UNIVERSITÀ DI PISA

SECURITY METHODS AND VERIFICATION

CHIARA BODEI

Anno accademico	2019/20
CdS	INFORMATICA
Codice	293AA
CFU	6

Moduli	Settore/i	Tipo	Ore	Docente/i
SECURITY METHODS AND VERIFICATION	INF/01	LEZIONI	48	CHIARA BODEI

Obiettivi di apprendimento

Conoscenze
Lo studente che ha completato con successo il corso sarà in grado di mostrare una buona conoscenza delle questioni di sicurezza che nascono in informatica e di avere un'idea di come i metodi formali possano aiutare ad affrontarli.
Inoltre lo studente acquisirà la capacità di leggere e comprendere articoli di ricerca sui metodi formali applicati alla sicurezza

Modalità di verifica delle conoscenze
La capacità dell'allievo di spiegare correttamente i principali argomenti presentati durante il corso sarà valutata attraverso le prove di verifica intermedie. Con un seminario su un argomento di ricerca scelto insieme all'insegnante, lo studente darà prova di essere in grado di leggere, comprendere uno o più articoli di ricerca sarà valutato e dare un seminario su un argomento di ricerca scelto insieme all'insegnante.

Metodi:

- Seminario finale
- Prove periodiche scritte

Capacità
Lo studente acquisirà la capicità di orientarsi sui principali argomenti presentati durante il corso.
Acquisirà inoltre la capacità di leggere, comprendere articoli di ricerca sugli argomenti affrontati nel corso.
Alla fine, gli studenti doverebbero acquisire un modo di pensare i sistemi, conscio dei possibili problemi di sicurezza. Dovrebbero aver capito quali sono i problemi principali e quali sono i modi per aumentare la sicurezza dei sistemi, progettandola insieme ai sistemi fin dall'inizio.

Modalità di verifica delle capacità
L'accertamento delle capacità avviene tramite le prove di verifica intermedie e il seminario finale.

Prerequisiti (conoscenze iniziali)
Non sono richieste particolari conoscenze iniziali. Una conoscenza elementare della crittografia è certamente utile.

Programma (contenuti dell'insegnamento)
Il corso è pensato per offrire un'ampia panoramica della sicurezza nelle reti e nelle apllicazioni software. Esamineremo le basi teoriche della sicurezza e le metodologie formali utilizzate per progettare, analizzare e verificare sistemi e applicazioni. Saranno affrontati anche aspetti sperimentali.
Lelezioni affronteranno in particolare i seguenti argomenti.

- Sicurezza *language-based*
- Principi di progettazione di protocolli di sicurezza

- Sicurezza relativa al flusso di informazione
- Sicurezza Java, *stack inspection*, e controllo degli accessi
- Sicurezza delle applicazioni web

Bibliografia e materiale didattico

Il materiale del corso è composto principalmente da una raccolta di articoli da rivista e da convegno e da lucidi.

Indicazioni per non frequentanti

Gli studenti non frequentanti possono trovare sulla pagina web del corso l'elenco degli argomenti presentati per ogni singola lezione, con le slide proiettate e i riferimenti al materiale didattico rilevante.
Le modalità d'esame per gli studenti non frequentanti sono identiche a quelle per gli studenti frequentanti.

Modalità d'esame

L'esame consiste nella preparazione di un seminario. Per dare il seminario è necessario aver superato le due prove di verifica intermedie o un test scritto finale equivalente.

Pagina web del corso