al, minicurso do SBSeg 2009.

16/3: Aula 7

- Autenticação: senhas; senhas descartáveis; desafio/resposta; certificados de autenticação.
-  **Atividade 4: Quebra de senhas** (prazo: aula 12)
- **Leitura complementar:**
 - [The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes](#), IEEE Symposium on Security and Privacy, 2012.
 - [Of passwords and people: measuring the effect of password-composition policies](#), Komanduri et al, 2011.

21/3: Aula 8

- Autenticação: técnicas biométricas
- **Leitura complementar:**
 - [Introdução à Biometria](#). Costa et al, SBSeg 2006.
-  **Atividade 5: Questionário sobre biometria** (entrega em 24h)

23/3: Aula 9

- Autenticação: Kerberos; infraestruturas de autenticação local.
- **Atividade 6: autenticação SSH por certificados**
-  **Atividade 7:** Experimento [PAM Authentication](#) do [SEED Project](#) (texto de apoio: [PAM system administrator's Guide](#)) (prazo: aula 15)
- Sortear apresentações da atividade 8

28/3: Aula 10

-  **Atividade 8:** seminários sobre [Tópicos em autenticação](#)

30/3: Aula 11

- **Atividade 8** (cont.)
- **Leitura complementar:**
 - [Gerenciamento de Identidades Federadas](#). Wangham et al, SBSeg 2010.

4/4: sem aula**6/4: Aula 12**

-  **Atividade 9:** seminários sobre [Aspectos de Governança da Segurança](#) (entrega até aula 13)

11/4: Aula 13

- **Atividade 9** (cont.)

13/4: sem aula**18/4: Aula 14**

- **Atividade 9** (cont.)

20/4: Aula 15

-  **Prova 1** (conteúdo do bimestre)

25/4: Aula 16

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias.
- **Atividade 10:** Experimento [Same-Origin Policy](#) do [SEED Project](#) (leia com **muita atenção** a seção 3 do documento), (prazo: aula 19)
- Sorteio das [demonstrações de ataques](#) (grupos de 3 alunos de graduação, 1 de pós-graduação)

27/4: Aula 17

- Controle de acesso: políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis; políticas baseadas em atributos.
- **Leitura complementar:**
 - RBAC: [Role-Based Access Controls](#), 1992; [Role-Based Access Control Models](#), 1996.
 - ABAC: [Guide to Attribute Based Access Control \(ABAC\) Definition and Considerations](#), 2014.
 - UCON: [The UCONabc usage control model](#), 2004.
-  **Atividade 11** (alunos do *stricto sensu*): resumo sobre modelos de controle de acesso: Clark-Wilson, Brewer-Nash (*Chinese wall*), Graham-Denning (Harrison-Ruzzo-Ullman), Take-Grant, Low Watermark, Lipner Integrity, [Object capabilities](#), com 2 páginas no formato IEEE 2 colunas (prazo: aula 23)

2/5: Aula 18

- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows; mudança de privilégios.
- Credenciais de processo em UNIX: [credentials.c](#)

- Sorteio dos temas da atividade 15 (3 alunos por grupo)

4/5: Aula 19



- **Atividade 12:** Experimento [Set-UID Program Vulnerability](#) do [SEED Project](#) (prazo: aula 22)

9/5: Aula 20

- **Atividade 13:** [Buffer overflow](#) (demo)

11/5: Aula 21



- **Atividade 14:** Experimento [Capability exploration](#) do [SEED Project](#) (prazo: aula 25)

16/5: Aula 22



- **Atividade 15:** seminários sobre [frameworks de controle de acesso](#)

18/5: Aula 23

- **Atividade 15:** cont.

23/5: Aula 24

- Sistemas de Detecção de Intrusão (palestra prof. André Grégio)
- **Leitura complementar:**
 - [NIST Guide to Intrusion Detection and Prevention Systems \(IDPS\)](#), 2007
 - [Intrusion Detection Systems: A Survey and Taxonomy](#), 2000.

25/5: Aula 25

- Auditoria: coleta de dados; análise de dados; auditoria preventiva.
- **Atividade 16:** [Explorando sistemas de logs](#)

30/5: Aula 26



- **Atividade 17:** [demonstrações de ataques](#) (**peso 2**, prazo: aula 26)

1/6: Aula 27

- Demonstrações de ataques (cont.)

6/6: Aula 28

- Demonstrações de ataques (cont.)

8/6: Aula 29

- Demonstrações de ataques (cont.)

13/6: Aula 30

- **Prova 2** (conteúdo do bimestre)

4/7: exame final

- Prova sobre todo o conteúdo da matéria, incluindo conteúdos dos trabalhos/projetos propostos e leituras recomendadas ao longo do semestre.

From:

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

Permanent link:

https://wiki.inf.ufpr.br/maziero/doku.php?id=sc:cronograma_2017-1

Last update: **2017/06/02 23:10**

