Principali informazioni sull'insegnamento	
Titolo insegnamento	Metodi Formali per la Sicurezza
Corso di studio	Magistrale in Sicurezza Informatica
Crediti formativi	4+1+1(6)
Denominazione inglese	Formal Methods for Computer Security
Obbligo di frequenza	No
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Francesco Paolo Caforio	francescopaolo.caforio@uniba.it

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Informatico	INF/01 – Informatica	6

Modalità di erogazione	
Periodo di erogazione	I semestre
Anno di corso	II
Modalità di erogazione	Lezioni frontali 47 ore (32 Teoria 15 Esercitazione e/o Laboratorio)

Organizzazione della didattica	
Ore totali	150
Ore di corso	47
Ore di studio individuale	103

Calendario	
Inizio attività didattiche	Ottobre 2020
Fine attività didattiche	Gennaio 2021

Syllabus	
Prerequisiti	Conoscenze di base fornite dalle lauree triennali in Informatica, quali programmazione, linguaggi di programmazione, algoritmi e fondamenti Conoscenze di base sulla Teoria dell'Informazione, sull'Analisi dei Sistemi e sui Metodi Formali Capacità di astrazione e formalizzazione Capacità di applicare le conoscenze per indagare fenomeni che si presentano in pratica
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, riportati nei quadri A4a, A4b e A4c della SUA, compreso i risultati di	*Conoscenza e capacità di comprensione* Conoscenze su modelli formali per l'analisi e la valutazione della proprietà computazionalmente interessanti di sistemi informatici critici e complessi *Conoscenza e capacità di comprensione applicate*

apprendimento trasversali)	Conoscenza delle soluzioni esistenti in letteratura e capacità di analizzarle rispetto a problemi reali Capacità di applicare i concetti appresi nella valutazione di sistemi informatici critici e complessi *Autonomia di giudizio* Consapevolezza della necessità di trattare formalmente i sistemi informatici Autonomia nell'analisi critica delle conoscenze acquisite *Abilità comunicative* Illustrare in modo adeguato problemi, rischi e soluzioni Mostrare con un'opportuna modellazione alcune proprietà specifiche del sistema modellato
Contenuti di insegnamento	Introduzione ai "metodi formali per la sicurezza" Contesto, problemi, obiettivi Proprietà computazionalmente interessanti Un modello per la sicurezza in rete Mobile Ad-hoc NETwork Sistemi Grid Reti di Petri Concetti di base Rappresentazione algebrica Estensioni Proprietà Alcuni esempi di applicazioni tipiche: Modellazione di protocolli di routing di una Mobile Ad-hoc NETwork Abstract State Machine (ASM) Concetti di base Il metodo ASM Distributed Abstract State Machine Analisi di proprietà di sistemi mediante ASM Analisi della starvation e del deadlock mediante ASM Esempi di applicazione delle ASM: Modellazione di Grid - Modellazione di Kerberos - Modellazione di N-AODV e BN-AODV Communicating Sequential Processes (CSP) Introduzione a CSP Operatori per il parallelismo in CSP Esempio di applicazione: Introduzione alla sicurezza in CSP

Programma	
Testi di riferimento	E. Börger, R. Stärk, Abstract State Machine, Springer 2003 E. Börger, A. Raschke, Modeling Companion for Software Practitioners, Springer, 2018 C.A.R. Hoare, Communicating Sequential Processes, Prentice Hall International, 1985 (disponibile in

	http://www.usingcsp.com./cspbook.pdf) R. David, H. Alia, Discrete, Continuous, and Hybrid Petri Nets, Springer 2003 R. Milner, Communication and Concurrency, Prentice Hall International 1995 AA.VV. The Go Programming Language, (disponibile sul sito http://golang.org) AA.VV. Erlang Programming Language, (disponibile sul sito http://www.erlang.org)
Note ai testi di riferimento	Ulteriore materiale didattico, prodotto dal docente, sarà reso disponibile in ADA - Piattaforma e-learning del Dipartimento di Informatica. L'accesso è consentito solo agli studenti iscritti all'insegnamento Di ulteriori riferimenti di approfondimento sugli argomenti trattati saranno indicate le fonti bibliografiche
Metodi didattici	Lezioni frontali ed esercitazioni pratiche orientate al model checking per dare una rappresentazione formale astratta di un sistema, esprimere le proprietà da verificare in un opportuno formalismo e verificare se le proprietà sono soddisfatte nel modello
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	Tesina + prova orale Svolgimento di una prova in itinere durante il corso con eventuale valenza esonerante in vista dell'esame finale
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Verificare l'apprendimento dei concetti e le capacità di applicarli per risolvere problemi specifici La valutazione si articola in una parte generale su tutti gli argomenti trattati nel corso ed una parte di approfondimento in forma di tesina su un argomento specifico scelto dagli studenti. La tesina di approfondimento potrà avere sia natura concettuale che applicativa con la possibilità di approfondire qualsiasi argomento trattato durante il corso
Altro	Si consiglia la frequenza delle lezioni e lo studio costante durante lo svolgimento del corso, anche al fine di partecipare in maniera attiva alle esercitazioni pratiche che si svolgeranno durante le lezioni