Principali informazioni sull'insegnamento			
Titolo insegnamento	**Sicurezza nelle reti e nei sistemi distribuiti**		
Corso di studio	**LAUREA MAGISTRALE IN SICUREZZA INFORMATICA**		
Crediti formativi	6 (4+1+1)		
Denominazione inglese	Network and distributed systems security		
Obbligo di frequenza	no		
Lingua di erogazione	italiano		
Docente responsabile	Nome Cognome	Indirizzo Mail	
	Sebastiano Pizzutilo	sebastiano.pizzutilo@uniba.it	
Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	b	INF/01	4 T1 1 T2 1 T3
Modalità di erogazione			
Periodo di erogazione	I semestre		
Anno di corso	I		
Modalità di erogazione	Lezioni frontali, esercitazioni, presentazione e discussione progetto		
Organizzazione della didattica			
Ore totali	32+15+68+10+25= 150		
Ore di corso	32 ore di lezione frontale + 15 ore di esercitazione		
Ore di studio individuale	68+10+25 di progetto individuale		
Calendario			
Inizio attività didattiche	25 settembre 2018		
Fine attività didattiche	21 dicembre 2018		
Syllabus			
Prerequisiti	Conoscenza dell'architettura di un sistema di elaborazione digitale, dei protocolli di comunicazione digitale in reti di calcolatori e di matematica di base.		
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, compreso i risultati di apprendimento trasversali)	• ***Conoscenza e capacità di comprensione*** Lo studente dovrà acquisire ottime conoscenze e competenze riguardanti i concetti fondamentali della sicurezza digitale nelle comunicazioni di rete, le metodologie informatiche e gli strumenti tecnologici fondamentali per svolgere attività di ricerca, progettazione, sviluppo, testing e gestione di sistemi informatici sicuri. • ***Conoscenza e capacità di comprensione applicate*** Lo studente dovrà conoscere le tecniche, i metodi di progettazione e la realizzazione di sistemi informatici		

	sicuri, di base e applicativi, al fine di collaborare all'analisi e alla valutazione tecnica dello stato di sicurezza attuale di un sistema informatico; dovrà inoltre essere in grado di conoscere e proporre innovazioni che contraddistinguono la disciplina della sicurezza in rete e nei sistemi distribuiti. • ***Autonomia di giudizio*** Sulla base della conoscenza dei fondamenti essenziali della sicurezza delle reti e delle tecniche per la sicurezza nelle reti e nei sistemi distribuiti, lo studente dovrà avere la capacità di formulare valutazioni sulle scelte tecnico-progettuali relative alle infrastrutture di rete degli enti nei quali potrà operare. Lo studente dovrà inoltre essere in grado di proporre soluzioni volte al miglioramento della sicurezza di un sistema informatico. • ***Abilità comunicative*** Le abilità comunicative saranno sviluppate per consentire agli studente di interloquire con professionisti specialisti e non specialisti sulla analisi e valutazione dello stato di sicurezza attuale di un sistema informatico attraverso l'utilizzo di modelli e di evidenze empiriche. Lo studente dovrà saper proporre, motivare e valutare soluzioni alternative e selezionare le tecnologie più appropriate per gestire e manutenere un sistema informatico sicuro. Saranno svolte attività per migliorare la capacità di comunicazione e sintesi dei contenuti appresi e dei temi elaborati, favorendo in particolare lo svolgimento di presentazioni sia in lingua italiana sia in lingua inglese. Sarà inoltre favorita la partecipazione attiva a seminari e workshop organizzati con la collaborazione di professionisti ed esperti del settore. • ***Capacità di apprendere*** Verrà stimolata e valutata la conoscenza acquisita dallo studente inerente i metodi e le tecniche per la sicurezza delle reti e nei sistemi distribuiti, in relazione alle minacce, alle tipologie di attacchi, alle tecnologie disponibili per la sicurezza, per il rilevamento delle intrusioni e per il controllo degli accessi. Verranno valutate anche le conoscenze e competenze acquisite relative alle tecniche per la sicurezza in architetture orientate ai servizi (SoA) e nei sistemi distribuiti. Verranno valutate anche le capacità critiche dello studente nell'evidenziare le possibili implicazioni etiche delle

	tecniche e degli strumenti presentati nel corso, con evidente riferimento alla deontologia professionale delle diverse figure che operano nel settore della sicurezza informatica.
Contenuti di insegnamento	
Programma	1. Introduzione : la sicurezza digitale nelle reti 1.1 Elementi di base e terminologia della Network Security 1.2 Il modello di riferimento delle comunicazioni di rete ISO/OSI 1.3 L'architettura di sicurezza OSI : le raccomandazioni X800 1.4 Gli attacchi, i servizi ed i meccanismi per la Network Security 2 **Servizi per la sicurezza** 2.1 Autenticazione, X509 2.2. Controllo accessi, 2.3 Segretezza dei dati, 2.4 Non ripudiabilità, 3. **Meccanismi di sicurezza**: 3.1 cifratura, 3.2 firma digitale, 3.3 autenticazione, 3.4 algoritmi di Needham-Schroeder 3.5 controllo degli accessi 3.6 Integrità dei dati 3.7 PKI Systems **4. Attacchi alla sicurezza** 4.1 attacchi DoS *4.2 attacchi DDOS* **5 La sicurezza a livello di Sistema Operativo** 5.1. Introduzione 5.2 Secure Routing **6. La difesa** 6.1 . Designing Firewalls: A Survey 6.2 Classificazione dei Firewall 6.3 Security nelle Virtual Private Networks 6.4 Definizione e terminologia delle VPN 6.5 IP Security (IPSec) 6.6 IPSecArchitecture and Components **7. IDS e IPS** 7.1 IDS 7.2 IntrusionDetection Versus IntrusionProtection 7.3 IntrusionPrevention Systems **8. La sicurezza nei sistemi distribuiti** 8.1 Grid Security 8.2 Grid Security Infrastructure

	8.3 Grid Network Security **9 . La sicurezza nei sistemi wireless** 9.1. Mobile Agent Security 9.2 IEEE 802.11 Security 9.3 Wired Equivalent Privacy 9.4 Le Mobile Ad Hoc Networks 9.5 Vulnerabilità delle MANET **10. Il modello alla base della sicurezza e l'etica della sicurezza digitale**
Testi di riferimento	William Stallings Sicurezza delle reti ed. Pearson, Prentice Hall 2007 A.Tanenbaum, M. Van Steen Sistemi Distribuiti ed. Pearson, Prentice Hall 2007 cap. 9 Computer Security Handbook, Sixth Edition, Volume 1/ 2 Edited by Seymour Bosworth, Michel E. Kabay and Eric Whyne Copyright © 2014 by John Wiley & Sons, Inc.
(Note ai testi di riferimento)	Verranno distribuiti articoli scientifici pubblicati sulle più recenti ricerche sui temi del corso
Metodi didattici	Lezioni frontali, esercitazioni, attività di laboratorio. Il corso prevede lo svolgimento di attività individuali e di gruppo sotto il tutorato del docente nella forma di casi di studio.
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	prove in itinere ed esami che prevedono prove scritte e/o prove pratiche e/o colloqui orali.
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)	Una buona conoscenza della tassonomia della sicurezza digitale è un criterio di valutazione sufficiente dello studente. La capacità di interagire con gli altri studenti e di valutare criticamente un sistema di sicurezza valutandone gli aspetti tecnici e quelli etici sarà un ulteriore elemento di valutazione molto positiva.
Altro	