REGOLAMENTO DIDATTICO E ORGANIZZATIVO DEL CORSO *MINOR* IN

Cybersecurity IT e OT

PARTE I – INFORMAZIONI GENERALI

Proposta di attivazione

prima istituzione

Anno accademico

2023-24

Dipartimento di riferimento

Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche

Corso interdipartimentale

no

Organo di gestione

L'organo collegiale di gestione è il Collegio Didattico di Ingegneria Informatica, Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche

Collaborazione con ente esterno

no

PARTE II – ORGANIZZAZIONE DIDATTICA E AMMINISTRATIVA

Il corso in breve

La protezione dei sistemi informatici, delle reti e dei programmi dagli attacchi digitali sta assumendo una sempre maggiore rilevanza nella società moderna.

Attualmente, sia individui, sia organizzazioni, possono essere oggetto di attacchi informatici, solitamente finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni sensibili e all'estorsione. Con l'avvento della quarta rivoluzione industriale, facilitata dalle comunicazioni 5g, anche il mondo produttivo e quello delle grandi infrastrutture critiche sono divenuti oggetto di attacchi informatici. Il fine ultimo è quello di causare malfunzionamenti o blocchi con conseguente riduzione di operatività, elevato danno economico e un accresciuto rischio per la popolazione.

Il corso vuole costituire una offerta formativa di alto livello sia per gli studenti di Roma Tre, sia per professionisti esterni, nel settore della cybersecurity. In particolare, verranno affrontate tematiche di base ed avanzate relative a due tipologie di applicazioni: quelle più propriamente appartenenti al settore dell'Information Technology tradizionale (IT) e quelle che fanno riferimento all'Operation Technology (OT) ovvero sistemi a logiche programmabili (PLC) e sistemi di supervisione di impianto (SCADA).

Le lezioni del corso minor sono offerte in modalità *blended* al fine di ottimizzare la partecipazione a tutte le attività formative da parte degli studenti dell'Ateneo, nonché garantire la fruibilità a studenti esterni o studenti lavoratori. La modalità *blended* consiste nell'offrire, oltre alla didattica tradizionale svolta in aula, streaming e registrazioni delle lezioni, il tutto combinato con strategie didattiche che creino un setting formativo collaborativo in grado di mettere lo studente al centro del processo di apprendimento rendendolo attivo e proattivo.

Lista delle attività didattico-formative che compongono il corso

GOMP	attività didattico-formativa e relativo SSD	semestre	docente e relativo SSD	ore di didattica assistita	CFU
20801961	Sistemi Operativi (ING-INF/05)	I	Stefano Iannucci (ING-INF/05)	54	6
20810140	Cybersecurity (ING-INF/05)	I	Maurizio Pizzonia (ING-INF/05)	54	6
20801960	Reti e Sistemi per l'Automazione (ING-INF/04)	II	Chiara Foglietta (ING-INF/04)	54	6
20810206	Sistemi IoT per le Grandi Infrastrutture (ING-INF/04)	II	Stefano Panzieri (ING-INF/04)	54	6
TBD	Cyber Intelligence*	II	Selene Giupponi	27	3

TBD	Opacity and cybersecurity in discrete event systems*	I	Federica Pascucci e Graziana Cavone	9	1

*Il corso è attivato all'interno del percorso minor. Non sono previsti oneri finanziari su tale corso in quanto corso di dottorato coperto come compito didattico (e/o a titolo gratuito) da personale interno o esterno al Dipartimento di riferimento

Ulteriori informazioni sulle attività didattico-formative

Sistemi Operativi (Operating Systems).

Programma:

I sistemi operativi costituiscono l'ambiente principale in cui vengono eseguiti tutti gli applicativi e i servizi dei sistemi informatici. Pertanto, sono elementi estremamente critici per quanto concerne la loro sicurezza. Il corso di Sistemi Operativi mira a fornire agli studenti una solida comprensione dei principi fondamentali di questi ambienti.

In particolare, verranno trattati algoritmi di scheduling, processi, e thread. Inoltre, verranno affrontate tematiche relative alla virtualizzazione e alla gestione della memoria principale e secondaria, incluse le tecniche di paging e di segmentazione. Per quanto concerne invece la memoria secondaria, saranno trattate le basi della gestione dei file e dei filesystem. Infine, verranno introdotte tecniche e librerie per la comunicazione e la sincronizzazione, necessarie per la programmazione parallela. Questa base teorica consentirà agli studenti di comprendere il funzionamento interno dei sistemi operativi e la gestione delle risorse di sistema fornendo le basi per l'analisi delle vulnerabilità informatiche di questi sistemi.

Lingua di svolgimento: italiano

Testi adottati: Andrew S. Tanenbaum, Herbert Bos. Modern. I Moderni Sistemi Operativi quinta edizione. Pearson, 2023.

Modalità di erogazione: *blended*

Modalità di valutazione: esame scritto. La valutazione tende ad accertare la conoscenza delle nozioni di basi sui sistemi operativi e della programmazione parallela.

Cybersecurity

Programma:

Il corso in cybersecurity ha come obiettivo di fornire un quadro organico dei vari aspetti della sicurezza per sistemi informatici e delle reti. Inoltre, fornisce strumenti metodologici per comprendere, valutare e progettare gli aspetti di sicurezza per tali sistemi. Più in dettagli il corso prevede i seguenti argomenti.

Vulnerabilità di software e reti: input fidato e non fidato, validazione dell'input. Vulnerabilità di applicazioni scritte in linguaggi interpretati, code injection. Injection in pagine web: XSS. Cross site request forgery. OWASP. Attacchi di tipo buffer overflow, privilege excalation,

intrusioni via rete tramite servizi aperti, intrusione via documenti non fidati (via e-mail, via web o altro). Sniffing, mac flood, ARP poisoning, vulnerabilità del DNS, attacco di Kaminsky. TCP session hijecking, attacchi MitM, DoS e Distributed DoS, Route hijecking.

Pianificazione della sicurezza: contenuti del piano di sicurezza, analisi dei rischi.

Contromisure: principi di progettazione di politiche e meccanismi di sicurezza. Modelli: AAA, confinamento, DAC, MAC, access control matrix. Tecniche crittografiche: richiami di crittografia (hash, message authentication codes, crittografia simmetrica, stream/block ciphers, operation modes, crittografia asimmetrica, firma digitale), attacchi birthday, rainbow, qualità delle chiavi, generazione di numeri pesudo-casuali. Protocolli di autenticazione e di scambio di chiavi. Attacchi replay e reflection. Nonces. Perfect Forward Secrecy. Diffie-Helman. Certificati, certification authority, public key infrastructure e loro vulnerabilità. Applicazioni della crittografia: protocolli ssl, tls, ssh, virtual private network, ipsec, ecc. Protocolli di autenticazione punto-punto e in rete locale, radius. Altre applicazioni. Considerazioni sui sistemi per la rilevazione automatica dei problemi (quali IDS statistici e basati su intelligenza artificiale), falsi positivi e negativi. Sicurezza dei sistemi: passwords e loro vulnerabilità, metodologia di hardening, assessment e auditing. unix: controllo di accesso discrezionario, sicurezza nel filesystem, autenticazione, PAM, syslog. Sicurezza delle reti: Firewalling: firewall stateless e statefull, connessioni, syn-proxy e syn-cookies, load balancing e high availability, linux netfilter ed esempi di configurazioni. Sicurezza di rete a livello 1 e 2. Proxy applicativi, Intrusion detection systems di rete. Authenticated Data Structures. Distributed Ledger Technologies and Bitcoin. Smart contracts. Cybersecurity nelle grandi organizzazioni.

Lingua di svolgimento: italiano

Testi adottati: dispense fornite dal docente

Modalità di erogazione: *blended*

Modalità di valutazione: Esame scritto + progetto/tesina. Per il progetto, il docente propone una lista di argomenti ma gli studenti possono proporre argomenti di proprio interesse (es, gli studenti lavoratori possono proporre argomenti che risultano rilevanti nel proprio contesto lavorativo).

Reti e Sistemi per l'Automazione (Industrial Control Systems and Networks)

Programma: il programma del corso inizia con l'analisi delle caratteristiche del mondo OT e di come in tale ambiente le problematiche per la realizzazione e la sicurezza di un sistema informatico siano profondamente diverse rispetto al mondo IT. Per questa ragione, è necessario analizzare e comprendere le caratteristiche dei sistemi di controllo OT, come PLC (Programmable Logic Controller) e sistemi SCADA (Supervisory Control And Data Acquisition), e dei loro specifici protocolli di comunicazione. I protocolli di comunicazione nel mondo industriale sono molteplici ed eterogenei. Per questa ragione, il corso prevede un'analisi critica dei principali protocolli di comunicazione (ad esempio PROFIBUS, MODBUS, CANBUS) e delle ultime innovazioni (come PROFINET, ETHERCAT, DNP3.0, OPC UA) per comprendere le ragioni per cui tali sistemi siano attualmente uno dei maggiori

obiettivi per attacchi cyber che possono causare problemi per risvolti ambientali, psicologici sulla popolazione, economici e di sicurezza.

Lingua di svolgimento: italiano

Testi adottati:

Pasquale Chiacchio, Francesco Basile “Tecnologie informatiche per l’automazione,” seconda edizione, McGraw-Hill Libri Italia, 2004.

C. Bonivento, L. Gentile, A. Paoli, “Sistemi di automazione industriale: architetture e controllo”. McGraw-Hill, 2011

W. Bolton, Programmable Logic Controllers, Sixth Edition, Newnes, 2015 ISBN 9780128029299

Knapp, E.D. and Langill, J.T., Industrial Network Security, Second Edition, Syngress, 2014 ISBN 0124201148

Modalità di erogazione: *blended*

Modalità di valutazione: Elaborazione di un progetto ed esame orale. La valutazione accerta le conoscenze di base per quello che riguarda PLC e sistemi SCADA e i principali protocolli di comunicazione. Lo studente deve dimostrare una capacità critica per i sistemi e i protocolli del mondo OT.

Sistemi IoT per le Grandi Infrastrutture (OT Cybersecurity)

Programma: il rischio cyber per la Operational Technology, in costante ascesa in tutte le analisi in termini sia quantitativi, sia di criticità, è oggi ai primi posti in tutte le agende Nazionali ed Europee. Il corso esaminerà i diversi contesti, dal manifatturiero alle infrastrutture critiche, per analizzare rischi e vulnerabilità connessi alla minaccia cyber. Verranno descritti i principali vettori di attacco e come questi abbiamo effetti sulle architetture informatiche tipiche dei sistemi OT sia relativamente agli apparati informatici, sia in relazione alle reti industriali più diffuse. Saranno introdotte le tematiche sulla interdipendenza e complessità nei sistemi infrastrutturali e verranno forniti supporti normativi e tecnologici per la valutazione del rischio in presenza di forti interconnessioni. Dal punto di vista delle contromisure saranno esaminati i principali apparati informatici per il mondo OT in grado di analizzare tali reti e di intercettare possibili attacchi. Verranno inoltre discusse le ultime normative in termini di cybersecurity: NIS 2, Nuovo regolamento Macchine, NIST, Strategia di Cybersicurezza Nazionale e sarà esaminato il ruolo della nuova Agenzia per la Cybersicurezza Nazionale (ACN).

Lingua di svolgimento: italiano

Testi adottati: Appunti del docente

Modalità di erogazione: *blended*

Modalità di valutazione: Elaborazione di un progetto ed esame orale. La valutazione tende ad accertare l’apprendimento dei concetti di base di valutazione del rischio in sistemi interconnessi con particolare riferimento al rischio cyber e le principali problematiche di

cybersecurity del mondo OT includendo le contromisure più efficaci e le principali normative del settore.

Cyber Intelligence

Programma:

Fondamenti dell'Intelligence: Overview del Joint Intelligence Tradecraft; Relazione tra dati e Intelligence: ciclo di vita nell'Intelligence; Fonti della Intelligence Information.

Cyber Threat Intelligence: Aspetti principali della Cyber Threat Intelligence; Dagli Observables agli Indicators Threat Actors e TTPs; Approfondimento della Pyramid of Pain; Livelli di Threat Intelligence: Tactical, Operational e Strategic Threat Intelligence; Lifecycle di un Advanced Persistent Threats (APT); Modelli e Framework utilizzati per la caratterizzazione degli attacchi/incidenti; Mandiant APT Attack Model; Cyber Kill Chain Model Diamond Model Introduzione al MITRE ATT&CK Framework.

Cyber Threat Intelligence nel processo di Incident Response: Integrazione della CTI nei processi di un SOC Esempi di workflow di CTI; Utilizzo della Digital Forensics per l'analisi dei malicious artifacts; Esempi di analisi di log/eventi di sicurezza e del traffico di rete per identificare indicatori; Categorizzazione e identificazione delle principali classi di codici malevoli; Tecniche e strumenti di rilevamento e analisi automatica dei codici malevoli; Impiego di tecniche OSINT per l'analisi di malware; Data Pivoting e Link Analysis; Identificazione di adversary infrastructure e loro caratteristiche Intelligence data aggregation e data visualization

Cyber Threat Information: Producing e Consuming delle Threat Information Introduzione ai linguaggi CybOX, MAEC, CAPEC e Linguaggio STIX; Meccanismi di Security Testing Introduzione e impiego delle Regole Yara Introduzione e impiego delle Regole Snort; Esempi di Analisi di Cyber Threat Intelligence Cyber Threat Information Sharing; Utilizzo del Traffic Light Protocol (TLP) Standard Protocollo TAXII Introduzione alla piattaforma MISP.

Threat Intelligence Platforms (TIP): Threat Modeling; Utilizzo del Maturity Model nella Cyber Threat Intelligence; Caratteristiche e utilizzo delle Threat Intelligence Platforms.

Scrittura di un Threat Intelligence Report

Lingua di svolgimento: italiano

Testi adottati: Mastering Cyber Intelligence. Jean Nestor M. Dahj. Packt Publishing (29 aprile 2022).

Modalità di erogazione: *blended*

Modalità di valutazione: lezioni frontali e valutazione tramite colloqui con il docente e analisi del report di Threat Intelligence

Opacity and Cybersecurity in discrete event systems

Programma:

La diffusione di Internet of Things (IoT) e big data in ambito industriale ha creato nuovi modi di comunicazione tra diversi dispositivi. Questo ha comportato una crescente attenzione alle questioni di sicurezza legate alla crescente attività dei servizi di rete.

La sicurezza delle informazioni e dei sistemi cyber-fisici richiede che le informazioni riservate o lo stato di un dispositivo non debbano essere scoperte da intrusi. In questo corso questa caratteristica, nota come opacità, verrà esaminata considerando la modellazione dei sistemi ad eventi discreti (DESs).

A tale scopo in questo corso verrà introdotto il formalismo degli automi a stati finiti deterministici, il concetto di osservatore per tali sistemi e la proprietà di opacità basata sullo stato e sul linguaggio. Nel corso verranno anche proposti problemi di verifica dell'opacità nel quadro della sicurezza informatica.

Lingua di svolgimento: italiano/inglese

Testi adottati: Dispense a cura del docente

Modalità di erogazione: *blended*

Modalità di valutazione: Elaborazione di un progetto. La valutazione tende ad accertare l'apprendimento dei concetti di base relativi ai sistemi ad eventi discreti e alla proprietà di opacità.

Numero minimo e massimo di iscritti ammissibili

Numero minimo: 5

Numero massimo: 30

Requisiti di ammissione

Il corso *minor* è ad accesso libero. Per essere ammessi al corso *minor* occorre essere in possesso di un diploma di scuola secondaria di secondo grado o di altro titolo di studio equipollente conseguito all'estero, riconosciuto idoneo secondo la normativa vigente. Per seguire proficuamente il corso sono tuttavia richieste le seguenti competenze di base:

- Conoscenza di linguaggi di programmazione
- Conoscenza delle architetture dei calcolatori
- Conoscenza delle reti dei calcolatori

Criteri di selezione dei partecipanti

La selezione degli studenti avverrà in base al curriculum e tenderà ad accertare la presenza dei requisiti di base necessari a una fruizione proficua del corso *minor*.

Laddove il numero massimo di posti sia superato, gli studenti, comunque in possesso delle competenze di base, saranno selezionati sulla base dei seguenti criteri:

- Ultimo titolo di studio conseguito: dottorato di ricerca (10 punti); laurea magistrale o magistrale a ciclo unico (8 punti); laurea triennale (5 punti); diploma di scuola secondario di secondo grado (2 punti);
- Voto di laurea (qualora conseguita ed in relazione all'ultimo titolo di laurea o laurea magistrale conseguito): 110 lode (10 punti); 100-110 (8 punti); inferiore a 100 (5 punti);
- Voto di diploma (qualora non si sia conseguita la laurea): 100 e 100 con lode (10 punti); 95-99 (8 punti); inferiore a 95 (5 punti);
- Atri titoli coerenti con le attività didattiche previste dal corso *minor* (fino a 5 punti).

A parità di punteggio sarà data priorità a chi ha titolo di studio più avanzato;

A parità dei precedenti sarà data priorità ai richiedenti con età anagrafica inferiore.

Contributi di iscrizione

Gli studenti regolarmente iscritti a un corso di laurea o di laurea magistrale dell'Ateneo, anche in qualità di studenti in mobilità internazionale in ingresso, e gli studenti di Dottorato di Roma Tre possono iscriversi gratuitamente al corso *minor* per il medesimo anno accademico, fatto salvo il pagamento dell'imposta di bollo.

Coloro che non siano contemporaneamente iscritti a un corso di laurea o di laurea magistrale dell'Ateneo o siano Dottorandi di Roma Tre nel medesimo anno accademico sono tenuti al pagamento del contributo di iscrizione dell'importo di euro 480,00, oltre imposta di bollo.

Coloro i quali si trovino in condizioni di disabilità, con riconoscimento di handicap ai sensi dell'articolo 3, commi 1 e 3, della legge 5 febbraio 1992, n. 104, o con un'invalidità pari o superiore al 66%, sono esonerati dal pagamento dei contributi di iscrizione al corso e versano esclusivamente l'imposta di bollo.

Eventuali agevolazioni economiche

Nessuna agevolazione prevista

Prova finale

La prova finale non è prevista.