

Course unit title:	Network and System Security		
Course unit code:	WSS533		
Type of course unit:	Elective		
Level of course unit:	Master		
Year of study:			
Semester when the unit is delivered:			
Number of ECTS credits allocated :	10		
Name of lecturer(s):	Dr George Hadjichristofi		
Aim of the Course	The aim of the course is to explore security challenges in wireless and mobile systems and expose students to security issues in web applications. The course will cover the operation of security mechanisms in wireless mobile networks, and investigate various security protocols. Emphasis is also given on web application security challenges through the analysis of attacks and their countermeasures.		
Learning outcomes of the course unit:	<ul style="list-style-type: none"> • Explain the underlying principles of network security in wireless technologies • Describe the operation of cryptographic algorithms and protocols underlying network security applications in mobile systems • Develop the ability to design and analyze authentication protocols • Discuss the issue of key management and routing in mobile wireless networks • Describe the current Web technologies security mechanisms, their attacks and countermeasures • Develop sufficient knowledge to protect Web applications 		
Mode of delivery:	Face-to-face		
Prerequisites:	None	Co-requisites:	None
Recommended optional program components:	None		
Course contents:	<ul style="list-style-type: none"> • Overview of security threats and problems • 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) 		

	<ul style="list-style-type: none"> • Understand 802.1x protocol packet structure and operation • Security in wireless networks: <ul style="list-style-type: none"> • Security in WPAN (802.15 / Bluetooth) • Security mechanisms in GSM, 3G, UMTS • Ad Hoc networks and wireless sensor networks <ul style="list-style-type: none"> ○ Secure routing ○ Key management ○ Secure data propagation • Thwarting malicious and selfish behavior in wireless environments • Key Management protocols over wireless devices (WPA/RSN, TKIP, AES-CCMP) • Future Developments
Recommended and/or required reading:	
Textbooks:	<p>W. Stallings, "Network Security Essentials: Applications and Standards", Prentice Hall, 3rd Ed., 2007, ISBN 0-13-238033-1.</p> <p>"Security and Cooperation in Wireless Networks" by Levente Buttyan and Jean-Pierre Hubaux, 2007</p> <p>"Implementing 802.1X Security Solutions for Wired and Wireless Networks", Jim Geier, 2008</p> <p>"Security In Wireless LANS And MANS," Thomas Hardjono, Lakshminath R. Dondeti , 2005</p> <p>"Real 802.11 Security : Wi-Fi Protected Access and 802.11i" Jon Edney, William A. Arbaugh, 2003</p> <p>"Security for Ubiquitous Computing," Frank Stajano , June 15, 2002</p>
References:	<p>M. Bishop, "Intro to Computer and Network Security", 2005</p> <p>Kaufman, Perlman, "Network security: Private communication in a public world"</p> <p>C.P. Pfleeger and S.L. Pfleeger, "Security in Computing", Prentice Hall, 4th Ed., 2007, ISBN 0-13-239077-9.</p> <p>W. Stallings and L. Brown, "Computer Security: Principles and Practice", Prentice Hall, 1st Ed., 2008, ISBN 0-13-600424-5.</p> <p><u>A list of relevant academic papers* :</u></p> <p>Wenjing Lou and Yuguang Fang , "A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions", 2007</p> <p>George Hadjichristofi, A. Pipis, V. Vasiliou, and A. Pitsillides , "Security in Sensor Networks", 2009</p> <p>G. Hadjichristofi, J. Adams, and N. Davis, "A Framework for Key Management in Ad hoc networks," 2005</p> <p>Yih-Chun Hu, Adrian Perrig, David B. Johnson "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", 2002</p> <p>"SPINS: Security Protocols for Sensor Networks" Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, 2001</p>

	<p>“Bluetooth™ Security White Paper” Bluetooth SIG Security Expert Group, 2002</p> <p>“Certificate Revocation System Based on Peer-to-Peer CRL Distribution” Matei Ciobanu Morogan, Sead Muftic, Proceedings of the DMS 03 conference, Miami, US, September 2003</p> <p>“Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,” National Institute of Standards and Technology Special publication 800–48</p> <p>Q. Li, S. Zhu and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," infocom 2010, San Diego, CA, March 2010, pp. 1-9.</p> <p>I.R. Chen, F. Bao, M.J. Chang, and J.H. Cho, "Trust Management for Encounter-based Routing in Delay Tolerant Networks," IEEE Globecom 2010.</p> <p>*these papers are just an indication. More papers exists in the literature</p>
<p>Planned learning activities and teaching methods:</p>	<p>The taught part of course is delivered to the students by means of lectures, conducted with the help of computer presentations. Lecture notes and presentations are available through the web for students to use in combination with the textbooks. Furthermore theoretical principles are explained by means of specific examples and solution to specific problems.</p> <p>Lectures are supplemented with unsupervised computer laboratory and homework where students apply their gained knowledge and identify the principles taught in the lecture sessions.</p> <p>The course will also utilize research paper analysis and presentation allowing students to gain knowledge on the state of the art on specific security topics.</p>
<p>Assessment methods and criteria:</p>	<ul style="list-style-type: none"> • Paper Presentation and analysis of state of the art (publications): 25% • Project: 35% • Final Exam 40%
<p>Language of instruction:</p>	<p>English</p>