Cronograma 2014

 As atividades marcadas com  deverão ser entregues ao professor (PDF por e-mail), para avaliação.

Aula 1: 26/5

- 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. C. Landwehr. Intl Journal on Information Security, Vol. 1 issue 1, Jul 2001.
  - Basic Concepts and Taxonomy of Dependable and Secure Computing. A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr. IEEE Transactions on Dependable and Secure Computing, Vol. 1 issue 1, Jan 2004.

Aula 2: 2/6

- Discussão sobre a última análise de artigo.
- Criptografia: cifragem e decifragem; criptografia simétrica; criptografia assimétrica.
- Leitura complementar: Algoritmo de troca de chaves de Diffie-Helmann
-  **Atividade 1**: Explicar passo-a-passo os algoritmos de criptografia RSA (assimétrico, bloco), DES (simétrico, bloco) e RC4 (simétrico, fluxo). Podem ser usadas versões simplificadas dos algoritmos.

Aula 3: 9/6

- Discussão sobre a última atividade.
- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.
-  **Atividade 2**: certificados digitais.
- **Atividade 3**: apresentação (15') sobre tópicos em certificação digital: X509 Attribute Certificate, Certificate Revocation List, S/MIME, SPKI/SDSI, PGP, Convergence.
- **Leitura**: Modelos de criptografia de chave pública alternativos. Goya et al, SBSeg 2009.

Aula 4: 14/7

- 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: 21/7

- Autenticação: desafio/resposta; certificados de autenticação; Kerberos; infraestruturas de autenticação local.
- **Atividade 4**: apresentação (15') sobre infraestruturas de autenticação local e tópicos relacionados: PAM, XSSO, GSSAPI, SSPI, BSD Auth, JAAS, OATH (HOTP e TOTP).

Aula 6:28/7

- **Atividade 5**: apresentação (20') sobre **autenticação em rede** (SASL, CHAP, EAP, RADIUS, SRP) ou **autenticação distribuída** (OpenID, CardSpace, Shibboleth, Higgins, PGP web of trust).
- **Leitura**: Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.

Aula 7: 4/8

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias; políticas baseadas em domínios; políticas baseadas em papéis.
- **Leituras**:
  - The Confused Deputy. Norm Hardy, ACM SIGOPS Operating Systems Review, 1988.
  - Attribute-Based Access Control, NIST, 2014
  - A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC, R. Sandhu, 2012.
- **Atividade 6**: 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*, ABAC, UCON_{ABC} (até 2 páginas no formato IEEE).

Aula 8: 11/8

- Apresentação dos estudos de caso da aula anterior
- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows; mudança de privilégios.

Aula 9: 18/8

- **Atividade 7**: Experimento Set-UID Program Vulnerability do SEED Project (em grupos de 2)

Aula 10: 25/8

- **Atividade 8**: Estudos de caso sobre *frameworks* de controle de acesso avançados:
  - AppArmor
  - Capsicum
  - Polkit
  - SELinux
  - Smack
  - Trusted BSD MAC
  - Windows MIC
  - Windows UAC

Aula 11: 1/9

- Monitoração e auditoria
- **Leitura complementar**:
  - Intrustion Detection and Prevention Systems, NIST 2007.
  - Intrusion Detection Systems: A Survey and Taxonomy, Axelsson, 2000.
- **Análise de artigo 3**: The base-rate fallacy and the difficulty of intrusion detection, S. Axelsson, 2000.
- OU **Atividade 9**: Explorando Sistemas de Logs