Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și Tehnologia Informației

COURSE DESCRIPTION

1. Program identification information

1.1 Higher education institution	**National University of Science and Technology Politehnica Bucharest**
1.2 Faculty	**Electronics, Telecommunications and Information Technology**
1.3 Department	**Telecommunications**
1.4 Domain of studies	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies	Masters
1.6 Programme of studies	Advanced Wireless Communications

2. Date despre disciplină

2.1 Course name (ro) (en)	Protocoale de securitate pentru comunicații wireless Wireless Communications Security Protocols
2.2 Course Lecturer	Conf. Dr. Octavian Catrina
2.3 Instructor for practical activities	Conf. Dr. Octavian Catrina

2.4 Year of studies	2	2.5 Semester	I	2.6. Evaluation type	E	2.7 Course regime	Ob
2.8 Course type		DS	2.9 Course code	UPB.04.M3.O.21-22		2.10 Tipul de notare	Nota

3. Total estimated time (hours per semester for academic activities)

3.1 Number of hours per week	2.5	Out of which: 3.2 course	1.50	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	35.00	Out of which: 3.5 course	21	3.6 seminary/laboratory	14
Distribution of time:					hours
Study according to the manual, course support, bibliography and hand notes Supplemental documentation (library, electronic access resources, in the field, etc) Preparation for practical activities, homework, essays, portfolios, etc.					55
Tutoring					0
Examinations					3
Other activities (if any):					0
3.7 Total hours of individual study	65.00				
3.8 Total hours per semester	100				
3.9 Number of ECTS credit points	4				

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	Cryptographic algorithm, Computer Networks. Computer Programming

4.2 Results of learning	Basic knowledge associated to the disciplines listed above.

5. Necessary conditions for the optimal development of teaching activities (where applicable)

5.1 Course	Lecture hall equipped with video projector, screen, blackboard/whiteboard.
5.2 Seminary/ Laboratory/Project	Laboratory equipped with computers and video projector. The software used in the lab, JDK and Eclipse, runs on both WIndows and Linux and is free.

6. General objective *(Reffering to the teachers' intentions for students and to what the students will be thought during the course. It offers an idea on the position of course in the scientific domain, as well as the role it has for the study programme. The course topics, the justification of including the course in the currcula of the study programme, etc. will be described in a general manner)*

The general objective of this discipline is to familiarize students with concepts, technologies, architectures and protocols used in practice to ensure the security of data communications and telecommunications networks. The motivation for studying communication security derives from the fact that the widespread use of information technology, in all fields of activity, has not only brought important advantages, but also unprecedented security risks. The security of data communications is of particular importance, as they play an essential role in the operation of distributed IT systems and, at the same time, provide the main avenues of attack on these systems.
The course introduces fundamental security concepts and technologies, as well as standardized security architectures and protocols, used in telecommunications networks, enterprise networks, and the Internet:
- Security functions: data authentication, participant authentication, data privacy, access control. Cryptographic solutions used to implement these features, along with their security models, standard security properties, and attack examples.
- Protocols for communication channels that ensure data authentication and data confidentiality.
- Authentication and key distribution protocols: design principles, attacks and security analysis.
- Security protocols for the Network level: IPsec, IKE; virtual private networks secured using IPsec.
- Security protocols for the Transport level: TLS, SSH; virtual private networks secured using TLS.

The course provides theoretical and practical knowledge to understand the fundamental aspects of security protocols in order to be able to design, implement, configure and maintain them. The presentation of the theoretical concepts is accompanied by practical work in the laboratory: in the first lab, students familiarize themselves with representative examples of standardized security protocols (IPsec, IKE), and in the following labs they implement and test a series of security protocols, using typical constructions and standardized cryptographic algorithms.

7. Competences *(Proven capacity to use knowledge, aptitudes and personal, social and/or methodological abilities in work or study situations and for personal and proffesional growth. They refflect the empolyers requirements.)*

Specific Competences	- Rigorous definition of communication security requirements and functions, the types of cryptographic algorithms used to implement them, and the standard security properties they must satisfy (upon which protocol security design and analysis is based). - Description, analysis and explanation of typical security protocol constructions (especially their security properties), advantages and disadvantages of different categories of solutions in the context of practical applications with different requirements (for example, protocols based on secret-key cryptography, protocols based on public-key cryptography and mixed solutions). - Development of communication security solutions that meet the security, scalability and performance requirements of the applications, using standard components.

Transversal (General) Competences	- Methodical analysis of the problems encountered in the activity, identifying the elements for which there are established solutions, thus ensuring the fulfillment of professional tasks. - The ability to adapt to new technologies and to document oneself (in Romanian and English), for professional and personal development, through continuous training. - Ability to think in scientific terms, search and analyze data independently, and draw and present conclusions or identify solutions. - The ability to analyze and synthesize: present the acquired knowledge in a synthetic way, as a result of a systematic analysis process. - Ability to cooperate with specialists in the field and work in a team, communicating effectively and coordinating efforts with the others to solve problems. - Compliance with the principles of academic ethics, in particular, the correct citation of bibliographic sources used in the documentation activity.

8. Learning outcomes *(Synthetic descriptions for what a student will be capable of doing or showing at the completion of a course. The learning outcomes reflect the student's acomplishments and to a lesser extent the teachers' intentions. The learning outcomes inform the students of what is expected from them with respect to performance and to obtain the desired grades and ECTS points. They are defined in concise terms, using verbs similar to the examples below and indicate what will be required for evaluation. The learning outcomes will be formulated so that the correlation with the competences defined in section 7 is highlighted.)*

Knowledge	*The result of knowledge aquisition through learning. The knowledge represents the totality of facts, priciples, theories and practices for a given work or study field. They can be theoretical and/or factual.* - Knows the domain-specific notions and topics covered in the course: security functions, cryptographic algorithms and their security properties, typical protocol constructions, standardized solutions for protocols and their components. - Knows how security concepts, cryptographic algorithms and security protocols are used in practice, to understand and rigorously specify the security and performance requirements or properties of applications and to develop solutions that meet these requirements.
Skills	*The capacity to apply the knowledge and use the know-how for completing tasks and solving problems. The skills are described as being cognitive (requiring the use of logical, intuitive and creative thinking) or practical (implying manual dexterity and the use of methods, materials, tools and intrumentation).* - Identifies and formulates (basic) communications security risks and requirements. - Analyze, describe and explain the role and operation of the components of a communication security solution (functions, algorithms, protocols), using specific terminology. - Identifies, implements and tests communication security solutions based on standard components (algorithms and protocols) to meet application requirements.

Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* - Selects appropriate bibliographic sources, understands them and analyzes them. - Respects the principles of academic ethics (for example, correctly citing the bibliographic sources used during documentation). - Demonstrates responsiveness to new learning contexts. - Demonstrates collaboration with other colleagues and teaching staff in carrying out teaching activities - Demonstrates autonomy in organizing the learning situation or in solving problems. - Realizes the value of his contribution in the field of engineering to the identification of viable and sustainable solutions to solve problems in social and economic life (social responsibility). - Analyzes and capitalizes on business/entrepreneurial development opportunities in the field. - Demonstrates real-life situation management skills.

9. Teaching techniques *(Student centric techniques will be considered. The means for students to participate in defining their own study path, the identification of eventual fallbacks and the remedial measures that will be adopted in those cases will be described.)*

The teaching process uses both expository (lecture, exposition) and conversational-interactive teaching methods, based on discovery learning models facilitated by direct and indirect exploration of reality (conceptual or practical experiments), but also on action-based methods , such as exercise, practical activities and problem solving.

The teaching activity uses lectures based on PowerPoint presentations illustrated by images and diagrams (architectures, messages, diagrams for algorithms and interactions) so that the information is easier to understand and assimilate. PowerPoint presentations are supplemented with examples built interactively on the board. Introductory presentations of courses and laboratory work highlight the connection with previously presented concepts.

In the lab, students explore, implement, and test typical constructions of security protocols for secure communication channels. Implementation exercises are essential to correctly understand the operations performed and the messages transmitted by these protocols. Also, experiments with these implementations allow to follow step by step the evolution of the state of the protocols and the information accessible to the adversary. Both the Eclipse integrated programming environment and the cryptographic libraries used are freely available and students can easily install them on their own computers.

The teaching process takes into account the crucial differences between communications security and the other disciplines in the field of electronic and telecommunications engineering. In this field, we face adversaries who want to compromise the operation of the system and have the necessary knowledge, skills and resources to understand and possibly overcome our protection measures, not only with physical phenomena whose behavior is predictable based on mathematical models. Furthermore, the fulfillment of security properties is difficult or impossible to test (experimentally) so we must rely on rigorous theoretical security analyses. Attack examples play an important role in understanding vulnerabilities and the solutions used by security protocols.

10. Contents

COURSE		
Chapter	**Content**	**No. hours**
1	Introduction. Threats and attacks on communications security. Security functions and cryptographic solutions for their implementation. Example: Security of WiFi networks.	3

2	Security protocol components (I): Data confidentiality using secret key algorithms (ENCS). Security properties. Block cipher. Typical constructions of ENCS schemes using block ciphers.	3
3	Security protocol components (II): Data authentication using secret key (MAC) algorithms. Security properties. Cryptographic hash functions. Typical constructions of MAC schemes using hash functions or block ciphers.	3
4	Secure channel protocols. Data communications protected by authenticated encryption. Security properties. Typical constructions of authenticated-encryption schemes. Examples of secure channel protocols used in practice (IPsec, TLS Record, WiFi).	3
5	Security protocol components (III): Data confidentiality and authentication using public-key algorithms (ENCP, SIG). Security properties. Typical constructions of ENCP and SIG schemes using one-way functions based on the RSA problem and the discrete logarithm problem.	4
6	Security protocol components (IV): Key generation and distribution. Typical constructions for generating pseudorandom bit-strings and deriving secret keys using MAC algorithms. Distribution of public keys. Certificates and Public Key Infrastructure.	3
7	Authenticated Key Exchange protocols. Typical protocol constructions for authenticating the participants and establishing secret keys based on secret-key cryptography and public-key cryptography. Security properties. Attacks.	6
8	Protocols for creating secure communication channels. Typical examples of authenticated key exchange protocols used in practice (IKEv2, TLS Handshake).	3
	Total:	28

Bibliography:

1. Catrina Octavian, Security Protocols for Wireless Communications, electronic course support (Moodle platform): https://curs.upb.ro/2021/course/view.php?id=9563
2. Catrina Octavian. Cryptographic Algorithms and Protocols. MATRIX ROM, Bucharest, 2016. ISBN 978-606-25-0249-2.
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996, 2001. Available online: http://cacr.uwaterloo.ca/hac/
4. The specifications of the cryptographic algorithms studied in the course are available online in the NIST publications (National Institute of Standards and Technology, https://www.nist.gov/) and IETF RFCs.

LABORATORY

Crt. no.	Content	No. hours
1	Communication security in practice: Virtual private networks that ensure data authenticity and confidentiality ("secure VPNs") built using IPsec, GRE and IKEv2. Implementation, experiments and analysis using a network emulator, protocol analyzer and Cisco routers.	4
2	Implementation of secure channel protocols (providing data authetnication and confidentiality) using authenticated encryption. Application implemented in Java using the standard library of cryptographic classes (SecPro1). Experiments and analysis.	2
3	Implementation of Authenticated Key Exchange (AKE) protocols (I): Constructions based on secret-key cryptography. Application written in Java using the standard library of cryptographic classes (SecPro2). Experiments and analysis.	4

4	Implementation of Authenticated Key Exchange (AKE) protocols (II): Constructions Based on Public Key Cryptography and Public Key Infrastructure. Application made in Java using the standard library of cryptographic classes (SecPro3). Experiments and analysis.	4
	Total:	14
Bibliography: Catrina Octavian, Security Protocols for Wireless Communications, lab descriptions and initial Java projects (Moodle platform): https://curs.upb.ro/2021/course/view.php?id=9563 The documentation of the software libraries used in the lab is available online: Java Cryptography Architecture Reference Guide, documentation of the Java standard cryptographic classes.		

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade
11.4 Course	- Knowledge of security concepts, techniques, algorithms and protocols studied in the course. - Ability to describe, analyze and explain the operation and the security properties of the protocols and their components in various situations encountered in practice (communication scenarios, attacks).	Written exam	50%
11.5 Seminary/laboratory/project	Analysis, design, implementation and testing of elementary applications that ensure communications security, based on the examples made during laboratory work.	Lab examination	50%
11.6 Passing conditions			
The students must obtain minimum of 50/100 for the verification papers and minimum 50/100 for the laboratory examination.			

12. Corroborate the content of the course with the expectations of representatives of employers and representative professional associations in the field of the program, as well as with the current state of knowledge in the scientific field approached and practices in higher education institutions in the European Higher Education Area (EHEA)

Modern society is based on a vast network of information systems used in economy, finance and administration, in essential infrastructures and services, as well as in the daily life of citizens. This massive deployment of information and communication technologies has brought both important advantages and unprecedented security risks.

Security technologies have therefore become essential components of this network of computer systems. These technologies provide a wide range of security functions and services: they allow access to resources and services only to legitimate users, protect the integrity, authenticity and confidentiality of data, ensure the availability of systems, networks and services. In particular, the security of data communications is of particular importance, as they play an essential role in distributed computing systems and, at the same time, provide the main avenues of attack on these systems. The IT industry requires engineers with a multidisciplinary qualification, able to solve the security problems of distributed systems, networks and applications, with solid knowledge of electronics, communication technologies and information security.

Therefore, the course meets the current and prospective requirements of the global economy in the fields of Electronics and Telecommunications. It provides graduates with essential theoretical and practical knowledge on information security, which improves their competitiveness and allows them to be employed quickly after graduation, being perfectly framed in the policy of the Politehnica University of Bucharest, both from the point of view of content and structure, as well as from the point of view of the skills and international openness offered to students.

Date	Course lecturer	Instructor(s) for practical activities
10.10.2024	Conf. Dr. Octavian Catrina	Conf. Dr. Octavian Catrina

Date of department approval	Head of department
27.10.2024	Conf. Dr. Serban Georgica Obreja

Date of approval in the Faculty Council	Dean
25.10.2024	Prof. Dr. Mihnea Udrea