FACULTAD DE INGENIERIA
Universidad de Buenos Aires

Planificaciones

6669 - Criptografía y Seguridad Informática

Docente responsable: PAGOLA HUGO ALBERTO

OBJETIVOS

Dar el respaldo básico, y los conocimientos y las técnicas necesarias para que el alumno pueda especificar y/o desarrollar sistemas en los que los métodos criptográficos sean parte fundamental o un componente.
Concientizar al alumno de los posibles problemas de seguridad informática en los Sistemas Operativos, aplicaciones y redes TCP/IP, encarándose la problemática actual y la evolución a futuro.
Que el alumno pueda desarrollar íntegramente un proyecto especifico, a acordar con la cátedra, basándose en el conocimiento adquirido durante el curso y en búsqueda bibliográfica propia.

CONTENIDOS MÍNIMOS

-

PROGRAMA SINTÉTICO

Conceptos básicos de seguridad: Servicios y Mecanismos de Seguridad, Tipos de ataques. Técnicas básicas de Criptografía y Criptoanalisis. Criptografía clásica y Criptografía moderna.

Técnicas modernas de clave privada: Cifrado en bloque. La norma AES. Historia. Normalización. Otros cifrados bloque. Combinaciones de cifradores. Cifrados stream. Modos de Operación

Cifradores Asimétricos: Fundamentos Matemáticos, Algoritmos RSA y El Gammal
Funciones hash one-way. y de MAC

Esquemas de Seguridad: Distribución de claves Simétricas, Esquema Básico con KDC Esquema Básico sin KDC. Administración de Claves Publicas, Directorio Publico, Autoridad de Claves Publicas, Autoridad Certificante y Certificados. Generación de claves compartidas con Diffie-Hellman.

Seguridad en Sistemas operativos. Listas de Control de Acceso, Seguridad del File System, Control de Acceso, Buffer Overflow. Cuentas y su defensa. Auditoria.

Seguridad de Redes e Internet: Protocolos de Autenticación, Kerberos, Single Sign On. Infraestructura de Clave Publica PKI, Autoridad Certificante,Certificados X.509, principales campos, Cadena de Certificación, Anulación de Certificados, listas CRL. Seguridad de WWW Protocolo SSL. Seguridad en IP, IPSec, Protocolo AH y ESP, Modos Tunel y Transporte IKE, VPNs. Firewalls. Capa 7: Web Application Firewalls.

Seguridad en Empresas: Modelos y Políticas de Seguridad. Firma Digital. Administración de Identidades, Identidades y Cuentas, Directorio Corporativo, Gestión de Identidades.

Gestion del Riesgo: Magerit

Auditoría: Auditoria Interna, Auditoria Externa. De cumplimiento y Sustantivas. Evidencia. Controles.Actividades de Control. Auditoria Basada en riesgos. Auditoria de un SO, de red. SOX.

PRD: Plan de recuperacion de desastres.

PROGRAMA ANALÍTICO

1. Introducción - Encripción Convencional
1.1. Conceptos básicos de Seguridad:
1.1.1. Servicios y Mecanismos de Seguridad
1.1.2. Tipos de Ataques
1.1.3. Seguridad Computacional y Seguridad Incondicional
1.2. Técnicas básicas de Criptografía:
1.2.1. Cifradores clasicos, cesar, vigenere. Cifrado-descifrado, criptoanálisis.
1.2.2. Vernam, One time Pad
1.3 Generación de números primos. Generación de números al pseudoaleatorios. PRNG usando hash y hmac sp800-90.
1.4 Cifradores de Bloque y Cifradores Stream
2. Primitivas Criptográficas
2.1. Cifradores Asimétricos
2.1.1. Fundamentos Matemáticos.
2.1.1.1. Campos Finitos
2.1.1.2. Aritmetica Modular, Maximo Comun Divisor, Algoritmo de Euclides
2.1.1.3. Coprimos, Funcion de Euler, Conjunto de Residuos, Teorema de Euler, Inversas: Euclides Extendido.

2.1.1.4. Algoritmo Acelerado para el cálculo de Potencias.
2.1.2. RSA, El Gammal
2.2. Cifradores Simétricos
2.2.1. Fundamentos Matemáticos.
2.2.1.1. Aritmética de Polinomios Modular. Polinomios Irreductibles, Campo de Polinomios. MCD. Campos Finitos GF(2n). Polinomio del AES
2.2.1.2. Algoritmo de Multiplicación Acelerada con polinomio AES
2.2.2. AES – Rijndael: Historia, Normalización, Descripción del Algoritmo. Primitivas.
2.2.3. Modos de Operación: ECB, CBC, CFB, OFB, CTR
2.3. Funciones de Hash y MAC. HMAC
2.3.1. Funciones One-Way
2.3.2. Hash, Propiedades de las funciones de Hash, SHA
2.3.3. MAC, Requerimientos, DAA Data Authentication Algoritm
2.3.4. Ataque del Cumpleaños
3. Esquemas de Seguridad
3.1. Distribución de claves Simétricas
3.1.1. Esquema Básico con KDC
3.1.2. Esquema Básico sin KDC: Con Clave Maestra
3.2. Generación de números Pseudoaleatorios, Norma ANSI X9.17
3.3. Administración de Claves Publicas
3.3.1. Anuncio Publico y Directorio Publico
3.3.2. Autoridad de Claves Publicas
3.3.3. Autoridad Certificante y Certificados
3.4. Administración de Claves de Sesión Compartidas:
3.4.1. Distribución de claves compartidas utilizando criptografía publica
3.4.2. Generación de claves de sesión compartidas con Diffie-Hellman
3.5. Esquemas de Firma
3.6. Esquemas de Identificación
4. Seguridad de Computadores
4.1. Unix: Linux
4.1.1. Cuentas y su defensa.
4.1.2. File System, procesos
4.1.3. Seguridad en el uso de recursos: Listas de Control de Acceso.
4.1.4. Auditoria y logs
4.1.5. Apache, SSH, OpenSwan.
4.2. Auditorias y Logs,
5. Problemas, amenazas, ataques, defensa y prevención.
5.1.1. Problemas de Implementación y del protocolo TCP/IP.
5.1.2. Amenazas Pasivas:
5.1.2.1. Análisis de Trafico
5.1.3. Ataques y Códigos Maliciosos:
5.1.3.1. Desbordamiento de buffer (Buffer Overflow)
5.1.3.2. Cross Site Scripting (XSS).
5.1.3.3. Carreras: (Race Condition)
5.1.3.4. Inyección SQL
5.1.3.5. Denegación de Servicio.
5.1.3.6. Suplantación (Spofing)
5.1.4. Defensa y Prevención
5.1.4.1. Intrusion Detection Systems

6. Seguridad de Redes e Internet
6.1. Protocolos de Autenticación:
6.1.1. Kerberos, Single Sign On
6.2. Infraestructura de Clave Publica PKI
6.2.1. Autoridad Certificante
6.2.2. Certificados X.509, principales campos
6.2.3. Cadena de Certificación, Anulación de Certificados, listas CRL. OCSP.
6.2.4. Autofirad de Fechado. Sellado de Tiempo.
6.2.5. Arquitecturas de Certificacion. Certificación cruzada
6.3. Seguridad de WWW:
6.3.1. Protocolo SSL. SSL de una via. de dos vias. Terminadores SSL. SSL Pinning. HSTS.
6.4. Seguridad en IP, IPSec:
6.4.1. Protocolo AH y ESP, Modos Tunel y Transporte IKE, VPNs, IPv6

6.5. Comercio Electrónico. Gateways de Pago
6.5.1. Protocolo SET “Secure Electronic Transaction”
6.5.1.1. Firma Dual
6.5.1.2. Compra, Autorización de Pago
6.6. Seguridad en IP Firewalls:DMZ. PAT. NAT.
6.7. Capa2: VLANS. 802.1X. Asignacion dinamica de vlans.

7. Seguridad en Empresas
7.1. Modelos y Políticas de Seguridad
7.2. Firma Digital
7.2.1. Firma Básica, Firma Fechada por una TSA (Time Stamping Authority)
7.2.2. Firma Validada con consulta CRL a la Autoridad.
7.2.3. PKCS #10 solicitud de certificación. PKCS #7 sintaxis del mensaje criptográfico
7.3. Administración de Identidades
7.3.1. Identidades y Cuentas
7.3.2. Directorio Corporativo
7.3.3. Gestión de Identidades
7.4. Auditoria.
7.4.1. Interna y Externa. Sustantiva y de cumplimiento.
7.4.2. Evidencia. Controles.Actividades de Control. Auditoria Basada en riesgos.
7.4.3. Auditoria de un SO, de red. SOX.
7.5. PRD: Plan de recuperacion de desastres.

8. Otros Temas (solo algunos cuatrimestres)
8.1. Smart Cards, Sistemas Biométricos
8.2. Intrusion Detection Systems
8.3. Seguridad del email, PGP, S/MIME
8.4. MAGERIT. Análisis de Riesgo.
8.5. Aspectos Legales de la Seguridad Informática
8.5.1. El delito informático, tipos de delitos
8.5.2. Leyes de protección de datos personales
8.5.3 Informatica Forense

BIBLIOGRAFÍA

• William Stallings; "Cryptography and Network Security:Principles and Practice ", 7th ed; Prentice Hall, Inc; 2016, ISBN: 13: 978-0134444284.
• Stuart McClure, Joel Sambray and George Kurtz, "Hacking Exposed: Network Security Secrets and Solutions", 7th Edition, Osborne/McGraw-Hill, 2012, ISBN-13: 978-0071780285
• Antonio Villalón Huerta; "Seguridad en UNIX y redes 2da Edición, 2002
• Antonio Villalón Huerta; Administración de sistemas Unix. Apuntes en PDF (Mayo 2005).
• Manuel José Lucena Lopez, "Criptografía y Seguridad en Computadores", Julio 2006
• Simson Garfinkel and Gene Spafford; "Practical Unix and Internet Security" 2nd ed; O'Reilly & Associates, Inc. 1996.
• Douglas R. Stinson; "Cryptography - Theory and Practice", 2nd Edition, CRC Press, Inc.; 2002.

RÉGIMEN DE CURSADA

Metodología de enseñanza

Clases Teórico Practico. Introducción teórica de los temas, con practicas donde se resuelven y discuten los trabajos prácticos. Para finalizar la materia el alumno desarrolla el conocimiento adquirido en clase mediante la confección de un trabajo practico final.
Los alumnos son separados en grupos y se les asigna un trabajo practico especifico al comienzo del cuatrimestre.

Modalidad de Evaluación Parcial

La modalidad de evaluación del aprendizaje se logra mediante una evaluación parcial escrita, la cual cuenta con dos fechas de recuperación.
Existe, una evaluación final o coloquio integrador, que podrá ser rendido como máximo en 3 oportunidades.
El alumno desarrolla un trabajo práctico grupal de un tema de Seguridad a acordar con la cátedra.
La calificación definitiva será el promedio de la evaluación parcial y final aprobadas, modificándose ese promedio por la calificación obtenida en las prácticas y en el trabajo grupal.

CALENDARIO DE CLASES

Semana	Temas de teoría	Resolución de problemas	Laboratorio	Otro tipo	Fecha entrega Informe TP	Bibliografía básica
<1> 05/03 al 10/03	U1: Fundamentos de Seguridad Informática					
<2> 12/03 al 17/03	U1:Cifradores Clásicos	U1:Cifradores Clásicos				
<3> 19/03 al 24/03	U2: Clasificación Cifradores Modernos U2.1 Campos Finitos1		U4 Linux			
<4> 26/03 al 31/03	U2.1 RSA U2.2 Campos Finitos 2	U2.1 RSA, El Gammal				
<5> 02/04 al 07/04	U2.2 AES Confidencialidad con simetricos Modos de Operación	U4 Linux 2 - repaso redes	Selección de temas Grupales			
<6> 09/04 al 14/04	U2.3 Hash – MAC U3 Esquemas de Seguridad, Administración de claves Simétricas	Dieffe Hellman	Selección de temas Grupales			
<7> 16/04 al 21/04	U3 Administración de claves públicas. Dieffie Hellman		Definición de temario de temas Grupales			
<8> 23/04 al 28/04	U5 Problemas, amenazas, ataques, defensa y prevención.				Entrega TP1	
<9> 30/04 al 05/05	U6 SSO - Kerberos SET – SSL		Revision temas parcial			
<10> 07/05 al 12/05	U6 Seguridad en Redes: ipsec			PARCIAL		
<11> 14/05 al 19/05	U6 Seguridad en Redes ipsec2 U6 Infraestructura PKI			TP Tunel IPSEC		
<12> 21/05 al 26/05	Recuperatorio			TP Tunel IPSEC	Entrega TP Tunel IPSec	
<13> 28/05 al 02/06	U7 Modelos y Políticas de Seguridad. Firma Digital.			TP Autoridad Certificante Tunel SSL		

Semana	Temas de teoría	Resolución de problemas	Laboratorio	Otro tipo	Fecha entrega Informe TP	Bibliografía básica
	Administración de Identidades					
<14> 04/06 al 09/06	Auditoria				Revisión trabajos alumnos	
<15> 11/06 al 16/06	Presentación Trabajos de Alumnos				Presentación Trabajos alumnos	
<16> 18/06 al 23/06	2do Recuperatorio				Presentación Trabajos alumnos	

CALENDARIO DE EVALUACIONES

Evaluación Parcial

Oportunidad	Semana	Fecha	Hora	Aula
1º	11			
2º	13			
3º	16			
4º				