



DATOS IDENTIFICATIVOS

Seguridade

Materia	Seguridade			
Código	V05G300V01543			
Titulación	Grao en Enxeñaría de Tecnoloxías de Telecomunicación			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OB	3	1c
Lingua de impartición	Castelán			
Departamento	Enxeñaría telemática			
Coordinador/a	Fernández Masaguer, Francisco			
Profesorado	Fernández Masaguer, Francisco			
Correo-e	f_masaguer@yahoo.es			
Web	http://fatic.uvigo.es			

Descrición xeral Nesta asignatura estúdanse, dun xeito unificado, os principais problemas ou ameazas de seguridade nas redes e servizos telemáticos, e preséntanse distintas técnicas para protexelos.

Primeiro abórdase o tema desde un punto de vista xeral, de forma que os conceptos, servizos e técnicas de seguridade que se estudan, sexan aplicables a calquera tipo de rede, servizo telemático ou sistema de información a securizar. Este bloque fórmano os temas 1 ao 4. Isto leva a tratar con detalle os tres temas centrais da seguridade: a parte algorítmica (cifrado, firma dixital e integridade), os protocolos de autenticación, e os procedementos de xestión e negociación de claves. O obxectivo é que o alumno adquira unha adoitada base que lle capacite para facilitar a súa comprensión das técnicas particulares que cada aplicación requira así como para aplicalo a outros ámbitos que teña que afrontar.

Logo trátase o tema dunha forma algo máis particular, revisando os problemas, técnicas e estándares de seguridade nalgúns dos entornos de comunicación de máis prevalencia na actualidade. Así dedícase un tema á seguridade a nivel IP, protocolo central na arquitectura Internet, e outro tema á seguridade na Web, dada a vixencia actual deste medio de intercomunicación telemática. Preséntanse os principais problemas de seguridade no comercio electrónico a través da Web e estúdase o funcionamento do Paypal, un dos métodos de pago máis utilizados na Web. Dada a utilización cada vez maior das comunicacións por medio inalámbrico e os seus particulares problemas de seguridade, dedícase tamén un tema a eles. Péchase o curso cunha introducción a outros dous temas de transcendencia crecente: as redes e software malicioso e o análise forense de sistemas de información.

Competencias de titulación

Código	
A3	CG3 Coñecemento de materias básicas e tecnoloxías que capaciten o alumnado para a aprendizaxe de novos métodos e tecnoloxías, así como para dotalo dunha gran versatilidade para adaptarse a novas situacións.
A4	CG4 Capacidade para resolver problemas con iniciativa, para a toma de decisións, a creatividade, e para comunicar e transmitir coñecementos, habilidades e destrezas, comprendendo a responsabilidade ética e profesional da actividade do Enxeñeiro Técnico de Telecomunicación.
A6	CG6 Facilitade para o manexo de especificacións, regulamentos e normas de obrigado cumprimento.
A37	CE28/TEL2 Capacidade para aplicar as técnicas en que se basean as redes, servizos e aplicacións telemáticas, tales como sistemas de xestión, sinalización e conmutación, encamiñamento e enrutamento, seguridade (protocolos criptográficos, tunelado, devasas, mecanismos de cobro, de autenticación e de protección de contidos), enxeñaría de tráfico (teoría de grafos, teoría de colas e teletráfico) tarificación e fiabilidade e calidade de servizo, tanto en contornas fixas, móbiles, persoais, locais ou a gran distancia, con diferentes anchos de banda, incluíndo telefonía e datos.

Competencias de materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
---------------------------------	---------------------------------------

Coñecemento dalgunhas das teorías matemáticas nas que se sustenta a seguridade dos algoritmos e protocolos criptográficos usados para a protección de redes e servizos.	A3
Coñecemento dos principios e funcionamento dos principais algoritmos de cifrado, firma dixital e hash usados como soporte dos servizos de seguridade incorporados nas redes e servizos telemáticos, sistemas de telecomunicación e sistemas de información.	A3
Coñecemento dos diferentes métodos, técnicas e protocolos de autenticación, acode-persoas, persoa-maquina, maquina-maquina.	A3
Dotar ao alumno da capacidade de analizar os problemas de seguridade dunha sistema de información, rede ou servizo telemático, avaliar os riscos asociados e de implantar as técnicas apropiadas para garantir un nivel adecuado de seguridade.	A4
Capacidade para aplicar as técnicas de seguridade en que se basean as redes, servizos e aplicacións telemáticas, tales como protocolos criptográficos, tunelado, devasas, mecanismos de cobro, de autenticación e de protección de contidos.	A37
Facilitar o manexo e coñecemento de especificacións e normativas de seguridade.	A6 A37

Contidos

Tema	
1 Fundamentos matemáticos da seguridade.	- Nocións de Teoría da Complexidade. - Revisión de Teoría de Números.
2. Algoritmos de cifrado, firma dixital e hash	- Cifrado. Principios de cifrado de Shannon. Cifrado en fluxo e cifrado en bloque. Algoritmos DES e AES. Modos de traballo dos cifradores en bloque. - Integridade e Algoritmos de Hash. - Criptosistemas de chave pública. Algoritmos de sinatura dixital: RSA, ElGamal e DSA.
3. Certificación e PKIs.	- Problemática da seguridade na criptografía asimétrica. Certificación e formatos de certificados. - Modelos de confianza. Confianza plana e modelo PGP. Confianza en terceiros e autoridades de certificación. - Infraestruturas de certificación. Ruta de Certificación. Revocación de certificados.
4. Protocolos de autenticación e convenio de clave.	- Métodos de autenticación. - Ameazas a un protocolo de autenticación. Contramedidas. - Requisitos dun protocolo de convenio de chave. Protocolo D-H. - Autenticación en criptosistemas simétricos. Casos de estudo: GSM y Kerberos. - Autenticación en criptosistemas asimétricos. Casos de estudo: autenticación X509 e SSL. - Protocolos baseados en contraseñas: SRP.
5. Seguridade no nivel de Rede	- Análise de ameazas no nivel de rede. - Arquitectura de seguridade en IP. - Protocolo IPsec. Túneles IPsec. IPsec e NAT. - Xestión de chaves. Protocolos IKE, ISAKMP e OAKLEY.
6. Seguridade na Web e comercio electrónico	- Problemas de seguridade na Web. - Protocolos SSL e TLS. - Certificación na Web. - Principios de comercio electrónico e protocolos de pago. Sistema PayPal.
7. Seguridade en comunicacións inalámbricas e protocolos AAA.	- Ameazas a seguridade en comunicacións inalámbricas. - Wireless Application Protocol (WAP). WTLS. Protocolos WEP, WPA, WPA2. - Protocolos AAA: RADIUS e DIAMETER.
8. Seguridade de Sistemas.	- Cortalumes e sistemas contra intrusiones. - Software e redes maliciosas. Botnets. - Análise Forense de Sistemas de Información.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Sesión maxistral	19	38	57
Resolución de problemas e/ou exercicios	2	0	2
Resolución de problemas e/ou exercicios de forma autónoma	0	10	10
Traballos tutelados	6	28	34
Prácticas de laboratorio	11	22	33
Probas de resposta longa, de desenvolvemento	2	10	12
Probas prácticas, de execución de tarefas reais e/ou simuladas.	1	0	1
Traballos e proxectos	1	0	1

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente	
	Descrición
Sesión maxistral	Exposición mediante presentación en powerpoint e pizarra dos contidos teóricos da asignatura. Desenvolveranse os temas teóricos da materia que non queden cubertos polas outras metodoloxías empregadas.
Resolución de problemas e/ou exercicios	Resolveranse algúns exercicios do boletín, de forma que sirvan de guía para a resolución autónoma polo alumno do resto de exercicios do boletín.
Resolución de problemas e/ou exercicios de forma autónoma	O grupo resolverá de forma autónoma os exercicios do boletín non realizados nas horas presenciais. As diversas solucións que xurdan ao abordar cada problema, serán postas en común para acordar a mellor forma de resolución. As dúbidas xurdidas acordaranse e poderán exporse ao tutor nas horas normais de tutoría.
Traballos tutelados	Presentaranse varios traballos teóricos e prácticos a desenvolver, entre os cales cada grupo debe elixir un. Na clase tipo C, exporase a cada grupo os obxectivos do traballo, ferramentas hardware e software a usar, forma de acometelo e realizarase un seguimento a cada grupo.
Prácticas de laboratorio	O alumno desenvolverá unha práctica no laboratorio, enfocada tanto a madurar e levar a práctica os contidos teóricos, como a mellorar a súa capacidade para o desenvolvemento e/ou implantación de redes e servizos seguros.

Atención personalizada	
Metodoloxías	Descrición
Sesión maxistral	O alumno debe interactuar co profesor nas horas de tutoría normais para: 1. Tutelar o traballo que elixa ou propoña, tanto antes como durante a súa realización, validando a orientación, organización, parte descriptiva e ausencia de erros. 2. Resolver calquera tipo de dúbida concernente á orientación e realización das prácticas de laboratorio. 3. Dúbidas que se lle susciten ao alumno sobre a realización dos exercicios do boletín.
Prácticas de laboratorio	O alumno debe interactuar co profesor nas horas de tutoría normais para: 1. Tutelar o traballo que elixa ou propoña, tanto antes como durante a súa realización, validando a orientación, organización, parte descriptiva e ausencia de erros. 2. Resolver calquera tipo de dúbida concernente á orientación e realización das prácticas de laboratorio. 3. Dúbidas que se lle susciten ao alumno sobre a realización dos exercicios do boletín.
Resolución de problemas e/ou exercicios	O alumno debe interactuar co profesor nas horas de tutoría normais para: 1. Tutelar o traballo que elixa ou propoña, tanto antes como durante a súa realización, validando a orientación, organización, parte descriptiva e ausencia de erros. 2. Resolver calquera tipo de dúbida concernente á orientación e realización das prácticas de laboratorio. 3. Dúbidas que se lle susciten ao alumno sobre a realización dos exercicios do boletín.
Traballos tutelados	O alumno debe interactuar co profesor nas horas de tutoría normais para: 1. Tutelar o traballo que elixa ou propoña, tanto antes como durante a súa realización, validando a orientación, organización, parte descriptiva e ausencia de erros. 2. Resolver calquera tipo de dúbida concernente á orientación e realización das prácticas de laboratorio. 3. Dúbidas que se lle susciten ao alumno sobre a realización dos exercicios do boletín.
Resolución de problemas e/ou exercicios de forma autónoma	O alumno debe interactuar co profesor nas horas de tutoría normais para: 1. Tutelar o traballo que elixa ou propoña, tanto antes como durante a súa realización, validando a orientación, organización, parte descriptiva e ausencia de erros. 2. Resolver calquera tipo de dúbida concernente á orientación e realización das prácticas de laboratorio. 3. Dúbidas que se lle susciten ao alumno sobre a realización dos exercicios do boletín.

Avaliación		
	Descrición	Cualificación
Resolución de problemas e/ou exercicios de forma autónoma	Valoración dos dous boletíns de problemas/exercicios. O grupo deberá entregar o boletín 1 antes da semana 10 e o 2 antes da semana 15.	10
Probas de resposta longa, de desenvolvemento	Exame final da materia. Este exame constará duns 8 a 10 exercicios/problemas/cuestións sobre os contidos impartidos no curso.	50
Probas prácticas, de execución de tarefas reais e/ou simuladas.	Proba de grupo na que o profesor valorará a práctica de laboratorio, revisando o seu funcionamento cos integrantes do grupo presentes. Esta proba realizarase na semana 15.	20

Traballos e proxectos	Proba de grupo. Valoración do proxecto ou traballo tutelado realizado polo grupo (tipo C). O grupo fara unha demostración ao profesor do proxecto ou traballo realizado e resultados obtidos. O grupo debera entregar o traballo antes da semana 15. Todos os integrantes do grupo deben estar presentes no momento da presentación.	20
-----------------------	--	----

Outros comentarios sobre a Avaliación

• ELECCIÓN DE AVALIACIÓN CONTINUA.

Os alumnos que opten por avaliación continua deberán comunicalo explicitamente ao profesor antes da semana 4 do curso académico. A comunicación sera por correo electrónico.

• CONVOCATORIA DE FIN DO CUATRIMESTRE.

A avaliación continua esta formada polos exercicios a realizar de forma autonoma, polo traballo tutelado e polas prácticas de laboratorio, representando en total o 50% da asignatura, segun se especifica enriba no descriptivo das probas.

Os alumnos que non elixan EC faran un exame final polo 80% da nota, xunto coa practica de laboratorio que completase o outro 20%.

O exame final sera o mesmo para todos os alumnos, tantos para os que opten por avaliación continua como para os que non. No caso dos de avaliación continua conta como o 50% da nota, mentres que para os que non opten por avaliación continua conta polo 80% da nota final.

• CONVOCATORIA DE XULLO

Para os alumnos que non opten en maio por avaliación continua, realizarase un exame final cun valor do 80% xunto co laboratorio que representase o 20%. Gárdase a nota do laboratorio de Xaneiro.

Os alumnos que opten en Xaneiro por EC, poderán seguir optando en xullo por EC ou ben cambiar á opción d avaliación final. Os alumnos que así o fagan deberán comunicalo explícitamente ao profesor por correo electrónico.

- No primeiro caso, é dicir, dos que sigan por EC en xullo, gárdase a nota do boletín de problemas, a nota do traballo tutelado e da practica do laboratorio. Aínda así, o alumno ten a posibilidade de mellorar calquera delas ata chegar á puntuación máxima correspondente.
- No segundo caso, realizase un exame final polo 80% da nota e as prácticas de laboratorio polo 20%.

A cualificación obtida nas practicas de laboratorio e traballos en grupo será válida so durante o curso academico no que se realicen e no seguinte.

Considerarase a un alumno como "non presentado" se non seguiu a avaliación continua e non se presentou a o examen final.

Bibliografía. Fontes de información

F. Fernandez Masaguer, **Seguridad en Redes y Sistemas de Informacion**, 1ª ed.,

R.Perman, C. Kaufman, M.Speciner, **Network Security: Private communications on a public world**, 2ª ed.,

Joseph Migga Kizza, **Guide to Computer Network Security**, 2ª ed.,

Douglas R. Stinson, **Cryptography. Theory and Practice.**, 3ª ed.,

Benjamin M. Lail, **Broadband Network & Device Security**, 1ª ed.,

Recomendacións

Materias que se recomenda cursar simultaneamente

Arquitecturas e servizos telemáticos/V05G300V01645

Servizos de internet/V05G300V01501

Materias que se recomenda ter cursado previamente

Matemáticas: Álgebra lineal/V05G300V01104

Redes de ordenadores/V05G300V01403
