CC51D SEGURIDAD DE DATOS

Prof. Alejandro Hevia
Semestre Primavera 2006

Requisitos: CC41B, CC42A

Contenidos:

1) Introducción a la Seguridad Computacional
   - Propiedades de seguridad, confianza
   - Ataques, vulnerabilidades
   - Por que seguridad es más difícil de lo que parece, como pensar seguridad de software

2) Criptografía
   - Cifradores clásicos, one-time pad
   - Simétrica vs. Asimétrica
   - Encriptación simétrica, funciones de hash
   - Encriptación asimétrica, firmas digitales
   - Autentificación de mensajes
   - Confianza: PKI y autoridades certificadoras
   - Aplicaciones, errores usuales (ataques) en sistemas criptográficos, otros temas

3) Seguridad de Sistemas
   - Control de Acceso: teoría y práctica
   - Mecanismos, políticas
   - Autentificación: contraseñas, biometría, de una vez, mecanismos avanzados
   - Estudio de casos y aplicaciones

4) Amenazas Actuales
   - Vulnerabilidades y ataques
   - Ataques de buffer overflow (stack smashing, errores de formato), Inyección de código (cross site scripting, SQL injection)
   - Malware: virus, gusanos, spyware, bots, phishing, Spam.
   - Ataques y defensas
   - Ingeniería social

5) Diseño de Software Seguro
   - Atacar y parchar vs. estrategias de largo plazo: principios
   - Análisis de riesgos
   - Introducción a la programación Segura
   - Confinamiento

6) Seguridad de Redes I
   - Protocolos de autentificación, negociación de claves (Diffie-Helman)

- Casos (Kerberos, Single-sign-on, autentificación web) y aplicaciones
- Infraestructura: TCP, DNS (DNSSEC), SMTP, ruteo

7) Seguridad de Redes II
- Ataques de denegación de servicios (DoS)
- Cortafuegos, gateways y topologías de redes seguras
- Sistemas de detección de intrusos (IDS)
- Sistemas del mundo real: IPSec, IKE, SSL
- Seguridad Web

8) Temas Misceláneos (según alcance el tiempo)
- Votación Electrónica
- Sistemas de Anonimato
- Sistemas anti-copia (DRM)
- Aspectos Éticos, Sociales de la privacidad de información

Sistema de evaluación:

- 2 controles + cuatro tareas.

Bibliografía:

Obligatoria:

1) "A Classical Introduction to Cryptography: Applications for Communications Security" (Hardcover)
by Serge Vaudenay
Publisher: Springer; 1 edition (September 16, 2005)
ISBN: 0387254641

2) "Cryptography and Network Security" (4th Edition)
by William Stallings
Publisher: Prentice Hall; 4 edition (November 16, 2005)
ISBN: 0131873164

3) "Building Secure Software: How to Avoid Security Problems the Right Way" (Hardcover)
by John Viega, Gary McGraw
Publisher: Addison-Wesley Professional; 1st edition (September 24, 2001)
ISBN: 020172152X

Lectura altamente recomendada:

1) "Firewalls and Internet Security: Repelling the Wily Hacker"
Second Edition (Paperback)
by William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin

Publisher: Addison-Wesley Professional; 2 editions (February 24, 2003)
ISBN: 020163466X

2) "Fundamentals of Computer Security" (Hardcover)
by Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry
Publisher: Springer; 1 edition (March 10, 2003)
ISBN: 3540431012

3) "Inside Network Perimeter Security (2nd Edition)" (Paperback)
by Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey
Publisher: Sams; 2 edition (March 4, 2005)
ISBN: 0672327376