Course Title	Network and System Security				
Course Code	WSS533				
Course Type	Specialization (Elective)				
Level	Master (2nd Cycle)				
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	Students are taught the course through lectures by means of computer presentations. Lectures are integrated by invited talks from experts from industry. Guided individual and/or group project is given to enable students apply their gained knowledge and identify the principles taught in the lecture sessions. The course also utilizes research literature review allowing students to gain knowledge on the state of the art on specific security topics; thus, encouraging students to identify a specific problem related to some possible open research issues, gather relevant scientific information about how others have addressed the problem, investigate/analyze/evaluate and compose this information in written and/or orally. Lecture notes and presentations are available for students to use in combination with the textbooks and references, through the university's e-learning platform.
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 assessment of the course includes a final written exam, an individual and/or group project and research literature review. The weights for each assessment component are: • Research Literature Review: 25% • Project Work: 35% • Final Exam: 40%
Language	English