Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**IoT Security**
Corso di studio	Corso di Laurea Magistrale in Computer Science (LM18)
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	Inglese
Anno di corso	Primo
Periodo di erogazione	2^semestre, le date esatte sono riportate nel manifesto/regolamento
Obbligo di frequenza	No, ma la frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Docente/i

Nome e cognome	Luigi Alfredo Grieco
Indirizzo mail	alfredo.grieco@poliba.it
Telefono	0805963911
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari.
Sede virtuale	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Sito web del docente	https://dei.poliba.it/alfredo-luigi-grieco
Ricevimento (giorni, orari e modalità, es. su appuntamento)	sempre disponibile a fissare appuntamenti ad hoc, previo contatto via mail.

Syllabus

Obiettivi formativi	Inquadrare le principali metodologie di progettazione di sistemi IoT sicuri

Prerequisiti	Prerequisiti culturali: conoscenza del networking e dei concetti di sistema distribuiti.
Contenuti di insegnamento (Programma)	**Parte I** I sistemi IoT: requisiti, casi d'uso e tecnologie. I sistemi wireless: metodologie di progettazione. La comunicazione a corto raggio: RFID, IEEE 802.15.4, BLE. La comunicazione a lungo raggio: LPWAN, SigFox, NB-IoT. **Parte II** Sicurezza nei sistemi IoT: privacy, controllo degli accessi, tecniche di cifratura, autenticazione, sicurezza fisica, sicurezza dei nodi terminali e delle infrastrutture di rete.
Testi di riferimento	● Parte I: The Internet of Things, connecting the objects to the web. Wiley. 2010. ● Parte II: William Stallings, Cryptography and Network Security: Principles and Practice. Pearson. VII Ed. 2016. Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	La bibliografia sarà integrata con le diapositive disponibili sulla piattaforma e-learning

Organizzazione della didattica

Ore

Totali	Didattica frontale	Laboratorio/esercitazione	Progetto	Studio individuale
62 ore	32 ore	30 ore	0 ore	90 ore

CFU/ETCS				
6 CFU	4 CFU	2 CFU	0 CFU	

Metodi didattici

Lezioni ed esercitazioni supportate da slide e dimostrazioni.

Risultati di apprendimento previsti

Conoscenza e capacità di comprensione	o apprendere i sistemi IoT: requisiti, casi d'uso e tecnologie. o apprendere i sistemi wireless: metodologie di progettazione o apprendere la comunicazione a corto raggio: RFID, IEEE 802.15.4, BLE. o apprendere la comunicazione a lungo raggio: LPWAN, SigFox, NB-IoT. o apprendere la Sicurezza nei sistemi IoT: privacy, controllo degli accessi, tecniche di cifratura, autenticazione, sicurezza
Conoscenza e capacità di comprensione applicate	● acquisizione delle competenze necessarie per risolvere problemi in aree nuove o non aree nuove o poco conosciute riguardanti questioni legate agli ecosistemi IoT. ● il corso è supportato da casi di studio reali e i contenuti sono ideali per gli sviluppatori che costruiranno le soluzioni IoT (sicure) del futuro.
Competenze trasversali	**Autonomia di giudizio** Integrazione delle conoscenze acquisite nel curriculum per gestire problemi complessi anche sulla base di informazioni limitate e incomplete. **Abilità comunicative** Capacità di comunicare i risultati ottenuti a interlocutori specialisti e interlocutori non specialisti, così come lo sviluppo di competenze collaborative indispensabili per il lavoro di gruppo **Capacità di apprendere in modo autonomo** Mostrare di aver sviluppato capacità di intraprendere in autonomia ulteriori approfondimenti su argomenti attinenti.

Valutazione	
Modalità di verifica dell'apprendimento	L'esame si svolge mediante prova orale (voto in trentesimi).
Criteri di valutazione	● **Conoscenza e capacità di comprensione:** lo studente dovrà dimostrare di conoscere e di aver compreso i concetti fondamentali attinenti: ● I sistemi IoT: requisiti, casi d'uso e tecnologie. ● I sistemi wireless: metodologie di progettazione. ● La comunicazione a corto raggio: RFID, IEEE 802.15.4, BLE. ● La comunicazione a lungo raggio: LPWAN, SigFox, NB-IoT. ● Sicurezza nei sistemi IoT: privacy, controllo degli accessi, tecniche di cifratura, autenticazione, sicurezza fisica, sicurezza dei nodi terminali e delle infrastrutture di rete. ● **Conoscenza e capacità di comprensione applicate:**

	Lo studente dovrà dimostrare di saper applicare i concetti fondamentali attinenti: ● I sistemi IoT: requisiti, casi d'uso e tecnologie. ● I sistemi wireless: metodologie di progettazione. ● La comunicazione a corto raggio: RFID, IEEE 802.15.4, BLE. ● La comunicazione a lungo raggio: LPWAN, SigFox, NB-IoT. ● Sicurezza nei sistemi IoT: privacy, controllo degli accessi, tecniche di cifratura, autenticazione, sicurezza fisica, sicurezza dei nodi terminali e delle infrastrutture di rete. ● **Autonomia di giudizio:** Lo studente dovrà dimostrare di saper formulare un proprio giudizio sulle scelte relative conoscenze acquisite. ● **Abilità comunicative:** Lo studente dovrà dimostrare di saper comunicare le conoscenze acquisite nonché motivare le proprie scelte implementative in modo appropriato. ● **Capacità di apprendere:** Lo studente dovrà dimostrare di aver acquisito la capacità di approfondire in autonomia gli argomenti di studio.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	I risultati di apprendimento previsti saranno misurati mediante prova orale e 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 ● https://www.uniba.it/it/ricerca/dipartimenti/informatica ● https://elearning.uniba.it/ I programmi di tutti gli insegnamenti sono disponibili al seguente link: ● https://elearning.uniba.it/ Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei regolamenti didattici dei Corsi di Studi disponibili nel sito: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/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. _____ Il link al corso sulla piattaforma e-learning del dipartimento: Piattaforma e-learning UNIBA - https://elearning.uniba.it/

Main information on the course

Course name	**IoT Security**
Degree	Master's Degree Course in Computer Science (LM18)
Academic year	2024/25
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	6 CFU (each CFU corresponds to 25 hours (h) of student's time); CFU are of type T1, T2 or T3 T1 = 8 h lecture + 17 h individual study T2 = 15 h practice + 10 h individual study T3 = 25 h individual study
Settore Scientifico Disciplinare	
Course language	English
Course year	First
Course period	Second Semester - exact dates can be found in the didactic regulations
Course attendance requirement	None, but it is highly recommended to attend classes
Website of the Degree	https://www.uniba.it/en/research/departements/computer-science?set_language=en

Teacher(s)

Name and Surname	Luigi Alfredo Grieco
email	alfredo.grieco@poliba.it
phone	0805963911
office	Department of Computer Science, Via Orabona 4, 70125, Bari.
e-learning platform	UNIBA e-learning platform - https://elearning.uniba.it/
Teacher's homepage	https://dei.poliba.it/alfredo-luigi-grieco
Office hours	Always available to make ad hoc appointments, by contacting us via email.

Syllabus

Course goals	Outline the main methodologies for designing secure IoT systems
Prerequisites/requirements	Cultural prerequisites: knowledge of networking and distributed systems.
Course program	**Part I** IoT systems: requirements, use cases and technologies. Wireless systems: design methodologies. Short range communication: RFID, IEEE 802.15.4, BLE. Long range communication: LPWAN, SigFox, NB-IoT. **Part II** Security in IoT systems: privacy, access control, encryption techniques, authentication, physical security, terminal node and infrastructure security net.
Books of reference	● Part I: The Internet of Things, connecting the objects to the web. Wiley. 2010.

	● Part II: William Stallings, Cryptography and Network Security: Principles and Practice. Pearson. VII Ed. 2016. Students who wish can borrow texts from the Library. Is it convenient to check availability via the University Library System https://opac.uniba.it/easyweb/w8018/index.php?lang=eng.
Notes to the books	The bibliography will be integrated with the slides available on e-learning platform

Organization of the didactic activities

Hours				
Total	Lectures	Practice sessions	Project work	Individual study
62 hours	32 hours	30 hours	0 hours	90 hours
CFU/ETCS				
6 CFU	4 CFU	2 CFU	0 CFU	

Teaching methods

	Lessons and exercises supported by slides and demonstrations.

Expected learning outcomes

Knowledge and understanding	o learn about IoT systems: requirements, use cases and technologies. o learn wireless systems: design methodologies o learn short-range communication: RFID, IEEE 802.15.4, BLE. o learn long range communication: LPWAN, SigFox, NB-IoT. o learn Security in IoT systems: privacy, control of access, encryption techniques, authentication, security
Applying knowledge and understanding	● acquisition of the skills necessary to solve problems in areas new or not new or little-known areas regarding issues related to IoT ecosystems. ● the course is supported by real case studies and the contents are ideal for students developers who will build the (secure) IoT solutions of the future.
Other skills	*Making judgements* Integration of acquired knowledge into the curriculum to manage problems complex even on the basis of limited and incomplete information. *Communication* Ability to communicate the results obtained to specialist and non-specialist interlocutors, as well as the development of collaborative skills essential for group work

	Learning skills Show that you have developed the ability to independently undertake further projects insights on relevant topics.

Assessment	
Assessment methods	The exam takes place through an oral test (grade out of thirty).
Evaluation criteria	● **Knowledge and understanding:** the student must demonstrate that he knows and understands the concepts relevant fundamentals: ● IoT systems: requirements, use cases and technologies. ● Wireless systems: design methodologies. ● Short range communication: RFID, IEEE 802.15.4, BLE. ● Long range communication: LPWAN, SigFox, NB-IoT. ● Security in IoT systems: privacy, access control, techniques encryption, authentication, physical security, end node security e of network infrastructures. ● **Applied knowledge and understanding:** The student must demonstrate the ability to apply the relevant fundamental concepts: ● IoT systems: requirements, use cases and technologies. ● Wireless systems: design methodologies. ● Short range communication: RFID, IEEE 802.15.4, BLE. ● Long range communication: LPWAN, SigFox, NB-IoT. ● Security in IoT systems: privacy, access control, techniques encryption, authentication, physical security, end node security e of network infrastructures. ● **Judgment autonomy:** The student must demonstrate that they are able to formulate their own judgment on the choices relating to acquired knowledge. ● **Communication skills:** The student must demonstrate the ability to communicate the knowledge acquired as well justify your implementation choices appropriately. ● **Ability to learn:** The student must demonstrate that he has acquired the ability to delve deeper into autonomy in the topics of study.
Measurements and final grade	The expected learning outcomes will be measured by oral exam and rated out of thirty.
Further information	Students are advised to rely exclusively on the information/communications provided on the official websites of the Department of Computer Science, or on social groups only if established and administered exclusively by the teachers of the relevant courses: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea ● https://www.uniba.it/it/ricerca/dipartimenti/informatica ● https://elearning.uniba.it/ The programs of all courses are available at the following link: ● https://elearning.uniba.it/

The information that all students should know is written in the teaching regulations of the Courses of Study available on the site:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea

Students are advised to be wary of information and materials circulating on unofficial sites or social groups, as they are often found to be unreliable , incorrect or incomplete . If you have any doubts, ask the teacher for a meeting according to the reception procedures.

The link to the course on the department's e-learning platform:

UNIBA e-learning platform - https://elearning.uniba.it/