1.	Course title	**Mobile and Web Applications Security**		
2.	Course code	KK-Z-07		
3.	Study program	**Coding and Cryptography**		
4.	Unit offering the course	**FCSE**		
5.	Undergraduate/master/PhD	**Master**		
6.	Year/semester 1(2)/summer/elective	7. ECTS: **6**		
8.	Teacher(s)	Assoc. Prof. Ljupcho Antovski, Assis. Prof. Goce Armentski		
9.	Course prerequisites	None		
10.	Goals (competences): The course will enable the students to be aware of possible threats and attacks on web and mobile application and their discovery. Detailed elaboration will be given on the approaches to achieve greater security in mobile and web applications with the use of: web services security, use of secure design of mobile operating systems, implementation of mechanisms for protection on application level, improvement of Ajax security, web services security. After the completion of the course, the students are expected to be able to: configure web services protection, design secure mobile application solutions, and implement appropriate techniques for protection of mobile and web applications. The students will be able to analyze certain weakness in the current mobile and web applications and to propose solutions to overcome these.			
11.	Course content: - Modelling web security - Configuring HTTP security - Detection of unauthorized content modification - Protection of the interaction between the database and application - Management of session authentication - Validation of input - Web services protection - Scanning of application weaknesses - Model for security of mobile operation systems			
12.	Teaching methods: Lectures supported by slide presentations, interactive lectures, trainings (using lab equipment and software packages), team work, case studies, invited guests and lectures, individual practical assignments presentations, seminar paper, e-learning (forums, consultations).			
13.	Total available time	6 ECTS x 30 hours = 180 hours		
14.	Distribution of the available time	45 +30 + 60 + 0 + 45 = 180 hours		
15.	Teaching activities	15.1.	Lectures	45 hours
		15.2.	Training (labs, problem solving), seminar and team work	30 hours
16.	Other activities	16.1.	Project work	60 hours
		16.2.	Self study	0 hours

		16.3.	Home work	45 hours

17.	Grading		
	17.1.	Tests	0 points
	17.2.	Seminar work/project (written or oral presentation)	80 points
	17.3.	Active participation	20 points

18.	Grading criteria	to 50 points	5 (five) (F)
		from 50 to 59 points	6 (six) (E)
		from 60 to 69 points	7 (seven) (D)
		from 70 to 79 points	8 (eight) (C)
		from 80 to 89 points	9 (nine) (B)
		from 90 to 100 points	10 (ten) (A)
19.	Final exam prerequisites	Successfully completed activities 15.1 and 15.2	
20.	Course language	Macedonian and English	
21.	Quality assurance methods	Internal evaluation and student questionnaires	

22. Literature

22.1. Compulsory

No.	Authors	Title	Publisher	Year
1.	Michal Zalewski	The Tangled Web: A Guide to Securing Modern Web Applications	No Starch Press	2011
2.	Himanshu Dwivedi, Chris Clark, David Thiel	Mobile Application Security	McGraw-Hill Osborne Media	2010
3.	Bryan Sullivan	Web Application Security, A Beginner's Guide	McGraw-Hill Osborne Media	2011

22.2. Additional

No.	Authors	Title	Publisher	Year
1.	Jeff Six	Application Security for the Android Platform: Processes, Permissions, and Other Safeguards	O'Reilly Media	2011
2.	Joel Scambray, Vincent Liu, Caleb Sima	Hacking Exposed Web Applications, 3rd Edition	McGraw-Hill Osborne Media	2010
3.	Bryan Sullivan	Ajax Security	Addison-Wesley Professional	2007