DEREE COLLEGE SYLLABUS FOR:

ITC 3632 SECURITY OF WIRELESS, IoT, AND MOBILE NETWORKS **3/0/3**
(Fall 2020)
UK LEVEL: 5
UK CREDITS: 15

PREREQUISITES:	ITC 2024 Computer Networks & Cybersecurity Fundamentals ITC 2088 Introduction to Programming ITC 2101 Principles of Wireless, IoT, and Mobile Networks ITC 3006 Mathematics for Computing MA 2010 Statistics I ***or*** MA 2021 Applied Statistics for Business ***or*** MA 2025 Applied Statistics for Science
COREQUISITES:	ITC 3431 Cryptography and Network Security
CATALOG DESCRIPTION:	Security challenges in wireless, mobile and IoT networks; Interference and jamming in wireless systems; 802.11 Authentication and Key Management; WEP, WAP functions, protocols and configurations for realizing authentication, key distribution, integrity, confidentiality and anonymity in wireless access networks for mobile users. Authentication and confidentiality in 4G mobile telephony systems. Identity and Access Management (IAM) for the Internet of Things.
RATIONALE:	The course exposes the students to the main security challenges of wireless and mobile networks, as well as, the corresponding solutions.
LEARNING OUTCOMES:	As a result of taking this course, the student should be able to: 1. Explain the threats for mobile users and operators and the corresponding security needs. 2. Examine wireless and IoT protocols in terms of the level of security, effectiveness and complexity. 3. Compare the security mechanisms and protocols in popular wireless communication systems and IoT.
METHOD OF TEACHING AND LEARNING:	In congruence with the teaching and learning strategy of the college, the following tools are used: • Classroom lectures, laboratory practical sessions using various simulations tools and progress meetings. • Office hours held by the instructor to provide further assistance to students. • Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources.
ASSESSMENT:	**Summative**:

1st assessment: Midterm Exam Short essay questions and case problems.	**30%**
2nd assessment: Portfolio of student work, including project progress and oral assessment (not eligible for 2nd marking)	**10%**
Final assessment: Individual Project literature review, design, implementation (code, script or simulation)	**60%**

	Formative: Take-home short problems **0%** The formative assessments aim to shape teaching and prepare students for the summative assessments. The 1st summative assessment tests the LOs 1 and 2. The 2nd summative assessment tests the LOs 1-3. The final summative assessment tests the LOs 1-3. *The final assessment tests all learning outcomes of this module, therefore students pass the module if the average module grade is 40% or higher.*
INDICATIVE READING:	**REQUIRED READING:** W. Osterhage, *Wireless Network Security*, CRC Press, 2nd edition, 2018, ISBN-10: 1138093793, ISBN-13: 978-1138093799 **RECOMMENDED READING:** 1. R. Meyers, *Wireless Network Security: Introduction and Explanation of Cybersecurity and Hacking Technology for Wireless System, Kali Linux Tools and Other,* independently published, 2019. 2. R. Meyers, *Linux for Hackers: A Complete Step-by-Step Guide to Hacking Wireless Network Security and Server Database with Technology Ecosystem Linux*, independently published, 2019. 3. P. Lea, *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security*, 1st edition, Packt Publishing, 2018. 4. C. Buchanan & V. Ramachandran, *Kali Linux Wireless Penetration Testing Beginner's Guide - Third Edition: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack*, 3rd Revised edition, Packt Publishing, 2017. 5. J. Wright & J. Cache, *Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions*, McGraw-Hill Education; 3rd edition, 2015. 6. R. K. Nichols, P. C. Lekkas, *Wireless Security: Models, Threats, and Solutions: Models, Threats and Solutions, 1st Edition*, 2001, McGraw-Hill Telecom Professional. ISBN-10: 0071380388, ISBN-13: 978-0071380386
INDICATIVE MATERIAL: *(e.g. audiovisual, digital material, etc.)*	**REQUIRED MATERIAL**: N/A **RECOMMENDED MATERIAL:** N/A
COMMUNICATION REQUIREMENTS:	Daily access to the course's site on the College's Blackboard CMS. Communication using proper written and oral English. Use of word processing and presentation graphics SW for documentation and presentation of deliverables and the final project.
SOFTWARE REQUIREMENTS:	MS-Office, MS-Visio Python Kali Linux Virtual Machines, VMWare Aircrack-ng Wireshark

HARDWARE REQUIREMENTS:	Isolated WiFi access points. Desktops/laptops with sniffing network cards. Small IoT platforms.
WWW RESOURCES:	• http://wireless.csail.mit.edu/ • https://lids.mit.edu/labs-and-groups/wireless-information-and-network-sciences-laboratory-winslab • https://ieeeaccess.ieee.org/ • https://people.eecs.berkeley.edu/~daw/research/wireless.html • http://mydecamp.eu/ • https://www.cybrary.it/ • https://resources.infosecinstitute.com/category/wireless-security/#gref • http://icsdweb.aegean.gr/awid/ • https://www.nsf.gov/awardsearch/showAward?AWD_ID=1829553 • https://www.lifewire.com/ • https://www.rfwireless-world.com/
INDICATIVE CONTENT:	1. Review of the fundamentals of Wireless & Mobile Systems 2. Threats and vulnerabilities of wireless and mobile networks 3. Security standards of current wireless and mobile networks 4. Common attacks against wireless networks 5. Privacy concerns: location, tracking, traffic analysis.