Università degli Studi di Enna "Kore"

Facoltà di Ingegneria ed Architettura

Anno Accademico 2020 – 2021

A.A.	Settore Scientifico Disciplinare		CFU	Insegnamento	Ore di aula		Mutuazione	
2020/21	*ING-INF/05*		9	**Sicurezza dei Sistemi Informatici e Laboratorio**	56		No	
Classe	**Corso di studi**			**Tipologia di insegnamento**	**Anno di corso e Periodo**		**Sede delle lezioni**	
L8	Ingegneria Informatica			Caratterizzante	III Anno Secondo Semestre		Plesso di Ingegneria	
N° Modulo	Nome Modulo	Tipologia lezioni	Ore	Docente	SSD	Ruolo	Interno	Affidamento
No		Lezioni Frontali Laboratorio	48 8	Vincenzo Conti vincenzo.conti@unikore.it	ING-INF/05	PA	Si	Istituzionale

Prerequisiti

Per una corretta fruizione del corso sarebbe auspicabile che lo studente abbia già acquisito conoscenze, capacità ed abilità teoriche e/o applicate sia per quanto riguarda la programmazione ad oggetti sia per quanto riguarda l'analisi matematica

Propedeuticità

Nessuna.

Obiettivi formativi

Studio e analisi delle minacce delle vulnerabilità e del rischio associato ai sistemi informatici al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una determinata soglia di tollerabilità.

Risultati di apprendimento (Descrittori di Dublino):

Alla fine del corso, gli studenti dovranno aver conseguito le seguenti abilità, conoscenze e competenze:

Conoscenza e capacità di comprensione (knowledge and understanding): Lo studente alla fine del corso acquisirà una buona conoscenza delle principali tecniche e algoritmi di crittografia per la cifratura/decifratura dei messaggi, di autenticazione e protezione dei sistemi informatici. Sarà in grado di analizzare e comprendere il codice sorgente dei principali algoritmi utilizzati per la protezione dei sistemi informatici.

Capacità di applicare conoscenza e comprensione (applying knowledge and understanding): Lo studente sarà in grado di valutare le caratteristiche, i vantaggi e le limitazioni dei principali sistemi analizzati. Sarà in grado di progettare, analizzare e valutare le soluzioni software a problemi di sicurezza di media complessità. Sarà anche in grado di sviluppare le soluzioni software, valutandone la qualità in termini di semplicità, efficacia ed efficienza.

Autonomia di giudizio (making judgements): Lo studente sarà in grado sia di effettuare l'analisi di un problema di sicurezza che di progettare, a partire da precise specifiche, una opportuna soluzione software. Sarà in grado di valutarne la qualità di una soluzione software in termini di semplicità, leggibilità, efficienza e possibilità di riutilizzo. L'autonomia di giudizio verrà valutata esaminando le soluzioni proposte dagli studenti a problemi di sicurezza di media complessità. Lo studente verrà incoraggiato inizialmente a trovare e valutare autonomamente soluzioni ai problemi posti, al fine di potere comprendere la qualità e l'utilità delle soluzioni proposte successivamente dal docente.

Abilità comunicative (communication skills): Lo studente acquisirà la capacità di comunicare ed esprimere problematiche inerenti all'oggetto del corso. Sarà in grado di sostenere conversazioni su tematiche relative alla sicurezza informatica e all'implementazioni software di algoritmi al fine di contrastare tale tematica. Sarà in grado di utilizzare un linguaggio semplice e chiaro per la descrizione dei processi di analisi e di sintesi di soluzioni di sicurezza a problemi di media complessità. Il carattere interattivo delle lezioni dovrà permettere il miglioramento delle abilità comunicative dello studente.

Capacità d'apprendimento (learning skills): Lo studente dovrà sviluppare la capacità di apprendere i processi di analisi e di sintesi relativi alla codifica di algoritmi di cifratura/decifratura e autenticazione di media complessità e alla relativa implementazione di librerie e strumenti software. Il grado di apprendimento sarà valutato non in base alla capacità di memorizzare concetti specifici ma in base alla capacità di ricostruire ex novo, partendo dal minor numero possibile di idee generali di base, le migliori soluzioni software.

Contenuti e struttura del corso

N.	ARGOMENTO	TIPOLOGIA	DURATA
1	Concetti sulla Sicurezza Informatica: Attacchi, Servizi, Meccanismi	Frontale	2h
2	Cifratura Simmetrica Classica e Criptoanalisi	Frontale	8h
3	Introduzione Cifratura Simmetrica Moderna: Cifrari a Blocchi	Frontale	2h
4	Concetti di base sulla Teoria dei Numeri e sui Campi Finiti	Frontale	2h
5	Algoritmi di Crittografia: DES, Double DES, Triple DES, AES	Frontale	12h
6	Modi di Funzionamento dei Cifrari a Blocchi	Frontale	4h
7	Generatori di Numeri Pseudo-Casuali e Cifrari a Flusso	Frontale	4h
8	Introduzione Cifratura Asimmetrica: Chiave Pubblica e Chiave Privata	Frontale	2h
9	Algoritmi RSA e a Curva Ellittica	Frontale	6h
10	Protocollo Scambio Chiave di Sessione: Diffie-Hellaman	Frontale	2h
11	Protocollo Scambio Chiave Pubblica e Certificati	Frontale	2h
12	Cenni sull'Autenticazione Utente: Sistemi Biometrici	Frontale	2h
13	Laboratorio: Applicazioni della sicurezza ai sistemi informatici	Laboratorio	8h

Attività pratiche in aula ed esercitative/laboratoriali:
Durante il corso e sequenzialmente alle lezioni di natura teorica è previsto lo sviluppo di algoritmi e tecniche relative ai sistemi di sicurezza studiati. Durante le ore esercitative/laboratoriali è previsto lo sviluppo di un sistema di sicurezza.

Testi adottati

Testi principali:
Crittografia e sicurezza delle reti – William Stallings – McGraw-Hill Editore

Materiale didattico a disposizione degli studenti:
Slide del corso

Modalità di accertamento delle competenze

L'obiettivo della prova d'esame consiste nel verificare il livello di raggiungimento delle conoscenze, competenze e abilità in accordo con i descrittori di Dublino. Il voto sarà dato in trentesimi e varierà da 18/30 a 30/30 con lode. L'accertamento delle competenze si basa su un esame espletato in un'unica giornata solamente tramite una prova orale basata sull'esposizione degli argomenti trattati durante il corso.
Il voto sarà espresso, secondo il seguente schema di valutazione:

- Ottimo (30-30 e lode): Ottima conoscenza e comprensione degli argomenti trattati. Ottima capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Eccellenti capacità espositive.
- Molto buono (26-29): Buona conoscenza e comprensione degli argomenti trattati. Buona capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Ottime capacità espositive.
- Buono (24-25): Buona conoscenza e comprensione degli argomenti trattati. Discreta capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Buone capacità espositive.
- Discreto (21-23): Discreta conoscenza e comprensione degli argomenti trattati. Limitata capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Discrete capacità espositive.
- Sufficiente (18-20): Conoscenza minima degli argomenti trattati e limitata capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Sufficienti capacità espositive.
- Insufficiente: Manca di una conoscenza accettabile degli argomenti trattati e non dimostra una sufficiente capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Scarsa capacità espositiva.

Orari di lezione e date di esame

Gli orari di lezione saranno pubblicati sulla pagina web del corso di laurea almeno due mesi prima dell'inizio delle lezioni:
http://www.unikore.it/index.php/ingegneria-informatica-attivita-didattiche/calendario-lezioni

Le date di esami saranno pubblicati sulla pagina web del corso di laurea almeno due mesi prima dell'inizio della sessione d'esami:
http://www.unikore.it/index.php/ingegneria-informatica-esami/calendario-esami#

Modalità e orari di ricevimento

Gli orari di ricevimento saranno pubblicati sulla pagina personale del docente:
http://www.unikore.it/index.php/ingegneria-informatica-persone/docenti-del-corso/itemlist/category/1511-conti

Note

Nessuna.