UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO | DIPARTIMENTO DI INFORMATICA

Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Sicurezza nelle Reti e nei Sistemi Distribuiti**	
Corso di studio	Laurea Magistrale in Sicurezza Informatica	
Anno Accademico	2024/25	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)		6 CFU
Settore Scientifico Disciplinare	INF/01	
Lingua di erogazione	Italiano	
Anno di corso	Primo	
Periodo di erogazione	2^semestre	
Obbligo di frequenza	La frequenza è fortemente raccomandata	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica	

Docente/i

Nome e cognome	Fabio Calefato
Indirizzo mail	fabio.calefato@uniba.it
Telefono	080 571 2213
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 665, 6^ piano
Sede virtuale	Piattaforma ADA - https://elearning.uniba.it
Sito web del docente	https://collab.di.uniba.it/fabio
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Venerdì dalle 11:00 alle 13:00, previo appuntamento

Syllabus

Obiettivi formativi	Lo studente apprenderà i concetti fondamentali della sicurezza delle reti di calcolatori e nei sistemi distribuiti, con particolare riferimento ai livelli applicativi della pila di protocolli TPC/IP.

Prerequisiti	Le seguenti conoscenze preliminari facilitano ed accelerano la comprensione degli argomenti dell'insegnamento: ● conoscenza dei principali protocolli di rete Internet.
Contenuti di insegnamento (Programma)	• Parte I: Fondamenti di crittografia applicata alla sicurezza delle reti ○ Riservatezza della comunicazione tramite cifratura simmetrica ○ Principi di cifratura simmetrica ○ Cifrari a blocchi e a flusso ○ Generatori di numeri casuali e pseudocasuali ○ Riservatezza della comunicazione tramite cifratura asimmetrica ○ Approcci all'autenticazione dei messaggi ○ Funzioni hash sicure e MAC ○ Principi di cifratura asimmetrica ○ Firma digitale • Parte II: Sicurezza nei protocolli di rete ○ Protocolli di distribuzione delle chiavi e autenticazione utente ○ Distribuzioni di chiave di cifratura tramite cifratura simmetrica ○ Cenni su Kerberos ○ Distribuzioni di chiavi tramite cifratura asimmetrica ○ Cenni su X.509 ○ Lo stack TCP/IP ○ Architettura dell'e-mail ○ Sicurezza nella posta elettronica: S/MIME e PGP ○ Sicurezza a livello di trasporto: HTTPS e SSH ○ Sicurezza a livello IP: IPSec ○ Internet Key Exchange ○ Cenni su sicurezza delle reti Wi-Fi • Parte III: Sicurezza dei sistemi ○ Malware e classificazione dei malicious software ○ Intrusion detection systems ○ Firewall
Testi di riferimento	Per i contenuti relativi alla sicurezza delle reti e dei sistemi: • William Stallings, Network Security Essentials: Applications and Standards (6th Edition), Pearson. Per la parte relativa alla descrizione dei protocolli di rete e dello stack TCP/IP: • J.F. Kurose & K.W. Ross, Reti di calcolatori e Internet - Un approccio top-down (8 edizione), Pearson.
Note ai testi di riferimento	I libri di testo sono integrati con gli appunti presi a lezione e con le slide del docente disponibili sulla piattaforma di e-learning ADA.

Organizzazione della didattica

Ore			
Totali	Didattica frontale	Pratica (laboratorio, progetto, esercitazione, altro)	Studio individuale
150 ore	32 ore	30 ore	88 ore
CFU/ETCS			
6 CFU	4 CFU	2 CFU	

Metodi didattici	
	Lezioni frontali supportate da slide ed esercitazioni in aula Lezioni in modalità flipped classroom.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	● *Conoscenza e capacità di comprensione* ○ Conoscere i concetti di base della sicurezza di rete. ○ Conoscere i fondamenti di crittografia applicati alla sicurezza in rete ○ Conoscere le principali forme di attacco alla sicurezza delle reti Conoscere le principali forme di difesa dagli attacchi alla sicurezza delle reti
Conoscenza e capacità di comprensione applicate	● *Conoscenza e capacità di comprensione applicate* ○ Acquisire familiarità con la prevenzione di attacchi che compromettano la disponibilità, l'integrità e la riservatezza delle informazioni scambiate in rete.
Competenze trasversali	**Autonomia di giudizio** ○ Mostrare di aver acquisito autonomia di giudizio sulle scelte relative alla sicurezza nel funzionamento delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Abilità comunicative** ○ Mostrare di essere in grado di comunicare in modo appropriato le caratteristiche e le specifiche tecniche relativamente alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Capacità di apprendere in modo autonomo** ○ Mostrare di aver sviluppato capacità di intraprendere in autonomia ulteriori approfondimenti su argomenti attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti.

Valutazione	
Modalità di verifica dell'apprendimento	L'esame si svolge mediante prova scritta (voto in trentesimi). Tale prova nel rispondere a un questionario contenente domande a risposta chiusa o aperta e brevi esercizi.
Criteri di valutazione	**Conoscenza e capacità di comprensione:** ○ Lo studente dovrà dimostrare di conoscere e di aver compreso i concetti fondamentali attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Conoscenza e capacità di comprensione applicate:** ○ Lo studente dovrà dimostrare di saper applicare i concetti fondamentali attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli

	applicativi distribuiti, al fine di evitare e prevenire minacce alla riservatezza, disponibilità, e integrità delle informazioni ivi scambiate. **Autonomia di giudizio:** ○ Lo studente dovrà dimostrare di saper formulare un proprio giudizio sulle scelte relative alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti **Abilità comunicative:** ○ Lo studente dovrà dimostrare di saper comunicare le conoscenze acquisite nonché motivare le proprie scelte implementative in modo appropriato, con riferimento alle caratteristiche tecniche attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti. **Capacità di apprendere:** ○ Lo studente dovrà dimostrare di aver acquisito la capacità di approfondire in autonomia gli argomenti attinenti alla sicurezza delle reti di calcolatori, dei protocolli di Internet, e degli applicativi distribuiti.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	I risultati di apprendimento previsti saranno misurati mediante prova scritta è valutata in trentesimi.
Altro	Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea ● https://www.uniba.it/it/ricerca/dipartimenti/informatica ● https://elearning.di.uniba.it/ I programmi degli insegnamenti sono disponibili qui: ● https://programmi.di.uniba.it/ Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

Main information on the course

Course name	**Security in Networks and Distributed Systems**
Degree	Laurea Magistrale in Sicurezza Informatica
Academic year	2024/25
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	6 CFU
Settore Scientifico Disciplinare	
Course language	Italian
Course year	First
Course period	2nd semester
Course attendance requirement	None, but it is highly recommended to attend classes
Website of the Degree	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica

Teacher(s)

Name and Surname	Fabio Calefato
email	fabio.calefato@uniba.it
phone	080 571 2213
office	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 665, 6^ piano
e-learning platform	ADA Platform - https://elearning.uniba.it/course/view.php?id=2796
Teacher's homepage	https://collab.di.uniba.it/fabio
Office hours	Friday 11:00 - 13:00, by appointment

Syllabus

Course goals	The student will learn the fundamental concepts of computer network security and distributed systems security, with particular emphasis on the application layers of the TCP/IP protocol stack.
Prerequisites/requirements	*The following preliminary knowledge facilitates and accelerates the understanding of the course topics:* • *knowledge of the main Internet network protocols.*
Course program	Part I: Fundamentals of cryptography applied to network security • Communication confidentiality through symmetric encryption • Principles of symmetric encryption • Block and stream ciphers • Random and pseudorandom number generators • Communication confidentiality through asymmetric encryption • Approaches to message authentication • Secure hash functions and MACs • Principles of asymmetric encryption • Digital signature Part II: Security in network protocols • Key distribution protocols and user authentication • Encryption key distributions through symmetric encryption • Overview of Kerberos • Key distributions through asymmetric encryption • Overview of X.509 • The TCP/IP stack • Email architecture

	• Email security: S/MIME and PGP • Transport layer security: HTTPS and SSH • IP layer security: IPSec • Internet Key Exchange • Overview of Wi-Fi network security Part III: System security • Malware and classification of malicious software • Intrusion detection systems • Firewalls
Books of reference	For content related to network and system security: • William Stallings, Network Security Essentials: Applications and Standards (6th Edition), Pearson. For the part related to the description of network protocols and the TCP/IP stack: • J.F. Kurose & K.W. Ross, Computer Networking: A Top-Down Approach (8th edition), Pearson.
Notes to the books	The textbooks are supplemented with notes taken during lectures and the instructor's slides available on the Ada e-learning platform.

Organization of the didactic activities

Hours			
Total	Lectures	Practice sessions	Individual study
150 hours	32 hours	30 hours	88 hours
CFU/ETCS			
6 CFU	4 CFU	2 CFU	

Teaching methods

- Lectures supported by slides and in-class exercises.
- Flipped classroom lectures

Expected learning outcomes

Knowledge and understanding	• Understand the basic concepts of network security. • Understand the fundamentals of cryptography applied to network security. • Understand the main forms of network security attacks. • Understand the main forms of defense against network security attacks.
Applying knowledge and understanding	• Gain familiarity with preventing attacks that compromise the availability, integrity, and confidentiality of information exchanged over the network.
Other skills	*Making judgements* • Demonstrate having acquired autonomy in judgment regarding choices related to the security of computer networks, Internet protocols, and distributed applications. *Communication* • Demonstrate the ability to appropriately communicate the characteristics and technical specifications related to the security of computer networks, Internet protocols, and distributed applications. *Learning skills*

	• Demonstrate having developed the ability to independently pursue further studies on topics related to the security of computer networks, Internet protocols, and distributed applications.

Assessment	
Assessment methods	The exam is conducted through a written test (graded out of thirty). This test involves answering a questionnaire containing multiple-choice or open-ended questions and brief exercises.
Evaluation criteria	**Knowledge and understanding:** The student must demonstrate knowledge and understanding of the fundamental concepts related to the security of computer networks, Internet protocols, and distributed applications. **Applied knowledge and understanding:** The student must demonstrate the ability to apply the fundamental concepts related to the security of computer networks, Internet protocols, and distributed applications in order to avoid and prevent threats to the confidentiality, availability, and integrity of the information exchanged therein. **Judgment autonomy:** The student must demonstrate the ability to formulate their own judgment regarding choices related to the security of computer networks, Internet protocols, and distributed applications. **Communication skills:** The student must demonstrate the ability to communicate the knowledge acquired and justify their implementation choices appropriately, with reference to the technical characteristics related to the security of computer networks, Internet protocols, and distributed applications. **Learning ability:** The student must demonstrate the ability to independently deepen their understanding of topics related to the security of computer networks, Internet protocols, and distributed applications.
Measurements and final grade	The expected learning outcomes will be measured through a written test and graded out of thirty.
Further information	Students are advised to rely exclusively on information and communications provided through the official websites of the Department of Computer Science or social groups if they are established and managed solely by the course instructors: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea • https://www.uniba.it/it/ricerca/dipartimenti/informatica • https://elearning.di.uniba.it/ Course syllabi are available here: • https://programmi.di.uniba.it Important information for all students is outlined in the academic regulations and study manifests available on the website:

	• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea Students are encouraged to be cautious of information and materials circulating on unofficial websites or social groups, as they often contain unreliable, incorrect, or incomplete information. For any doubts, students should request a meeting with the instructor following the procedures outlined for office hours.