Università degli Studi di Enna "Kore"

Facoltà di Ingegneria ed Architettura

Anno Accademico 2016 – 2017

A.A.	Settore Scientifico Disciplinare		CFU	Insegnamento	Ore di aula		Mutuazione	
2016/17	*ING-INF/05*		6	Sicurezza nei Sistemi Informatici (a scelta)	48		No	
Classe	**Corso di studi**			**Tipologia di insegnamento**	**Anno di corso e Periodo**		**Sede delle lezioni**	
L8	Ingegneria Informatica e delle Telecomunicazioni			Caratterizzante	3° Anno Secondo Semestre		Facoltà di Ingegneria e Architettura	
N° Modulo	Nome Modulo	Tipologia lezioni	Ore	Docente	SSD	Ruolo	Interno	Affidamento
1		Lezioni frontali Esercitazioni	38 10	Vincenzo Conti vincenzo.conti@unikore.it 0935 536445	ING-INF/05	RTD	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 procedurale 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 e autenticazione dei messaggi nei sistemi informatici. Sarà in grado di analizzare e comprendere il codice sorgente dei principali algoritmi utilizzati per la protezione dei sistemi informatici. La capacità di comprensione dello studente verrà valutata, dopo l'esposizione dei principali concetti, durante le lezioni frontali con un dialogo diretto con gli studenti.

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. Tale capacità verrà valutata principalmente durante le ore di esercitazione.

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 la valutazione e 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

Lezioni frontali:

N.	ARGOMENTO	TIPOLOGIA	DURATA
1	Introduzione al corso	Frontale	1h
2	Attacchi alla sicurezza	Frontale	1h
3	Meccanismi di sicurezza	Frontale	2h
4	Tecniche di crittografia	Frontale	2h
5	Modello ci cifratura simmetrico classico	Frontale	2h
6	Tecniche di sostituzione	Frontale	2h
7	Cifratura a blocchi	Frontale	2h
8	Algoritmo DES (Data Encryption Standard)	Frontale	2h
9	Lo standard AES (Advanced Encryption Standard)	Frontale	4h
10	Sviluppi della cifratura simmetrica	Frontale	2h
11	Doppio e triplo DES	Frontale	2h
12	Modalità di funzionamento della cifratura a blocchi	Frontale	2h
13	Crittografia a chiave pubblica	Frontale	4h
14	Algoritmo RSA	Frontale	4h
15	Gestione delle chiavi	Frontale	2h
16	Applicazioni della sicurezza	Frontale	4h
17	Esercitazioni	Esercitazioni	10h

Attività esercitative / Lavoro di gruppo:
Sviluppo di algoritmi e tecniche relative ai sistemi di sicurezza trattati durante il corso.

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'accertamento delle competenze si basa su un esame orale espletato in un'unica giornata e svolto in una delle due modalità di seguito descritte secondo la scelta fatta dallo studente alla fine del corso:
1) Discutendo la messa a punto di un progetto al fine di risolvere in modo efficiente un dato problema di sicurezza. Il progetto è assegnato prima della fine del corso e dovrà essere presentato in uno degli esami già fissati nel calendario didattico. Il progetto potrà essere svolto o singolarmente o in gruppo;
2) Discutendo una serie di tematiche di sicurezza relative agli argomenti trattati durante il corso.

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.