



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



**Bollettino Notiziario - A.A. 2024/2025**

## **LAUREA MAGISTRALE IN INTERNATIONAL CYBERSECURITY AND CYBERINTELLIGENCE (ORD. 2023)**

### **Curriculum: Corsi comuni**

### **CYBERPHYSICAL AND IOT SECURITY**

**Titolare:** Dott. ALESSANDRO BRIGHENTE

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Conoscenze base di architettura degli elaboratori e principali protocolli di rete (TCP, UDP, IP). Capacità di analizzare codice, capire il suo funzionamento, e modificarlo in base alle necessità.

**Conoscenze e abilità da acquisire:**

Alla fine del corso, lo studente sarà in grado di - Analizzare un flusso di controllo e capirne le operazioni fondamentali, con particolare riferimento al protocollo CAN. Capacità di implementare attacchi a livello controllo e a livello rete. Capacità di analizzare il traffico CAN bus e inferire informazioni sul suo funzionamento. - Implementare semplici controllori e testarne la sicurezza. - Analizzare un programma ladder logic per PLC e capirne il funzionamento. Implementare attacchi in grado di alterarne il funzionamento e progettare programmi sicuri. - Comprendere il funzionamento dei principali protocolli industriali, implementare attacchi ad integrity ed availability, e sviluppare contromisure. - Comprendere il funzionamento dei protocolli di posizionamento di droni e procedure di fail safe. Implementare attacchi di GPS spoofing per deviare le traiettorie. - Implementare protocolli di remote attestation per dispositivi IoT ed analizzarne le performance.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali comprendenti sia teoria che laboratori. In particolare, l'attività di laboratorio ha l'obiettivo di fornire allo studente le conoscenze basilari sugli attacchi e tecniche di prevenzione.

**Contenuti:**

Fundamentals - What is a Cyber-Physical System - Security Requirements in CPS Automotive Security - The CAN bus protocol - Error handling in CAN bus and bus-off attack - Network attacks on CAN bus - Keyless cars security and attacks to distance bounding protocols Autonomous Driving - Introduction to controllers - Levels of automation and modes of operation - Attacks on controllers and countermeasures Industrial Control Systems - Industrial Control Network Protocols - PLC and their functioning - Attacks and countermeasures to industrial control systems Drones - Drone components and basic functioning - Protocols for drone location and fail-safe procedures - Drone detection systems Internet of Things - Network protocols for the internet of things - Remote attestation - Intrusion and anomaly detection

**Modalità di esame:**

La totalità dei punti dell'esame, è suddivisa secondo i seguenti criteri: 40%: report di metà corso su un lavoro di implementazione di attacchi e contromisure su un topic a scelta della prima parte del corso 40%: report di fine corso su un lavoro di implementazione di attacchi e contromisure su un topic a scelta della seconda parte del corso 20%: esame teorico finale (10 domande a scelta multipla)

**Criteri di valutazione:**

I criteri di valutazione riflettono la padronanza delle conoscenze e abilità acquisite dallo studente secondo la sezione "Conoscenze e abilità d'acuisire". L'esame finale valuta la conoscenza dei concetti base introdotti durante il corso.

**Testi di riferimento:**

Walid M., et al., Cyber-Physical Systems: A Model-Based Approach. : Springer, 2021 E.D. Knapp, Industrial Network Security. : Elsevier, 2011

**Eventuali indicazioni sui materiali di studio:**

## DIGITAL FORENSICS AND BIOMETRICS

**Titolare:** Prof. SIMONE MILANI

**Mutuato da:** Laurea magistrale in Cybersecurity (Ord. 2020)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

### Prerequisiti:

La frequentazione del corso richiede la conoscenza di elementi di base di calcolo, algebra lineare (operazioni elementari sulle matrici, inversione, diagonalizzazione) e teoria della probabilità (variabili aleatorie, funzioni distribuzione/densità di massa/probabilità e loro proprietà). Viene richiesta una conoscenza di base del linguaggio Python e delle tecniche principali di machine learning. Qualora lo studente non possedesse tali competenze, verranno indicati dei materiali per uno studio individuale.

### Conoscenze e abilità da acquisire:

Il corso è strutturato in modo da fornire agli studenti una buona conoscenza sia tecnica sia teorica delle problematiche legali e delle tecniche di analisi sui dati digitali. In dettaglio, il corso porterà gli studenti ad acquisire e sviluppare le seguenti conoscenze. 1. Conoscenza delle principali tecniche di indagine digitale forense. 2. Conoscenza dei principali modelli matematici che regolano i fenomeni alla base delle tecniche di indagine forense su dati digitali. 3. Conoscenza dei principali scenari applicativi. 4. Conoscenza delle principali misure biometriche. Gli studenti svilupperanno le seguenti abilità. 1. Capacità di utilizzo delle tecniche di analisi presentate nel corso. 2. Capacità di implementazione dei principali algoritmi presentati nel corso. 3. Capacità di identificare la metodologia di indagine corretta dato uno specifico caso reale. 4. Capacità di svolgere un'indagine digitale in maniera corretta dal punto di vista degli aspetti procedurali. 5. Capacità di presentare un'indagine digitale utilizzando una terminologia tecnico-legale corretta. Gli studenti avranno inoltre l'opportunità di sviluppare e testare tecniche e algoritmi di analisi forense in alcune esperienze di laboratorio.

### Attività di apprendimento previste e metodologie di insegnamento:

Nell'ambito del corso, le attività e le metodologie di insegnamento prevedono 20 lezioni frontali in aula dove su supporto informatico (powerpoint) e alla lavagna vengono presentati i contenuti del corso. Saranno presentati dei casi reali e verranno svolte esercitazioni tramite problemi alla lavagna e quiz interattivi. Tali contenuti verranno inoltre chiariti con esempi pratici in 4 lezioni in laboratorio in cui ogni studente potrà applicare alcune tecniche di indagine. Nelle sessioni di laboratori, verrà utilizzata la programmazione in linguaggio Python e la piattaforma Google Colaboratory (disponibili gratuitamente).

### Contenuti:

Introduzione alla digital forensics. L'elaborazione dei dati digitali in contesti legali. Parte a: Digital forensics a.1) Acquisizione di prove digitali. a.1.1. Introduzione, identificazione di file come elementi di prova, acquisizione dei dati, autenticazione, elaborazione e analisi, documentazione dei risultati. Mantenimento della "Chain of Evidence". a.1.2. Tecniche di cifratura su disco, tecniche di violazione degli algoritmi di cifratura. a.2) Network forensics. a.2.1. I protocolli di trasmissione dei dati e i server web. a.2.2. Tecniche di intercettazione: sniffing, analisi dei dati da router, analisi dei file di log su server, acquisizione ed elaborazione del traffico su reti wireless. a.2.3. Rilevamento di intrusioni su rete. a.2.4. Strategie antiforensic: cifratura e mascheramento. Il protocollo TOR. a.3) Multimedia forensics. a.3.1. L'acquisizione del dato multimediale. I modelli della camera digitale e del microfono. a.3.2. Autenticazione della sorgente per immagini/video da stima del rumore (PRNU) o identificazione da firmware (interpolazione CFA, tecniche di compressione). a.3.3. Embedding di dati multimediali: steganografia e steganalisi, watermarking. a.3.4. Tecniche di alterazione di immagini/video e loro rilevamento. a.3.5. Alcuni casi reali. a.3.6. Autenticazione dell'origine del dato audio. Le alterazioni sui file audio e il loro rilevamento. a.4) Rilevamento di anomalie a.4.1. Tecniche e algoritmi di anomaly detection a.4.2. Algoritmi di tipo avversario. Adversarial Machine Learning a.4.3. Tecniche avversarie iterative: Generative adversarial Networks Parte b: Sistemi di identificazione biometrica b.1 Riconoscimento facciale b.1.1 Schema generale di un sistema di riconoscimento facciale b.1.1 Alineamento e normalizzazione b.1.2 Estrazione delle feature facciali b.1.3 Tecniche di identificazione e verifica b.1.4 Problematiche e attacchi ad un sistema di riconoscimento facciale b.2 Identificazione tramite impronte digitali b.1.1 Schema generale di un sistema di riconoscimento impronte b.1.2 Rilevamento delle minutiae b.1.3 Allineamento dell'impronta b.1.4 Problematiche e attacchi ad un sistema di riconoscimento impronte b.3 Sistemi di riconoscimento dell'iride b.3.1 Identificazione dell'iride b.3.2 Compensazione dell'orientamento, posa, ingrandimento b.3.3 Confronto dell'iride b.4 Riconoscimento vocale b.5 Analisi di sequenze DNA b.6 Analisi della camminata b.7 Altre misure biometriche

### Modalità di esame:

La verifica delle conoscenze e delle abilità attese verrà effettuata tramite una prova scritta e lo sviluppo di un progetto finale (da documentare tramite report) o di una relazione scientifica sulla letteratura. I report andranno consegnati almeno un giorno prima dell'esame finale. La valutazione finale sarà costituita dalla media pesata della valutazione della prova scritta (60%) e dei report (40%). Gli argomenti di valutazione della prova scritta verranno chiaramente indicati nel materiale fornito e durante la lezione.

### Criteri di valutazione:

La valutazione finale sarà determinata in base al livello di conoscenza dello studente degli argomenti del corso e alla capacità di applicare alcune tecniche di analisi. Gli argomenti di valutazione verranno chiaramente indicati nel materiale fornito e durante la lezione. In dettaglio, i criteri di valutazione sono: 1. Completezza delle conoscenze acquisite nell'analisi del dato digitale. 2. Completezza delle conoscenze relative agli aspetti normativi e procedurali relativi al ruolo dell'esperto forense. 3. Capacità di implementare e utilizzare diversi algoritmi di digital forensics. 4. Proprietà di linguaggio tecnico-legale. 5. Conformità ed efficacia nell'identificazione delle tecniche di indagine più opportune rispetto allo scenario applicativo considerato. 6. Abilità di programmazione. 7. Qualità nell'esposizione orale. Il giudizio finale terrà conto sia dei risultati raggiunti sia dell'impegno e dell'interesse dello studente nella materia trattata.

### Testi di riferimento:

Klette, Reinhard, Concise Computer Vision. Springer London: , 2014 Bishop, Christopher M., Pattern recognition and machine learning. New York: Springer, 0 Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, J. D. Tygar, Adversarial Machine Learning. Cambridge: Cambridge University Press, 2019 Hani Farid, Photo Forensics. : MIT Press, 2019 Watt, Jeremy; Borhani, Reza, Machine learning refinedrisorsa elettronicafoundations, algorithms, and applicationsJeremy Watt, Reza Borhani, Aggelos Katsaggelos. New York: Cambridge University Press, 2016

### Eventuali indicazioni sui materiali di studio:

Il materiale di studio è costituito da lucidi e appunti sulle lezioni forniti dal docente prima di ogni lezione. Gli appunti sono generati da diversi articoli scientifici e testi sull'argomento. L'attività didattica frontale utilizzerà lucidi, appunti alla lavagna, ed esempi di programma che potranno essere verificati a

## FORMAL METHODS FOR CYBER-PHYSICAL SYSTEMS

**Titolare:** Prof. DAVIDE BRESOLIN

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Il corso richiede familiarità con alcuni concetti matematici e informatici di base, quali teoria degli automi e della computabilità, logica. Non ci sono corsi propedeutici.

**Conoscenze e abilità da acquisire:**

Un sistema cyber-fisico consiste in una collezione di dispositivi informatici in grado di interagire in modo continuo con il mondo fisico tramite sensori e attuatori. Tali sistemi sono sempre più diffusi nelle società moderne, dagli edifici intelligenti ai dispositivi medici alle automobili. Questo corso offre un'introduzione ai principi di progettazione, specifica, modellazione e analisi dei sistemi ciberfisici, fornendo le seguenti conoscenze e competenze: 1. Capacità di modellare un sistema ciberfisico. 2. Capacità di formulare le proprietà che il sistema dovrebbe rispettare in modo matematicamente rigoroso. 3. Capacità di progettare e implementare un algoritmo di verifica per i sistemi ciberfisici, e di comprenderne e analizzarne i risultati. 4. Capacità di utilizzare algoritmi e strumenti per la sintesi automatica di controllori, e di comprenderne e analizzarne i risultati.

**Attività di apprendimento previste e metodologie di insegnamento:**

Il corso comprende lezioni frontali, attività di laboratorio e assignment da svolgere fuori dalle ore di lezione. Le lezioni frontali introducono le conoscenze di base e gli argomenti teorici. Le attività di laboratorio permettono di provare le metodologie e gli strumenti appresi su semplici casi di studio. Gli assignment richiedono l'implementazione di soluzioni originali e la loro applicazione a casi di studio di media complessità.

**Contenuti:**

Sistemi ciberfisici: definizione e caratteristiche chiave. Modelli formali per sistemi ciberfisici: modelli sincroni e asincroni. Verifica dei sistemi ciberfisici: proprietà di sicurezza e liveness, model checking, algoritmi enumerativi e tecniche simboliche. Sintesi di controllori per sistemi ad eventi discreti.

**Modalità di esame:**

Esame scritto per la parte di teoria. Per la parte pratica, due assignment da svolgere e consegnare durante il semestre di lezione, o in alternativa, un progetto.

**Criteri di valutazione:**

I criteri di valutazione sono i seguenti: 1. Completezza delle conoscenze acquisite; 2. Proprietà della terminologia tecnica utilizzata; 3. Capacità di modellare un sistema ciberfisico e le proprietà desiderate 3. Capacità di utilizzare strumenti di verifica formale per i sistemi ciberfisici 4. Capacità di progettare e implementare algoritmi di verifica per sistemi ciberfisici 5. Capacità di utilizzare strumenti per la sintesi automatica di controllori

**Testi di riferimento:**

Alur, Rajeev, Principles of cyber-physical systems. Cambridge: MS, MIT, 2015

**Eventuali indicazioni sui materiali di studio:**

Il corso ha una sezione dedicata sul Moodle STEM. Il Moodle raccoglierà le dispense del corso, le specifiche dettagliate delle attività di laboratorio, gli esercizi e le loro soluzioni. Verrà usato anche per comunicazioni e aggiornamenti da parte dei Docenti.

## FUNDAMENTALS OF CRYPTOGRAPHY

**Titolare:** Prof. CARLO MARICONDA

**Mutuato da:** Laurea magistrale in Cybersecurity (Ord. 2020)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 40A+8E; 6,00

**Prerequisiti:**

Per la prima parte (CRYPTOGRAPHY, Prof. Mariconda; primo semestre, 6 CFU): Gli argomenti dei corsi di Algebra (congruenze, gruppi e gruppi ciclici, campi finiti), Analisi I (calcolo differenziale ed integrale, serie numeriche) del corso di studi in Matematica. Per la seconda parte (Prof. Conti nel I semestre e Prof. Migliardi nel II semestre; 6 CFU): OS, Programming.

**Conoscenze e abilità da acquisire:**

Per la prima parte A (Prof. Mariconda; 6 CFU): Lo scopo della prima parte del corso è quello di offrire una panoramica delle basi teoriche necessarie per permettere uno studio critico dei protocolli crittografici usati oggi in molte applicazioni (autenticazione, commercio digitale). Nella prima parte verranno esposti gli strumenti matematici di base (essenzialmente dalla teoria elementare ed analitica dei numeri) necessari per comprendere il funzionamento dei moderni metodi a chiave pubblica. Nella seconda parte vedremo come applicare queste conoscenze per studiare in modo critico alcuni protocolli crittografici. La seconda parte è suddivisa in due moduli: Modulo B: nel primo modulo (Prof. Conti; 3 CFU, I semestre): gli studenti saranno in grado di identificare, classificare, descrivere, spiegare e correlare i concetti chiave degli attacchi e delle difese informatiche. Modulo C: nel secondo modulo della seconda parte (Prof. Migliardi; 3 CFU, II semestre): Valutare i rischi a cui è esposto un sistema IT, Spiegare come funziona un attacco, Descrivere, spiegare e generalizzare le vulnerabilità del software, Evitare le insidie del software.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali in classe. Per la prima parte (CRYPTOGRAPHY) sono previste attività in aula, partecipazione attiva e saranno disponibili i video delle lezioni.

**Contenuti:**

La prima parte (Prof. Mariconda; 6 CFU) costituisce anche l'insegnamento di CRYPTOGRAPHY per i corsi ICT FOR INTERNET AND MULTIMEDIA,

COMPUTER ENGINEERING, COMPUTER SCIENCE, MATHEMATICS, International Cybersecurity and Cyberintelligence. Fatti teorici di base: Aritmetica modulare. Numeri primi. Teorema piccolo di Fermat. Teorema del resto cinese. Campi finiti: ordine di un elemento e radici primitive. Test di pseudoprimalità. Test di Agrawal-Kayal-Saxena. Metodo RSA: prima descrizione, attacchi. Metodo di Rabin e la sua connessione con la fattorizzazione degli interi. Metodi di logaritmo discreto. Come calcolare il logaritmo discreto in un campo finito. Metodi elementari di fattorizzazione. Alcune osservazioni sul setaccio quadratico di Pomerance. Protocolli e algoritmi. Algoritmi crittografici fondamentali. Metodi simmetrici (storici, DES, AES). Metodi asimmetrici. Attacchi. Firma digitale. Generatori pseudocasuali (osservazioni). Scambio di chiavi, scambio di chiavi in tre passaggi, divisione del segreto, condivisione del segreto, trasmissione del segreto, marcatura temporale. Firme con RSA e logaritmo discreto. Simboli di Legendre e di Jacobi, legge di reciprocità quadratica e applicazioni alla crittografia. Per la seconda parte (Prof. Conti and Prof. (da determinare); 6 CFU): Introduction to Cybersecurity, User Authentication, Access Control, Database Security, Malicious Software, Denial-of-Service Attacks, Intrusion Detection, Firewalls and Intrusion Prevention Systems, Operating System Security, Trusted Computing and Multilevel Security. The execution environment of a program and the vulnerabilities resulting from the threat model of the time. Languages and threat models. Control hijacking: attack. Control hijacking: defense. Security of operating systems and principle of least privilege necessary (and examples of privilege escalation). Sandboxing and interaction with legacy code. Flaw search techniques.

#### Modalità di esame:

gli studenti dell'insegnamento di CRYPTOGRAPHY devono sostenere solo la prima parte A, quelli di CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES devono sostenere i moduli A, B, C. Per la prima parte A (CRYPTOGRAPHY, Prof. Mariconda; 6 CFU): Esame scritto, prova orale se ritenuta necessaria. In alternativa all'esame finale sono proposte prove intermedie e lavori individuali (esercizi, peer review). Per la seconda parte - modulo B (Prof. Conti, 3 crediti): Esame scritto, progetti assegnati da svolgere a casa, esame orale. - modulo C (Prof. Migliardi, 3 crediti): Esame scritto. Per ogni modulo lo studente può scegliere tra 5 date possibili per sostenere l'esame, senza nessun vincolo di esclusione tra l'una e l'altra, anche se la consegna del compito ad una prova successiva annulla la precedente. - \*\*Modulo A:\*\* 2 prove nella sessione invernale, 1 esame a giugno-luglio, 2 esami ad agosto-settembre. - \*\*Modulo B:\*\* 2 prove nella sessione invernale, 2 esami a giugno-luglio, 1 esame ad agosto-settembre. - \*\*Modulo C:\*\* 2 prove a giugno-luglio, 1 esame a settembre, 2 esami a gennaio-febbraio (dell'anno successivo). Il voto finale per gli studenti del corso CYBERSECURITY and CRYPTOGRAPHY: PRINCIPLES AND PRACTICES è determinato dalla media ponderata dei tre esami parziali—A (Prima parte del corso, 6 crediti, I semestre), B (Primo modulo della seconda parte del corso, 3 crediti, I semestre) e C (Secondo modulo della seconda parte del corso, 3 crediti, II semestre)—in proporzione ai rispettivi crediti. Tutti e tre gli esami parziali devono essere completati all'interno dello stesso anno accademico (in particolare, gli esami dei Moduli A e B devono essere completati entro la fine di settembre, mentre l'esame del Modulo C può essere completato nella sessione invernale dell'anno successivo). Al termine di ogni sessione d'esame, i voti degli studenti che hanno superato tutte e tre le parti vengono automaticamente registrati su Uniweb (non è richiesta alcuna registrazione). Di norma, salvo altre indicazioni della commissione, gli studenti che rifiutano il voto finale dovranno ripetere tutti e tre i moduli.

#### Criteri di valutazione:

Per la prima parte (Prof. Mariconda; 6 CFU): Si prevedono due percorsi possibili: per chi frequenta e studia regolarmente è previsto un bonus costituito dagli esiti di valutazioni in itinere su lavori a casa singoli o di gruppo da utilizzare in un appello nella prima sessione di esami dopo il corso o nei tre esami parziali durante il corso, altrimenti la prova è costituita dal solo appello finale. Durante la prova scritta finale lo studente dovrà rispondere ad alcune domande relative al programma svolto e risolvere alcuni esercizi dimostrando di aver compreso gli argomenti del corso. Il voto costituisce l'esito finale per l'insegnamento di Cryptography. Per la seconda parte (Prof. Conti and Prof. Migliardi; 3+3 CFU): Valutazione sia della competenza teorica che della capacità operativa di applicare quanto appreso a un caso reale. Il voto per gli studenti che seguono l'intero insegnamento di CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES è dato dalla media pesata in proporzione ai CFU dei voti della prima parte e della seconda parte.

#### Testi di riferimento:

Hoffstein J., Pipher J., Silverman J., An introduction to mathematical cryptography (2nd ed.). New York: Springer, 2014 Stallings, William; Brown, Lawrie, Computer security principles and practice. Boston [etc.]: Pearson, 2015 Pflieger, Charles P.; Pflieger, Shari Lawrence, Security in Computing. : Prentice Hall; 5 edition, 2015 Wenliang Du, Computer Security: a hands-on approach. : Create Space Independent Publishing Platform, 1 ed, 2017

#### Eventuali indicazioni sui materiali di studio:

Per la prima parte (6 CFU) il testo di riferimento è: Hoffstein J., Pipher J. e Silverman J. - An introduction to mathematical cryptography. 2nd ed. Undergraduate Texts in Mathematics. New York, NY: Springer (2014) Per la prima parte sono testi di consultazione e approfondimento: 1) N. Koblitz - A Course in Number Theory and Cryptography -Springer, 1994. 2) H. Knospe - A Course in Cryptography - American Mathematical Society, 2019. 3) R. Crandall, C. Pomerance - Prime numbers: A computational perspective - Springer, 2005. 4) B. Schneier - Applied Cryptography - Wiley, 1994. 5) A. Languasco, A.Zaccagnini - Manuale di Crittografia - Hoepli Editore, 2015. (Italian).

## FUNDAMENTALS ON INTERNATIONAL CYBERSECURITY

**Titolare:** Prof. HENRIQUE MANUEL DINIS DOS SANTOS

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 26A+4E; 6,00

#### Prerequisiti:

Nessuno

#### Conoscenze e abilità da acquisire:

Questo corso si propone di introdurre gli studenti ai fondamenti della Cybersecurity da una prospettiva internazionale, utilizzando i framework standardizzati delle principali organizzazioni coinvolte, sia per applicazioni generali che settoriali. Oltre alle competenze relative a queste conoscenze, l'obiettivo è anche quello di sviluppare le capacità pratiche degli studenti nell'utilizzo dei modelli di gestione della sicurezza delle informazioni, esplorando l'analisi delle minacce e del loro impatto in modo completo e internazionale. L'obiettivo dell'insegnamento di sviluppare negli studenti le capacità di: - caratterizzare le proprietà fondamentali della sicurezza informatica; - identificare le minacce e i rischi informatici potenziali e analizzare gli scenari di minaccia in contesti locali e internazionali; - ricordare le migliori pratiche associate alla sicurezza informatica; - identificare il quadro giuridico e normativo applicabile alla sicurezza informatica; - discutere gli schemi di valutazione della cybersecurity e di risposta agli incidenti a livello nazionale e internazionale.

#### Attività di apprendimento previste e metodologie di insegnamento:

Le lezioni sono quasi tutte tenute on line. Il metodo di insegnamento è espositivo con analisi di casi reali, discussione in classe e lavoro pratico.

#### Contenuti:

1. Fondamenti del Cyberspazio e della Cybersicurezza - concetti e definizioni principali - principali approcci alla Cybersecurity - contesti e quadri di riferimento 2. Modelli e quadri di Cybersecurity (compresi gli approcci ISO/IEC, NIST ed ENISA) - il ruolo della gestione del rischio - confronto tra i principali approcci alla gestione del rischio - caratterizzazione dei controlli di sicurezza 3. Panoramica di attacchi, metodi e tecniche - tabella di marcia dei tipici attacchi informatici - tecniche di exploit e loro impatto 4. Dagli obiettivi di sicurezza alle politiche: modelli e metodi - principali strategie di mitigazione -

mappatura degli obiettivi e dei controlli di sicurezza - impatto della maturità 5. Valutazione della cybersecurity: metriche e quadri di misurazione - efficienza dei controlli di sicurezza - tassonomia delle metriche di sicurezza - quadri per la valutazione della sicurezza informatica 6. Sintesi delle norme e degli standard internazionali di cybersecurity - norme e regolamenti principali - contesti applicativi

**Modalità di esame:**

L'esame di compone di quattro parti, ciascuna contribuisce al voto finale come indicato: 1) partecipazione attiva e discussioni (10%) 2) un breve progetto (30%) 3) una tesina (20%) 4) una prova scritta (40%)

**Criteri di valutazione:**

Partecipazione attiva e discussioni (durante il semestre) Frequenza alle lezioni, seguito e partecipazione alle discussioni Breve progetto (4a e 10a settimana) Il progetto, svolto in gruppo, ha l'obiettivo di valutare la competenza pratica degli studenti nell'applicazione di modelli di Cybersecurity e nello sviluppo di soluzioni inquadrare nei temi presentati. La valutazione si baserà sulla capacità dimostrata dagli studenti di: - utilizzare correttamente i concetti e gli strumenti indicati (25%); - descrivere in modo corretto e oggettivo le esperienze e i risultati raggiunti (30%); - collaborare nel lavoro di gruppo, e integrare le competenze di ciascun membro per una migliore efficienza nello svolgimento dei compiti assegnati (25%); - comunicare adeguatamente le soluzioni sviluppate e difendere le scelte effettuate con argomentazioni solide (20%) Tesina (fine semestre) Tesina su un argomento a scelta degli studenti, mediante approvazione del docente. La valutazione si baserà sulla capacità dello studente di: - scrivere in modo chiaro, strutturato, logico (30%); - identificare e fare riferimento alla letteratura pertinente (20%); - argomentare adeguatamente le questioni e le soluzioni descritte (30%); - fornire intuizioni personali originali e basarle su argomentazioni ragionevoli e convincenti (20%). Prova scritta (fine semestre) La prova finale consiste in un test con domande a risposta multipla (concetti e fondamenti) e due domande aperte: 3 punti: conoscenze e abilità da buone a ottime. Più dell'80% delle domande a scelta multipla sono corrette e le argomentazioni fornite nelle domande aperte sono complete, chiare, coerenti e persuasive. 2 punti: tra il 60% e l'80% delle domande a scelta multipla sono corrette e le argomentazioni fornite nelle domande aperte sono incomplete, ma comunque coerenti. 1 punto: tra il 40% e il 60% delle domande a scelta multipla sono corrette e le argomentazioni fornite nelle domande aperte sono incomplete, non sviluppate e incoerenti. 0 punti: meno del 40% delle domande a scelta multipla sono corrette e gli argomenti forniti nelle domande aperte sono incompleti, fuori campo o sono completamente sottosviluppati.

**Testi di riferimento:**

H. Santos, Cybersecurity: A Practical Engineering Approach. : CRC Press, 2022 Whitman, M. E., & Mattord, H. J., Principles of information security. : Cengage learning, 2021 E. Tikk, M. Kerttunen, Routledge Handbook of International Cybersecurity. : Routledge, 2020 K. Thakur, P. Al-Sakib Khan, Cybersecurity Fundamentals: A Real-World Perspective. : CRC Press, 2020

**Eventuali indicazioni sui materiali di studio:**

Testi per consultazione: B. Schneier, "Click Here to Kill Everybody", Audible Inc., 2018 M. Aiken, "The Cyber Effect", Spiegel & Grau, 2017

**INTERNATIONAL MANAGEMENT OF CYBERSECURITY**

**Titolare:** da definire

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 11A+5E+16L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

**LAW AND DATA**

**Titolare:** Dott.ssa FIORELLA DAL MONTE

**Mutuato da:** Laurea magistrale in Data Science (Ord. 2023)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

No prerequisites

**Conoscenze e abilità da acquisire:**

The course aims to introduce non-law students to a proper understanding of the main legal issues related to the processing of data, personal and non. The first part of the course aims to enable students to approach EU personal data protection regulation. In the second part, instead, students will reflect on the main problems related to the use of data-intensive technologies (big data and artificial intelligence) and the technical and legal solutions now debated.

**Attività di apprendimento previste e metodologie di insegnamento:**

Classes Seminars Workshops Preassigned readings.

**Contenuti:**

All the info about the course are on Moodle - Introduction to Law and Legal Studies - Introduction to the EU Law - Introduction to the EU GDPR - The concept of data; personal, sensitive and economic data; big data - Property of data, choices in the management of data - The right to be forgotten - Civil and criminal aspects of profiling activity - Automatic data processing, human responsibilities - The Data Protection Officer and DP Authorities - Civil and criminal protection of privacy - Sanctioning powers and system - Open Data for the public interest - Big data (collection, analysis, processing) and their influence on fundamental rights - Digital Surveillance - Facial Recognition: Open Issues - Disinformation - Artificial Intelligence in the EU law

**Modalità di esame:**

Written Exam

**Criteri di valutazione:**

The grading scale used to assess the students is the Italian one, with the highest score of 30/30 and a minimum score of 18/30 (sufficient) (info: here). The students will be graded according to their level of theoretical and practical knowledge of the fields covered throughout the course and their capacity to critically reflect on the most contentious legal issues on data-intensive technologies.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

The course has no official textbooks. Students can study on their notes and the additional material provided by the instructor. Nevertheless, here are some helpful handbooks to approach some modules. These books are not mandatory, and students have sole discretion to refer them. ? Mireille Hildebrandt (2020). Law for Computer Scientists and Other Folk, OUP (open access: here) – especially chapters 2-3-4-5-9-10 ? Paul Voigt, Axel von dem Bussche (2017). The EU General Data Protection Regulation (GDPR). A practical guide, Springer (unipd access: here) ? European Fundamental Rights Agency (2018). Handbook on European data protection law, Luxembourg (open access: here) ? Karen Yeung, Martin Lodge (2019). Algorithmic Regulation, OUP (Public Law Dept. Library) – especially chapters 2-3-4-6-7-11

**MACHINE LEARNING TECHNIQUES FOR EVENT CORRELATION (CANALE A)**

**Titolare:** Prof. FABIO VANDIN

**Mutuato da:** Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Conoscenze di Base di Analisi Matematica, Probabilità, Statistica, Algebra Lineare, Algoritmi, e elementi di base di Programmazione.

**Conoscenze e abilità da acquisire:**

Lo scopo del corso è di fornire i principi fondamentali del problema di apprendimento e di introdurre i principali algoritmi per la regressione e la classificazione. Il corso includerà esercitazioni al computer. Alla fine del corso lo studente avrà le seguenti conoscenze ed abilità: 1. Conoscerà i principi fondamentali e le principali metodologie dell'apprendimento automatico. 2. Sarà in grado di affrontare problemi di apprendimento supervisionato e non supervisionato. 3. Saprà applicare queste metodologie a diversi scenari e problemi. 4. Sarà in grado di selezionare la metodologia più adatta alla soluzione di uno specifico problema di apprendimento sulla base delle caratteristiche del problema e dei dati a disposizione. 5. Avrà le competenze per utilizzare e adattare sistemi software in grado di risolvere i problemi considerati. 6. Se possibile saranno fornite anche competenze relative ad argomenti più avanzati come sparsità, boosting e deep learning.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni teoriche con utilizzo sia di lucidi che della lavagna. Esercitazioni in aula con coinvolgimento degli studenti. Esercitazioni al computer (in laboratorio), anche con l'utilizzo di casi di studio. Tutto il materiale didattico presentato durante le ore di lezione frontale sarà reso disponibile sulla piattaforma elearning ( <http://elearning.dei.unipd.it> ).

**Contenuti:**

Motivazioni, componenti del problema di apprendimento e applicazioni dell'apprendimento automatico. Apprendimento supervisionato e non supervisionato. Parte I: Apprendimento supervisionato. 1. Introduzione: Dati, classi di modelli, funzioni di costo. 2. Modelli probabilistici e ipotesi sui dati. Funzione di regressione. Regressione e Classificazione. 3. Bontà di un modello, complessità, compromesso tra distorsione e varianza (dimensione di Vapnik-Chervonenkis, errore di generalizzazione). 4. Modelli per la regressione: regressione lineare (scalare e multivariata), selezione di variabili, modelli lineari nei parametri, regolarizzazione. 5. Classi di modelli non lineari: Sigmoidi, Reti Neurali. 6. Metodi "Kernel": Support Vectors Machines. 7. Metodi per la classificazione: Regressione Logistica, Reti Neurali, Perceptron, Classificatore di Bayes, SVM, Deep Learning. 8. Validazione e selezione dei modelli: errore di generalizzazione, compromesso tra distorsione e varianza, cross validation. Determinazione della complessità del modello. Parte II: Apprendimento non supervisionato 1. Analisi di clusters: K-means, misture di Gaussiane e stima EM. 2. Riduzione della dimensionalità: analisi delle componenti principali (PCA).

**Modalità di esame:**

La valutazione delle conoscenze e delle abilità acquisite viene effettuata mediante due contributi: 1. Una prova scritta a libro chiuso in cui lo studente deve risolvere dei problemi, al fine di verificare l'acquisizione dei principali ingredienti e strumenti del problema di apprendimento, la capacità analitica nel loro utilizzo e la capacità di interpretare i risultati tipici in un problema pratico di apprendimento. 2. Esercitazioni al computer (facoltative) rivolte all'acquisizione

delle competenze, anche pratiche, per l'utilizzo degli strumenti di machine learning. Queste esercitazioni, da svolgere a casa, consentono di verificare la capacità di mettere in pratica i concetti teorici acquisiti. Lo studente deve produrre una breve relazione che descriva le metodologie utilizzate per risolvere il progetto assegnato assieme ai risultati ottenuti. Il voto finale sarà basato sulla prova scritta con un bonus fino ad un massimo di 3 punti per gli studenti che svolgeranno le esercitazioni di laboratorio

#### **Criteri di valutazione:**

La valutazione con cui verrà effettuata la verifica delle conoscenze e delle abilità acquisite considera: 1. La completezza delle conoscenze acquisite per quanto riguarda gli strumenti per la predizione (regressione e classificazione). 2. La capacità di risolvere un problema di apprendimento attraverso le tecniche proposte 3. La proprietà nella terminologia tecnica usata, sia scritta che orale 4. L'originalità e indipendenza nella identificazione delle metodologie più adatte a risolvere uno specifico problema di apprendimento. 5. La capacità di interpretare i risultati in un problema pratico di apprendimento 6. Abilità nell'utilizzo degli strumenti informatici per l'apprendimento automatico 7. L'abilità analitica e pratica nell'uso di questi strumenti per la soluzione di semplici problemi.

#### **Testi di riferimento:**

Murphy, Kevin P., Machine Learning: a probabilistic perspective.. : Mit press, 2012 Shalev-Shwartz, Shai; Ben-David, Shai, Understanding machine learning: from theory to algorithms.. : Cambridge University Press, 2014 T. Hastie, R. Tibshirani, J. Friedman, The Elements of Statistical Learning.. : Springer, 2008 C. M. Bishop, Pattern Recognition and Machine Learning.. : Springer, 2006

#### **Eventuali indicazioni sui materiali di studio:**

Il corso sarà basato sui libri di testo: "Understanding Machine Learning: from Theory to Algorithms", "Machine Learning, a probabilistic perspective", "Pattern Recognition and Machine Learning", e "The Elements of Statistical Learning" (vedi Sezione "Testi di Riferimento"). Materiale aggiuntivo e informazioni dettagliate sulle modalità d'esame sono rese disponibili sul sito web del corso, accessibile dalla pagina <http://elearning.dei.unipd.it>

## **MACHINE LEARNING TECHNIQUES FOR EVENT CORRELATION (CANALE B)**

**Titolare:** Dott.ssa BARBARA DI CAMILLO

**Mutuato da:** Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

#### **Prerequisiti:**

Conoscenze di Base di Analisi Matematica, Probabilità, Statistica, Algebra Lineare, Algoritmi, e elementi di base di Programmazione.

#### **Conoscenze e abilità da acquisire:**

Lo scopo del corso è di fornire i principi fondamentali del problema di apprendimento e di introdurre i principali algoritmi per la regressione e la classificazione. Il corso includerà esercitazioni al computer. Alla fine del corso lo studente avrà le seguenti conoscenze ed abilità: 1. Conoscerà i principi fondamentali e le principali metodologie dell'apprendimento automatico. 2. Sarà in grado di affrontare problemi di apprendimento supervisionato e non supervisionato. 3. Saprà applicare queste metodologie a diversi scenari e problemi. 4. Sarà in grado di selezionare la metodologia più adatta alla soluzione di uno specifico problema di apprendimento sulla base delle caratteristiche del problema e dei dati a disposizione. 5. Avrà le competenze per utilizzare e adattare sistemi software in grado di risolvere i problemi considerati. 6. Se possibile saranno fornite anche competenze relative ad argomenti più avanzati come sparsità, boosting e deep learning.

#### **Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni teoriche con utilizzo sia di lucidi che della lavagna. Esercitazioni in aula con coinvolgimento degli studenti. Esercitazioni al computer (in laboratorio), anche con l'utilizzo di casi di studio. Tutto il materiale didattico presentato durante le ore di lezione frontale sarà reso disponibile sulla piattaforma elearning ( <https://stem.elearning.unipd.it/> ).

#### **Contenuti:**

Motivazioni, componenti del problema di apprendimento e applicazioni dell'apprendimento automatico. Apprendimento supervisionato e non supervisionato. Parte I: Apprendimento supervisionato. 1. Introduzione: Dati, classi di modelli, funzioni di costo. 2. Modelli probabilistici e ipotesi sui dati. Funzione di regressione. Regressione e Classificazione. 3. Bontà di un modello, complessità, compromesso tra distorsione e varianza (dimensione di Vapnik-Chervonenkis, errore di generalizzazione). 4. Modelli per la regressione: regressione lineare (scalare e multivariata), selezione di variabili, modelli lineari nei parametri, regolarizzazione. 5. Classi di modelli non lineari: Sigmoidi, Reti Neurali. 6. Metodi "Kernel": Support Vectors Machines. 7. Metodi per la classificazione: Regressione Logistica, Reti Neurali, Perceptron, Classificatore di Bayes, SVM, Deep Learning. 8. Validazione e selezione dei modelli: errore di generalizzazione, compromesso tra distorsione e varianza, cross validation. Determinazione della complessità del modello. Parte II: Apprendimento non supervisionato 1. Analisi di clusters: K-means, misture di Gaussiane e stima EM. 2. Riduzione della dimensionalità: analisi delle componenti principali (PCA).

#### **Modalità di esame:**

La valutazione delle conoscenze e delle abilità acquisite viene effettuata mediante due contributi: 1. Una prova scritta a libro chiuso in cui lo studente deve risolvere dei problemi, al fine di verificare l'acquisizione dei principali ingredienti e strumenti del problema di apprendimento, la capacità analitica nel loro utilizzo e la capacità di interpretare i risultati tipici in un problema pratico di apprendimento. 2. Esercitazioni al computer (facoltative) rivolte all'acquisizione delle competenze, anche pratiche, per l'utilizzo degli strumenti di machine learning. Queste esercitazioni, da svolgere a casa, consentono di verificare la capacità di mettere in pratica i concetti teorici acquisiti. Lo studente deve produrre una breve relazione che descriva le metodologie utilizzate per risolvere il progetto assegnato assieme ai risultati ottenuti. Il voto finale sarà basato sulla prova scritta con un bonus fino ad un massimo di 3 punti per gli studenti che svolgeranno le esercitazioni di laboratorio

#### **Criteri di valutazione:**

La valutazione con cui verrà effettuata la verifica delle conoscenze e delle abilità acquisite considera: 1. La completezza delle conoscenze acquisite per quanto riguarda gli strumenti per la predizione (regressione e classificazione). 2. La capacità di risolvere un problema di apprendimento attraverso le tecniche proposte 3. La proprietà nella terminologia tecnica usata, sia scritta che orale 4. L'originalità e indipendenza nella identificazione delle metodologie più adatte a risolvere uno specifico problema di apprendimento. 5. La capacità di interpretare i risultati in un problema pratico di apprendimento 6. Abilità nell'utilizzo degli strumenti informatici per l'apprendimento automatico 7. L'abilità analitica e pratica nell'uso di questi strumenti per la soluzione di semplici problemi.

#### **Testi di riferimento:**

Murphy, Kevin P., Machine Learning: a probabilistic perspective. : MIT press, 2012 T. Hastie, R. Tibshirani, J. Friedman, The Elements of Statistical

**Eventuali indicazioni sui materiali di studio:**

Il corso sarà basato sui libri di testo: "Understanding Machine Learning: from Theory to Algorithms", "Machine Learning, a probabilistic perspective", "Pattern Recognition and Machine Learning", e "The Elements of Statistical Learning" (vedi Sezione "Testi di Riferimento"). Materiale aggiuntivo e informazioni dettagliate sulle modalità d'esame sono rese disponibili sul sito web del corso, accessibile dalla pagina <https://stem.elearning.unipd.it/>

<b>MALWARE</b>
----------------

**Titolare:** da definire

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 14A+2E+16L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

<b>MOBILE APPLICATIONS SECURITY</b>
-------------------------------------

**Titolare:** Prof.ssa ELEONORA LOSIOUK

**Mutuato da:** Laurea magistrale in Cybersecurity (Ord. 2020)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Qualsiasi linguaggio di programmazione orientato agli oggetti.

**Conoscenze e abilità da acquisire:**

Acquisizione dei concetti fondamentali di sicurezza del sistema operativo Android. Alla fine del corso, gli studenti avranno acquisito le conoscenze necessarie per analizzare un dispositivo mobile o un'applicazione mobile e identificarne le possibili vulnerabilità.

**Attività di apprendimento previste e metodologie di insegnamento:**

Prima di ogni lezione, il docente pubblica un video in cui illustra gli argomenti della lezione. Gli studenti devono vedere il video prima di partecipare alla lezione. All'inizio della lezione, il docente rilascia un breve questionario per verificare se gli studenti abbiano compreso i concetti principali descritti nella lezione registrata. Il questionario viene somministrato attraverso la piattaforma Moodle. L'insegnante, quindi, risponde a qualsiasi dubbio o domanda. Il docente individua i gruppi di lavoro scegliendo i componenti di ciascun gruppo (i gruppi saranno diversi per ogni nuovo laboratorio) e rilascia il nuovo laboratorio. Anche se tutti i gruppi sono incoraggiati a svolgere il laboratorio, l'insegnante seleziona il gruppo che dovrebbe risolverlo e illustra la soluzione agli altri gruppi, facendo una presentazione una settimana dopo il rilascio del laboratorio. Durante la lezione successiva, il gruppo selezionato presenta la sua soluzione e risponde alle domande del docente o degli altri studenti. Se l'insegnante è soddisfatto della prestazione del gruppo, ogni membro del gruppo riceve un bonus che verrà sommato al voto ottenuto durante l'esame finale.

**Contenuti:**

Gli argomenti sono i seguenti: - Architettura interna del sistema operativo Android. - Componenti di un'app mobile (Activity, Service, Content Provider, Broadcast Receiver). - Tecniche di analisi delle app. - Tecniche di reverse engineering per app. - Valutazione della vulnerabilità delle app. - Tecniche di analisi statica e dinamica per app. - Sfruttamento della vulnerabilità delle app.

**Modalità di esame:**

L'esame finale consisterà in una serie di domande a risposta multipla su tutti gli argomenti del corso. Il bonus accumulato con la partecipazione durante il semestre verrà sommato al voto ottenuto all'esame. Poiché la partecipazione non è obbligatoria, uno studente può ottenere il voto massimo (es. 30L) anche senza frequentare il corso.

**Criteri di valutazione:**

Conoscenza dei concetti presentati durante il corso.

**Testi di riferimento:**

Elenkov, Nikolay, Android security internals : an in-depth guide to Android's security architecture. : No Starch Press, 2015

<b>OPERATING SYSTEMS SECURITY</b>
-----------------------------------

**Titolare:** Prof. LINAS BUKAUSKAS

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 12A+4E+16L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

<b>PRIVACY PRESERVING INFORMATION ACCESS</b>
--

**Titolare:** Dott. GUGLIELMO FAGGIOLI

**Mutuato da:** Laurea magistrale in Cybersecurity (Ord. 2020)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Requested competencies: + Undergraduate level knowledge of statistics + Background on algorithms and linear algebra + Basic knowledge of Databases

**Conoscenze e abilità da acquisire:**

The objective of the course is to learn what are the main challenges to privacy protection in the information access environment and what solutions can be adopted to preserve privacy. At the end of the course, the student is expected to learn: + How to define privacy and classify threats and techniques according to Solove's Taxonomy. Additionally, the student is expected to know basic elements of the European regulation concerning the protection of privacy. + Main statistical techniques adopted to achieve privacy in a computational environment (k-anonymity, l-diversity and t-closeness and differential privacy). + Main challenges linked to privacy protection, possible solutions and protection approaches for information access technologies, such as databases, search engines and recommender systems.

**Attività di apprendimento previste e metodologie di insegnamento:**

+ Lectures + Labs + Seminars of visiting colleagues on research topics and/or seminars by companies on the use and perspectives for innovative products based on Privacy-Preserving information access systems, stage opportunities, simulation of job interviews. + Oral presentation of research papers: to highlight the fact that this line of research is cutting-edge, students will present a paper among a pool of highly recent research papers. The presentation will be followed by a proactive discussion with the rest of the class.

**Contenuti:**

The course focuses on how to face the principal privacy challenges that arise when developing information access solutions. The course will cover the following privacy-preserving information access related topics: The first part of the course details the definition of privacy from both societal and legal aspects. During the first module, the student learns about Solove's Taxonomy and how to classify the different privacy-related aspects. The course provides basic elements of the European regulation on privacy protection. The second part of the course focuses on the most known computational techniques to grant privacy. The student learns the main computational and statistical approaches used to achieve privacy and/or anonymity, such as k-anonymity, l-diversity and t-closeness, and Differential Privacy. The main part of the course focuses on information access, privacy threats linked to the use of databases, search engines and recommender systems. The student learns how state-of-the-art techniques are used to preserve users' privacy. More in detail, the following aspects will be covered: + Databases: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, microdata and macrodata protection and geomasking. + Information Retrieval and Search Engines: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, privacy risks linked to Search Engines and IR systems, development and evaluation of Privacy preserving IR models and Searchable encryption. + Recommender systems: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, analysis of the risks

associated with collaborative filtering and social recommender systems, federated learning for privacy-preserving RS.

**Modalità di esame:**

Individual oral exam with questions and exercises on the topics covered during the lectures. - Projects to document, design, develop, implement, and code privacy-preserving techniques, carried out via homeworks during the semester. - Final presentation of a research paper about privacy-preserving approaches.

**Criteri di valutazione:**

The evaluation will be based on the comprehension and knowledge of the notions and methodologies specific to privacy-preserving information access techniques, on the capability of identifying potential threats and weaknesses of the information access systems and correctly deploying countermeasures and protection strategies. Students will be evaluated on the capability of carrying out comparative analyses of the different solutions required to handle the various information access channels, but also on the capability of recognizing commonalities. Furthermore, the evaluation will also include the active participation of the students in the lectures and in the discussion of cutting-edge research papers.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

The teaching material consists of: - instructor's slides - suggested readings - additional material shared during lectures All the teaching material is available on the Moodle platform.

**QUANTUM CRYPTOGRAPHY AND SECURITY**

**Titolare:** Prof. NICOLA LAURENTI

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Il corso richiede conoscenze di base di fisica quantistica, informazione quantistica, teoria dell'informazione, crittografia e sicurezza. Un breve ripasso dei necessari concetti di informazione e tecnologie quantistiche, sicurezza e crittografia sarà svolto all'inizio del corso.

**Conoscenze e abilità da acquisire:**

La crittografia quantistica è a volte presentata come una scatola magica capace di fornire una soluzione definitiva ad ogni problema nel campo della sicurezza dell'informazione, altre volte come una visione astratta e idealizzata inadatta ad essere efficace in contesti realistici. Questo corso mira invece a permettere agli studenti di sviluppare la propria visione critica di questa area innovativa ed entusiasmante dell'information security, che rappresenta anche una delle più affascinanti e realistiche applicazioni della fisica quantistica, fornendo loro: - una formulazione solida e coerente dei modelli e delle architetture fondamentali dei meccanismi di crittografia quantistica, comprendendo minacce ed attacchi; - un'illustrazione dettagliata delle opportunità tecnologiche e delle loro limitazioni, la scelta degli osservabili, gli inconvenienti pratici, la chiusura dei loopholes; - una discussione rigorosa delle dimostrazioni di sicurezza e della derivazione di metriche di sicurezza dalla stima dei parametri osservati - esperienze pratiche di laboratorio sia hardware (con dispositivi ottici su banco) che software (per l'elaborazione delle informazioni). Si prevede che gli studenti acquisiscano le seguenti abilità: - saper valutare criticamente la necessità e la fattibilità di soluzioni basate su crittografia quantistica per specifiche esigenze di sicurezza; - saper identificare le soluzioni tecnologiche che meglio si adattano al meccanismo crittografico richiesto in un dato contesto; - valutare i parametri richiesti al sistema per le soluzioni opportune.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali ed esperienze di laboratorio

**Contenuti:**

Introduzione: ripasso di informazione e tecnologie quantistiche, di servizi, meccanismi e misure di sicurezza. Generatori aleatori quantistici (QRNG): a variabili discrete, a variabili continue, aspetti tecnologici, QRNG certificati dalla disuguaglianza di Bell, semidevice independent QRNG, randomness extractor. Distribuzione di chiavi crittografiche per via quantistica (QKD): protocolli (prepare-and-measure, entanglement-based, continuous-variable), aspetti tecnologici e non ideali, modelli di attacco, algoritmi di post-elaborazione e dimostrazioni di sicurezza, uso di decoy states, QKD device independent, twin-field QKD, reti QKD, memorie e ripetitori quantistici. Altri meccanismi di sicurezza quantistici: comunicazione diretta segreta, information commitment quantistico, secret sharing quantistico, firme digitali quantistiche.

**Modalità di esame:**

Lo studente dovrà consegnare le proprie relazioni individuali delle esperienze di laboratorio, e successivamente sostenere un esame orale tradizionale con domande analitiche e discussione critica degli argomenti del corso.

**Criteri di valutazione:**

L'esame orale mira ad accertare il livello a cui lo studente ha acquisito: - una solida comprensione dei concetti fondamentali di crittografia quantistica; - la capacità di applicare modelli generali ad esempi particolari di dispositivi, algoritmi e protocolli; - una visione critica nel valutare problemi e soluzioni in protocolli specifici; - la capacità di identificare chiaramente le corrispondenze tra funzionalità astratte e elementi tecnologici, includendo la modellizzazione degli aspetti non ideali. Le relazioni di laboratorio, che verranno anche discusse all'esame orale, mirano ad accertare il lavoro dello studente e la sua comprensione delle singole esperienze, in collegamento con gli argomenti del corso.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

A causa del carattere innovativo ed avanzato degli argomenti del corso non sono disponibili libri di testo con una trattazione sufficientemente completa e coerente. Lucidi e appunti per le lezioni saranno perciò forniti dai docenti. Tuttavia i seguenti articoli di revisione descrivono aspetti avanzati di QKD e QRNG in maniera ampia ed esauriente: - V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301 (2009). - F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. 92, 025002 (2020). - M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. 89, 015004 (2017). - X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," Npj Quantum Inf. 2, 16021 (2016). Ulteriori

## RAPID REACTION AND FIRST RESPONSE

**Titolare:** da definire

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 14A+2E+16L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

## RESEARCH PROJECTS

**Titolare:** da definire

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** +5E+1L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

## SECURE SOFTWARE DEVELOPMENT

**Titolare:** Prof. FRANCESCO RANZATO

**Mutuato da:** Laurea magistrale in Computer Science (Ord. 2021)

**Periodo:** I anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Conoscenze di base dei linguaggi di programmazione. L'insegnamento non prevede propedeuticità.

**Conoscenze e abilità da acquisire:**

Il corso mira ad introdurre metodi e strumenti per la specifica del comportamento run-time dei programmi, l'analisi statica e la verifica automatica dei programmi e, più in generale, dei sistemi software. In particolare, il corso fornisce una introduzione alla semantica formale dei linguaggi di programmazione ed ai metodi formali per la loro analisi statica e verifica.

**Attività di apprendimento previste e metodologie di insegnamento:**

L'insegnamento prevede lezioni frontali (o in modalità telematica) e la risoluzione in modo indipendente a casa di vari esercizi e/o lo sviluppo di un progetto di verifica del software. Sono previste lezioni invitate di ospiti ricercatori su tematiche avanzate di verifica del software.

**Contenuti:**

- Semantica dei programmi: Modellazione del comportamento (in particolare il comportamento input/output) dei programmi mediante la teoria dell'ordinamento e dei punti fissi. (cf. [https://en.wikipedia.org/wiki/Semantics\\_\(computer\\_science\)](https://en.wikipedia.org/wiki/Semantics_(computer_science))) - Analisi statica e verifica di programmi mediante interpretazione astratta: L'interpretazione astratta è una notoria tecnica basata su una approssimazione della semantica dei programmi che permette di specificare le proprietà dei programmi deducibili mediante analisi statica e di provarne la correttezza. (cf. [https://en.wikipedia.org/wiki/Abstract\\_interpretation](https://en.wikipedia.org/wiki/Abstract_interpretation)) - Analisi statica dataflow di programmi: tecnica per dedurre staticamente informazioni sull'insieme dei possibili valori delle variabili nei vari punti del programma. Un grafo di flusso del controllo è utilizzato per determinare le parti di un programma a cui un particolare valore assegnato ad una variabile potrebbe propagarsi. Le informazioni raccolte sono spesso utilizzate dai compilatori (come gcc e javac) per ottimizzare un programma. (cf. [https://en.wikipedia.org/wiki/Data-flow\\_analysis](https://en.wikipedia.org/wiki/Data-flow_analysis)) - Strumenti di verifica del software: ad esempio, Clousot (Microsoft, USA), Interproc (INRIA, Francia), Jandom (Università di Pescara) (cf. [https://en.wikipedia.org/wiki/List\\_of\\_tools\\_for\\_static\\_code\\_analysis](https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis))

**Modalità di esame:**

Esame orale e/o progetto software, possibilmente suddivisi in parti distinte.

**Criteri di valutazione:**

L'esame orale verte su vari esercizi che lo studente deve svolgere in modo indipendente a casa. Il progetto di laboratorio verte su qualche tool di verifica del software.

**Testi di riferimento:**

H. Riis Nielson, F. Nielson, Semantics with Applications: A Formal Introduction. : Wiley, 1992 Antoine Minè, Tutorial on static inference of numeric invariants by abstract interpretation. : Now, The Essence of Knowledge, 2017

**Eventuali indicazioni sui materiali di studio:**

Le slide utilizzate a lezione verranno distribuite.

<b>SECURITY OF APPLICATIONS</b>
---------------------------------

**Titolare:** da definire

**Periodo:** I anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 12A+4E+16L; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE