Universidade Vigo

Subject Guide 2013 / 2014

IDENTIFYING DATA

(*)Seguridade				
Subject	(*)Seguridade			
Code	V05G300V01543			
Study programme	(*)Grao en Enxeñaría de Tecnoloxías de Telecomunicación			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	3rd	1st
Teaching language	Spanish			
Department				
Coordinator	Fernández Masaguer, Francisco			
Lecturers	Fernández Masaguer, Francisco			
E-mail	f_masaguer@yahoo.es			
Web	http://faitic.uvigo.es			
General description	In this course are studied , in an unified way, the main problems and threats to security in networks and telematic services, and distinct techniques to protect them are presented. First the subject is considered from a general point of view, so that the concepts, services and security techniques studied, can be applied to any type of network, telematic service or information system to secure. This block is formed by chapters 1 to 4. This carries to treat with detail the three central subjects of security: the algorithmic part (encipherment, digital signature and integrity), the authentication problem and the procedures of key management. The aim is to give the student the knowledge and practice to entitle him/her to ease his understanding of the particular techniques that each application can require and to apply them to other scenarios that he(she) have to face. Afterwards the subject is considered in a more particular way, reviewing the problems, techniques and standards of security in some of the communication environments of greater prevalence in actuality. Thus a chapter is devoted to the security to the IP level, central protocol in the Internet architecture, and another chapter to the security in the Web, given the current importance of this way of telematic intercommunitation. The main security problems in electronic commerce using the Web are presented, studiing in particular the operation of Paypal, one of the payment methods more used in the Web. Given also the every time greater utilisation of wireless communications and his particular security problems, one chapter is devoted to the subject. The course is closed with an introduccion to other two subjects of increasing transcendence: botnets, malicious networks and software, and the forensic analysis of information systems.			

Competencies

Code	
A3	CG3: The knowledge of basic subjects and technologies that capacitates the student to learn new methods and technologies, as well as to give him great versatility to confront and update to new situations
A4	CG4: The ability to solve problems with initiative, to make creative decisions and to communicate and transmit knowledge and skills, understanding the ethical and professional responsibility of the Technical Telecommunication Engineer activity.
A6	CG6: The aptitude to manage mandatory specifications, procedures and laws.
A37	CE28/TEL2 The ability to apply the techniques that are basis of computer networks, services and applications, such as management, signaling and switching, routing and securing systems (cryptographic protocols, tunneling, firewalls, charging mechanisms, authentication and content protection) traffic engineering (graph theory, queuing theory and teletraffic) rating, reliability and quality of service in both fixed, mobile, personal, local or long distance environments with different bandwidths, including telephony and data.

Learning aims

Expected results from this subject	Training and Learning Results
Knowledge of some of the mathematic theories in which support the security of the cryptographic algorithms and protocols used for the protection of networks and services.	A3
Knowledge of the principles and operation of the main encryption, digital signature and hash algorithms used as the base of the security services incorporated in telematic networks and services.	A3
Knowledge of the different and more important methods, techniques and protocols of authentication, used to protect networks.	A3
Endow to the student of the capacity to analyse the problems of security of an information system, network or telematic service, evaluate the risks associated and implement the appropriate techniques to guarantee a suitable level of security.	A4
Ability to apply the security techniques used by the networks, services and telematic applications, such as cryptographic protocols, tunneling, firewalls, Internet payment mechanisms, authentication and protection of contents.	A37
Facilitate the handle and knowledge of specifications and normative about security.	A6 A37

Contents

Topic	
1 Mathematics foundations of security.	- Notions of Complexity Theory. - Notions of Number Theory.
2. Cypher, digital signature and hash algorithms	- Encrytion. Shannon principles. Stream and block cyphers. DES and AES algorithms Cypher modes of operation - Integrity and hash algorithms. - Public key cryptosystems. RSA, ElGamal and DSA.
3. Certification and Public Key Infrastructures.	- Security problems of asimetric cryptography. Certification and certificate formats. - Trust models. Flat trust model and PGP. Third partiy trust model and certification authorities. - Certificate Infrastructures. Certification path and revocación of certificates.
4. Authentication and key agreement protocols.	- Authentication methods. - Threats to an authentication protocol. Countermeasures. - Requirements of a key agreement protocol. Diffie-Hellman protocol. - Authentication in simmetric cryptosistems. Cases of study: GSM and Kerberos. - Authentication in asimetric cryptosistems. Cases of study: X509 and SSL. - Passwords based protocols: SRP.
5. Security at the network layer	- Threats in the network layer. - IP Security Architecture. - IPsec Protocol. IPsec tunnels. IPsec and NAT. - Key manegement protocols: IKE, ISAKMP and OAKLEY.
6. Security in the Web and electronic commerce.	- Problems of security in the Web. - Protocols: SSL and TLS. - Certification in the Web. - Principles of electronic commerce and payment protocols. PayPal system.
7. Wireless security and AAA protocols.	- Threats to security in wireless environments. - Wireless Application Protocol (WAP). WTLS. Protocols WEP, WPA, WPA2 (802.11i). - AAA Protocols: RADIUS and DIAMETER.
8. Systems Security.	- Firewalls and systems against intrusions. - Malicious software and networks. Botnets. - Forensic analysis of systems.

Planning

	Class hours	Hours outside the classroom	Total hours
Master Session	19	38	57
Troubleshooting and / or exercises	2	0	2
Autonomous troubleshooting and / or exercises	0	10	10
Tutored works	6	28	34
Laboratory practises	11	22	33
Long answer tests and development	2	10	12
Practical tests, real task execution and / or simulated.	1	0	1

Jobs and projects	1	0	1

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Master Session	Exhibition by means of powerpoint presentations and blackboard of the theoric contents of the course. They will develop the theoretical subjects of the matter that do not remain covered by the others methodologies employed.
Troubleshooting and / or exercises	Some problems and exercises of the bulletin will be solved, so that they can serve as a guide for the autonomuous resolution by the group of the rest of exercises or questions. The solution to similar problems will be given also to students to ease the reaization of the bulletin.
Autonomous troubleshooting and / or exercises	The group will solve in an autonomous form the exercises, cuestions or problems of the bulletin not solved in the face-to-face hours. The diverse solutions that arise when tackling each problem, will be put in common to agree the best form of solution. The doubts arisen will be agreed and will be exposed to the tutor in normal tutor time.
Tutored works	Several theoretical and practical works to develop will be explained to the students, between which each group will have to choose one. In the C class type, will expose to each group the aims of the work, hardware and software tools to use, form to tackle it and will realise a follow-up to each group.
Laboratory practises	The student will developed some practices in the laboratory, focused to mature and carry to practice the theoretical concepts , as to improve his ability for the engineering of secure networks and services.

Personalized attention

Methodologies	Description
Master Session	The student can interact with the teacher in normal tutorial time to: 1. Follow the work or project selected, before and during his development, to validate its orientation, organization and aims, descriptive part and absence of errors. 2. Solve any type of doubt concerning the orientation, understandings, errors and realization of laboratory practices. 3. Doubts that appears to the student on his realization of the bulletin exercises and questions and about the theoretical contents of the course.
Laboratory practises	The student can interact with the teacher in normal tutorial time to: 1. Follow the work or project selected, before and during his development, to validate its orientation, organization and aims, descriptive part and absence of errors. 2. Solve any type of doubt concerning the orientation, understandings, errors and realization of laboratory practices. 3. Doubts that appears to the student on his realization of the bulletin exercises and questions and about the theoretical contents of the course.
Troubleshooting and / or exercises	The student can interact with the teacher in normal tutorial time to: 1. Follow the work or project selected, before and during his development, to validate its orientation, organization and aims, descriptive part and absence of errors. 2. Solve any type of doubt concerning the orientation, understandings, errors and realization of laboratory practices. 3. Doubts that appears to the student on his realization of the bulletin exercises and questions and about the theoretical contents of the course.
Tutored works	The student can interact with the teacher in normal tutorial time to: 1. Follow the work or project selected, before and during his development, to validate its orientation, organization and aims, descriptive part and absence of errors. 2. Solve any type of doubt concerning the orientation, understandings, errors and realization of laboratory practices. 3. Doubts that appears to the student on his realization of the bulletin exercises and questions and about the theoretical contents of the course.
Autonomous troubleshooting and / or exercises	The student can interact with the teacher in normal tutorial time to: 1. Follow the work or project selected, before and during his development, to validate its orientation, organization and aims, descriptive part and absence of errors. 2. Solve any type of doubt concerning the orientation, understandings, errors and realization of laboratory practices. 3. Doubts that appears to the student on his realization of the bulletin exercises and questions and about the theoretical contents of the course.

Assessment

	Description	Qualification
Autonomous troubleshooting and / or exercises	Assessment of the two bulletins of problems/exercises. The group will have to deliver bulletin 1 before week 10 and bulletin 2 before week 15.	10
Long answer tests and development	Final exam of the course. This exam will consist of about 8 to 10 exercises/problems/questions on the contents given in the course.	50

Practical tests, real task execution and / or simulated.	Proof of group in which the professor will value laboratory practices, reviewing his operation with all group members present. This proof will be realised in week 15.	20
Jobs and projects	Assessment of the tutee project or work realised by the group (type C). The group will do a demonstration to the teacher of the project or work realised and results obtained. The group must deliver the work before week 15. All the members of the group have to be present at the moment of presentation.	20

Other comments on the Evaluation

- CHOICE OF CONTINUOUS EVALUATION .

  The students that opt by continuous evaluation (EC) must communicate it explicitly to the teacher before week 4 of the course. This communication must be made by electronic mail.

- ANNOUNCEMENT OF END OF FOUR-MONTH PERIOD.

  The continuous evaluation (EC) is formed by the exercises to realise of autonomous form, by the tutee work or proyect and by the laboratory practices, representing in total 50% of the course, as indicated in the assesment. The students that do not choose EC will do a final exam by 80% of the final note, together with the laboratory that will complete the other 20%.

  The final exam will be the same for all the students, that is, for both EC and not EC students. In the case of EC students this exam will count by 50% of the note, whereas for not EC students will count by 80% of the note.

- ANNOUNCEMENT OF JULY

  The students that have not opted during the four-month period for EC, will do a final exam with a value of 80% of the final note together with the laboratory that will represent the other 20%. Of the May announcement it is saved both the laboratory and the exam note.

  The students that have opted during the normal cuatrimester by EC, can follow in July by EC or change to not EC. The students that change to not EC MUST communicate it explicitly to the teacher by electronic mail.

  1. In the first case, that is for the students than continue by EC in July, the note of the bulletin, laboratory practices and tutee work is saved from the January announcement. However, the student has the option to improve any of them until his corresponding maximum note.
  2. In the second case, not EC students in July, will do a final examination by 80% of the note, and laboratory practices by 20%.

  The ratings obtained in the laboratory and group works will be valid only during the academic course in that they realise and in the following.

  It will be considered to the student as "no presented" if he/she has not followed the EC and has not presented to the final examination.

Sources of information

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

R.Perlman, 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.,

Recommendations

Subjects that are recommended to be taken simultaneously

(*)Arquitecturas e servizos telemáticos/V05G300V01645

(*)Servizos de internet/V05G300V01501

Subjects that it is recommended to have taken before

(*)Matemáticas: Álxebra lineal/V05G300V01104

(*)Redes de ordenadores/V05G300V01403