SRSC - Generic Course Planning Reference

Program Topics / Lectures & Refs.					Lab/Hands-On Activities.		Practical / Assegnments	TPs / Deliverable Dates
Weeks	**Date**	**Ch.**		**Topic**	**Labs**	**Lab Ref.**		
W1	**15/Sep**	**0**		**Course presentation / overview**	**Lab 1**	References for initial instalalations / Suggested Off-Line Activities	TP-0 Work Assignment	
		1		Introduction				
			1.1	Initial concepts and terminology				
	17/Sep		1.2	Security policies				
			1.3	Frameworks and standards				
			1.4	Security model for CNSS in a Didtributed Systems Security Model Approach				
			1.5	Fundamental security design principles				
		2		**CNSS Foundations and models**				
			2.1	OSI X.800 and IETF Internet Security Frameworks				
			2.2	Adversray model and threats vs. Security services, properties and mechanisms				
			2.3	Secure channels, P2P vs. E2E Security				
			2.4	Communications security and TCP/IP Security stack				
			2.5	End systems and protection mechnanisms				
W2	**22/Sep**	**3**		**Applied cryptography and cryptographic methods and tools**	**Lab 2**	Java, JCA and JCE	TP-1 Project Assignment	
			3.1	Symmetic Cryptography and Algs.		Programming with JCE / Cryptography in Java		
						Programming with Symmetric Crypto Algsms, Modes and Padding		
						Hand-On Demos, Discussion and Proposed Exercices		

W3	**29/Sep**		3.2 Asymmetric Crypto and Algorithms 3.3 Diffie-Hellman Agreement 3.3 Secure Hashing 3.4 MACs, HMACs and CMACs	**Lab 3**	Programming with Asymmetric Cryptography Secure Public-Key Envelopes Private/Public Key Management Facilities Hand-On Demos, Discussion and Proposed Exercices
W4	**6/Oct**		3.5 Digital Signatures Algorithms, constructions and patterns 3.6 Other cryptographic tools 3.7 Emerging crypto	**Lab 4**	Secure Hashing and Programming with MACs (HMACs, CMACs) Programming with Digital Signatures Performance of Crypto Methods and the openssl tool Hand-On Demos, Discussion and Proposed Exercices
W5	**13/Oct**	**4**	**Key Distribution and secure establishment of Secure Associations** 4.1 Key distribution w/ symmetric crypto 4.2 Key distribution with asymmetric crypto 4.3 DH-based key distribuiton	**Lab 5**	Diffie-Hellman Aggrement: Programming in Java Hand-On Demos, Discussion and Proposed Exercices
W6	**20/Oct**		4.4 Kerberos authentication and key-establishment 4.5 Authentication protocols: PAP. CHAP. 4.6 X509 Authentication 4.7 PKI / PKIX Framework		TP1 Development

W7	**27/Oct**		***NO CLASS Evaluation (Test1),*** ***Date to be defined: Period: 26 - 31 / Oct***		TP1 Development and conclusion	TP1 Project Deliverable	Until 1/Nov
W8	**3/Nov**	**5.**	**User-Authentication** 5.1 PWD-based authentication 5.2 Authentication factors and MFA 5.3 SSO and FIM 5.4 OAuth				
W9	**5/Nov**	**6**	**Access-Control** 6.1 Models: MAC, DAC, RBAC, ABAC, CBAC 6.2 Access Control Mechanisms: ACLs and Capabilities 6.3 Examples: OS File System Access Control 6.4 Access-Control Management and Frameworks	**Lab 6** **Lab 7**	Programming with JSSE TLS and Web Sec Auditing/Analysis	TP2 Project Assignment	
W10	**10/Nov**	**7**	**TCP/IP Security stack** 7.1 TCP/IP Security services and standards 7.2 TLS and Web Security 7.3 SSH		Programming with JSSE **Lab 8** Web Security wih TLS-enabled REST		
W11	**17/Nov**		7.4 Email Security Email security model and standards 7.5 Emal and E2E Security PGP S/MIME	**Lab 9**	Homomorphic Encryption Library / Practical Use		

W12	**24/Nov**		7.6	IPSec IPSec and IPSec-Suite Protocols	TP2 Development	
			7.7	VPNs		
W13	**15/Dec**	**8**		**Systems security**	TP2 Development and Conclusion	TP2 Project Deliverable — Until 13/Dec
			8.1	OS-Level security		
			8.2	Permiter defenses: IPS, IDS		
W14	**22/Dec**	**8**	8.3	Virtualization		
			8.4	Isolation and Containment		
			8.5	Runtime security: Attestation, TPMs and	Demo / Use of TEE in Intel SGX	
			8.6	Case-Study: SGX-Enabled Trusted		
Evaluation (Test2), Date to be defined: ***Period: 4 - 15 /Jan***						