AGU Department of Computer Engineering
2021-2022 Fall Semester
COMP 414 Network Security

COURSE RECORD

Code	**COMP 414**
Name	**Network Security**
Hour per week	3 (3 + 0)
Credit	3
ECTS	6
Level/Year	Undergraduate
Semester	Fall, Spring
Type	Elective
Prerequisites	COMP 308 Computer Networks
Coordinator(s)	Dr. Samet TONYALI
Description	In a modern world, almost all of us has some type of electronic (and most of the time, smart) devices to connect to the Internet for accessing social media platforms, reading news, using instant messaging applications, and so on. Unfortunately, some malicious people target security of any online services that we communicate with. Here, in this course, students learn internals of these attacks and countermeasures that they need to take to protect security of those services and their users.
Objectives	Students will grasp a conceptual understanding of network security issues, challenges, and mechanisms Students will describe common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms. Students will develop basic skills of secure network architecture and explain the theory behind the security of different cryptographic algorithms Students will learn to develop secure communication protocols
Learning Outcomes	*By the end of the course, the student will be able to* LO1. List basic principles and practices in computer and network security LO2. Explain the major types of threats to information security and the associated attacks LO3. Use cryptographic algorithms and methods that are used in the past and present LO4. Analyze communication protocols in terms of security LO5. Test communication protocols in terms of security LO6. Create secure communication protocols
Additional Info	
Requirements	
Teaching Methodology	Learners will be provided with as many opportunities of hands-on practice as possible with the aim of striking a balance between learner-centeredness and sufficient guidance. Various forms of interaction (i.e., pair work and group work) will also be encouraged to cater for learners with different learning styles. Additionally, individuals will be expected to produce both in-class writings and homework assignments in addition to the reading tasks, which will encourage them to reflect and think critically. Technology will also be incorporated into the classroom procedures in order to create a better learning environment.
Reading List	**Course Textbook:** Cryptography and Network Security: Principles and Practice, Stallings, William, Pearson, 7th Edition. The author's web page related to the textbook: http://williamstallings.com/Cryptography/Crypto7e-Student/ **Additional Materials:**

	Introduction to Modern Cryptography, Katz, J., Lindell, Y., CRC Press, 3rd Edition. The author's web page related to the textbook: http://www.cs.umd.edu/~jkatz/imc.html
Ethical Rules and Course Policy	• For the AGU Make-up policy, please refer to the website https://goo.gl/HbPM2y section 26. • Eating and drinking is permitted unless it offends other students • English should always be used to communicate with one another during instruction hours. • Please, respect the allotted times provided for breaks. • Cell phones are allowed but their voices must be turned down. If cellphone usage bothers the instructor or the class, the instructor has the final say on the issue. Consequences include but are not limited to loss of participation points, extra assignments, and/or being asked to leave the classroom. • Please, bring the required materials, specifically your laptop computers.

ASSESSMENT

Evaluation Criteria	**Weight** (%)
Quizzes	10%
Assignments	20%
Group Project & Presentation	25%
Midterm Exam	20%
Final Exam	25%
Total	100%

For a detailed description of grading policy and scale, please refer to the website https://goo.gl/HbPM2y section 28.

COURSE LOAD

Activity	**Duration** (hour)	**Quantity**	**Work Load** (hour)
In class activities	2	14	28
Async Materials (Videos, Readings, etc.)	1	13	13
Group work for project	40	1	40
Research (web, library)	1	4	4
Required Readings	2	13	26
Pre-work for Presentation	3	1	3
Pre-work for Midterm	24	1	24
Pre-work for Final	24	1	24
Assignments	2	4	8
		General Sum	**170**

ECTS: 6 (Work Load/25-30)

WEEKLY SCHEDULE

W	**Date**	**Topic**	**Activities/Assignments**	**Outcomes**
1	Oct 4-8	Introduction to Information Security	Flipped learning	LO1, LO2
2	Oct 11-15	Symmetric Cryptography and Hash Functions	Flipped learning	LO1, LO2, LO3, LO6

3	Oct 18-22	Asymmetric Cryptography	Flipped learning, ***Project Proposal***	LO1, LO2, LO3, LO6
4	Oct 25-29	Key Management and User Authentication	Flipped learning, Assignment 1 Out	LO3, LO6
5	Nov 1-5	Attacks and Web Security	Flipped learning	LO1, LO2, LO4
6	Nov 8-12	IP Security	Flipped learning	LO2, LO3, LO6
7	Nov 15-19	***Fall Break***		
8	Nov 22-26	VPNs and Firewall	Flipped learning, Assignment 2 Out	LO3, LO5
9	Nov 29 – Dec 3	***Lecture-Free Week***	A pen-tester will be invited to share their experience.	
10	Dec 6-10	Intrusion Detection/Prevention Systems	Flipped learning, ***Midterm Exam***	LO3, LO5
11	Dec 13-17	Network Access Control and Cloud Security	Flipped learning, Assignment 3 Out, Project Progress Report Due	LO4, LO5
12	Dec 20-24	Wireless Network Security	Flipped learning	LO3, LO4
13	Dec 27-31	Electronic Mail Security	Flipped learning	LO4
14	Jan 3-7	Malicious Software	Flipped learning, Assignment 4 Out	LO2, LO4, LO5
15	Jan 10-14	Project Presentations	Group work	LO3, LO4, LO5, LO6
16	Jan 17-26	***Final Exam***	Project Report and Source Code Submission Due	

Prepared by Dr. Samet TONYALI

*****This syllabus is tentative (it can be altered at the discretion of the instructor)*****