UNIVERSITY *of* NICOSIA

Course Code	Course Title	ECTS Credits
MBA-735A	Business Data Communication and Security	7.5
Department	**Semester**	**Prerequisites**
School of Business	Fall, Spring, Summer	None
Type of Course	**Field**	**Language of Instruction**
Elective	MIS	English
Level of Course	**Year of Study**	**Lecturer(s)**
2nd Cycle	1st or 2nd	Dr. Dimosthenis Georgiadis
Mode of Delivery	**Work Placement**	**Co-requisites**
Face-to-face	N/A	None
Recommended Optional Programme Components: N/A		

Objectives of the Course:

The main objectives of the course are to:

- Acquire the computer networking knowledge as well as the existing connectivity technologies and the required infrastructure which comprises the key steps involved in the communication process.
- Identify the key issues for the realization of the LAN/WAN/MAN network architectures and the hybridized existing form in the business environment and enterprise.
- Establish a solid knowledge of the layered approach that makes design, implementation and operation of extensive networks possible. To learn the 7-layer OSI network model (each layer and its responsibilities) and understand the TCP/IP suite of protocols and the networked applications supported by it.
- Establish a solid knowledge of the layered approach that makes design, implementation, and operation of extensive networks possible.
- Acquire the knowledge of the basic protocols involved in wired/wireless communication process. These include the characteristics of the required infrastructure for Local Area Networks (MAC CSMA-CD/Ethernet, Token Ring, FDDI, and others) as well as the Wide Area Networks using the TCP/IP (visualizing TCP/IP mechanisms and variations), and UDP/IP. Additionally, the Voice over IP (VoIP) technology in the business communications world will be examined.
- Link different network performance concepts and traffic issues for Quality of Service (QoS) in broadband communication as well as the network economics of the enterprise.

- Learn the basic design principles of broadband wired and wireless communication networks (802.11x) in the business environment. Moreover to gain the ability to design reliable wireless networks and to learn the way to model and analyze the structural performance for some commonly used in business network architectures.
- Motivate the need for network security practices in organizational units.
- Provide students with basic knowledge on various concepts of classical computer and network security paradigms.
- Build foundations to assess contemporary security policies and security mechanisms within organizations and illustrate the balance of the managerial and technical aspects of network security.

Learning Outcomes:

After completion of the course, students are expected to be able to:

- Discuss the physical and logical as well as the electrical characteristics of digital signals and the basic methods of data transmission.
- Identify the importance of the ISO 7-layer reference model.
- Identify and requirements hosted in communication protocols and give an overview of data communication standards, how these standards were developed and under which assumptions they were adopted.
- Figure the area of computer networks in terms of connectivity, mobility and the role of metrics, with emphasis on the range of communication protocols utilized.
- Explore basic protocols involved in wired/wireless communication process. Local Area Networks (MAC-CSMA-CD/Ethernet, Token Ring, FDDI, and others), and for Wide Area Networks using the TCP/IP, UDP/IP.
- Discuss the design principles of wired and wireless communication networks. Moreover, to learn the way to model and analyze the structural performance for some commonly used network architectures. Understand the functions and architectures of LAN and WAN, analyze and design LAN architecture and the design and deployment requirements.
- Analyze the electrical interface and the basics of digital data transmission.
- Link different network performance concepts and traffic issues for Quality of Service (QoS) in broadband communication as well as link the above concepts with the network economics of the enterprise.
- Gain the ability to design reliable wireless networks and to learn the way to model and analyze the structural performance for some commonly used in business network architectures.
- Explain fundamentals and technologies of physical, data-link and network layers.
- Have a basic knowledge on the fundamentals of cryptography such as symmetric/asymmetric encryption, digital signatures, and hash functions.
- Discuss and explain current network authentication applications, PKI, Web security and their vulnerabilities that are exploited by intentional and unintentional attacks.

- Be able to identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic network defense tools.
- Differentiate between organizational security policies and security mechanism.
- Be able to analyze the security needs of a small enterprise, design a strategic plan to address those security requirements, and select the appropriate tools to implement the organizational policies.
- Appreciate the importance of ethics as a network security practitioner.

Course Contents:

1. Basic concepts of connectivity and networking, uses of computer networks, network architectures and topologies, layering and protocols, metric units, basic probability theory.
2. Physical layer, theoretical basis for data communication, guided transmission media, wireless transmission, communication satellites.
3. Network layer, switching and routing, packet vs. circuit switching, protocols and services, internetworking protocols, IP, ICMP, ARP, DHCP, and VPN. Routing principles, the network layer and its usage in the Internet.
4. Transport layer services and protocols, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), TCP congestion control.
5. Applications, networked applications (mail, file transfer, www), multimedia applications (RTP, H.323) and other modern real time end-to-end protocols.
6. Network performance concepts and traffic issues for Quality of Service (QoS) in broadband communication. Association of all the subsequent metrics with the network economics of an enterprise.
7. Security considerations in business applied network systems. Architectures and approaches in facing possible intrusions and intrusion detection.
8. Motivation and introduction to information security
9. Overview of the discipline of cryptography - algorithms and protocols underlying network security applications, encryption, hash functions, digital signatures, and key exchange
10. Authentication protocols, including Kerberos and PKI
11. Overview of computer and network threats and attacks, including denial of service, flooding, sniffing and traffic redirection, exploit attacks, infrastructure attacks (DNS hijacking, route black holing, etc.)
12. Contemporary network defence countermeasures such as intrusion detection tools and firewalls
13. Planning and implementing security policies for an organization with real-world case studies
14. Real-world case studies throughout the course wherever applicable

Learning Activities and Teaching Methods:

Lectures, lab presentations, lab tutorials, theoretical exercises and assignments

Assessment Methods:

| Attendance and Participation |
| Tests/Quizes/Projects |

Mid-Term (1)
Final Exam (1)

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
Andrew S. Tanenbaum, David J. Wetherall	*Computer Networks, 5/E*	Prentice Hall	2010 $_{4th}$ and 5th Edition	0132126958

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
William Stallings	*Business Data Communications 6/E*	Prentice Hall	2006	0131442570
M. Merkow, J. Breithaupt	*Information Security: Principles and Practices*	Prentice Hall	2006	0131547291
B.A. Forouzan	*Data Communications and Networking*	McGraw-Hill	2003	0072515848
James F. Kurose and Keith W. Ross	*Computer Networking: A Top-Down Approach Featuring the Internet*	Addison Wesley, 2nd Edition	2002	0-201-97699-4
G. Dhillon	Principles of Information Systems Security: Texts and Cases	John Willey and Sons	2006	0471450561
R. Anderson	Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition	John Willey and Sons	2008	0470068523
W. Stallings	Network Security Essentials: Applications and Standards, 3rd edition	Prentice Hall	2007	0132380331