Syllabus

Course Description

Course Title	Network Security
Course Code	76264
Course Title Additional	
Scientific-Disciplinary Sector	
Language	Italian
Degree Course	Bachelor in Computer Science
Other Degree Courses (Loaned)	
Lecturers	Prof. Fabrizio Maria Maggi, maggi@inf.unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/41895 dr. Florian Hofer, Florian.Hofer@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/37220
Teaching Assistant	
Semester	First semester
Course Year/s	3
CP	12
Teaching Hours	80
Lab Hours	40
Individual Study Hours	180
Planned Office Hours	36
Contents Summary	Module 1: Computer Networks • Introduction to computer networks • ISO OSI reference model • Internet applications and application protocols (HTTP, SMTP, DNS) • Network protocols: TCP/IP, Ethernet • Sockets and RPCs

	• Failure robustness, security Module 2: Information Security • Basic definitions: CIA, threat, attack, vulnerability, access control • Risk assessment • Basics of cryptography • Network attack and defense • Usability • Security policies
Course Topics	Module 1: Computer Networks This course provides a solid background in computer networks. Theory will be intertwined with discussions of how the introduced concepts are used in practice, using the Java framework as a reference. This will show why distributed systems matter in real contexts. Module 2: Information Security The course introduces the fundamental concepts of computer and network security, outlining the main threats and strategies for protecting data, applications, and infrastructure. It begins with an overview of key concepts in system and network security, highlighting the principles of information confidentiality, integrity, and availability, as well as authentication, authorization, and accountability. It also introduces a range of cyber threats, including viruses, worms, Trojans, ransomware, and spyware, explaining how they can compromise data and system security. The course then explores the basic mechanisms of cryptography. It explains the differences between symmetric and asymmetric cryptography, key management methods, and the use of digital signatures to ensure data authenticity and integrity. It also covers hashing, the properties of hash functions, and issues related to collisions. In addition, the course describes methods for secure key exchange and practical applications of digital certificates. Another focus of the course is web application security. Common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), are analyzed, with explanations of how attackers can exploit them. The role of cookies in web application security is described in detail. Software security is also discussed, including buffer overflow vulnerabilities and the main strategies for

	preventing them. The course covers security device architectures and related infrastructure, describing firewalls, intrusion detection and prevention systems (IDS/IPS), proxies, and other devices. It also explores the role of public key infrastructures (PKI) and digital certificates in ensuring authenticity in digital communications. A dedicated module focuses on network security, with particular attention to secure communication protocols, access control, network segmentation, and techniques for protecting against eavesdropping. Threats such as ARP poisoning, DNS poisoning, and man-in-the-middle attacks are presented alongside countermeasures to mitigate them. Finally, the course focuses on risk management and resilience strategies. Topics include risk assessment, threat analysis, and the development of security policies and mitigation plans. Concepts such as redundancy, fault tolerance, backup systems, and disaster recovery are explored in depth.
Keywords	Module 1: Computer Networks Internet, TCP/IP, Networks, Protocols Module 2: Information Security Cryptography, Web Application Security, Software Security, Network Security, Risk Management
Recommended Prerequisites	Module 1: Computer Networks The course requires basic knowledge of data structures and algorithms, as well as foundational Java programming skills. Module 2: Information Security Students should be familiar with basic programming concepts, data structures and algorithms.
Propaedeutic Courses	
Teaching Format	Module 1: Computer Networks The course includes frontal lectures and lab exercises. Module 2: Information Security Frontal classroom lectures and lab sessions.
Mandatory Attendance	Attendance is not mandatory but strongly recommended. Non-attending students should contact the lecturer at the start of the course to agree on the modalities of the independent study.

Specific Educational Objectives and Learning Outcomes	Knowledge and understanding - D1.11 Know in detail the principles of computer networks and distributed systems - D.12 know in detail the internet fundamental principles and the methodologies for their design and development. - D1.14 Know critical security aspects of information systems, the basic concepts of security and techniques for the development of secure systems. Applying knowledge and understanding - D2.09 Be able to plan and program in distributed programming environments and in digital networks. - D2.11 Be able to evaluate the quality of information systems and to identify critical aspects. - D2.17 Ability to analyse and improve data privacy and data security features in the context of complex software infrastructures. - D2.19 Be able to apply the own knowledge in different working contexts. Making judgements - D3.1 Be able to collect and interpret useful data and to judge information systems and their applicability. - D3.2 Be able to work autonomously according to the own level of knowledge and understanding. Communication skills - D4.1 Be able to use one of the three languages English, Italian and German, and be able to use technical terms and communication appropriately. - D4.2 Be able to use modern communication systems, even at a distance. - D4.5 Be able to work in teams for the realization of IT systems. Learning skills: - D5.1: Have developed learning capabilities to pursue further studies with a high degree of autonomy. - D5.3: Be able to follow the fast technological evolution and to learn cutting edge IT technologies and innovative aspects of last generation information systems.

Specific Educational Objectives and Learning Outcomes (additional info.)	
Assessment	Module 1: Computer Networks The assessment consists of an oral exam (D1.11, D1.12, D4.1, D5.1, D5.3) and lab reports, which contain practical excercises (D1.11, D1.12, D2.9, D4.1, D4.2) and project work (D2.9, D3.1, D3.2, D4.2, D5.1). Module 2: Information Security - Project work to test knowledge application skills - Oral exam with verification questions and discussion of the project
Evaluation Criteria	Module 1: Computer Networks Marks are distributed as follows: 30% for the lab reports and 70% for the oral exam. Attending the lab is not mandatory but is recommended, as it can help improve the oral exam grade. Module 2: Information Security Assessment 1: project work (30%) Assessment 2: oral exam (70%) A passing grade on the project is a prerequisite for taking the oral exam, as the oral exam begins with a discussion of the project. Relevant for assessment 1: skills in applying knowledge in a practical setting, ability to summarize in your own words, ability to explain things balancing conciseness and completeness. Relevant for assessment 2: clarity of answers, ability to recall principles and methods used in information security, skill in applying knowledge about information security.
Required Readings	Module 1: Computer Networks James Kurose e Keith Ross. Computer Networking: A Top-Down Approach. Pearson, Boston Munich, 7ª edizione, aprile 2016. ISBN 978-0-13-359414-0.

	Module 2: Information Security CompTIA Security+ Guide to Network Security Fundamentals 6thEdition, Mark Ciampa ISBN 978-1337288781 Material provided in the form of slides and scientific papers provided by the teacher.
Supplementary Readings	Module 1: Computer Networks Andrew Tanenbaum e David Wetherall. Reti di computer. Pearson, Boston, 5a edizione, settembre 2010. ISBN 978-0-13-212695-3. Andrew S. Tanenbaum e Maarten van Steen. Sistemi distribuiti: Principles and Paradigms. CreateSpace Independent Publishing Platform, Paesi Bassi, 2a edizione, febbraio 2016. ISBN 978-1-5302-8175-6 Module 2: Information Security Computer & Internet Security: A Hands-on Approach 3a Edizione ISBN: 978-17330039-4-0 Computer Security: A Hands-on Approach 3a edizione ISBN: 978-17330039-5-7
Further Information	Module 1: Computer Networks Software used: Wireshark (https://www.wireshark.org) Java (https://openjdk.org) *nix tools (*sh, *ssh, iproute2, dig, tracepath..) Module 2: Information Security Software used: Provided by teacher during lectures/lab sessions
Sustainable Development Goals (SDGs)	Quality education

Course Module

Course Constituent Title	Computer Networks
Course Code	76264A
Scientific-Disciplinary Sector	IINF-05/A
Language	Italian
Lecturers	dr. Florian Hofer, Florian.Hofer@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/37220
Teaching Assistant	
Semester	First semester
CP	6
Responsible Lecturer	
Teaching Hours	40
Lab Hours	20
Individual Study Hours	90
Planned Office Hours	18
Contents Summary	• Introduction to computer networks • ISO OSI reference model • Internet applications and application protocols (HTTP, SMTP, DNS) • Network protocols: TCP/IP, Ethernet • Sockets and RPCs • Failure robustness, security
Course Topics	This course aims at providing a solid background in computer networks. Theory will be intertwined with discussions about how the notions introduced are exploited in practice, taking the Java framework as reference. This will allow to see in real contexts why distributed systems are important.
Teaching Format	The course includes frontal lectures and lab exercises. Software used: Wireshark (https://www.wireshark.org) Java (https://openjdk.org) *nix tools (*sh, *ssh, iproute2, dig, tracepath..)

Required Readings	James Kurose and Keith Ross. Computer Networking: A Top-Down Approach. Pearson, Boston Munich, 7th edition, April 2016. ISBN 978-0-13-359414-0.
Supplementary Readings	Andrew S. Tanenbaum and Maarten van Steen. Distributed Systems: Principles and Paradigms. CreateSpace Independent Publishing Platform, The Netherlands?, 2nd edition, February 2016. ISBN 978-1-5302-8175-6

Course Module

Course Constituent Title	Information Security
Course Code	76264B
Scientific-Disciplinary Sector	IINF-05/A
Language	Italian
Lecturers	Prof. Fabrizio Maria Maggi, maggi@inf.unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/41895
Teaching Assistant	
Semester	First semester
CP	6
Responsible Lecturer	
Teaching Hours	40
Lab Hours	20
Individual Study Hours	90
Planned Office Hours	18
Contents Summary	• Basic definitions: CIA, threat, attack, vulnerability, access control • Risk assessment • Basics of cryptography • Network attack and defense • Usability • Security policies
Course Topics	The course introduces the fundamental concepts related to the security of computer systems and networks, illustrating the main threats and strategies to protect data, applications, and

	infrastructures. The instruction begins with an overview of the key concepts in system and network security, highlighting the principles of confidentiality, integrity, and availability of information, as well as the concepts of authentication, authorization, and accountability. The course also presents the variety of cyber threats, including viruses, worms, trojans, ransomware, and spyware, and explains how these can compromise the security of data and systems. Subsequently, the course delves into the basic mechanisms of cryptography. It explains the differences between symmetric and asymmetric cryptography, methods for key management, and the use of digital signatures to ensure data authenticity and integrity. The concept of hashing is also addressed, including the properties of hash functions and the issues related to collisions. Additionally, the course describes methods for secure key exchange and practical applications of digital certificates. Another focus of the course is web application security. The most common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), are analyzed, explaining how attackers can exploit them. Software security is discussed, including issues related to buffer overflows, and the main strategies to prevent such vulnerabilities are illustrated. The course also covers the architectures of security devices and related infrastructures. Firewalls, intrusion detection and prevention systems (IDS/IPS), proxies, and other devices are described. The role of public key infrastructures (PKI) and digital certificates is examined in depth, as they are essential for ensuring authenticity in digital communication. A specific module is dedicated to network security, with particular attention to secure communication protocols, access control, network segmentation, and techniques for protecting against interception. Threats such as ARP poisoning, DNS poisoning, and man-in-the-middle attacks are illustrated, along with countermeasures to mitigate them. Finally, the course focuses on risk management and resilience

	strategies. Topics include risk assessment, threat analysis, the definition of security policies, and mitigation plans. Concepts such as redundancy, fault tolerance, backup systems, and disaster recovery are explored in detail.
Teaching Format	Frontal lectures and Laboratories
Required Readings	CompTIA Security+ Guide to Network Security Fundamentals 6thEdition, Mark Ciampa ISBN 978-1337288781 Material provided in the form of slides and scientific papers provided by the teacher.
Supplementary Readings	Computer & Internet Security: A Hands-on Approach 3a Edizione ISBN: 978-17330039-4-0 Computer Security: A Hands-on Approach 3a edizione ISBN: 978-17330039-5-7 Internet Security: A Hands-on Approach 3a edizione ISBN: 978-17330039-6-4