FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	Nombre			
CC5312	Seguridad Computacional			
Nombre en Inglés				
Computer Security				
SCT	Unidades Docentes	Horas de Cátedra	Horas Docencia Auxiliar	Horas de Trabajo Personal
6	10	3,0	1,5	5,5
Requisitos			Carácter del Curso	
CC3201 Bases de Datos, CC4302 Sistemas Operativos			Electivo para Ingeniería Civil en Computación.	

Resultados de Aprendizaje

Al término del curso, el alumno demuestra que

- Maneja los conceptos básicos de seguridad computacional como ataques, vulnerabilidades, y seguridad de sistemas en general, y evalúa informadamente la seguridad de un sistema computacional,
- Identifica el uso correcto de algoritmos criptográficos basados en cifradores de bloque, funciones de hash y primitivas basadas en teoría de números, entre otros en cuanto a su aplicación en soluciones criptográficas para problemas de confidencialidad y autentificación en redes de computadores,
- Identifica las causas y mecanismos detrás de las vulnerabilidades de software más comunes (incluído factores humanos), manejando detalles de implementación que causan dichas vulnerabilidades. Además maneja las herramientas básicas para prevenir y mitigar dichos ataques,
- Identifica los distintos problemas de seguridad y las medidas posibles de mitigación presentes en las redes de datos y protocolos de comunicación actuales,
- Maneja los mecanismos y problemas detrás de la seguridad web y de dispositivos móviles, y diseña soluciones que mejoran la seguridad y/o los ataques en dichos sistemas, y
- Identifica y maneja conceptos y mecanismos asociados a la respuesta a incidentes, privacidad de datos , y anonimato en Internet.

Metodología Docente	Evaluación General
Clases expositivas y tareas individuales o en grupo de programación y/o teóricas.	La evaluación se basa en 3 controles y un exámen, más varias (entre 4 y 5) tareas de programación y teóricas. Se sigue la ponderación siguiente: NC= Promedio_Controles*60% + Ex*40% NT=(NT1+.... +NTn)/n NF= 0.6*NC + 0.4*NT

Unidades Temáticas

Número	Nombre de la Unidad	Duración en Semanas
1	Herramientas y Conceptos Básicos	1

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Motivación, por qué se necesita la seguridad, bugs en software y vulnerabilidades 2. Conceptos de amenazas, adversarios, y propiedades u objetivos de seguridad 3. Modelo mental de la seguridad 4. Principios básicos de la Seguridad 5. El problema de los ataques internos	Al término de la unidad, el alumno: • Identifica las motivaciones y conceptos fundamentales asociados a ataques de sistemas computacionales, y a las propiedades que se busca preservar • Identifica principios básicos de la seguridad • Identifica las causas fundamentales de la dificultad de los ataques internos	• Anderson, Cap. 1 y 2 • Stallings, Cap. 1

Número	Nombre de la Unidad	Duración en Semanas
2	Introducción a la Criptografía	3

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
6. Conceptos básicos, historia y criptografía clásica 7. Criptografía Simétrica versus Asimétrica 8. Encriptación Simétrica, Funciones de hash, Autentificación de mensajes 9. Cifradores de flujo y aleatoriedad, problemas. 10. Encriptación Asimétrica (Clave Pública), Firmas digitales 11. PKI y certificados, confianza, problemas del modelo 12. SSL/TLS, funcionamiento y ataques	Al término de la unidad, el alumno: • Identifica los conceptos básicos asociados a la criptografía tales como confidencialidad y autentificación • Maneja las distintas estrategias para proveer confidencialidad y autenticidad de datos en los casos de comunicación simétrica y asimétrica (clave pública) • Identifica mecanismos para proveer aleatoriedad y sus potenciales problemas	• Anderson, Cap. 5 • Stallings, Cap. 2,19,20,21, 22 • Vaudenay, Cap. 1,2,3,6,9,10, y 12

	• Maneja mecanismos para implementar PKI (public key infrastructure) e identifica sus principales problemas.	

Número	Nombre de la Unidad	Duración en Semanas
3	Técnicas y Herramientas de Ataque y Defensa	2,5

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
13. Vulnerabilidades y ataques 14. Ataques de secuestro del flujo del programa (Buffer Overflows, Interger overflow, injección de código, Return Oriented Programming) 15. Estrategias de protección, Sandboxing, aislamiento	Al término de la unidad, el alumno: • Identifica y discrimina errores de vulnerabilidades • Maneja los principales ataques de secuestro de flujo, siendo capaz de identificar instancias así como implementar alguno de ellos. • Maneja estrategias de protección y mitigación para estos ataques	• Anderson, Cap. 8, 21 y 23 • Stallings, Cap. 11,12

Número	Nombre de la Unidad	Duración en Semanas
4	Malware	1,5

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
16. Malware, su génesis e historia 17. Tipos de malware, causas y comportamiento 18. Estrategias de prevención de ataques de malware 19. Estrategias de detección de malware 20. El factor humano, ingeniería social	Al término de la unidad, el alumno: • Identifica los tipos de malware, sus causas, comportamiento y consecuencias • Maneja las distintas estrategias para prevenir el ataque de malware • Identifica las estrategias para detectar malware.	• Stallings, Cap. 7, 14

Número	Nombre de la Unidad	Duración en Semanas
5	Seguridad de Sistemas Operativos y Redes	4

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
21. Control de acceso, mecanismos y políticas 22. Seguridad básica de Sistemas Operativos 23. Autentificación, mecanismos básicos y avanzados 24. Seguridad de protocolos de red, TCP/IP, DNS, ruteo 25. Seguridad perimetral, cortafuegos, IDS/IPS 26. Ataques de Denegación de Servicio	Al término, el alumno: • Identifica mecanismos de control de acceso e políticas. • Identifica los principales mecanismos de seguridad de los sistemas operativos • Maneja mecanismos de autentificación • Identifica las principales fuentes de problemas de seguridad de protocolos de redes, y estrategias para su prevención y mitigación	• Stallings, Cap. 3,4,6,8,9,23, 24 • Anderson Cap. 6,8,9,20,21

Número	Nombre de la Unidad	Duración en Semanas
6	Seguridad Web y Móvil	2

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
27. Seguridad web, conceptos 28. Modelo de seguridad del cliente navegador 29. Ataques típicos: XSS, SQL Injection, secuestro de sesión, security downgrade, man-in-the-browser, y estrategias de prevención/mitigación de estos ataques 30. Conceptos de seguridad móvil y principales ataques	Al término, el alumno: • Maneja los conceptos de seguridad web, y modelos de seguridad de este caso. • Identifica los principales ataques y sus mecanismos de prevención y/o mitigación • Identifica los principales problemas y soluciones para segurizar dispositivos móviles	• Stallings, Cap. 12

Número	Nombre de la Unidad	Duración en Semanas
7	Temas Misceláneos	1

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
31. Respuesta a Incidentes, estrategias y operación 32. Threat Intelligence, y evaluación de posibles ataques 33. Privacidad y Anonimato, problemas y herramientas	Al término, el alumno: • Identifica las herramientas, procedimientos y mecanismos para proveer respuesta a incidentes, y threat intelligence • Identifica los principales desafíos en proveer confidencialidad de datos personales y maneja herramientas que permiten resolver parcialmente el problema.	• Stallings, Cap. 16,17,18 • Anderson Cap. 7, 24

Bibliografía

1. Computer Security, Principles and Practice, W. Stallings y L. Brown, 2008
2. Security Engineering, 2nd edition, Ross Anderson, 2008.

Vigencia desde:	Otoño 2016
Elaborado por:	Alejandro Hevia