

Syllabus

Kursbeschreibung

Titel der Lehrveranstaltung	Software and Systems Security
Code der Lehrveranstaltung	76097
Zusätzlicher Titel der Lehrveranstaltung	
Wissenschaftlich-disziplinärer Bereich	IINF-05/A
Sprache	Englisch
Studiengang	Master in Software Engineering
Andere Studiengänge (gem. Lehrveranstaltung)	
Dozenten/Dozentinnen	Prof. Barbara Russo, Barbara.Russo@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/2242 Dott. Diaeddin M A Rimawi, Diaeddin.Rimawi@unibz.it https://www.unibz.it/en/faculties/engineering/academic-staff/person/46519
Wissensch. Mitarbeiter/Mitarbeiterin	
Semester	Erstes Semester
Studienjahr/e	2
KP	6
Vorlesungsstunden	40
Laboratoriumsstunden	20
Stunden für individuelles Studium	90
Vorgesehene Sprechzeiten	18
Inhaltsangabe	<ul style="list-style-type: none"> - Computer Security Technology and Principles - Data security - Software and Network Security and Trusted Systems

	<ul style="list-style-type: none"> - Social security - System Vulnerabilities and Attacks - Security Management
Themen der Lehrveranstaltung	<p>The Software and Systems Security course provides students with a comprehensive understanding of the principles, technologies, and practices required to protect software, systems, networks, and data against evolving cyber threats. The course covers the foundations of computer security, including confidentiality, integrity, availability, authentication, access control, and cryptographic techniques, as well as methods for securing data throughout its lifecycle. Students explore secure software development, network security, trusted systems, and the identification and mitigation of system vulnerabilities and cyberattacks. The course also examines the human dimension of cybersecurity, including social engineering, security awareness, and organizational security policies, together with the principles of security management, risk assessment, incident response, and regulatory compliance. Special attention is given to the growing role of Artificial Intelligence in cybersecurity, examining how AI and machine learning can enhance threat detection, anomaly detection, malware analysis, automated incident response, and vulnerability management, while also addressing the security and privacy challenges introduced by AI systems, such as adversarial attacks, model robustness, and the secure deployment of AI-enabled applications.</p>
Stichwörter	<p> Cybersecurity Network Security System security Software security Data Security AI and Cybersecurity </p>
Empfohlene Voraussetzungen	<p> Computer system architecture Python programming also AI-assisted </p>
Propädeutische Lehrveranstaltungen	
Unterrichtsform	<p>Frontal lectures and lab assignments</p>
Anwesenheitspflicht	<p>Not compulsory, but recommended especially for the labs. Non-attending students must contact the lecturer at the start of the</p>

	course to agree on the modalities of the independent study.
Spezifische Bildungsziele und erwartete Lernergebnisse	<p>Knowledge and Understanding:</p> <ul style="list-style-type: none"> - D1.1 possess solid knowledge of both the fundamentals and the application aspects of the various fundamental areas of computer science; - D1.4 have an in-depth knowledge of the principles, structures and use of processing systems for the automation of software systems <p>Applying knowledge and understanding:</p> <ul style="list-style-type: none"> - D2.1 know how to apply the fundamentals of empirical analysis of ICT data for the construction of mathematical models for the evaluation and prediction of characteristics of applications and software systems; <p>Making judgments:</p> <ul style="list-style-type: none"> - D3.2 ability to plan and re-plan a technical project activity and to carry it out within the defined deadlines and objectives; <p>Communication skills:</p> <ul style="list-style-type: none"> - D4.1 ability to present the contents of a scientific/technical report in a set time in front of an audience, including non-specialists; - D4.4 ability to prepare and deliver presentations with technical content in English; <p>Learning skills:</p> <ul style="list-style-type: none"> - D5.2 ability to independently keep up to date with developments in the most important fields of information technology;
Spezifisches Bildungsziel und erwartete Lernergebnisse (zusätzliche Informationen)	
Art der Prüfung	Final grade: 50% project work and 50% written exam
Bewertungskriterien	<p>Lab assessment must be positive (i.e., 18 or higher) to access the written exam.</p> <p>Relevant for the assessment:</p> <p>Lab assessment: ability to apply in autonomy and develop further instruments introduced during the lectures/labs and needed to</p>

	<p>accomplish tasks and perform little studies with data. Ability to report in a professional manner also using the appropriate terminology and concepts of the course.</p> <p>Written exam: being able to master the terminology of the course; being able to evaluate tools and techniques and their technical details for specific domain of use; being able to solve exercises or summarize theoretical concepts.</p>
Pflichtliteratur	<p>Ross Anderson, Security Engineering, Editore: Wiley, ISBN: 0-471-38922-6 http://www.cl.cam.ac.uk/~rja14/book.html</p> <p>Paul C. van Oorschot Computer Security and the Internet: Tools and Jewels https://people.scs.carleton.ca/~paulv/toolsjewels.html</p> <p>William Stallings Lawrie Brown Computer Security Principles and Practice, 5th edition Published by Pearson (July 28, 2023) © 2024</p> <p>Dafydd Stuttard, Marcus Pinto The web application hacker's handbook: discovering and exploiting security flaws. John Wiley & Sons, Inc., USA.</p> <p>Dieter Gollmann Computer Security John Wiley & Sons Inc</p>
Weiterführende Literatur	<p>Supplementary readings will be given during the lectures</p>
Weitere Informationen	<p>Software used: Python, Ollama and open source models for prompt engineering</p>
Ziele für nachhaltige Entwicklung (SDGs)	<p>Nachhaltiger Konsum und Produktion, Industrie, Innovation und Infrastruktur</p>