Seguridad en Sistemas de Información

Curso en Zacatenco y Tamaulipas [Q2 2013]

Luis J. Dominguez Perez

Cinvestav, Mayo 13 de 2013

"Crypto without security is useless. The reverse is also true." –@DogeMocenigo

Contenido, sección 1

Temario

Evaluación

Contenido

- Introducción a la Criptografía
- Criptografía Simétrica y Asimétrica
- PKI

- Firma electrónica
- SSL
- Virus modernos
- Votaciones electrónicas
- Dinero electrónico
- Privacidad y Seguridad

Contenido, sección 2

Temario

Evaluación

Aspectos de evaluación

- Examen: 30%
- Proyecto 1: 10%
- Proyecto 2: 15%
- Monografía/Exposición: 15%
- Proyecto 3: 30%

Proyectos de evaluación

#	Actividad	Fecha de entrega
1	SHA-3 en Magma	2013-06-24
2	Servidor de páginas y correo	2013-07-01
M	Análisis / Exposición	2013-07-08
3	Proyecto Final	2013-07-14

Ver reglas para el envío de documentos

Reglas para el envío de documentos

- Se acepta el envío de documentos solamente por correo electrónico a: ldominguez @ tamps.cinvestav.mx
- Se deberá de empaquetar en un archivo comprimido debidamente etiquetado: i.e. tarea1_nombre.zip
- Se deberá de cifrar el archivo con PGP, utilizando su clave privada, y mi clave pública. Mi clave se encuentra en: PublicLuisTamps.asc
- La hora de entrega es a la media noche del día indicado. Se restará 10% por cada día de retraso
- El plagiarismo está penado severamente. La documentación que no traiga bibliografía causa baja
- Toda tarea deberá de estar acompañada de su documentación: Programas 2-4 páginas en formato LNCS (monografías de 5 a 7 páginas). Excedente se ignorará.

Análisis/Exposición

Temas a escoger: (al 1ro de julio)

- RC4
- Biometric authentication
- WEP y WAP2
- Cloud Security
- PGP

Proyecto 3

A escoger, pida confirmación al día 1ro de julio (la falta de confirmación indica no entregado):

- Mi Solcedi
- Análisis de la seguridad de las Facturas del SAT
- Implementación de esquema de estampillas de tiempo
- Implementación de esquema de almacenamiento seguro de largo plazo
- Análisis de BitCoin, instalación de software, minado
- Diseño/Implementación de Denuncia Anónima
- Diseño/Implementación de Dinero Electrónico
- Diseño/Implementación de Votaciones Electrónicas
- Implementación de un Ataque de Diccionario

Más opciones:

- Sistema de firmado de documentos (digitalización)
- Sistema de bóveda segura
- Sistema de control de retroalimentación anónima al profesor
- Sistema de autenticación a celulares
- Sistema de acceso a documentos confidenciales
- Estudio/análisis de privacidad y seguridad en redes sociales
- Bitácora segura de acceso a internet
- Políticas de seguridad

⋮

- Propuesta de Software de Seguridad