MODELLO D (inglese)	
General Information	
Academic subject	IoT Security
Degree course	Master Degree (MSc) in Computer Science (LM18)
Curriculum	Security Engineering
ECTS credits	6
Compulsory attendance	No, but attendance is strongly recommended
Language	English

Subject teacher	Name Surname	Mail address	SSD
	Giuseppe Desolda	giuseppe.desolda@uniba.it	INF/01
	Antonio Piccinno	antonio.piccinno@uniba.it	INF/01

ECTS credits details			
Basic teaching activities	Lectures Guided exercises	4 T1 credits 2 T2 credits	

Class schedule	
Period	2nd semester
Year	1st year
Type of class	Lecture - workshops

Time management	
Hours	62
Hours of lectures	32 (4 credits)
Tutorials and lab	30 (2 credits)

Academic calendar	
Class begins	1st March 2021
Class ends	4th June 2021

Syllabus	
Prerequisites/requirements	Formal prerequisites: none Cultural prerequisites: knowledge of networking and distributed system concepts (necessary), knowledge of a programming language (relevant), first year first semester courses.
Expected learning outcomes (according to Dublin Descriptors) (it is recommended that they are congruent with the learning outcomes contained in A4a, A4b, A4c tables of the SUA-CdS)	*Knowledge and understanding* The course is about the new paradigm of objects interacting with people, with information systems, and with other objects, the technology used to build these kinds of devices, how they communicate, how they store data, and the kinds of distributed systems needed to support them. Because of the widespread of IoT technologies rising the IoT to one of the most popular tech trends, manufacturers need to take the necessary steps to secure devices and protect them from attackers. The course will focus on creative thinking and hands-on project development. The students will learn about IoT concepts and standards; components of an IoT System; IoT Applications and examples of IoT solutions; challenges in IoT implementation, mainly on how IoT devices can be built and IoT systems can be developed securely. The course does not have the intention of being a comprehensive course about the technologies involved in IoT security. The focus will be more on the possibilities and threats offered by the

	different technologies, and on the creative thinking techniques to find innovative and secure applications of combinations of such technologies in real-life scenarios. The students will learn how to define a threat model of a real-world IoT device and how to locate all possible attacker entry points by taking a practitioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. *Applying knowledge and understanding* Acquisition of the necessary skills to solve problems in new or unfamiliar areas regarding issues related to IoT ecosystems, with emphasis on cybersecurity aspects. The course is supported by real-world case studies and the contents ideal for developers who will build the IoT (secure) solutions of the future. *Making informed judgments and choices* Integration of the knowledge acquired in the curriculum to manage complex problems also on the basis of limited and incomplete information. Acquiring autonomy of judgment with respect to the ethical implications and professional responsibilities of IT practice. *Communicating knowledge and understanding* Ability to communicate the results obtained to specialist and non-specialist interlocutors, as well as the development of collaborative skills that are indispensable for teamwork. *Capacities to continue learning* In order to stimulate the ability to learn autonomously, students are recommended, in addition to the main didactic material, other bibliographic sources to expand some specific topics not covered in detail by the teacher. The student must then prepare a presentation of the assigned topic to be illustrated to the teacher and the other students in the class.
Contents	**Course Syllabus** • Introduction to the IoT course and to the Pervasive Computing • Advanced concepts on Pervasive Computing • Foundamentals on Internet of Things technologies • Arduino programming • IoT and Usable Security • Penetration test • IoT protocols (e.g., MQTT, AMQP) • Publish–subscribe architecture • Creation of a prototype of an IoT banking system
Course program	
Bibliography	• Mala, D. Jeya, ed. *Integrating the Internet of Things into software engineering practices*. IGI Global, 2019. • Boxall, J. 2013. Arduino Workshop: A Hands-On Introduction With 65 Projects. No Starch Press - 392 pages • Gupta, A. (2019). *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*. Apress.

	• The IoT course — Internet of Things @ WiLMALab, Department of Computer Science and Engineering • The Internet of Things. The MIT Press (https://mitpress.mit.edu/books/internet-things) • Nurse, J.R.C., Atamli-Reineh, A., and Martin, A.P. 2016. ‘Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home’. Proc. HCI2016
Notes	Bibliography will be integrated with the slides available on the e-learning platform.
Teaching methods	Lectures and tutorials supported by slides and demos. During the practice lessons students will use and implement IoT systems and security aspects like defensive mechanisms and penetration tests.
Assessment methods (indicate at least the type written, oral, other)	The learning assessment will already begin during the laboratory lessons. Lab assessment: - tasks assigned and supervised by the lecturer (for students regularly attending the course) - implementation of an IoT environment and its security aspects assigned by the lecturer (for students not regularly attending the course) Oral assessment: - oral presentation of the case study assigned during the lessons, including questions about the course program (for all students)
Evaluation criteria (Explain for each expected learning outcome what a student has to know, or is able to do, and how many levels of achievement there are.	The students should know the concepts presented and discussed during classes and be familiar with the tools introduced in the tutorials and lab sessions. The score of the exam is given by means of a mark in 30th. The oral examination accounts for 60% of the score, the discussion of the Lab work accounts for about 30% of the final grade, the active participation of students in frontal and online activities will be about 10% of the final grade.
Further information	