CIT224 Information Security Principles, and Standards Course Syllabus

Course Name	Information Security Principles, and Standards
Course Code	CIT224
Course Type	Major Area Elective
Course Level	Undergraduate
AKTS Credit	5 ECTS
Course hours per week (Institutional)	3
Practice hours per week	2
Laboratory hours per week	-
Academic Semester	2013 -2014 Spring
Course coordinator(s)	Asst. Prof. Dr. Yoney Kirsal
Instruction system	
Medium language	English
Prerequisite	-
Suggestions related to course	Lecturing; This course utilizes the Moodle course management system to share information and resources. To access the course site, log on to this link: http://elearning.gau.edu.tr and select the course from list of courses. All course materials will be posted here.
Training required	N/A
Aim of the course	The aim of this module is to cover the principles and foundations of computer and network security. It aims at providing students with understanding the goals, issues, technologies, algorithms and protocols used in securing computer networks and associated systems. It will also provide an understanding of possible security breaches, security risk analysis and mechanisms to protect computer and network communication systems. It also studies an in-depth review of commonly-used security mechanisms and techniques, security threats and network-based attacks.
Learning outcomes	On completion of the module, the successful student will be able to: **Knowledge** 1. Understand and be critically aware of security threats and the available security mechanisms for combating security breaches 2. Critically discuss and understand the concepts of authentication and authorisation, intrusion detection and information security techniques. 3. Design, develop and implement hardware and software security applications. **Skills** 4. Critically appraise technical security systems 5. Critical awareness of the design and implementation of security mechanisms for a given network. 6. Be able to critically analyse security policies, services and mechanisms. 7. Carry out a risk analysis to create solutions for real world current and

		future security threats, including the implementation of innovative solutions (if required)
Course Content		• Attacks and threats • Cryptography overview Network authentication and key management • Kerberos • SSL • Web security • Firewalls • Wireless

	Week	**Topics**	
		Theory	**Practice**
Course content per week	1	**Introduction to course**	Introduction to course
	2-3	**Cryptography:** Basic definitions, security services, attacks and mechanisms Basic definitions, Substitutions techniques Feistel Chiper structure, DES, Mode of operations, 3DES, RSA	How to design a security plan for a small size organisation.
	4	**Use of Cryptography:** Link encryption, End-to-end encryption, Random number generation	Steps of Security wheel, while designing a security plan.
	5	**Key management:** Symmetric key distribution, distribution of public keys, use of public keys to distribute private keys, Diffie-hellman	Application of RSA algorithm. **Quiz 1 on WEEK 5**
	6	**Message authentication, Hash, Digital signature :** Authentication requirements, Authentication functions, MAC, SHA, MD5	Exercises on Authentication functions
	7	**Authentication protocols**: Kerberos, authentication procedures, PKI	Kerberos Authentication Protocol **Quiz 2 on WEEK 7**
	8	**Midterm Exam**	
	9	**Attacks and malicious software and Firewalls:** Basic definition, Trapdoors, Logic bombs, Trojan horse, Zombie, Virus, Worm, DDoS, Packet filter firewalls, Application level gateway	How to identify virus, Trojan horse and worm, how to use and implement firewalls
	10	**Intrusion Detection Systems:** Basic concepts, Anomaly and Misuse based detections, advanced concepts	Examples are given on TCP SYN flooding **Quiz 3 on WEEK 10**
	11	**Web security:** Web threats, Web security, SSL	Definitions on SSL and web security.
	12-13	**Wireless security: WEP, WPA, WPA2**	**Quiz 4 on WEEK 12**
	14	Revision	
	15	**Final exam**	

Course book and references :	• Forouzan, B. A. "Cryptography and Network Security, McGraw-Hill, 2008 • W. Stallings, "Cryptography and Network Security: Principles and Practice", Third Edition, Prentice Hall, 2007 • Kaufman, Perlman, and Speciner. Network Security: Private Communication in Public World, Second Edition, Prentice Hall PTR,

ASSESSMENT METHODS

Quizzes: 40%
Midterm: 20%
Final: 40%

Term Activities	**Number**	**Contribution percentage to course mark %**
Quizzes	**4**	**40**
Midterm Exam	**1**	**20**
Final Exam	**1**	**40**
TOTAL		**100**
Percentage of Classroom Activities		**60**
Percentage of Final Activities		**40**
TOTAL		**100**

Calculation work load within the framework of learning, teaching and evaluation activities

Activities	**Number**	**Time (Hour)**	**Total Work Load (hour)**
Weekly Theory Hour	14	3	42
Weekly Practice Hour	14	2	28
Quiz	4	7	28
Midterm	1	20	20
Final	1	32	32
TOTAL WORKLOAD (hour)= 150			
COURSE ECTS CREDIT=Total Work Load (hour) /(30 hour/ECTS)= 150 / 30 = 5			

GAU
THE AMERICAN UNIVERSITY
GIRNE CYPRUS

Programme and learning outcomes

Learning Outcomes (LO)	Programme Outcomes (PO)																
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PO 13	PO 14	PO 15	PO 16	PO 17
LO1	4	3	3		5	5			4		5		3	5			
LO2	4	4	3		5	5			4		5		3	5			
LO3	3	3	3		5	5			4		5		3	5			
LO4	3	3	3		5	5			4		5		3	5			
LO5	3	3	3		5	5			4	4	5		3	5			
LO6	4	3	2		4	3			3	2			2	3			
LO7	3	4			3	4			3	4	4		3	3			

*Contribution Level:
1 very low **2** low **3** medium **4** high **5** very high

CITT Department Programme Outcomes

1. Having adequate level of knowledge and skills in current/new computing and educational technologies.
2. Having sufficient communication and teaching skills in teaching profession.
3. Being able to teach updated computing technologies efficiently in English.
4. Being able to identify information technology problems through using various analysis and synthesis.
5. Being pragmatic to develop and apply persistent information technology solutions to educational and business problems.
6. Being able to use critical and computational thinking skills to produce alternative solutions at every level of project development life-cycle.
7. Being capable to work in disciplinary and interdisciplinary teamwork.
8. Being sensitive, reactive and responsive to professional, social and ethical issues. Having social and ethical awareness in teaching and in providing solutions to problems.
9. Having adequate level of knowledge and skills in current/new computer hardware, operating systems and computer networks.
10. Adequate level of knowledge and skills in current/new programming languages, programming paradigms (procedural and object-oriented) and programming environments (visual, console-based programming).
11. Being able to analyse, plan and manage educational software design and project development.
12. Having the capability of evaluating and criticising educational software design and development.

13. Adequate level of knowledge in using and integrating current/new e-learning and distance education systems such as learning management systems (LMS).
14. Having sufficient skills and knowledge in using instructional technology and material design.

15. Having skills to apply and use special teaching approaches, theories, teaching strategies, methods and techniques (such as to those people with disabilities).
16. Using appropriate measurement and evaluation techniques to assess students' learning and development in addition to supporting them with good level of feedback.

17. Having sufficient knowledge in the process of establishment of Republic of Turkey. Identifying social, cultural, political and economic problems through understanding Ataturk's principles and revolution.