SCHEDA DELL'INSEGNAMENTO (SI)

"SYSTEMS SECURITY"

SSD ING-INF/05*

DENOMINAZIONE DEL CORSO DI STUDIO: INGEGNERIA INFORMATICA

ANNO ACCADEMICO: 2023-2024

INFORMAZIONI GENERALI - DOCENTE

DOCENTE: VALENTINA CASOLA
TELEFONO: 0817683907
EMAIL: VALENTINA.CASOLA@UNINA.IT

INFORMAZIONI GENERALI - ATTIVITÀ

INSEGNAMENTO INTEGRATO (EVENTUALE):
MODULO (EVENTUALE):
CANALE (EVENTUALE):
ANNO DI CORSO (I, II): II
SEMESTRE (I, II): I
CFU:6

INSEGNAMENTI PROPEDEUTICI (se previsti dall'Ordinamento del CdS)

Nessuno.

EVENTUALI PREREQUISITI

Conoscenze di programmazione; conoscenze dei principi dell'ingegneria del software.

OBIETTIVI FORMATIVI

Il corso si pone l'obiettivo di fornire un'impostazione metodologica e tecnologica per il progetto di sistemi sicuri. Il corso prevede di analizzare le tecniche di progetto standard con riferimento allo sviluppo ed uso dei principali meccanismi di sicurezza, tra cui: meccanismi di autenticazione e controllo accessi, meccanismi di sicurezza crittografici, meccanismi per la protezione delle comunicazioni e dei sistemi distribuiti. Sono inoltre presentati i principali elementi per l'analisi dei rischi e delle minacce applicabili ad un sistema per guidare le fasi di progettazione e le principali tecniche di assessment e testing della sicurezza dei sistemi.

RISULTATI DI APPRENDIMENTO ATTESI (DESCRITTORI DI DUBLINO)

Conoscenza e capacità di comprensione

Lo studente deve dimostrare di conoscere e comprendere le problematiche relative al progetto di sistemi sicuri, con riferimento alle metodologie di analisi e progettazione, standard, presentate durante il corso, e considerando i vincoli specifici derivanti dalle tecnologie utilizzate. Deve inoltre dimostrare di comprendere le caratteristiche fondamentali di diversi meccanismi di sicurezza e di saper individuare i controlli più appropriati per soddisfare specifici requisiti di progettazione.

Capacità di applicare conoscenza e comprensione

Lo studente deve dimostrare di essere in grado di eseguire l'intero ciclo di analisi, progettazione e sviluppo di un sistema sicuro, dalla fase di analisi dei rischi e delle minacce alla identificazione dei meccanismi di controllo più opportuni, alla loro implementazione e corretta configurazione, fino al testing finale della sicurezza del sistema, utilizzando strumenti e ambienti di sviluppo di ampio utilizzo.

PROGRAMMA-SYLLABUS

Course Introduction: Basic terminology, Overview of system security, Policy/mechanism separation, Security requirements.

Fundamentals of cryptography: Symmetric cryptosystems: Block Cipher (DES, Skipjack….), Asymmetric cryptosystems: RSA, ECC; Key Management and distribution; Digital signature, Hash functions, Smart Card security; Public Key Infrastructure: PKCS Standards, X. 509 Certificates, Certificate Policies and Cross Certification; Java Cryptography Architecture; Digital Signature and PEC in the Italian law.

Identification and Authentication mechanism: Authentication mechanisms, Authentication protocols, Single Sign On, Kerberos, Identity Federation, OAuth, SAML, IAM (Identity and Access Management) Systems; credential management systems (Vault).

Access Control mechanism: Access Control models: Discretionary and Mandatory Access Control Models (DAC, MAC), Role based Access Control Models (RBAC), Other models: Attribute based Access Control (ABAC), Role hierarchy management, Conflict management; Access Control frameworks: XACML, Keycloack, Authentication and Authorization services.

System and Communication Protection mechanism: Attack taxonomy, Firewalls, Gateways, Intrusion Detection systems; Network segmentation and demilitarized zone (DMZ), Monitoring mechanisms; Auditing and Logging mechanisms.
Application and Network Security protocols: SSL, PGP, SMIME, VPN, IPv6.

Design of Secure Systems: standard risk-based development approach (NIST, ISO), Secure SDL methodologies, threats and vulnerabilities analysis, risk analysis, security controls identification techniques, security assessment, static and dynamic

security testing techniques. Design trade-offs: Security and Performances. Case studies: Web application security, Security in hw and embedded devices (IoT security, WSN security, FPGA security…..), Cloud Security.

MATERIALE DIDATTICO

Libro di testo: Stallings William – Computer Security, Principles and Practice 3rd Ed - Prentice Hall.
Dispense e presentazioni fornite dal docente relative ad argomenti teorici e applicativi.
Manuali e standard di riferimento dei meccanismi e metodologie di sicurezza utilizzati.
Codice relativo alle esercitazioni svolte in aula.

MODALITÀ DI SVOLGIMENTO DELL'INSEGNAMENTO

Il corso prevede circa il 70% di lezioni frontali in cui vengono affrontati gli argomenti teorici, mentre il restante 30% è riservato a lezioni pratiche ed esercitazioni riguardanti la progettazione, implementazione e valutazione di meccanismi di sicurezza studiati.

VERIFICA DI APPRENDIMENTO E CRITERI DI VALUTAZIONE

a) Modalità di esame:

L'esame si articola in prova	
scritta e orale	
solo scritta	
solo orale	x
discussione di elaborato progettuale	x
altro	

In caso di prova scritta i quesiti sono (*)	**A risposta multipla**	
	A risposta libera	
	Esercizi numerici	

(*) È possibile rispondere a più opzioni

La verifica dell'apprendimento prevede una prova orale orientata alla verifica della comprensione dei concetti teorici del corso e alla discussione di un elaborato.