UNIVERSITÀ DI PISA

FORMAL METHODS FOR SECURE SYSTEMS

CINZIA BERNARDESCHI

Academic year	2023/24
Course	COMPUTER ENGINEERING
Code	909II
Credits	9

Modules	Area	Type	Hours	Teacher(s)
FORMAL METHODS FOR SECURE SYSTEMS	ING-INF/05	LEZIONI	90	CINZIA BERNARDESCHI MAURIZIO PALMIERI

Obiettivi di apprendimento

Conoscenze

Lo studente che completa l'insegnamento con successo avrà conoscenze su (i) principi fondamentali della dependability di sistemi basati su computers (ii) metodi formali per la modellazione e la verifica di programmi e sistemi (iii) strumenti per analizzare e provare formalmente proprietà di security di sistemi. Verranno approfonditi i seguenti problemi di security: data confidentiality; malware detection; and cyber-physical systems security. Inoltre, lo studente avrà conoscenze sulle tecniche di fault tolerance e sulla valutazione quantitativa della dependability basata sui modelli.

Modalità di verifica delle conoscenze

Le conoscenze saranno verificate sull'abilità di illustrare i concetti fondamentali oggetto del corso usando la corretta terminologia, di risolvere esercizi sull'applicazione dei formalismi studiati e di presentare un progetto svolto in gruppo.

Capacità

Il corso fornirà gli studenti le capacità di (i) modellazione formale di componenti hardware e software, e di attacchi di sicurezza; (ii) verifica formale di proprietà di cybersecurity di un sistema usando tecnique di base. Inoltre, gli studenti saranno in grado di di usare approcci formali per modellare e valutare la dependability di sistemi basati su computers: modelli combinatori, modelli state-based. Infine, gli studenti acquisiranno la conoscenza degli standard internazionali per la safety e la security in ambito industriale.

Modalità di verifica delle capacità

Durante le sessioni di laboratorio verranno utilizzati semplici esempi per imparare a progettare sistemi dependable e per utilizzare strumenti di verifica formale. Gli studenti presenteranno e discuteranno la loro attività sul progetto periodicamente, mostrando la metodologia e gli strumenti applicati per risolvere il problema specifico. Gli studenti dovranno preparare un report scritto e fare una presentazione.

Modalità di verifica dei comportamenti

Durante la discussione del progetto, verrà valutata la correttezza della soluzione proposta, insieme con l'accuratezza delle attività.

Prerequisiti (conoscenze iniziali)

Nessuno

Indicazioni metodologiche

Lezioni in presenza con l'ausilio di lucidi.
Attività pratiche basate su materiale fornito dal docente, utilizzando omputers del laboratorio o personali dello studente.
Il materiale del corso sarà disponibile sul sito web del corso.

Programma (contenuti dell'insegnamento)

Dependability and security: non-malicious/malicious faults, errors and failures. Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability. Security Aware Hazard Analysis and risk assessment.
Quantitative evalutation of dependability: Series/Parallel models, fault/attack-trees, stochastic nets.

Background on formal methods: Automata theory, logic, program semantics.
Automated verification: model checking, theorem proving, abstract interpretation.
Security issues: Threat analysis and Risk assessment. Data confidentiality; malware detection; and cyber-physical systems security.
Standards: ISO 26262 "Road vehicles – Functional safety", ISO/SAE 21434:2021 "Road vehicles — Cybersecurity engineering"

Bibliografia e materiale didattico

- A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr.
  Basic Concepts and Taxonomy of Dependable and Secure Computing.
  IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1, 2004
- John Knight. Fundamentals of Dependable Computing for Software Engineers, Chapman & Hall, 2012
- Flemming Nielson, Hanne Riis Nielson, Formal Methods, Springer, 2019
- M. Nicol, W.H. Sanders, K.S. Trivedi. Model-Based Evaluation: From Dependability to Security. In: IEEE Transactions on Dependable and Secure Computing, vol. 1 (1), 2004

Lucidi delle lezioni e materiale delle attività pratiche fornite dal docente.

Indicazioni per non frequentanti

La frequenza non è obbligatoria ma è fortemente raccomandata.

Modalità d'esame

L'esame consiste in un test pratico e in una prova orale.
Il test pratico consiste di un progetto svolto in gruppo sull'applicazione di una tecnica specifica di modellazione/verifica ad un probema di cyber-security. Il progetto è svolto sotto la guida del docente, e deve essere completato e consegnato prima dell'esame.
La prova orale consiste in una discussione sugli argomenti del corso. Allo studente è richiesto di dimostrare le sue conoscenze sul materiale del corso.
Per sostenere la prova orale, è necessario avere superato la prova scritta.

Note

Nessuna.

Ultimo aggiornamento 07/11/2023 09:14