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	Mobile Communications

2. Date despre disciplină

2.1 Course name (ro) (en)				Securitatea calculatorului personal și a terminalelor mobile Security of Personal Computer and Mobile Terminals			
2.2 Course Lecturer				Prof. Dr. Ing. Octavian Fratu			
2.3 Instructor for practical activities				Conf. Dr. Razvan Craciunescu			
2.4 Year of studies	1	2.5 Semester	II	2.6. Evaluation type	E	2.7 Course regime	Ob
2.8 Course type		DA	2.9 Course code	UPB.04.M2.O.08-18		2.10 Tipul de notare	Nota

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

3.1 Number of hours per week	3	Out of which: 3.2 course	2.00	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	42.00	Out of which: 3.5 course	28	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.					54
Tutoring					0
Examinations					4
Other activities (if any):					0

3.7 Total hours of individual study	58.00
3.8 Total hours per semester	100
3.9 Number of ECTS credit points	4

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	Completion of the following courses: • Computer Programming and Programming Languages (1 and 2)
4.2 Results of learning	Acquisition of the following general knowledge: • Fundamental concepts in computer programming and operating systems

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

5.1 Course	The lecture will take place in a room equipped with a video projector and a computer.
5.2 Seminary/ Laboratory/Project	The laboratory will take place in a room with specific equipment, including: • Video projector, computer, specific software (virtual machines, Kali Linux), and internet access.

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 main purpose of this course is to provide students with a comprehensive understanding of the principles and challenges associated with the security of personal computers and mobile devices. The inclusion of this course in the curriculum is justified by the increasing relevance of cybersecurity in the digital era, where understanding the complexity of security for personal and mobile devices is essential for the protection of individual and organizational data.

The course aims to offer students a broad perspective on key topics related to the security of personal computers and mobile devices, including general security concepts, vulnerabilities, detection and prevention of cyberattacks, user accounts, and passwords, as well as security solutions for maintaining personal computers. By the end of the course, students will have a solid foundation in managing the security of personal computers (both stationary and portable), understand the security management process, and be able to develop a security policy.

The course also addresses topics such as cyberattack vectors, including viruses, worms, and other malicious agents, along with methods for detecting, removing, and understanding the pathways these attacks use to penetrate systems, such as email services, web services, computer networks, and personal computer interfaces. In addition, the course analyzes advanced security resources, data storage methods on personal computers using various operating systems, procedures and tools for identifying and recovering deleted or destroyed information, and techniques for extracting and interpreting data for forensic purposes.

- The laboratory focuses on the security of networks involving personal computers or mobile devices, offering an introduction to methods for exploiting networks, traffic analysis, and endpoint security (physical devices that connect and exchange information with a computer network).
- The project gives students the opportunity to use various virtual machines to discover vulnerabilities within a network.

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	• Demonstrates knowledge of basic theoretical concepts and methods for securing personal computers and mobile terminals. • Applies theoretical knowledge in practice and uses virtual machines to simulate various vulnerabilities and countermeasures. • Utilizes standardized methods and tools specific to cybersecurity for evaluating and planning the security management process of stationary or portable personal computers, depending on the problems to be solved, and identifies solutions. • Coherently and correctly argues and analyzes the application context of basic cybersecurity knowledge, using key concepts and specific methodology. • Communicates effectively in Romanian, using the scientific vocabulary specific to the field studied, both in writing and orally. • Communicates in English, demonstrating correct understanding and application of relevant vocabulary in the studied field.
Transversal (General) Competences	• Communicates effectively, especially during application sessions, coordinating efforts with others to solve medium-complexity problems. • Autonomy and critical thinking: ability to think scientifically, search and analyze data independently, identify solutions, and present conclusions. • Analytical and synthetic skills: synthesizes knowledge obtained as a result of systematic analysis. • Respects academic ethical principles: correctly cites bibliographic sources used in documentation. • Demonstrates emotional intelligence in managing socio-emotional situations in academic life, showing self-control and objectivity in decision-making or stressful situations.

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.* • Defines basic concepts of personal computer security. • Appropriately describes the fundamental concepts related to vulnerabilities in the operation of personal computers or mobile devices. • Highlights testing and evaluation methods for personal computer security. • Understands the differences between various types of cyber vulnerabilities. • Defines and uses basic elements of data analysis and processing on personal computers to identify vulnerabilities. • Correctly uses the main methods for analyzing personal computer and mobile terminal security. • Understands basic concepts related to personal computer security analysis.
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).* • Selects and groups relevant information in a given context, describing both theoretical and practical aspects of cybersecurity. • Uses cybersecurity concepts to correctly address problems. • Experimentally verifies identified solutions to detect cyber vulnerabilities and proposes effective countermeasures. • Formulates correct conclusions based on conducted experiments. • Argues problem-solving methods and solutions used for addressing issues.
Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* • Selects and groups relevant information in a given context, describing both theoretical and practical aspects of cybersecurity. • Uses cybersecurity concepts to correctly address problems. • Experimentally verifies identified solutions to detect cyber vulnerabilities and proposes effective countermeasures. • Formulates correct conclusions based on conducted experiments. • Argues problem-solving methods and solutions used for addressing issues.

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.)*

Lectures are delivered in an interactive manner, encouraging active student participation. Both traditional teaching methods (lectures and presentations) using PowerPoint presentations through multimedia tools and interactive methods based on questions and answers are used, constantly adapting the teaching process to students' ability to assimilate and learn (with additional repetition of certain notions and concepts when necessary).

Each lecture begins with a brief review of previous chapters, with a focus on the concepts discussed in the last lecture. Presentations use many images and diagrams to make the presented information easier to understand and assimilate. Complete course materials are available electronically on the faculty's Moodle platform.

Teaching in laboratory hours is based on oral communication and a detailed explanation of the methods used and the results obtained, in a constantly interactive manner. Students implement and evaluate the same problems independently, using the computer, software environment, and hardware equipment (when applicable). Laboratory exercises help students develop optimal communication relationships in a discovery-based learning climate. Laboratory materials are available to students electronically on the Moodle platform.

Teaching project knowledge involves detailed discussions, providing specifications regarding the project's final goal and necessary context (specific programs), as well as guidelines for discovering solutions to the requested problems. Project materials are available electronically on the Moodle platform.

10. Contents

COURSE		
Chapter	**Content**	**No. hours**
1	rinciples and Security Problems of Personal Computers, Laptops, and Mobile Terminals: General concepts regarding the security of personal computers, laptops, and mobile terminals Vulnerabilities. Methods of detecting and preventing cyberattacks User accounts and passwords Security solutions for maintaining personal computers, laptops, and mobile terminals	4
2	Security Management of Personal Computers, Laptops, and Mobile Terminals: The security management process Security policy	2
3	Cyberattack Vectors: Viruses, worms, and other destructive agents Procedures for detecting and eliminating cyberattack vectors Penetration paths of cyberattack vectors: email services, web services, computer networks, personal computer interfaces Spyware and Adware Perimeter security of personal computers. Filters. Firewalls	6
4	Maintaining Personal Computers, Laptops, and Mobile Terminals: Standard maintenance procedures for personal computers, laptops, and mobile terminals Windows-specific procedures Linux-specific procedures Android/iOS-specific procedures	6
5	Advanced Security Resources: Data storage methods in personal computers, laptops, and mobile terminals using different operating systems Procedures and tools for identifying and recovering deleted or destroyed information Extracting and interpreting digital data for forensic purposes	6

6	Trends in Cyberattack Evolution and Cybersecurity Measures: Behavioral analysis of personal computers, laptops, and mobile terminals, and their data flows Using artificial intelligence to detect behavioral anomalies associated with personal computers, laptops, and mobile terminals	4
	Total:	28

Bibliography:

1. O. Fratu, Securitatea calculatorului personal și a terminalelor mobile, suport de curs electronic pe platforma Moodle a facultății de ETT
2. T. Bradley, H. Carvey, Essential Computer Security, Syngress Publishing Inc., Rockland, USA, 2006, ISBN 1- 59749-114-4.
3. K. Fung, Network Security Technologies, 2nd Edition, Auerbach Publications, Boca Raton, USA, 2005, ISBN 0-8493-3027-0.
4. A. Earle, Wireless Security Handbook, Auerbach Publications, Boca Raton, USA, 2006, ISBN 0-8493-3378-4.
5. W. Stallings, L. Brown, Computer Security. Principles and Practice, Prentice Hall, 2008.

LABORATORY

Crt. no.	Content	No. hours
1	Work Safety. Introduction to Network Exploitation Describes how computers interact and communicate with each other. Introduces basic concepts of computer networks, followed by the methodology and tools required to attack various network services.	4
2	Network Security and Traffic Analysis Discusses basic concepts of network security and traffic analysis to identify and investigate network anomalies.	4
3	Endpoint Security Analyzes methods for monitoring the activity of personal computers.	2
4	Security Information and Event Management (SIEM) Analyzes the operation of a SIEM system and the creation of simple and advanced queries to search for specific answers from the logs of this system.	4
	Total:	14

Bibliography:
1. R. Craciunescu, Securitatea calculatorului personal și a terminalelor mobile, suport de laborator electronic pe platforma Moodle a facultății de ETT
2. T. Bradley, H. Carvey, Essential Computer Security, Syngress Publishing Inc., Rockland, USA, 2006, ISBN 1- 59749-114-4.
3. K. Fung, Network Security Technologies, 2nd Edition, Auerbach Publications, Boca Raton, USA, 2005, ISBN 0-8493-3027-0.
4. A. Earle, Wireless Security Handbook, Auerbach Publications, Boca Raton, USA, 2006, ISBN 0-8493-3378-4.
5. W. Stallings, L. Brown, Computer Security. Principles and Practice, Prentice Hall, 2008.

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade
11.4 Course	Understanding fundamental theoretical concepts related to personal computer security. Understanding how to apply theory to solve specific domain problems.	Written exam	50%
11.5 Seminary/laboratory/project	Understanding fundamental techniques for analyzing and processing vulnerabilities in personal computers or networks. Understanding how to simulate and implement (on a computer) the studied methods using specific programs.	Laboratory report for each laboratory session	50%
11.6 Passing conditions			
• Achieving 50% of the total score. • Fulfilling laboratory/project obligations (participation in scheduled sessions).			

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)

In the context of accelerated digitalization and increasingly sophisticated cyberattacks, there is growing demand in the job market for advanced information security skills. Employers and professional associations emphasize the need for graduates to have a solid understanding of network security, vulnerability management, cryptography, and related legislation. By covering a wide range of topics, from basic principles to advanced security management, the course addresses these needs.

The alignment with the European Higher Education Area (EHEA) standards ensures the quality of education and the international recognition of competencies, preparing students for the global job market and cybersecurity challenges. Graduates of this master's program will have the necessary skills to meet current qualification requirements, along with a modern, high-quality scientific and technical education that will enable quick employment after graduation. The course fits perfectly into the policy of the National University of Science and Technology POLITEHNICA Bucharest in terms of content, structure, and the international openness offered to students. Potential employers include both academic environments

(teaching and research profiles) and research and development environments in state and private institutions that use computer networks, personal computers, and various mobile terminals and are interested in managing their security or offering advanced local or network-level security services.

Date	Course lecturer	Instructor(s) for practical activities
01.10.2024	Prof. Dr. Ing. Octavian Fratu	Conf. Dr. Razvan Craciunescu

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