UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Software Security and Testing

2425-3-E3101Q123

Obiettivi

Il corso ha l'obiettivo di fornire consapevolezza dei problemi di sicurezza e affidabilità delle applicazioni software, e competenza sulle tecniche per affrontarli. In particolare, alla fine del corso lo studente avrà maturato la capacità di analizzare i punti di rischio e criticità nei sistemi informatici, di amministrare gli strumenti di difesa dei sistemi, di comprendere le fasi di un attacco osservato, e di analizzare e progettare soluzioni nei contesti applicativi che richiedono la convalida di affidabilità del software.

Contenuti sintetici

Origine del problema della sicurezza informatica. Eterogeneità delle competenze richieste nel settore sicurezza. Ruoli di attacco e di difesa nei sistemi informatici. Il problema di convalidare l'affidabilità del software. Metodi per il test del software: test funzionale, test strutturale, test basato su modelli. Infrastrutture per l'esecuzione del test. Tecniche di analisi statica e dinamica di programmi.

Programma esteso

1. Rischi nell'uso dei sistemi informativi, ruoli e competenze
2. Tecniche e protocolli per la sicurezza:

- Crittografia, errori di implementazione e attacchi
- Sicurezza nei sistemi operativi e nelle strutture di rete

3. Programmazione sicura:

- Errori di sicurezza nelle applicazioni
- Analisi di noti programmi che presentano vulnerabilita'

4. Programmi pericolosi: troiani, back-door, bombe logiche, virus, worm
5. Convalida di affidabilità del software: dimensioni del problema.
6. Testing:

- Test funzionale: fonti di informazione per derivare casi di test, il test funzionale o black-box, vantaggi e svantaggi rispetto ad un approccio random.
- Test Combinatorio: partizione delle categorie, combinazioni a coppie.
- Test Strutturale: copertura delle istruzioni, decisioni, condizioni e cammini.
- Infrastrutture per l'esecuzione dei test: driver, stub e oracoli

7. Analisi dei programmi:

- Distinzione fra analisi statica e analisi dinamica
- Tecniche di analisi statica: analisi simbolica

Prerequisiti

Nessun prerequisito essenziale. E' utile la comprensione di alcuni concetti base trattati negli insegnamenti di Fondamenti dell'informatica, di Programmazione 1, di Programmazione 2, di Reti e Sistemi Operativi, e di Analisi e Progettazione del Software.

Modalità didattica

Lezioni ed esercitazioni:

- 16 lezioni da 2 ore svolte in modalità erogativa in presenza;
- 10 esercitazioni da 2 ore svolte in modalità erogativa in presenza;

Attività di laboratorio assistita in aula:

- 6 attività di laboratorio da 3 ore svolte in modalità interattiva in presenza;
- 1 attività di laboratorio da 2 ore svolta in modalità interattiva in presenza;

Lingua di erogazione: italiano.

Materiale didattico

Testi di riferimento

Ross Anderson. Security Engineering. 2 ed, Wiley 2008

Mauro Pezzè, Michal Young. Software Testing and Analysis: Process, Principles and Techniques. John Wiley, 2008

Periodo di erogazione dell'insegnamento

Secondo semestre

Modalità di verifica del profitto e valutazione

La verifica dell'apprendimento comprende una prova scritta e una eventuale colloquio orale.

La prova scritta consiste nella risoluzione di esercizi che richiedono calcolo, esercizi che richiedono sviluppo di una soluzione ad un problema assegnato, domande sulle nozioni presentate, e domande di ragionamento e deduzione. Tutte le domande proposte sono a risposta aperta. Gli esercizi hanno la finalità di controllare le competenze di problem solving acquista durante il corso, e le domande permettono il controllo intensivo delle conoscenze teoriche e sulle capacità di riflessione autonoma su punti critici del programma. Solitamente la prova scritta si compone di 3 esercizi e 5 domande a risposta aperta. Gli esercizi sono valutati in base alla correttezza della soluzione proposta, e le domande aperte in base alla completezza e precisione delle risposte corrispondenti.

Il colloquio orale è opzionale e, se richiesto dallo studente, consiste in un colloquio che verte su tutti i punti del programma. Il risultato del colloquio complementa, in positivo o in negativo, il voto che deriva dalla valutazione della prova scritta.

La verifica dell'apprendimento può inoltre derivare dall'esito di due prove intermedie parziali, svolte in forma scritta con modalità equivalenti alla prova complessiva, ma vertenti sui contenuti di metà del programma ognuna. La prima prova parziale riguarda la parte di programma su convalida di affidabilità, test e analisi del software. La seconda prova parziale riguarda la parte di programma sulla sicurezza informatica. La valutazione finale deriva dalla media delle valutazioni delle due prove parziali, che devono però essere necessariamente entrambe sufficienti.

Orario di ricevimento

Su appuntamento

Sustainable Development Goals

IMPRESE, INNOVAZIONE E INFRASTRUTTURE