UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Matematica e Informatica
ANNO ACCADEMICO OFFERTA	2018/2019
ANNO ACCADEMICO EROGAZIONE	2018/2019
CORSO DILAUREA MAGISTRALE	INFORMATICA
INSEGNAMENTO	CYBERSECURITY
TIPO DI ATTIVITA'	C
AMBITO	20903-Attività formative affini o integrative
CODICE INSEGNAMENTO	19220
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/03
DOCENTE RESPONSABILE	GALLO PIERLUIGI Professore Associato Univ. di PALERMO
ALTRI DOCENTI	
CFU	6
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	102
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	48
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	**GALLO PIERLUIGI** Venerdì 15:00 17:00 Ufficio del docente

DOCENTE: Prof. PIERLUIGI GALLO

PREREQUISITI	Conoscenze di base di reti di calcolatori e di programmazione in Java o Python.
RISULTATI DI APPRENDIMENTO ATTESI	Conoscenza e capacita' di comprensione Al termine del corso l'allievo avra' acquisito le conoscenze sulla sicurezza, legati alla cifratura, alla sicurezza di sistema e di rete. Gli studenti acquisiranno gli strumenti matematici e gli algoritmi piu' diffusi per la sicurezza, la segretezza e la confidenzialita'. In particolare, gli allievi acquisiranno gli strumenti matematici, le primitive crittografiche e le modalita' operative per garantire confidenzialita' e integrita' dei dati sia nell'immagazzinamento che nel trasferimento dell'informazione, nonche' strumenti e metodologie per lo scambio delle chiavi crittografiche ed elementi di base delle criptovalute. Per ciascuno degli aspetti trattati sapranno riconoscere le principali vulnerabilita', le metodologie di attacco e le relative contromisure. Capacita' di applicare conoscenza e comprensione 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 sara' in grado ai applicare le conoscenze acquisite ed i concetti appresi nella progettazione di sistemi di sicurezza a livello di protocollo e di sistema utilizzando primitive crittografiche e modalita' operative standardizzate, nella valutazione delle vulnerabilita' offerte da sistemi, protocolli ed applicazioni e nell'applicazione di contromisure per ridurre ed eventualmente eliminare le vulnerabilita' rilevate. Autonomia di giudizio 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 fornira' un rinforzo delle conoscenze e abilita' acquisite e costituira' uno strumento con cui lo studente potra' compiere l'autovalutazione del livello raggiunto. Abilita' comunicative Al termine del corso l'allievo acquisira' l'uso del linguaggio tecnico relativo alla cybersecurity capace di esporre con padronanza di linguaggio e con chiarezza le caratteristiche dei sistemi di sicurezza, per garantire la protezione contro l'uso criminale o non autorizzato di dati elettronici, e di discutere dell'applicazione di opportune contromisure. L'allievo sapra' interloquire con colleghi progettisti e con i tecnici per affrontare e risolvere problemi relativi alla sicurezza delle reti e dei sistemi. Capacita' d'apprendimento La capacita' di apprendimento degli allievi verra' 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 sara' in grado di approfondire in modo autonomo gli argomenti affrontati.
VALUTAZIONE DELL'APPRENDIMENTO	La valutazione degli allievi sara' effettuata con differenti modalita: prova orale, progetto ed elaborato breve, discussione di un articolo scientifico. Tale molteplicita' di strumenti consentira' di valutare il raggiungimento dei risultati attesi. La conoscenza, la capacita' di comprensione e le capacita' comunicative verranno valutate mediante la prova orale. Le capacita' di applicare la conoscenza degli argomenti teorici sara' valutata mediante la predisposizione di un elaborato breve a corredo di un progetto assegnato. L'autonomia di giudizio e le capacita' di selezionare materiale di studio in modo autonomo saranno valutate mediante la discussione di un articolo scientifico a scelta dell'allievo, riguardante gli aspetti scientifici di uno degli argomenti del corso. Il voto complessivo sara' il valore medio ottenuto dalla valutazione delle tre componenti sopra indicate. Esito del voto 30-30 e lode: Eccellente/ottimo. Ottima conoscenza degli argomenti, ottima capacita' analitica anche in nuovi contesti; ottima proprieta' di linguaggio e di apprendimento. 27-29: Molto buono. Lo studente dimostra padronanza degli argomenti, piena proprieta' di linguaggio, e' in grado di applicare le conoscenze per risolvere i problemi proposti. 24-26: Buono. Conoscenza di base dei principali argomenti, discreta proprieta' di linguaggio, con limitata capacita' di applicare autonomamente le conoscenze alla soluzione dei problemi proposti. 21-23: Soddisfacente. Parziale padronanza degli argomenti del corso, soddisfacente proprieta' linguaggio, scarsa capacita' di applicare autonomamente le conoscenze acquisite.

	18-20: Sufficiente. Minima conoscenza degli argomenti del corso e del linguaggio tecnico, scarsissima o nulla capacita' di applicare autonomamente le conoscenze acquisite. Insufficiente: non possiede una conoscenza accettabile dei contenuti degli argomenti trattati nell'insegnamento.
OBIETTIVI FORMATIVI	Il corso si propone di fornire un'introduzione alla cybersecurity, tenendo conto delle vulnerabilita' dei sistemi e dei protocolli presentando le primitive criptografiche e le modalita' operative standardizzate per il loro corretto utilizzo in applicazioni reali. Gli argomenti trattati tengono conto sia degli aspetti di sicurezza di protocollo che di sistema. Il corso si propone i seguenti obiettivi formativi, raggruppati per tipologia di argomento. Un primo obiettivo formativo prevede l'analisi e la comprensione delle vulnerabiilta' delle reti, dei protocolli e dei sistemi hardware e software, i vari tipi di attacchi, le modalita' per la loro rivelazione e le relative contromisure. Un secondo obiettivo formativo riguarda l'uso di primitive crittografiche standardizzate per la cifratura di flussi, a blocchi, metodi per garantire l'autenticita' dei messaggi, per gestire le chiavi crittografiche, per firmare digitalmente dei documenti. Un terzo obiettivo formativo e' quello di rendere gli studenti capaci di valutare i benefici e le problematiche relative agli approcci centralizzati e decentralizzati ed i meccanismi di base che sottendono alle crypto valute, quali ad esempio il blockchain e renderli capaci di utilizzarli in vari contesti applicativi.
ORGANIZZAZIONE DELLA DIDATTICA	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. Ciascuno degli argomenti viene affrontato sotto tre aspetti complementari: i contenuti teorici,le vulnerabilita, le contromisure. Le lezioni frontali mirano a formare gli studenti stimolando la loro capacita' di comprensione ed evidenziando gli aspetti piu' importanti della materia. Le esercitazioni teoriche hanno l'obiettivo di stimolare negli allievi la capacita' d'apprendimento e di problem solving. Le attivita' di laboratorio, in parte svolte in gruppo, consentono agli allievi di esercitare la propria capacita' di applicare conoscenza e comprensione, aumentando l'autonomia di giudizio e migliorando le abilita' di comunicazione e di collaborazione. Gli studenti vengono guidati dal docente in tutte le fasi del loro apprendimento, mediante un continuo scambio tra rifereimenti teorici ed attivita' laboratoriali.
TESTI CONSIGLIATI	- D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, Ver. 0.4 - Sep. 30, 2017 https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup04.pdf - Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

PROGRAMMA

ORE	Lezioni
2	Introduzione alla cifratura simmetrica
2	generatori di numeri pseudocasuali e predicibilita'
2	sicurezza semantica, cifratura a blocchi, PRP
2	DES
2	Reti di Feistel e teorema di Luby-Rackoff
2	AES
2	cifrari a blocchi da PRG. Il metodo GGM
2	Modalita' operative e vulnerabilita'
2	Integrita' del messaggio
2	Certificati digitali
2	Firma digitale
2	SSL e TLS
2	Crittografia a chiave pubblica
2	La gestione delle chiavi
1	Password, phishing, spoofing
1	Smart cards
2	Vulnerabilita' di rete e delle applicazioni
2	Attacchi passivi ed attivi
2	Minacce persistenti avanzate
2	Identificazione, autenticazione, gestione degli accessi
1	One time passwords
2	firewall, IDS e IPS

PROGRAMMA

ORE	Lezioni
2	Consenso distribuito
2	Blockchain
2	Sistema di incentivi
1	Panoramica su approcci avanzati