Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI PRINCIPI E METODI DI CRITTOGRAFIA

SETTORE SCIENTIFICO

CFU

6

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI

/**/
L'obiettivo del corso è fornire agli studenti le conoscenze teoriche alla base dei principali algoritmi/protocolli crittografici impiegati in sicurezza informatica e rendere gli studenti in grado di applicare tali conoscenze nello sviluppo di sistemi software che offrano un determinato livello di sicurezza. Verrà evidenziato che la maggior parte degli attacchi informatici è rivolto alle vulnerabilità che si celano all'interno delle applicazioni software, che forniscono un facile percorso d'ingresso per compromettere i sistemi o lanciare attacchi informatici e malware. Saranno illustrate metodologie di progettazione e programmazione che garantiscano la sicurezza del codice. Saranno introdotti principi di gestione del rischio informatico e della sicurezza nei sistemi informativi alla luce degli adempimenti legislativi da rispettare.

RISULTATI DI APPRENDIMENTO ATTESI

/**/
Conoscenza e capacità di comprensione

Lo studente acquisirà la conoscenza delle fondamentali metodologie in materia di sicurezza informatica riconducibile ad una buona ingegnerizzazione del software, e sarà consapevole della necessità di applicarle per rispondere alla domanda di sicurezza e per ridurre i costi che comporta il trascurarle. Verrà illustrata l'analisi della sicurezza del software rivolta alla individuazione delle vulnerabilità.

Capacità di applicare conoscenza e comprensione

Lo studente acquisirà la capacità di valutare il codice software e le applicazioni al fine di identificare le vulnerabilità. Sarà in grado di implementare opportune attività che garantiscano la sicurezza nel corso di tutte le fasi del ciclo di vita del software, dalla analisi alla progettazione, sviluppo, test fino alla manutenzione.

Autonomia di giudizio

Lo studente sarà in grado di valutare le problematiche connesse alla sicurezza informatica in tutte le fasi del ciclo di sviluppo software nei vari ambiti di applicazione.

Abilità comunicative

Lo studente saprà presentare gli argomenti svolti nel corso con rigore formale e completezza.

Capacità di apprendimento

Lo studente sarà in grado di consultare la letteratura scientifica del settore per approfondire autonomamente gli argomenti del corso in relazione ad aspetti formali non approfonditi durante le lezioni.

Programma didattico

Programma didattico (per macro aree + numero lezioni previste)

1. Nozioni di sicurezza informatica. Cenni al Management della Sicurezza in Azienda. Tipi di attacchi (attivi e passivi), Servizi di sicurezza, Meccanismi di sicurezza. (lezioni previste n. 9)

2. Introduzione alla crittografia. Crittografia classica. Crittoanalisi e attacchi bruteforce. Cifrari simmetrici ed a chiave pubblica. Crittografia moderna (principi). Cifratura asimmetrica. Autenticazione di messaggi basata su cifratura simmetrica, asimmetrica o su MAC. Firma Digitale. Vulnerabilità dei protocolli di firma. (lezioni previste n. 9)

3. Introduzione alle problematiche di sicurezza in rete. Autenticazione. Protocolli di tipo challenge-response. Sicurezza web e vulnerabilità di siti Web. (lezioni previste n. 9)

4. Sicurezza di Sistema e del Codice, Intrusioni, Gestione delle Password, Software malicious (virus, worm, spyware, trojan, etc.). (lezioni previste n. 9)

Modalità di raccordo con altri insegnamenti (indicare le modalità e gli insegnamenti con i quali sarà necessario raccordarsi)

Nessun raccordo

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

/**/
L’esame può essere sostenuto sia in forma scritta che in forma orale.

L’esame orale consiste in un colloquio nel corso del quale il docente formula di solito tre domande. L’esame scritto consiste nello svolgimento di un test con 31 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.

Sia le domande orali che le domande scritte sono formulate per valutare sia il grado di comprensione delle nozioni teoriche sia la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l’elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dallo studente.

Le abilità di comunicazione e la capacità di apprendimento saranno valutate attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze, e-tivity report, studio di casi elaborati) proposti dal docente o dal tutor.

MODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI

/**/
L’iscrizione ed i rapporti con gli studenti sono gestiti mediante la piattaforma informatica che permette l’iscrizione ai corsi, la fruizione delle lezioni, la partecipazione a forum e tutoraggi, il download del materiale didattico e la comunicazione con il docente.

Un tutor assisterà gli studenti nello svolgimento di queste attività.

Attività di didattica erogativa (DE) 36 Videolezioni + 36 test di autovalutazione

Impegno totale stimato: 36 ore

Attività di didattica interattiva (DI) ed e-tivity con relativo feed-back al singolo studente da parte del docente o del tutor Redazione di un elaborato

Partecipazione a una web conference

Svolgimento delle prove in itinere con feedback

Svolgimento della simulazione del test finale

Totale 6 ore

Attività di autoapprendimento 108 ore per lo studio individuale

Libro di riferimento Dispense del docente.

LEZIONI

/**/
1 - Le basi della crittografia

2 - Crittografia simmetrica

3 - Crittografia asimmetrica

4 - Gli Algoritmi di Hash

5 - PKI

6 - Certificati X509

7 - Firma digitale

8 - RSA

9 - Curve ellittiche

10 - FIDO2

11 - Protocolli di scambio chiavi11

12 - TLS

13 - Attacchi MITM

14 - Crittografia e blockchain

15 - Crittografia Quantistica

16 - Password cracking

17 - Introduzione alla Malware Analysis

18 - Malware Storici e il processo di Malware Analysis

19 - Analisi Statica

20 - Analisi Dinamica

21 - Analisi Avanzata

22 - Analisi delle vulnerabilità sfruttate dagli malware

23 - Ambiente di laboratorio per l’analisi malware

24 - Tool di Analisi del Malware

25 - Analisi del Network Traffic

26 - Tecniche di evasione del malware

27 - Analisi di Particolari Infection Chain

28 - Threat Intelligence

29 - Indicatori di Compromissione e Modelli di Threat Intelligence

30 - Rilevamento del Malware e Prevenzione

31 - Windows Events e Regole di Rilevamento

32 - Computer Virology

33 - Meccanismi di difesa

34 - I sistemi operativi mobili

35 - Malware Analysis

36 - Android Malware Dissection Il/la docente si riserva il diritto di modificare l'elenco delle videolezioni