CC-51D Seguridad de Datos

(Introducción a la Seguridad Computacional y Criptografía)

Alejandro Hevia

ahevia@dcc.uchile.cl

Carácter del curso

- Electivo para Ingeniería Civil en Computación
- Carga docente de 10 UD.
- Requisitos formales:
  - CC42A (bases de datos?)
  - CC41B (Sistemas Operativos)
- Requisitos informales:
  - Madurez matemática (algebra, probabilidades)
  - Redes
  - Sistemas Operativos
  - Software de sistemas (CC41A)

Carácter del curso

- Horario de cátedra: 1.2 – 3.2
- Horario clase auxiliar/cátedra: 5.2
  - No hay auxiliar esta semana
  - Próximas varias (3) semanas habrá cátedra en auxiliar debido a viajes en Sept (1ra sem) y Oct (2da sem)
- Hora de consulta: Jueves 11am-1pm
  - Cualquier otro horario: 95% probabilidad ocupado, bajo su propio riesgo
  - Consultas por email: > 1-2 días en responder, no esperar respuesta instantánea

Curso “Nuevo”

- No se ha dictado en varios años
- Actualizado y (esperemos) mejorado
- Distinto a CC51K
  - Distinto material y énfasis
- “Nuevo” Profesor
  - Desventajas: temario variable, curso en rodaje, harto trabajo, cero paciencia con flojera, irresponsabilidad o deshonestidad
  - Beneficios: conocimiento y motivación del profesor, aprender bien el tema (teoría, conceptos claves, nuevas tendencias y ataques, prevención, etc), temas de memoria?

Programa

- Introducción a la Seguridad Computacional
  - Propiedades de seguridad, confianza
  - Ataques, vulnerabilidades
  - Por que seguridad es más difícil de lo que parece
- Criptografía
  - Simétrica vs. Asimétrica
  - Encriptación (simétrica), funciones de hash
  - Encriptación (asimétrica), firmas digitales
  - Autentificación de mensajes
  - Confianza: PKI y autoridades certificadoras
  - Aplicaciones, otros temas

ahevia@dcc.uchile.cl

Programa

- Seguridad de Sistemas
  - Control de Acceso: teoría y practica
  - Mecanismos, políticas
  - Autentificación: contraseñas, biometría, de una vez, mecanismos avanzados
  - Estudio de casos y aplicaciones
- Amenazas Actuales
  - Vulnerabilidades y ataques
  - Ataques de buffer overflow, Inyección de código
  - Malware: virus, gusanos, spyware, bots, phishing, Spam. Ataques y defensas
  - Ingeniería social

ahevia@dcc.uchile.cl

Programa

- Seguridad de Redes I
  - Protocolos de autentificación, negociación de claves
  - Casos (Kerberos, Single-sign-on, autentificacion web) y aplicaciones
  - Infraestructura: TCP, DNS, SMTP, ruteo
- Diseño de Software Seguro
  - Atacar y parchar vs. estrategias de largo plazo: principios
  - Análisis de riesgos
  - Programación Segura
  - Confinamiento

ahevia@dcc.uchile.cl

Programa

- Seguridad de Redes II
  - Ataques de denegación de servicios (DoS)
  - Cortafuegos
  - Sistemas de detección de intrusos (IDS)
  - Sistemas del mundo real: IPSec, IKE, SSL
  - Seguridad Web
- Temas Misceláneos
  - Votación Electrónica
  - Sistemas de Anonimato
  - Sistemas anti-copia (DRM)
  - Aspectos Éticos, Sociales

ahevia@dcc.uchile.cl

Programa: Advertencia

- Programa del curso todavía “en rodaje”
  - Pudiera variar
  - Ciertos temas se verán con mayor profundidad que otros
- Sujeto en parte al interés de los estudiantes
- Espero trabajo personal
  - Lectura de material recomendado (en Inglés usualmente)

Bibliografía Curso

- "Cryptography and Network Security“, William Stallings, Editorial Prentice Hall; 4ta edición (2005)
- "Building Secure Software: How to Avoid Security Problems the Right Way“, John Viega, Gary McGraw, Editorial Addison-Wesley; 1ra edición (2001)
- "A Classical Introduction to Cryptography: Applications for Communications Security“, Serge Vaudenay, Editorial Springer; 1ra edición (2005)

Bibliografía Opcional

- "Firewalls and Internet Security: Repelling the Wily Hacker“, William R. Cheswick, Steven M. Bellovin, Ariel D. Rubin, Editorial Addison-Wesley Professional; 2da edición (2003)
- "Fundamentals of Computer Security“, Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry, Editorial Springer; 1ra edición (2003)
- "Inside Network Perimeter Security“, Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, Editorial Sams; 2da edición (2005)

Grupo docente

- Un profesor de cátedra: Alejandro Hevia
- Un profesor auxiliar (en concurso)

Contacto y noticias

- En el fichero:
  - Frente a secretaría docente
- En el grupo de noticias del curso
  - Servidor: news.dcc.uchile.cl
  - Grupo: uch.ing.cursos.cc51d
- En la página Web del curso:
  - http://ucursos.ing.uchile.cl
- Vía mail:
  - cc51d@dcc.uchile.cl
  - ahevia@dcc.uchile.cl

Revisarlo frecuentemente es responsabilidad del estudiante

Evaluación

- La evaluación se realizará mediante:
  - Control escrito (1)
  - Examen final
  - Tareas y
  - Desarrollo de un proyecto.
- Nota de controles = NC (control + examen)
- Nota de tareas = NT (tareas + proyecto).

Evaluación

- El alumno debe aprobar tanto la nota de controles (control + examen) como la nota de tareas (tareas + proyecto).

No se aceptará ninguna situación de copia u otra falta de tipo ética

Evaluación

- Un control escrito
- Un examen final
  - No hay eximición
- El examen se pondera como un control y reemplaza la nota de control si es mayor que ésta (regla a confirmar).
- Nota Controles (NC):

$$NC = (C1 + EX + EX - \min\{C1, EX\}) / 2$$

Evaluación

- Cuatro tareas
- Las fechas de entrega de las tareas y proyecto son inamovibles.
- El proyecto se puede realizar en grupos de hasta dos alumnos.
- Desarrollo de un proyecto dividido en:
  - Presentación inicial.
  - Presentación del estado de avance.
  - Entrega final.

ahevia@dcc.uchile.cl

Evaluación

- La nota del proyecto equivale a cuatro notas de tareas:

  NT = (t1 + t2 + t3 + t4 + 4*proyecto) / 8

Nota final = (NC + NT) / 2.0

ahevia@dcc.uchile.cl

Varios

- No fumar

- Teléfonos celulares apagados

ahevia@dcc.uchile.cl

Tareas

- Cuatro tareas
  - Tanto teóricas (papel y lápiz) como prácticas (programación)
  - Depende de si hay auxiliar o no
- Calendario de Tareas
  - Se comunicará el Miércoles 26 de Julio
- Política de honestidad
  - 1ra copia: NF=1, antecedentes a la Escuela
  - 2da copia: NO hay (con probabilidad 1)

ahevia@dcc.uchile.cl

Modalidad de entrega

- Enviar las tareas a través de UCursos
- Debe incluir un archivo zip (usuario.zip) con:
  - El código fuente (archivos .java ó .C)
  - Los archivos compilados
  - Un archivo explicativo llamado LEEME.TXT
- Si teórica: sólo PDF

Modalidad de entrega

- Pueden ser enviadas hasta las 23:59 horas del día señalado para su entrega.
- No se aceptarán tareas atrasadas.

Proyecto

- Tema completamente libre
- Se publicará una lista de “temas”
  - Próximo Miércoles 26 Julio
  - http://www.dcc.uchile.cl/~ahevia/cc51d
  - No es obligación tomar uno de la lista: sea creativo!
    - Pero: Copiar software / aplicaciones existentes de la web == copia en tareas

Proyecto

- El proyecto debe contar con una página web
- Presentación de temas:
  - 9 de Agosto 2006
  - Debe entregar un informe escrito (puede ser la misma página web)
  - Incluir obligatoriamente un cronograma de actividades dividido por semanas

Proyecto

- Presentación de avance:
  - 13 de Septiembre 2006
  - Debe entregar un informe escrito (que complemente la página web)
- Presentación Final:
  - 15 Noviembre 2006
  - Debe entregar un informe escrito (que complemente la página web)

Just in case

- Aspectos Éticos del curso
  - Estudio de vulnerabilidades != invitación a atacar software
  - Política al respecto:
    Está absolutamente prohibido atacar (o intentar atacar) sistemas (computadores) que no son propiedad del estudiante mismo
    - Ilegal, NF=1, causal de expulsión
- Favor firmar documento de ética

Créditos

- El estilo de la presentación es cortesía de Patricio Inostroza