Universitat Autònoma de Barcelona

Advanced Networks and Security 2016/2017

Code: 42850
ECTS Credits: 6

Degree	Type	Year	Semester
4313797 Telecommunications Engineering	OB	1	1

Contact

Name: Ramon Marti Escale

Email: Ramon.Marti.Escale@uab.cat

Use of languages

Principal working language: english (eng)

Teachers

Joan Bartrina Rapesta

Prerequisites

Knowledge of basic network communications architecture is desired.

Objectives and Contextualisation

The objective of this module is to deepen in the communication networks and in its security. Specifically, it will centred in providing to the students knowledge on:

1. Introduction to the communication layers architecture and security in Internet
2. Description of the Internet architecture and the advanced routing protocols
3. Content Management services
4. Next Generation Internet protocols
5. Advanced network security

Skills

- Be capable of resolving convergence, interoperability and design of heterogeneous networks with local, access and truncal networks as well as the integration of telephone, data, television and interactive services.
- Be capable of understanding and knowing how to apply internet organisation and function, next generation internet technologies and protocols, components models, intermediary software and services.
- Capacity for modelling, designing, introducing, managing, operating, administrating and maintaining networks, services and content.
- Capacity for planning, decision-making and packaging of networks, services and applications considering the quality of service, direct and operating costs, the implementation plan, supervision, security procedures, scaling and maintenance and for managing and ensuring quality in the development process.
- Capacity for working in interdisciplinary teams
- Student should possess the learning skills that enable them to continue studying in a way that is largely student led or independent

- Students should know how to apply the knowledge they have acquired and their capacity for problem solving in new or little known fields within wider (or multidisciplinary) contexts related to the area of study
- Students should know how to communicate their conclusions, knowledge and final reasoning that they hold in front of specialist and non-specialist audiences clearly and unambiguously

Learning outcomes

1. Capacity for working in interdisciplinary teams
2. Integrate services and security in current and next generation internet.
3. Student should possess the learning skills that enable them to continue studying in a way that is largely student led or independent
4. Students should know how to apply the knowledge they have acquired and their capacity for problem solving in new or little known fields within wider (or multidisciplinary) contexts related to the area of study
5. Students should know how to communicate their conclusions, knowledge and final reasoning that they hold in front of specialist and non-specialist audiences clearly and unambiguously
6. Understand global internet architecture and the channelling protocols used.
7. Understand security procedures in networks, services and applications.
8. Understand the advanced mechanisms of cryptography and the main attacks and security mechanisms on the different levels of the web and in next generation internet.
9. Understand the architecture of content management services
10. Understand the design and administration mechanisms of content management services.
11. Understand the layers of architecture in internet communications, protocols and principal services.
12. Understand the main protocols associated with the next generation of internet.

Content

Structure and contents:

1. Protocols and Architectures

- Protocols, interfaces and services
- Network architectures

2. Advanced Routing Protocols

- Internet architecture
- RIP
- OSPF
- BGPv4

3. Content Management Services

- Content management services architecture
- Content management services design
- Content management services administration

4. Next Generation Internet

- IPv6
- Mobile IP
- Opportunistic Networks
    - Mobile ad-hoc networks (MANET)
    - Delay and Disruption Tolerant Networks (DTNs)
    - Wireless sensor networks
    - Service Advertisement and Discovery
    - Pervasive computing

Radio Frequency IDentification (RFID)
Mobile Agents

5. Network Security

- Advanced cryptography
  Security mechanisms
- Attacks and prevention mechanisms at the different network layers
  Attacks and prevention mechanisms at the network layer
  Attacks and prevention mechanisms at the transport layer
  Attacks and prevention mechanisms at the application layer
- Security in Next Generation Internet
  - Mobile IP security
  - Ad-hoc networks security
  - DTN security
  - Wireless Sensor Networks security
  - Pervasive computing security
  - RFID security
  - Mobile Agents security

Methodology

The work methodology will combine the face-to-face classes, the realisation of works in the laboratory, the realisation of works from recommended readings and the autonomous work of the student. It will make use of the virtual platform and the presentation of works related with the thematic blocks will be required.

During the course, we will carry out the following activities:

- Theory sessions, where the teacher will provide information on the knowledge of the subject and on strategies to acquire, expand and organise this knowledge. The active participation of the students will be encouraged during these sessions, for example posing discussions in those points that admit diverse technological solutions.
- Problems sessions, where the students will have to actively take part to consolidate the knowledge acquired resolving, presenting and debating related problems. Problems are distinguished from the exercises, which can be considered as trivial problems. The problems often will admit several solutions and will be able to originate debate between the students.
- Laboratory practical sessions, where small projects will be posed to be analysed and developed by the students in group. The sessions will be previously prepared, documented and programmed by the teacher, and the students will have to prepare them before assisting, reviewing the related theoretical knowledge and the basic technical aspects developmental. The practical sessions must serve to the students to attain the skills of the subject and contribute to attain some competitions such as the one of autonomous work.
- Preparation of the portfolio of the subject, in a virtual way through a wiki, collaborative work web tool. The students will have to work autonomously in teams in the research and the preparation of the corresponding material of the evidences of his theory and problems learning, and in the study of this material. The evidences comprise extensions of the different subjects exposed to the sessions of theory and collaborative resolution of problems. The teacher will do the follow-up of the work of the different teams, will provide feedback to the teams depending of the task done and of the doubts that pose or of the errors that manifest. The preparation of the portfolio has to serve to the students to contribute to attain the competitions of the subject. The teaching methodology and the evaluation go tightly tied to the wiki-based virtual portfolio system, that is the cohesive element of the different teaching activities during the course, and that allow a system of continued and formative evaluation, incorporated to the process of education/learning. The wiki will help the students to develop a constant work that will bring them to attain the knowledge proposed, and the skills and the competitions associated to the theory and problems parts.

Activities

Title	Hours	ECTS	Learning outcomes
Type: Directed			
Directed activities	45	1.8	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Type: Supervised			
Supervised activities	15	0.6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Type: Autonomous			
Autonomous activities	90	3.6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Evaluation

Evaluation systems

- Written tests: Partial and final written tests
- Delivery of reports or problems: Brief reports on specific subjects
- Work in the laboratory and corresponding memories: it will assess the previous preparation of the practice, the capacity to realise it in an efficient form and the quality of the analyses reflected in the memory.
- Presentations and participation in the problems and cases seminars: it will evaluate the previous preparation of the questions/exercises/cases assigned for the session

The final mark for the course, that includes the assessment of the acquisition of knowledge and skills, is calculated in the following way:

- 25%, from the mark of the work in the presentations and participation in the problems and cases seminars. The minimum required in this part is 5 out of 10.
  If the student passes the validation of knowledge tests and the minimum of the work in the portfolio is not reached, he/she will be able to recover this part before the closing date for marks.
- 40%, from the mark of the written tests. The minimum required in this part is 5 out of 10.
  To carry out the validation of the knowledge, there will be two partial tests during the year (a partial test to assess Part I of the course and a partial test to assess Part II of the course) and a final exam (to assess both parts).
  If the student gets more than 4 in any of the two partial tests, he/she will not be assessed again from this part in the final exam (the mark of this part will be the one from the partial exam). The final mark will be the average of the marks obtained in both parts. To calculate the average, the student must obtain more than a mark of 4 in each of the parts (either in the partials or in the final tests). In case that a student gets more than 4 in both partial tests, but the average is lower than 5, he/she will have to take the final exam of the part with a mark lower than5(in case both parts are lower than 5, the student will be able to decide if he wants to take the final exam of both parts or only 1 of them).
- 10%, from the mark of the work done in delivery of reports or problems. No minimum is required for this part.
- 25%, from the mark of the laboratory. The minimum required in this part is 5 out of 10.
  If the student does not get the minimum mark of the laboratory sessions, he/she will be able to recover this part before the closing date for marks.

A minimum final mark of 5 is required to pass the course.

When a student has not done any work in laboratory, has not taken any of the partial or final theory written tests, and has a mark lower than 5 in the work in the presentations and participation in the problems and cases seminars, it will be considered that there are not enough assessment evidences, and the final mark will be "not assessable."

Evaluation activities

Title	Weighting	Hours	ECTS	Learning outcomes
Delivery of reports or problems	10%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Presentations and participation in the problems and cases seminars	25%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Work in the laboratory and corresponding memories	25%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Written tests	40%	0	0	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Bibliography

- Aspectos avanzados de seguridad en redes. Jordi Herrera Joancomartí (coord.), Joaquín García Alfaro, Xavier Perramón Tornil. Segunda edición, febrero 2007. Fundació per a la Universitat Oberta de Catalunya (http://ocw.uoc.edu/informatica-tecnologia-y-multimedia/aspectos-avanzados-de-seguridad-en-redes/mate