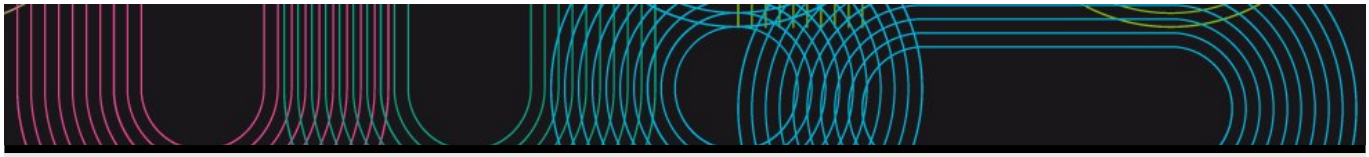

| IDENTIFYING DATA | | | | |
|---|---|---|---|---|
| **Network Security** | | | | |
| Subject | Network Security | | | |
| Code | V05G301V01305 | | | |
| Study programme | Grado en Ingeniería de Tecnologías de Telecomunicación | | | |
| Descriptors | ECTS Credits | Choose | Year | Quadmester |
| | 6 | Optional | 3rd | 1st |
| Teaching language | Spanish | | | |
| Department | | | | |
| Coordinator | Fernández Masaguer, Francisco<br>Rodríguez Rubio, Raúl Fernando | | | |
| Lecturers | Fernández Masaguer, Francisco<br>Rodríguez Rubio, Raúl Fernando | | | |
| E-mail | francisco.fernandez@det.uvigo.es<br>rrubio@det.uvigo.es | | | |
| Web | http://moovi.uvigo.gal | | | |
| General description | In this subject, the main security problems or threats in networks and telematic services are studied in a unified way, and different techniques are presented to protect them. The topic is first approached from a general point of view, so that the security concepts, services, and techniques studied are applicable to any type of network, telematic service, or information system to be secured. This block consists of topics 1 to 4. This leads to a detailed examination of the three central security topics: the algorithmic part (encryption, digital signature, and integrity), authentication protocols, and key management and negotiation procedures. The objective is for the student to acquire a solid foundation that enables them to understand the specific techniques required by each application as well as to apply them to other areas they may encounter. The topic is then addressed in a somewhat more specific way, reviewing the problems, techniques, and security standards in some of the most prevalent communication environments today. A topic is dedicated to security at the IP level, a central protocol in the Internet architecture, and another topic to web security, given the current relevance of this telematic communication medium, where the student will assimilate the theoretical and practical concepts of the SSL protocol, central to the security of transactions over the web. Due to the increasing use of wireless communications and their particular security issues, a topic is also dedicated to them. The course concludes with an introduction to two other topics of increasing importance: malicious networks and software, and forensic analysis of information systems. | | | |

| Training and Learning Results | |
|---|---|
| Code | |
| B3 | CG3: The knowledge of basic subjects and technologies that enables the student to learn new methods and technologies, as well as to give him great versatility to confront and adapt to new situations |
| B4 | 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. |
| B6 | CG6: The aptitude to manage mandatory specifications, procedures and laws. |
| C28 | 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. |
| D2 | CT2 Understanding Engineering within a framework of sustainable development. |
| D3 | CT3 Awareness of the need for long-life training and continuous quality improvement, showing a flexible, open and ethical attitude toward different opinions and situations, particularly on non-discrimination based on sex, race or religion, as well as respect for fundamental rights, accessibility, etc. |

**Expected results from this subject**

| Expected results from this subject | Training and Learning Results | | |
|---|---|---|---|
| Understand the foundations of the cryptographic science | B3 | | |
| To acquire the necessary knowledges to ensure the security of a computer or telematic system. | B3 | | |
| To acquire skills on the process of analysis of the attacks that can suffer a network and the main mechanisms of defence against them. | B4 | C28 | D3 |
| Know the main architectures of applicable security to the computer and telematic systems. | B4 | C28 | D3 |
| Know the main ideas of the norms and standard more important in matter of security in computer systems and communication networks. | B6 | C28 | D2 |

## Contents

| Topic | |
|---|---|
| 1 Mathematics foundations of security. | - Basic notions of Complexity Theory.<br>- Basic notions of Number Theory. |
| 2. Cypher, digital signature and hash algorithms | - Types of criptosistems and algorithms.<br>- Integrity and hash algorithms.<br>- Symetric key cryptosistems. Mac functions. Encrytion. Shannon principles. Stream and block cyphers. DES and AES algorithms Cypher modes of operation.<br>- Public key cryptosystems. RSA, DSA and elliptic curves.<br>- Influence of quantum computing on cryptography. |
| 3. Certification and Public Key Infrastructures. | - Security problems of asimetric cryptography. Certification and certificate formats.<br>- Trust models. Flat trust model and PGP. Third partiy trust model and certification authorities.<br>- Certificate Infrastructures. Certification path.<br>- Certificate revocation. |
| 4. Authentication and key agreement protocols. | - Authentication methods.<br>- Threats to an authentication protocol. Countermeasures.<br>- Requirements of a key agreement protocol. Diffie-Hellman protocol.<br>- Authentication in simmetric cryptosistems. Cases of study: GSM and Kerberos.<br>- Authentication in asimetric cryptosistems. Cases of study: X509 and SSL.<br>- Passwords based protocols: SRP, SAE.<br>- Single Sign On (SSO) |
| 5. Security at the network layer | - Threats in the network layer.<br>- IP Security Architecture.<br>- IPsec Protocol. IPsec tunnels. IPsec and NAT.<br>- Key manegement protocols: IKE, ISAKMP and OAKLEY. |
| 6. Security in the Web and electronic commerce. | - Problems of security in the Web.<br>- Protocols: SSL and TLS.<br>- Certification in the Web. |
| 7. Wireless security and AAA protocols. | - Threats to security in wireless environments.<br>- Wireless Application Protocol (WAP). WTLS. Protocols WEP, WPA, WPA2, WPA3.<br>- AAA Protocols: RADIUS. |
| 8. Systems Security. | - Firewalls and systems against intrusions.<br>- Malicious software and networks.<br>- Forensic analysis of systems. |

## Planning

| | Class hours | Hours outside the classroom | Total hours |
|---|---|---|---|
| Lecturing | 21 | 38 | 59 |
| Autonomous problem solving | 0 | 10 | 10 |
| Mentored work | 6 | 28 | 34 |
| Laboratory practical | 11 | 22 | 33 |
| Laboratory practice | 1 | 0 | 1 |
| Essay | 1 | 0 | 1 |
| Essay questions exam | 1 | 5 | 6 |
| Essay questions exam | 1 | 5 | 6 |

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

## Methodologies

| | Description |
|---|---|

| | |
|---|---|
| Lecturing | 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. In those subjects considered indispensable, will pose and will resolve some exercises that serve of help for the realisation of other similar by the student of autonomous form.<br>With this methodology, student will adquire part of CG3 y CE28 competences. |
| Autonomous problem solving | The student will solve in an autonomous form the exercises, cuestions or problems of the bulletin not solved in the face-to-face hours. The doubts arisen will be agreed and will be exposed to the tutor in normal tutor time.<br>This methodology is aimed to CG4 and CE28 competences. |
| Mentored work | Work in group. 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.<br>This methodology, is aimed to adquire part of CG4,CG6, CE28, CT2 and CT3 competences. |
| Laboratory practical | Work in group. The group 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.<br>This methodology, is aimed to CG6, CE28, CT2 and CT3 competences. |

**Personalized assistance**

| Methodologies | Description |
|---|---|
| Laboratory practical | Individualized monitoring of each group work. Comments of diverse options, recommendations and strategies for the good development of the project. Reviews with each group the level of understanding and advance of the project, particular doubts that can arise, design and Java coding errors. Help for the understanding of the JCA/JCE and JSSE packages. Individualized help for instalation of the keystore management tool and of the basic Java code of the practice. On the subject's website at Moovi (https://moovi.uvigo.gal), you can find instructions on how to request tutoring. |
| Mentored work | Individualized monitoring of each student in the group. General comments to the group of recommendations and strategies for the good development of the project. Reviews with each group of the level of understandings and advance of the project, particular doubts that can arise, design or approach errors and options of improvement. On the subject's website at Moovi (https://moovi.uvigo.gal), you can find instructions on how to request tutoring. |
| Autonomous problem solving | Reviews and comments of the diverse exercises proposed. The student will have in Faitic with the solucion to some of the proposed exercises. On the subject's website at Moovi (https://moovi.uvigo.gal), you can find instructions on how to request tutoring. |

**Assessment**

| | Description | Qualification | Training and Learning Results | | |
|---|---|---|---|---|---|
| Laboratory practice | Proof of group in which the teacher will value laboratory practises, reviewing his operation with the members of the group.<br>This proof will be made in the last or previous to last week of the four-month period as it will be published in Moovi platform in the firsts weeks of the four-month period.<br>All the members of the group have to be present at the moment of the presentation.<br>The teacher will do an authorship interview of which the level of participation of each student will be deduced and of which, together with the correct operation, the individual mark of each student will be determined. | 25 | B6 | C28 | D3 |
| Essay | Assessment of the tutored project or work realised by the group (type C). The group will do a demonstration to the teacher of the project or work done and results obtained.<br>This proof will be made in the last or previous to last week of the four-month period as it will be published in Moovi platform in the firsts weeks of the four-month period.<br>All the members of the group have to be presents in the moment of the presentation.<br>The teacher will do an authorship interview of which the level of participation of each student in the proyect will be deduced and of which, together with the correct operation, the individual mark of each student will be determined. | 25 | B4<br>B6 | C28 | D2<br>D3 |

| | | | | |
|---|---|---|---|---|
| Essay questions exam | Final exam of the course. This exam will consist of a group of exercises/questions on the contents given in the course. | 25 | B3 B4 | C28 |
| Essay questions exam | Partial exam of the course, neccesary for students that follow continuos evaluation. This exam will consist of a group of exercises/questions on the contents given until aproximately the middle of the theoretic course. | 25 | B3 B4 | C28 |

**Other comments on the Evaluation**

- CHOICE OF CONTINUOUS ASSESMENT.

  By default, it will be assumed that the students opt for continuous assessment (CA). If a student wishes to opt for global assessment (GA), they must inform the teaching staff before the end of week 5 of the semester. The communication must be made via email to the teaching staff.

- **ORDINARY OPPORTUNITY.**

  ***Continuous Assessment.*** The continuous assessment (CA) will be formed by:

  1. Laboratory Assignment B, representing 25% of the grade. This assignment must be submitted via Moovi. The specific submission date will be posted on Moovi in the first weeks of the semester, following a coordination meeting with the other subjects.
  2. Project C, representing 25% of the grade. This project must be submitted via Moovi. The specific submission deadline will be posted on Moovi in the first weeks of the semester, following a coordination meeting with the other subjects.
  3. Midterm exam covering the content taught up to approximately the middle of the semester, representing 50% of the total theory grade. This exam will be averaged with the final exam if the student scores a minimum of 4 out of 10 points. If the student scores below this, they will need to be reassessed on this part in the final exam.
  4. The scheduling of the different interim assessment tests will be approved by a Degree Academic Committee (CAG) and will be available at the beginning of the semester.
  5. Final theoretical exam, on the date agreed upon in the School Board meeting. There will be two cases:
     - Students who have passed the minimum grade on the midterm exam. This exam will cover topics taught from approximately the middle of the semester to the end. It will account for 25% of the total grade. To pass the course, students must achieve a minimum score of 4 out of 10 on this exam.
     - Students who have not achieved the minimum grade on the midterm exam. This exam will cover all topics covered in the theoretical course. It will account for 50% of the total grade. To pass the course, students must achieve a minimum score of 4 out of 10 on this exam, with at least 4 points in each of the two parts of the exam.

  ***Global Assessment.*** The global assessment (GA) will be formed by:

  1. A final theoretical exam worth 75% of the grade, consisting of two parts, will be held on the same day and time as the CA exam.
  2. Lab practices B, which will account for the remaining 25%, must be submitted via Moovi, with the deadline on the same day as the CA exam.
  3. To pass the course, students must achieve a minimum of 4.5 points out of 10 in each of the two parts

of the theoretical exam. They must also earn at least 1 point out of 2.5 in lab practices B.

The final exam will be the same for all students, both those opting for continuous assessment and those opting for global assessment.

- **EXTRAORDINARY OPPORTUNITY.**

For students who have opted for continuous assessment during the semester, the total grade will be determined as follows:

1. 50% from the theoretical part, 25% from lab practices B, and 25% from project C.
2. From the regular opportunity, the grades of the partial and final theoretical exams (provided they have met the minimum grade), lab practice B (provided the minimum has been met), and project C will be retained.
3. All students who have not achieved the minimum theoretical grade in either part of the regular opportunity must take the theoretical exam in this retake. However, they only need to take the part or parts where they did not meet the minimum. It is mandatory to score a minimum of 4 out of 10 in any part taken to pass the course.
4. Students who did not submit lab practice B in the regular opportunity or did not achieve the minimum grade in this part must complete and submit the same lab practice as in the regular opportunity. The deadline for submission will be the same as the day and time of the theoretical exam. It is mandatory to score a minimum of 1 point out of 2.5 in this part to pass the course.
5. Students who did not submit project C in the regular opportunity must take a written test on the same day as the theoretical exam, which will contribute 25% to the total grade. Therefore, there will be no actual submission of project C.

For students who have chosen global assessment in the regular opportunity, there will be a final exam worth 75%, along with lab work B representing 25%. The grade from the theoretical exam in the regular opportunity (provided it meets the minimum of 4.5 points) and lab work B (provided it meets the minimum of 1 out of 2.5 points) will be retained.

- **OTHER OBSERVATIONS.**
  - An student will be marked as "Not Present" if they have not followed continuous assessment and have not attended the final theoretical exam. Similarly, if a student is on CA and does not attend any exam (A, B, and C), they will be considered "Not Present."
  - Grades obtained in lab practice B and project C will only be valid during the academic year in which they are completed.
  - If the total grade is equal to or greater than 5 but the minimum grade has not been reached in any part, the final grade will be 4.9 points (fail).

- **ANNOUNCEMENT OF END OF CAREER.**
  - The evaluation in the end-of-degree session will consist of:
    - Theoretical exam (50%): Individual exam covering the course content, representing 50% of the total grade. Students must achieve a minimum score of 4 points (in each of the two parts of the exam) out of 10 to pass the course.
    - Lab work B (25%): Represents 25% of the grade, with a minimum requirement of 1 point out of 2.5.
    - Project C (25%): Represents 25% of the grade.

## Sources of information

### Basic Bibliography

F. Fernandez Masaguer, **Apuntes de Seguridad en Redes y Sistemas de Informacion,**, 1ª ed., 2024

William Stallings, **Cryptography and Network Security. Principles and practice.,**, 8ª, Pearson, 2020

### Complementary Bibliography

Joseph Migga Kizza,, **Guide to Computer Network Security**, 4ª Ed, Springer, 2015

M. Laurent Maknavicius, **Wireless and Mobile Network Security**, 1ª Ed, Wiley, 2014

R.Perlman, C. Kaufman, M.Speciner, **Network Security: Private communications on a public world,**, 2ª Ed, Prentice Hall, 2002

Enisa, **Botnets: Detection; Measurement, Disinfection & Defence,**, Enisa, 2011

## Recommendations

### Subjects that are recommended to be taken simultaneously

Architectures and Services/V05G301V01310
Internet Services/V05G301V01301

### Subjects that it is recommended to have taken before

Programming II/V05G301V01110