uc3m | Universidad Carlos III de Madrid
Departamento de Ingeniería Telemática

COURSE: SECURE ARCHITECTURES		
MASTER: CYBERSECURITY	**YEAR**: 2020/21	**TERM**: 2nd

WEEKLY PLANNING

WEEK	SESSION	DESCRIPTION	GROUPS (mark X)		Special room for session (computer classroom, audio-visual classroom…)	WEEKLY PROGRAMMING FOR STUDENT		
			LECTURES	SEMINARS/ LAB[1]		DESCRIPTION	CLASS HOURS	HOMEWORK HOURS (Max. 7h week)
1	1	Presentation of the course Introduction to Secure Architecture	X			Study about security design principles for secure architectures	1,66	5
1	2	Architecting Secure Cloud Computing	X			Analyze a case study on Cloud Computing Security, giving details on: security implications of going cloud, top threats, defense mechanisms and current tools/methodologies for cloud security assessment and certification	1,66	
2	3	SecDevOps + Lab I: Deployment a basic SecDevOps solution		X	Lab	Learn secure remote management solutions. Practice with a basic infrastructure that involves different OS.	1,66	7
2	4	Authorization: Concepts and AC models	X			Review and study traditional access control models (DAC, MAC, RBAC) and modern AC (ABAC). Discuss about advantages and disadvantages of each one.	1,66	
3	5	Languages and infrastructures for authorization	X			Study deployed languages and infrastructures (e.g., XACML and SAML) for access control in Web and Cloud Computing.	1,66	7
3	6	Lab II: Identity & Access Management (IAM)		X	Lab	Deploy and tests of a SAML-based authorization infrastructure. Experiment with different profiles	1,66	

4	7	Lab II (cont.): Identity & Access Management (IAM)		X	Lab	Deploy and tests of a SAML-based authorization infrastructure. Experiment with different profiles. Document and submit a report with answers to questions posed.	1,66	7
4	8	Multilevel and Multilateral Security Lab III: MLS with SELinux		X	Lab	Learn about classified Information, security models (e.g., Bel-LaPadula, Biba,etc.). Understand examples and practical considerations. Theoretical session. In the lab session, practice with MLS using a Linux Security Module (e.g., SELinux).	1,66	
5	9	Attack Tolerance	X			Study and identify DDoS protection mechanisms. Deploy a simple DoS attack and protection tools as a proof-of-concept.	1,66	7
5	10	Attack Tolerance (cont)		X	Lab	Deploy a simple DDoS attack and protection tools as a proof-of-concept. Review back-up and restoration strategies and systems.	1,66	
6	11	Physical Security	X			Study security against emanations. TEMPEST.	1,66	7
6	12	Students work presentation		X	Lab	Technical oral presentation and defense of the practical work done in Lab II. Document and submit the report.	1,66	
						Subtotal 1 lab sessions	19,92	40

[1] A maximum of 1-2

Total 1 (Hours of class plus student homework hours between weeks 1-7)	59,92

1-7		Tutorials, handing in, etc					10	
8		Assessment					3	7
						Subtotal 2	3	17

Total 2 (Hours of class plus student homework hours at week 8)	20

TOTAL (Total 1 + Total 2)	79,92