Facultad de Informática
Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA)
Grupo de Análisis, Seguridad y Sistemas (GASS)

C/ Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, España
Teléfono: 91 394 7638. Fax: 91 394 7547. Móvil: 695 196 893
E-mail: javiergv@fdi.ucm.es. URL: http://gass.ucm.es

ECL LA PLATA (ARGENTINA) – FEBRERO 2011

TÍTULO: Seguridad Informática

CO-DIRECTORES:

Prof. Dr. F. Javier Díaz
Profesor Titular de la Facultad de Informática
Decano de la Facultad de Informática
Director del Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI)
Teléfonos: (54) 221 - 4257240
(54) 221 - 4236609 int. 115
Móvil: (54) (9) 11 - 44168062
E-mail: jdiaz@unlp.edu.ar
Página web: www.linti.unlp.edu.ar

Prof. Dr. Luis Javier García Villalba
Profesor Contratado Doctor del Departamento de Ingeniería del Software e Inteligencia Artificial de la Facultad de Informática
Director del Grupo de Análisis, Seguridad y Sistemas (GASS), Grupo de Investigación 910623 de la Universidad Complutense de Madrid
Teléfonos: 91 394 76 38
695 19 68 93
Fax: 91 394 75 47
E-mail: javiergv@fdi.ucm.es
Página web: http://gass.ucm.es

FUNDAMENTACIÓN: En un mundo en el que la intimidad se ve amenazada, cada vez se hace más necesario mantenerse por delante de hackers, crackers, intrusos y personas interesa-das en violar nuestra intimidad.

OBJETIVOS: El objetivo es el de formar especialistas en los métodos de protección de la información y seguridad de las comunicaciones, con especial atención en la configuración y administración de sistemas y redes informáticas seguras y en la gestión segura de la información.

PROGRAMA:

1. Introducción y Motivación

1.1. Seguridad Informática
1.2. Seguridad Física
1.3. Seguridad Lógica
1.4. Premisas Básicas de Seguridad
1.5. Principios Universales de la Seguridad
1.6. El ciclo de vida de la seguridad
1.7. Políticas y Mecanismos de Seguridad Informática

2. Fundamentos de Seguridad Lógica

2.1. Marco conceptual: Riesgos, Amenazas y Ataques
2.2. Modelo de confianza
2.2. TCB
2.3. Modelos de Control de Acceso: CL, ACL, ACM
2.4. Modelos de Confidencialidad: Bell-La Padula
2.5. Modelos de Integridad: Biba
2.6. Clasificación de Información
2.7. Seguridad Multinivel (MLS)

3. Criptografía

3.1. Criptografía Clásica o Simétrica. Cifrador en Bloque. Cifrador de Flujo

3.2. Criptografía de Clave Pública o Asimétrica

3.3. Mecanismos de Autenticación de Mensajes. Funciones Hash

3.4. Firma Digital

3.5. Certificados Digitales (X.509, PKCS)

3.6. Autoridades de Certificación

3.7. PGP

4. Taxonomía de Ataques

4.1. DoS, DDoS

4.2. Intrusiones

4.3. MITM

4.4. BoF

4.5. Malware (virus, gusanos, troyanos)

4.6. Spyware

4.7. Phishing y Pharming

4.8. Hoaxes

4.9. SQL Injection

4.10. Cross Site Scripting

4.11. CSRF

4.12. Spoofing

4.13. SPAM

4.14. Esteganografía

4.15. Canales Encubiertos

4.16. Ingeniería Social

4.17. El Factor Humano en la Seguridad: CAPTCHAs ó Human Interactive Proofs (HIPs)

5. Infraestructura de Defensa

5.1. Modelos de Seguridad

5.2. Cortafuegos

5.3. Sistemas de Detección de Intrusos

5.4. Sistemas de Prevención de Intrusos

5.5. Antivirus

5.6. Filtros Antispam

5.7. Honeypots

5.8. Identificación Biométrica

5.9. VPNs

5.10. CERTs

6. Seguridad en Sistemas Operativos

6.1. Control de Acceso: DAC, MAC, RBAC, MLS

6.2. Control Criptográfico de alteración de ficheros

6.3. Confinamiento de Procesos y Demonios

6.4. Seguridad en Entornos MS Windows

6.5. Seguridad en Entornos *nix

METODOLOGÍA: La metodología combinará tanto la docencia teórica como la práctica a través de las ponencias y las actividades complementarias que se han programado. A los alumnos se les proporcionarán los materiales correspondientes a cada sesión; con un resumen de cada ponencia que incluirá una bibliografía básica, así como documentación de cada una de las actividades complementarias. De esta manera el alumno podrá adquirir habilidades prácticas y obtendrá una ilustración inmediata de los contenidos teórico-prácticos, mediante la comprobación interactiva.

ACTIVIDADES PRÁCTICAS: Se realizarán ejercicios de ataque y defensa de servidor WWW + BD. Habrá prácticas de firma digital y cifrado con PGP, Certificación con OpenSSL, Sniffers de Red, Configuración de IPTables, Ataques DoS, etc.

DURACIÓN: 50 horas más 10 de proyecto que los alumnos tendrán que presentar unos días antes de la finalización del curso.

PROCEDIMIENTO DE EVALUACIÓN: Al inicio del curso se asignará una actividad al alumno para que la entregue al final. La calificación se compondrá de la evaluación de esta actividad así como de un examen al término del curso. Ambos aspectos tendrán un peso del 50% de la nota final.

PERFIL DEL ALUMNO: Este curso está dirigido a las personas que tengan la responsabilidad de implementar, diseñar, administrar o gestionar entornos y sistemas informáticos y redes de comunicaciones (administradores de sistemas y redes, personal encargado de sistemas de seguridad, responsables de sistemas de gestión de información y administradores y personal encargado de la edición de páginas Web). También está dirigido a estudiantes de últimos cursos que deseen profundizar sus conocimientos en el Área de la Seguridad Informática. No es necesario poseer conocimientos avanzados sobre tecnologías de seguridad. Basta con estar familiarizado con los servicios de Internet: correo electrónico, WWW, etc., y tener ciertos conocimientos (no excesivamente avanzados) sobre sistemas operativos y programación (C++ o Java preferentemente). El resto de materias serán tratadas de forma autocontenida a lo largo del curso. Consecuentemente, el curso está especialmente dirigido a estudiantes de últimos cursos de ciertas Ingenierías y de ciertas Licenciaturas en Ciencias tales como Matemáticas, Físicas, etc.

CRONOGRAMA:

Unidad	Profesorado	Días de Impartición									
		1	2	3	4	5	6	7	8	9	10
1. Introducción y Motivación	LJGV - UCM										
2. Fundamentos de Seguridad Lógica											
3. Criptografía	FJD – UNLP										
4. Taxonomía de Ataques	PV – UNLP										
5. Infraestructura de Defensa	NM – UNLP										
6. Seguridad en Sistemas Operativos	ALSO – UCM										

Profesorado UCM:

LJGV: Luis Javier García Villalba

ALSO: Ana Lucila Sandoval Orozco

Profesorado UNLP:

FJD: Francisco Javier Díaz

NM: Nicolás Macia

PV: Paula Venosa