



GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Presentación del curso





Objetivos

- Crear o modificar políticas existentes de seguridad
- Conocer los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión
- Identificar qué técnicas de prevención hay contra los ataques más frecuentes
- Entender el funcionamiento de los diferentes protocolos criptográficos que se utilizan en la actualidad
- Conocer los sistemas de autenticación más importantes, identificando sus características



GRUPO DE SEGURIDAD INFORMÁTICA

Objetivos

- Entender la seguridad informática como un conjunto de metodologías
- Analizar la seguridad de una red o sistema informático, identificando los puntos vulnerables de la misma
- Detectar e identificar los distintos tipos de amenazas contra la seguridad física y lógica de plataformas informáticas
- Establecer mecanismos de protección de software (parches de seguridad, antivirus, antitroyanos y firewalls) y del sistema de comunicaciones (sistemas de gestión de claves seguras, sistemas de seguridad en protocolos y servicios y otros protocolos de seguridad)



GRUPO DE SEGURIDAD INFORMÁTICA

Equipo Docente

- Responsable del curso

- Dr. Ing. Gustavo Betarte, Prof. Titular (GSI-InCo)

- Teórico

- Ing. Alejandro Blanco, Prof. Adjunto (GSI-InCo)
- Mag. Ing. Eduardo Cota, Prof. Adjunto (GSI-IIE)
- Mag. Ing. Felipe Zipitría, Prof. Adjunto (GSI-InCo)

- Laboratorio

- Dr. Ing. Juan Diego Campo, Prof. Adjunto (GSI-InCo)
- Ing. Rodrigo Martínez, Asistente (GSI-InCo))



GRUPO DE SEGURIDAD INFORMÁTICA

Introducción



GRUPO DE SEGURIDAD INFORMÁTICA

Conceptos y propiedades básicas

- Qué es la Ingeniería de la Seguridad?
- Áreas de aplicación
- Conceptos y Propiedades básicas
- Algunas reflexiones sobre Seguridad Informática



GRUPO DE SEGURIDAD INFORMÁTICA

Criptografía aplicada



GRUPO DE SEGURIDAD INFORMÁTICA

Definiciones y fundamentos

- Motivación
- Introducción
 - Definición de criptografía
 - Definición de criptosistema
 - Definición de criptoanálisis
 - Fundamento matemático



GRUPO DE SEGURIDAD INFORMÁTICA

Algoritmos de cifrado

- Algoritmos criptográficos
 - Simétricos
 - Asimétricos
 - Discusión de ventajas y desventajas
- Generadores de números aleatorios
- Cifrados perfectos



GRUPO DE SEGURIDAD INFORMÁTICA

PKI, Hash y Ataques

- Firmas digitales
 - Certificados
 - Public-key infrastructure (PKI)
- Funciones Hash
- Reseña y utilidad de algunos algoritmos:
 - RSA, DES, AES, DSA, RC4, SHA-1, MD5, RIPEMD-160, Whirlpool
- Ataques a criptosistemas



GRUPO DE SEGURIDAD INFORMÁTICA

Protocolos

- Niveles de seguridad ofrecida por los algoritmos
- Protocolos y estándares



GRUPO DE SEGURIDAD INFORMÁTICA

Estado del arte

- Distribución y acuerdo de claves
- Estado al día de hoy
 - Reseña de los algoritmos y estándares más utilizados
- Proyección de futuro
 - Investigación actual y temas futuros



GRUPO DE SEGURIDAD INFORMÁTICA

Laboratorio

- Laboratorio 1
 - Ataques *Man in the Middle*
 - Análisis de MD5
 - GnuPG y OpenSSL



GRUPO DE SEGURIDAD INFORMÁTICA

IAAA, Políticas y Modelos de Seguridad



GRUPO DE SEGURIDAD INFORMÁTICA

Ejes temáticos

- Identificación y Autenticación
- Políticas de seguridad y modelos de control de acceso a/flujo de la información



GRUPO DE SEGURIDAD INFORMÁTICA

Identificación y Autenticación

- Passwords
 - Conceptos básicos
 - Problemas: Ingeniería social, ingreso, registro
 - Ataques y mecanismos de protección
- Mecanismos alternativos
 - Biometría: firmas, reconocimiento de rasgo personal (facial, huella dactilar, voz, iris)
 - Tokens: Tarjetas inteligentes, i-buttons, ...



GRUPO DE SEGURIDAD INFORMÁTICA

Políticas y Modelos de Seguridad

- Tipos de Políticas de Seguridad
 - Matriz de control de acceso: ACLs, Capabilities
 - Privilegio mínimo
 - Seguridad multi-niveles
- Modelos referencia
 - Bell-LaPadula
 - Verificación de propiedades de seguridad



GRUPO DE SEGURIDAD INFORMÁTICA

Políticas y Modelos de Seguridad

- Políticas Discrecionales (DAC e IBAC)
- Políticas Mandatorias (MAC)
- Políticas de Integridad (Biba, Clark-Wilson)
- Seguridad Multilateral (Chinese Wall)
- Políticas Basadas en Roles (RBAC)



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad de Sistemas



GRUPO DE SEGURIDAD INFORMÁTICA

Ejes temáticos

- Seguridad en Windows
- Seguridad en Unix



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en Windows

- Arquitectura de Windows
 - Domains y Registry
 - Active Directory
 - Group Policies
- Implementación de Control de Acceso
 - Principals, sujetos y objetos
 - Donde y como se evalúan



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en Unix

- Implementación de control de acceso
 - Principals, sujetos y objetos en UNIX
 - DAC en sistemas UNIX
- Políticas de complejidad de passwords
- Implementaciones de “*RBAC*” en Unix
 - SUDO, projects, SeLinux



GRUPO DE SEGURIDAD INFORMÁTICA

Laboratorio

- Laboratorio 2
 - Password cracking
 - Fortalecimiento de contraseñas
 - Escalada de privilegios



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en Bases de Datos



GRUPO DE SEGURIDAD INFORMÁTICA

Ejes temáticos

- Esquemas de Seguridad en Bases de Datos
 - DAC
 - MAC
 - RBAC
- Privilegios y control
- Bases estadísticas
- Integración con el Sistema Operativo
- Privacidad



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en redes TCP/IP



GRUPO DE SEGURIDAD INFORMÁTICA

Ejes temáticos

- Introducir los distintos tipos de problema existentes en las redes TCP/IP
- Tipos de ataque comunes a las redes
- Herramientas existentes
- Estado actual de la seguridad en Internet



Problemas en las redes TCP/IP

- Se presentan problemas de seguridad en todas las capas del modelo OSI simplificado
- TCP/IP (y la mayoría de los protocolos a su alrededor) no fueron pensados teniendo en cuenta la seguridad
- Veremos problemas y soluciones o paliativos en capa de enlace, capa de red, capa de transporte, y capa de aplicación



GRUPO DE SEGURIDAD INFORMÁTICA

Ataques

- Distintos tipos de ataques de red
- DOS, DDOS
- Ataques a través del DNS
- Phishing
- Portscans y ataques a servicios vulnerables



GRUPO DE SEGURIDAD INFORMÁTICA

Herramientas comunes

- Firewall
- VPN
- IDS
- Honeypots
- Black hole routing
- Otras



GRUPO DE SEGURIDAD INFORMÁTICA

Internet hoy

- Algunos números (estadísticas de hosts infectados, botnets, etc.)
- Acciones posibles ante distintas situaciones
- Quién está detrás de una IP
- Ataques comunes. Presentación de casos



GRUPO DE SEGURIDAD INFORMÁTICA

Laboratorio

- Laboratorio 3
 - Shell reversa
 - Firewalls: aplicación
 - VPNs: armado y configuración



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en las Aplicaciones



GRUPO DE SEGURIDAD INFORMÁTICA

Errores en los programas y defensas

- Ataques al Stack
- Bugs en el formato de los strings
- Ataques de Timing
- Defensas contra estos ataques



Ejes temáticos

- Veremos que el ingreso de información a los programas es su talón de aquiles
- Errores comunes en el desarrollo de aplicaciones:
 - Mal manejo de control de acceso
 - Mala utilización de abstracciones comunes
 - Enteros, strings, etc.
- Como paliar estas situaciones



GRUPO DE SEGURIDAD INFORMÁTICA

Diseño de código seguro

- Diseño modular
- Herramientas para desarrollar código seguro
- Analizadores de código seguro



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad en Aplicaciones Web

- Autenticación
- Manejo de sesiones y problemas asociados
- Problemas actuales:
 - Cross-site Scripting (XSS)
 - Cross-site Request Forgery (CSRF)
 - Etc.



GRUPO DE SEGURIDAD INFORMÁTICA

Laboratorio

- Laboratorio 4
 - Buffer overflow
 - Experimentos de ataques a aplicaciones utilizando las herramientas WebGoat y/o HacmeBank



GRUPO DE SEGURIDAD INFORMÁTICA

Metodología, Evaluación y Bibliografía



GRUPO DE SEGURIDAD INFORMÁTICA

Metodología

- Consultas de teórico y laboratorio: se informará en el sitio EVA del curso
- Los trabajos prácticos serán presentados por los docentes encargados del laboratorio
- Se contará con capacidad de acceso y uso de la infraestructura del laboratorio de seguridad durante la totalidad del período definido para la realización de cada práctica de laboratorio
- Página del curso:
<https://eva.fing.edu.uy/course/view.php?id=399>



Evaluación

- Electiva Técnica
 - Dos pruebas parciales (25% en cada parcial y 60% en total)
 - Trabajos prácticos (grupos de hasta 2 personas) (eliminadorio)
- Posgrado
 - Requerimientos de Electiva Técnica (trabajo práctico unipersonal)
 - Elaboración, escritura y presentación de estudio del estado del arte de un área de interés a ser propuesta por el equipo docente



GRUPO DE SEGURIDAD INFORMÁTICA

Bibliografía y material de referencia

- **D. Gollman**, *Computer Security*, Wiley, 2011
- **W. Stallings**, *Cryptography and Network Security*, Prentice Hall, 2006.
- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2008
- **A. Menezes, P. van Oorschot, and S. Vanstone**, *Handbook of Applied Cryptography*, CRC Press, 1996
 - Online <http://www.cacr.math.uwaterloo.ca/hac/>
- Diapositivas del curso y material de laboratorio
- Artículos de divulgación científica y tecnológica del área