Course Title	**Network and System Security**				
Course Code	**DLWSS533**				
Course Type	**Elective**				
Level	Master (2nd Cycle) – Distance Learning				
Semester	2 or 3				
Teacher's Name	**Chrysostomos Chrysostomou, PhD**				
ECTS	10	Lectures / week	3	Laboratories / week	0
Course Purpose	The aim of the course is to enable students develop the skills required for examining and analysing security challenges in wireless and mobile systems and expose students to security issues in web applications. The course covers the operation of security mechanisms in wireless mobile networks and investigates various security protocols. Emphasis is also given on web application security challenges through the analysis of attacks and their countermeasures.				
Learning Outcomes	By the end of the course, the students are expected to: 1. define and examine the underlying principles of network security in wireless technologies; 2. identify and illustrate the operation of cryptographic algorithms and protocols underlying network security applications in mobile systems; 3. develop the ability to design and analyze authentication protocols; 4. outline and assess the issue of key management and routing in mobile wireless networks; 5. describe, analyze and evaluate the current Web technologies security mechanisms, their attacks and countermeasures; 6. develop sufficient knowledge to protect Web applications; 7. perform research literature review and apply appropriate methods to pursue research or other detailed investigation of technical issues, and present, explain and report on the state of the art on specific security topics.				
Prerequisites	WSS501	Required	None		
Course Content	• **Introduction to Security:** Security properties. Attacks and threats categories. Security design at various network layers. • **Cryptography:** Symmetric and asymmetric encryption. Secure hash functions. Digital signatures. Key management. • **Access control:** Authentication. Design of authentication protocols, applications (Kerberos, public key infrastructure), certificates management, CRLs management, authorization. • **Web application security:** Web Security (Secure Socket Layer (SSL) and Transport Layer Security (TLS)). Open Web Application Security Project (OWASP). Top 10 attacks and countermeasures.				

	• **802.11 (Wi–Fi) Security:** WPA and 802.11i (WPA, EAP, RADIUS). 802.1x protocol packet structure and operation. • **Security in wireless networks:** Security in WPAN (802.15 / Bluetooth). Secure routing, Key management and Secure data propagation in Ad Hoc networks and wireless sensor networks. • **State of the art and Future Developments:** Thwarting malicious and selfish behaviour in wireless environments. Key Management protocols over wireless devices (WPA/RSN, TKIP, AES–CCMP).
Teaching Methodology	**Mode of Delivery: Distance Learning** The course is designed to introduce and explain the material students are expected to learn through an on-line learning environment. The on-line environment provides an opportunity for receiving on-line feedback from the Course Instructor during their study. In addition, students will be encouraged to interact both with other students and the instructor so as to feel part of an on-line community of learners that belong to the University network. The course content will be delivered through online material/notes, recorded lectures and/or narrated presentations. Therefore, students may be asked to download and study notes, tutorials and numerical exercises as well as watch recorded lectures/demonstrations or narrated presentations posted on the web addressing the main concepts of a particular unit. Furthermore, the planned communication and the dynamic/online interaction activities between the course instructor and the students will include asynchronous communication tools (Discussion Forum) that students may be asked to participate, wherever appropriate, in an online forum posting their views on certain topics covered in a particular unit; and synchronous communication tools (instant messaging, such as Skype, chat rooms, video-conferencing, etc.), that students may discuss on-line with the Instructor (s) and/or other students specific issues covered in a given unit. Moreover, a number of case study readings are also considered to illustrate that what students have studied in each unit is not just of academic or theoretical value but also has value in terms of improving real-life challenges.
Bibliography	Textbook: • W. Stallings, ***Cryptography and Network Security: Principles and Practice*** - Pearson, 7th Ed., 2017 [paper format] - Pearson, 8th Ed., 2020 [eText format] References: • Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, ***Security in Computing***, Prentice Hall, 5th Ed., 2015 • W. Stallings, ***Network Security Essentials: Applications and Standards***, Pearson, 6th Ed., 2017 • Levente Buttyan and Jean-Pierre Hubaux, ***Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing***, Cambridge University Press, 2007

	• Relevant academic research articles in the literature
Assessment	The Students are assessed via continuous assessment throughout the duration of the Semester, which forms the Coursework grade and the final written exam. The coursework and the final exam grades are weighted 50% and 50%, respectively, and compose the final grade of the course. Various approaches are used for the continuous assessment of the students, such as dynamic online activities, online quizzes, group project design, implementation and presentation. The assessment weight, date and time of each type of continuous assessment is being set at the beginning of the semester via the course outline. An indicative weighted continuous assessment of the course is shown below: • **An online quiz** (15% of total marks for module) • **One marked assignment/project** (15% of total marks for module) • **Presentation of project** (10% of total marks for module) • **Two dynamic interactive activities** (10% of total marks for module) • **One closed-book, 3-hour exam** (50% of total marks for module) Students are prepared for final exam, by revision on the matter taught, problem solving and concept testing and are also trained to be able to deal with time constrains and revision timetable. The criteria considered for the assessment of each type of the continuous assessment and the final exam of the course are: (i) the comprehension of the fundamental concepts and theory of each topic, (ii) the application of the theory in solving related problems and (iii) the ability to apply the above knowledge in complex real-life problems. The final assessment of the students is formative and summative and is assured to comply with the subject's expected learning outcomes and the quality of the course.
Language	English