



UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Ingegneria
ANNO ACCADEMICO OFFERTA	2023/2024
ANNO ACCADEMICO EROGAZIONE	2023/2024
CORSO DILAUREA MAGISTRALE	INGEGNERIA DEI SISTEMI CIBER-FISICI PER L'INDUSTRIA
INSEGNAMENTO	IOT E CLOUD SECURITY
TIPO DI ATTIVITA'	C
AMBITO	20917-Attività formative affini o integrative
CODICE INSEGNAMENTO	21507
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/03
DOCENTE RESPONSABILE	GIULIANO FABRIZIO Professore a contratto Univ. di PALERMO
ALTRI DOCENTI	
CFU	6
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	96
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	54
PROPEDEUTICITA'	
MUTUAZIONI	
ANNO DI CORSO	1
PERIODO DELLE LEZIONI	2° semestre
MODALITA' DI FREQUENZA	Facoltativa
TIPO DI VALUTAZIONE	Voto in trentesimi
ORARIO DI RICEVIMENTO DEGLI STUDENTI	GIULIANO FABRIZIO Lunedì 10:00 11:00

DOCENTE: Prof. FABRIZIO GIULIANO

PREREQUISITI	
RISULTATI DI APPRENDIMENTO ATTESI	<p>Conoscenza e capacità di comprensione</p> <p>Al termine del corso l'allievo avrà acquisito conoscenze e metodologie per per la realizzazione di sistemi IoT e cloud con riferimento alle problematiche della sicurezza. Nel corso verranno spiegate le modalità d'uso degli strumenti matematici e delle primitive crittografiche acquisite in corsi precedenti.</p> <p>Il corso riguarda la progettazione di sistemi IoT e cloud analizzando le problematiche tipiche di sicurezza in sistemi centralizzati e distribuiti in ambito industriale. Per ciascuno degli aspetti trattati sapranno riconoscere le principali caratteristiche, le metodologie analisi e di progettazione, problemi e relative contromisure.</p> <p>Capacità di applicare conoscenza e comprensione</p> <p>Le conoscenze spiegate durante le lezioni frontali verranno applicate in modo guidato durante le esercitazioni. Gli studenti applicheranno tali conoscenze in modo autonomo, durante la stesura dell'elaborato di progetto. Al termine del corso lo studente sarà in grado di applicare le conoscenze acquisite ed i concetti appresi nella progettazione di sistemi di comunicazioni per l'IoT a livello di protocollo e di sistema utilizzando protocolli di rete ed applicativi standard, ed introducendo tecniche crittografiche.</p> <p>Autonomia di giudizio</p> <p>Gli allievi saranno in grado di affrontare in autonomia problemi riguardanti gli argomenti del corso e prendere le opportune decisioni per trovare le relative soluzioni. Lo svolgimento delle esercitazioni fornirà un rinforzo delle conoscenze e abilità acquisite e costituirà uno strumento con cui lo studente potrà compiere l'autovalutazione del livello raggiunto.</p> <p>Abilità comunicative</p> <p>Al termine del corso l'allievo acquisirà l'uso del linguaggio tecnico relativo all'architettura IoT e Cloud, sarà capace di esporre con padronanza di linguaggio e con chiarezza le caratteristiche dei sistemi di comunicazione, prendendo in considerazione le problematiche di sicurezza e protezione contro l'uso non autorizzato di dati elettronici. L'allievo saprà interloquire con colleghi progettisti e con i tecnici per affrontare e risolvere problemi progettuali e di sviluppo dei sistemi IoT e Cloud.</p> <p>Capacità d'apprendimento</p> <p>La capacità di apprendimento degli allievi verrà stimolata con l'uso di tecniche quali il project work, il cooperative learning ed il brain-storming, utilizzate soprattutto durante le fasi di esercitazione. Lo studente sarà in grado di approfondire in modo autonomo gli argomenti affrontati.</p>
VALUTAZIONE DELL'APPRENDIMENTO	<p>La valutazione degli allievi sarà effettuata con differenti modalità: prova scritta e realizzazione di progetto ed elaborato breve.</p> <p>Il voto complessivo sarà il valore medio ottenuto dalla valutazione della prova scritta e del progetto.</p> <p>Esito del voto</p> <p>30-30 e lode: Eccellente/ottimo. Ottima conoscenza degli argomenti, ottima capacità analitica anche in nuovi contesti; ottima proprietà di linguaggio e di apprendimento.</p> <p>27-29: Molto buono. Lo studente dimostra padronanza degli argomenti, piena proprietà di linguaggio, è in grado di applicare le conoscenze per risolvere i problemi proposti.</p> <p>24-26: Buono. Conoscenza di base dei principali argomenti, discreta proprietà di linguaggio, con limitata capacità di applicare autonomamente le conoscenze alla soluzione dei problemi proposti.</p> <p>21-23: Soddisfacente. Parziale padronanza degli argomenti del corso, soddisfacente proprietà linguaggio, scarsa capacità di applicare autonomamente le conoscenze acquisite.</p> <p>18-20: Sufficiente. Minima conoscenza degli argomenti del corso e del linguaggio tecnico, scarsissima o nulla capacità di applicare autonomamente le conoscenze acquisite.</p> <p>Insufficiente: non possiede una conoscenza accettabile dei contenuti degli argomenti trattati nell'insegnamento.</p>
OBIETTIVI FORMATIVI	<p>Il corso si propone di fornire un'introduzione all'architettura IoT e cloud fornendo concetti di sicurezza dei dati e della loro comunicazione, tenendo conto delle vulnerabilità dei sistemi e dei protocolli presentando le primitive crittografiche e le modalità operative standardizzate per il loro corretto utilizzo in applicazioni reali. Un primo obiettivo formativo prevede l'analisi e la comprensione delle metodologie di comunicazione di rete, dei protocolli e dei sistemi hardware e software, e l'integrazione con piattaforme cloud per la raccolta e la gestione dei dati. Saranno analizzate le problematiche tipiche di sicurezza introducendo metodologie per la loro rivelazione e l'adozione di relative contromisure.</p>
ORGANIZZAZIONE DELLA DIDATTICA	<p>Il corso si compone di lezioni frontali per tutti gli argomenti. Per alcuni argomenti sono previste anche delle esercitazioni teoriche e lo svolgimento guidato di esercizi.</p> <p>Ciascuno degli argomenti viene affrontato sotto tre aspetti complementari: i</p>

	<p>contenuti teorici, le vulnerabilità, le contromisure.</p> <p>Le lezioni frontali mirano a formare gli studenti stimolando la loro capacità di comprensione ed evidenziando gli aspetti più importanti della materia. Le esercitazioni teoriche hanno l'obiettivo di stimolare negli allievi la capacità d'apprendimento e di problem solving. Le attività di laboratorio, in parte svolte in gruppo, consentono agli allievi di esercitare la propria capacità di applicare conoscenza e comprensione, aumentando l'autonomia di giudizio e migliorando le abilità di comunicazione e di collaborazione.</p> <p>Gli studenti vengono guidati dal docente in tutte le fasi del loro apprendimento, mediante un continuo scambio tra riferimenti teorici ed attività laboratoriali.</p>
TESTI CONSIGLIATI	<p>Course slides (available on the instructor's website). Selected articles from scientific literature on course topics.</p> <p>Designing the Internet of Things Adrian McEwen, Hakim Cassimally Stallings, "Wireless Communications and Networks", Prentice Hall, 2001 Introduction to Wireless & Mobile Systems, 3rd edition (Dharma Prakash Agrawal and Qing-An Zeng) William Stallings - Cryptography and Network Security, Seventh Edition, ISBN 10: 1292158581 ISBN 13: 9781292158587 Dan Boneh and Victor Shoup - A Graduate Course in Applied Cryptography, Version 0.5, Jan. 2020 - http://toc.cryptobook.us/book.pdf</p>

PROGRAMMA

ORE	Lezioni
4	Introduzione: Architettura IoT e cloud, ecosistema, sensing, comunicazione, protocolli internet, rischi per la sicurezza nell'IoT
4	Modelli di minacce per l'IoT ed il cloud (framework STRIDE, Jamming, HW integrity attack, tampering,...)
4	Tecnologie di comunicazione a medio raggio: lo standard 802.11. Architetture e sicurezza
4	Tecnologie di comunicazione a corto raggio: Bluetooth. Architettura e sicurezza
4	Tecnologie di comunicazione a lungo raggio: LoRaWAN, architettura e sicurezza
4	Cenni di reti internet, livello di rete e di trasporto.
4	Dispositivi IoT, Sensori, attuatori, gestione dell'energia
6	Programmazione di board IoT: Arduino.
4	Tecniche crittografiche per confidenzialità ed integrità
4	Metodologie di test sulla sicurezza nei sistemi IoT
4	SSL, TLS, HTTPS, SSH, gestione dell'identità
4	Protocolli applicativi per IoT: REST, MQTT e AMQP. Tecniche di sicurezza e minacce
4	Introduzione a Sistemi cloud e virtualizzazione