2025/11/06 13:39 1/3 Cronograma 2013

# Cronograma 2013

Aulas: segundas-feiras 18:40 a 22:10, sala B-204

Calendário (podem ocorrer mudanças, com a devida divulgação prévia aos alunos):

Da	ta	3/6	10/6	17/6	24/6	1/7	8/7	5/8	12/8	19/8	26/8	2/9
Au	la	Aula 1	Aula 2	Aula 3	Aula 4	Aula 5	Aula 6	Aula 7	Aula 8	Aula 9	Aula 10	Aula 11

#### Aula 1

- Introdução à disciplina; conceitos básicos; infraestrutura de segurança.
- Análise de artigo 1: A Review of Information Security Principles: escrever uma análise do artigo e indicar quais seriam os 5 princípios mais relevantes dentre os apresentados pelo autor, justificando-os.
- **Leitura**: Computer security. Carl E. Landwehr, Intl Journal on Information Security Vol. 1, No. 1, pp. 3-13, July, 2001.

#### Aula 2

- Discussão sobre a última análise de artigo.
- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- Atividade 1: Explicar passo-a-passo os algoritmos de criptografia RSA (assimétrico, bloco), DES (simétrico, bloco) e RC4 (simétrico, fluxo), apresentando um exemplo didático.

#### Aula 3

- Discussão sobre a última atividade.
- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.
- Atividade 2: certificados digitais.
- **Atividade 2'**: apresentação (15') sobre tópicos em certificação digital: X509 Attribute Certificate, Certificate Revocation List, S/MIME, PGP, SPKI/SDSI, Web of Trust, Convergence.
- Leitura: Modelos de criptografia de chave pública alternativos. Goya et al, SBSeg 2009.

### Aula 4

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis; técnicas biométricas.
- Análise de artigo 2: Of passwords and people: measuring the effect of password-composition policies, Komanduri et al, 2011.
- Leitura: Introdução à Biometria. Costa et al, SBSeg 2006.

# Aula 5

Autenticação: desafio/resposta; certificados de autenticação; Kerberos; infraestruturas de autenticação

local.

 Atividade 3: apresentação (15') sobre infraestruturas de autenticação local: PAM, XSSO, GSSAPI, SSPI, BSD Auth, JAAS.

## Aula 6

- Atividade 4: apresentação (20') sobre protocolos de autenticação (SASL, CHAP, EAP, RADIUS, SRP) ou sobre autenticação distribuída (OpenID, CardSpace, Shibboleth, Higgins).
- Leitura: Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.

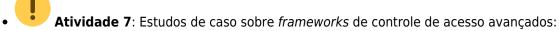
### Aula 7

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.
- Leitura: The Confused Deputy. Norm Hardy, ACM SIGOPS Operating Systems Review, 1988.
- Atividade 5: Artigo sobre modelos de controle de acesso: Clark-Wilson, Brewer-Nash (ou Chinese wall), Graham-Denning (ou Harrison-Ruzzo-Ullman), Take-Grant, Low Watermark, Lipner Integrity, Capability-based (até 2 páginas no formato IEEE).

## Aula 8

- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows; mudança de privilégios.
- Atividade 6: Experimento Set-UID Program Vulnerability do SEED Project (em grupos de 2)

### Aula 9



- AppArmor
- Capsicum
- Polkit
- SELinux
- Smack
- Trusted BSD MAC
- Windows MIC
- Windows UAC
- Leitura: Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC, R. Sandhu, 2012.

# Aula 10

- Auditoria: coleta de dados; análise de dados; auditoria preventiva.
- Atividade 8: explorando sistemas de logs
- Leitura: Anomaly-based network intrusion detection: Techniques, systems and challenges, 2010.
- Leitura: Intrusion Detection Systems, S. Axelsson, 2000.

# Aula 11



Atividade 9: Aspectos de Governança da Segurança

From:

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

Permanent link:

https://wiki.inf.ufpr.br/maziero/doku.php?id=sc:cronograma\_2013

Last update: 2014/02/11 16:36

