SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

Catalogo Attività di formazione

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Attività di formazione specialistica per dipendenti e professionisti

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Indice

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Contrastare la disinformazione: Strumenti e Tecniche per la gestione delle Minacce e dei Rischi

DESCRIZIONE CORSO

Il modulo approfondisce le principali minacce della disinformazione e le tecniche di verifica delle informazioni, con un focus su strumenti OSINT (Open Source INTelligence), valutazione delle fonti, propaganda e tecnologie emergenti come l'IA generativa e i deepfake, per formare professionisti capaci di gestire i rischi informativi.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARGOMENTI

Principali Minacce; Valutazione delle Fonti; Open Source Intelligence; Verifica delle Informazioni; Propaganda e Fallacie Argomentative; Echo Chamber e Filter Bubbles; Generative AI e DeepFake; Framework per la Valutazione del Rischio

TARGET

- Settore giornalistico: Redazioni, agenzie di stampa e professionisti dell'informazione che necessitano di competenze avanzate per contrastare la disinformazione (Giornalisti, fact-checker, editori e responsabili di comunicazione)
- Ambito aziendale: Ufficio comunicazione, brand reputation, marketing e PR, per la protezione dell'immagine aziendale e la gestione di crisi mediatiche (Responsabili PR, brand managers, e social media strategists)
- Pubblica amministrazione: Enti locali e nazionali interessati a contrastare la disinformazione nel contesto di politiche pubbliche e comunicazione istituzionale (Decision makers, Policy makers e funzionari pubblici responsabili di strategie di comunicazione e gestione delle crisi)
- Settore della sicurezza e della difesa: Intelligence e forze dell'ordine impegnate nella protezione da campagne di disinformazione e propaganda (Analisti OSINT, operatori di intelligence e responsabili di cyber security)
- Organizzazioni no-profit e ONG: Entità che combattono la disinformazione su temi globali, sociali o umanitari Istruzione e ricerca: Università, centri di ricerca e istituti di formazione (Studiosi di media, disinformazione e comunicazione, studenti di corsi di laurea o master in giornalismo, scienze della comunicazione, data science e sicurezza informatica)

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

ARTICOLAZIONE DEL CORSO

MODULO 1 (6 ORE) Principali minacce della disinformazione	**MODULO 2 (10ORE)** OSINT	**MODULO 3 (8 ORE)** Fact-Checking e Analisi dei contenuti	**MODULO 4 (6 ORE)** Analisi delle reti sociali	**MODULO 5 (6 ORE)** Generative AI, deepfake	**MODULO 6 (4 ORE)** Framework di valutazione del rischio
• Tipologie di disinformazione • Esempi pratici: Analisi di casi studio come Cambridge Analytica, campagne elettorali e crisi sanitarie. • Impatto della disinformazione	• Ciclo di Intelligence • Introduzione agli strumenti OSINT: (i) Acquisizione, (ii) Analisi, (iii) Visualizzazione • Limiti e Sfide • Casi di Esempio	• Criteri per la valutazione delle fonti • Analisi delle fonti online • Strumenti per l'analisi e la verifica di contenuti	Algoritmi e strumenti Polarizzazione, echo chamber e filter bubbles Casi di esempio	• Creazione e rilevamento di deepfake: immagini, video e audio • Generative AI per la creazione di testi persuasivi (e.g., LLM come ChatGPT) • Strumenti di rilevamento • Esempi di campagne mediatiche costruite con Generative AI	• DISARM (Disinformation Analysis and Risk Management) • ABCDE (Actor, Behaviour, Content, Degree, Effect) • Altri • Esempi di utilizzo: FIMI Report I e II

ARTICOLAZIONE DEL CORSO

LABORATORIO (16 ORE): Esercitazioni pratiche su verifica delle informazioni, fact-checking e analisi di contenuti manipolati con strumenti digitali e software per l'analisi di rete.

- 1 ora - Approfondimento di un caso di giornalismo investigativo svolto con strumenti OSINT da esperti, ad esempio: Bellingcat, RAND, etc.
- 2 ore - Analisi uno o più casi di disinformazione a scelta identificando: la tipologia di minaccia, gli attori, il messaggio, il target.
- 2 ore - Fact-checking su notizie reali utilizzando tool introdotti al corso.
- 5 ore - Analisi dei contenuti che per l'individuazione di narrative emergenti su dataset noti o acquisiti utilizzando tool di propaganda detection, clickbait, stance, etc.
- 5 ore - Utilizzo di tool (e.g., Gephi) per analisi delle reti sociali (misure di centralità, identificazione di community, etc.) su dataset noti o acquisiti.
- 1 ora - Produzione di un report di sintesi.

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Intelligenza Artificiale: progettazione sicura e robusta

DESCRIZIONE CORSO

Il modulo intende approfondire le diverse fasi della progettazione di un approccio basato sull'intelligenza artificiale in diversi ambiti applicativi, incluso la cybersecurity, evidenziando quali sono le minacce alla sicurezza. Verranno fornite le linee guida per la progettazione sicura e strumenti per la valutazione della sicurezza.

ARGOMENTI

Panoramica sui diversi approcci basati su Intelligenza Artificiale. Machine Learning, Deep Learning, generative Models. Apprendimento supervisionato e non supervisionato. Aspetti critici nella definizione del modello dei dati, nella gestione del training set, nella selezione dell'algoritmo di apprendimento e della stima dei parametri, criticità in fase operativa. Definizione dei threat models. tecniche di progettazione robusta. Strumenti per la valutazione della sicurezza e robustezza del sistema sviluppato.

TARGET

- Aziende di sviluppo software o integratori di soluzioni di terze parti.
- Progettisti e sviluppatori software.

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE) Elementi di base di AI, machine learning, deep learning	**MODULO 2 (8 ORE)** Data set, modelli di dati	**MODULO 3 (8 ORE)** Metodologie di utilizzo dei parametri	**MODULO 4 (8 ORE)** Tipologie di Errore e Threat Modelling	**MODULO 5 (8 ORE)** Tecniche di Mitigazione dei Problemi	**LABORATORIO (16 ORE)**
Introduzione ai concetti fondamentali Modelli generativi e applicazioni Potenziali rischi in ambito cybersecurity	Pre-elaborazione dei dati: pulizia, normalizzazione e gestione dei valori mancanti; Caratteristiche dei dataset; Modelli di dati e training set	Tecniche per la selezione dei parametri Validazione incrociata e grid search Metodologie di verifica delle prestazioni del modello Valutazione del modello Metriche di prestazione (precision, recall, F1-score, ROC curve) Analisi degli errori e miglioramento iterativo	Modelli di minaccia per i sistemi AI: Analisi delle vulnerabilità basate su compromissioni di confidentiality, integrity e availability (CIA). Impatti sulla purezza del dato: Manipolazioni dei dati di input (e.g., adversarial attacks). Robustezza ai dati rumorosi o manipolati.	Strategie per mitigare le minacce (Regularization e dropout per modelli robusti) Best practices per la progettazione sicura Principi di sicurezza by design. Creazione di un Modello AI Sicuro Applicazione di tecniche di hardening del modello per aumentare la robustezza Validazione e test del modello progettato. Monitoraggio continuo e auditing dei modelli	• Esercitazioni pratiche di progettazione di un sistema di machine learning, vulnerabilità e progettazione robusta e sicura in alcuni ambiti applicativi diversi. • Ripercorrere quanto fatto nella teoria e applicarlo su un caso di studio. Data set, progettazione, rischi e risoluzione

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Difesa dagli attacchi avanzati, offuscati e evasivi

DESCRIZIONE CORSO

Questo modulo affronta nel dettaglio le tecniche utilizzate per la realizzazione di attacchi evasivi, cioè attacchi che eludono i sistemi di difesa. Verranno illustrate le tecniche di offuscamento del codice che rendono difficile l'analisi statica e dinamica, e le tecniche di evasione per confondere o eludere i sistemi di analisi dinamica.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARGOMENTI

Panoramica sulle principali tecniche di rilevazione di attacchi, basati su firme e sull'analisi statistica. Analisi delle debolezze degli approcci di difesa. Tecniche di offuscamento del software e del traffico di rete. Effetti dell'offuscamento nella rilevazione di attacchi informatici. Attacchi sofisticati per eludere i sistemi di rilevazione delle minacce basati sulla analisi del traffico di rete o della esecuzione die processi. Tecniche di difesa avanzate per la rilevazione di attacchi offuscati e evasivi. Tecniche di difesa avanzate per la rilevazione di attacchi sofisticati. Machine e deep learning per la rilevazione di attacchi informatici.

TARGET

- Aziende che offrono servizi di gestione e sicurezza sistemi IT. SoC
- Analisti di sicurezza
- Threat Analyst

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE) Tecniche di Offuscamento del Codice e del Traffico di Rete	**MODULO 2 (8 ORE)** Analisi statica	**MODULO 3 (8 ORE)** Attacchi Sofisticati ed Evasivi	**MODULO 4 (8 ORE)** Tecniche di protezione	**MODULO 5 (8 ORE)** Tecniche di Difesa Avanzate
• Offuscamento del codice: • Tecniche statiche: trasformazioni del codice per renderlo meno comprensibile (e.g., renaming, control flow obfuscation). • Tecniche dinamiche: codice auto-modificante, packed executables. • Offuscamento del traffico di rete (Crittografia e tunnel crittografici VPN, SSH, HTTPS). • Tecniche di payload obfuscation e pattern evasion. • Rischi per i sistemi di rilevazione tradizionali.		• Attacchi per eludere sistemi di analisi dinamica • Tecniche anti-debugging e anti-virtualizzazione • Malware polimorfico e metamorfico • Attacchi network-based • Social Engineering • Principi psicologici alla base degli attacchi di social engineering • Tecniche comuni: phishing, spear-phishing, baiting, pretexting		• Tecniche di de-offuscamento per analisi statica e dinamica • Sistemi di rilevazione basati su behavior profiling

Difesa dagli attacchi avanzati, offuscati e evasivi

ARTICOLAZIONE DEL CORSO

LABORATORIO (16 ORE)

- Esempi di offuscamento del traffico di rete e di applicazioni software. Attacchi di social engeneering. Esempi di approcci basati sul machine learning per la rilevazione di attacchi informatici
- Approcci per attacchi sofisticati:
  - Sistemi di rilevazione adattivi: aggiornamento dinamico delle regole
- Analisi del contesto per mitigare attacchi evasivi
- Machine e Deep Learning per la Cybersecurity:
- Modelli per la rilevazione di anomalie nel traffico di rete (e.g., autoencoder, RNN)
- Applicazioni di classificatori supervisionati e non supervisionati
- Tecniche di addestramento e prevenzione di bias nei modelli AI per la sicurezza
- Ripercorrere quanto fatto nella teoria e applicarlo su un caso di studio.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Sicurezza del software: prevenzione delle vulnerabilità tramite programmazione sicura

DESCRIZIONE CORSO

Il modulo introduce le pratiche e tecniche per progettare, sviluppare e mantenere applicazioni sicure, proteggendole dalle vulnerabilità più comuni. Verranno forniti i fondamenti della sicurezza del software focalizzandosi su tecniche di programmazione sicura e difensiva, allo scopo di prevenire vulnerabilità e ridurre i rischi di attacco.

ARGOMENTI

Fondamenti di sicurezza del software; principi di programmazione sicura; programmazione difensiva; vulnerabilità comuni e prevenzione; testing di sicurezza; strumenti e framework di sicurezza; pratiche avanzate e DevSecOps; esercitazioni pratiche.

TARGET

- Imprese, enti e pubbliche amministrazioni che svolgono, a vari livelli, attività di sviluppo di software.
- Progettisti e sviluppatori di software
- Studenti di master e dottorato

ARTICOLAZIONE DEL CORSO

MODULO 1 (14 ORE)
Vulnerabilità comuni e prevenzione

- Esempi concreti di vulnerabilità tipiche in diversi ambiti e linguaggi di programmazione (es. stack overflow e format string in C, deserializzazione in Java, loose comparison in PHP, etc.)
- Tecniche di mitigazione e prevenzione

MODULO 2 (14 ORE)
Programmazione sicura e difensiva

- Standard esistenti
- Un esempio concreto: SEI CERT
- Esempi di codice vulnerabile e valutazione della sua compliance agli standard

LABORATORIO (12 ORE) Attraverso esercitazioni pratiche, casi studio e esempi reali, i partecipanti acquisiranno le competenze necessarie per scrivere codice robusto, sicuro e resistente agli errori.

- Esercitazioni pratiche
- Challenge tematiche sulla ricerca di vulnerabilità
- Esercizi di programmazione sicura e difensiva su casi pratici (es. programmi vulnerabili da fixare e/o sviluppo di piccoli esempi che siano compliant agli standard discussi

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Protocolli e tecnologie per l'autenticazione, l'identità e la firma digitale

DESCRIZIONE CORSO

Il modulo descrive i principali protocolli di autenticazione e le tecnologie comunemente nel contesto dell'autenticazione su rete. Il modulo mira anche ad approfondire la nozione di firma digitale, con particolare riferimento alla nozione tecnica di firma elettronica qualificata, e agli aspetti di sicurezza ad essa collegati.

ARGOMENTI

PARTE 1 (Peer-Entity Authentication e Digital Identity) Protocolli di autenticazione (password, Lamport, EKE, challenge-response, ZKP, etc.). Multi-factor authentication. Autenticazione biometrica. Gli standard FIDO e FIDO2. Protocolli e tecnologie per l'identità digitale federata e SSI-based.

PARTE 2 (Electronic Signatures) Primitiva crittografica di firma digitale. Firme elettroniche e documenti informatico. Certificati, revoca, PKI X.509. Firma elettronica avanzata e qualificata. Formati di firma (CADES, PADES, XADES, ASIC-S). Vulnerabilità. Validazione temporale qualificata. Dispositivo qualificato di firma. Firma remota.

TARGET

- Imprese e Pubbliche amministrazioni in particolare se appartenenti al perimetro. Studenti di Master e Dottorato.
- Personale IT per imprese e PA
- Studenti di master e dottorati nel settore IT con interesse verso cybersecurity o profili giuridici interdisciplinari.

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARTICOLAZIONE DEL CORSO

MODULO 1 (10 ORE) Protocolli di autenticazione	MODULO 2 (2 ORE) FIDO	MODULO 3 (10 ORE) Protocolli e standard per l'Identità digitale	MODULO 4 (4 ORE) Firme Elettroniche	MODULO 5 (6 ORE) Certificati e PKI per firme elettroniche
• Modelli base e avanzati per la gestione delle password • Multi-Factor Authentication (MFA) • Google Authenticator, Microsoft Authenticator. • U2F (Universal 2nd Factor) e dispositivi fisici di autenticazione. • Autenticazione biometrica	• Concetti principali: autenticazione senza password, protezione delle credenziali • Tecnologie associate: WebAuthn, UAF (Universal Authentication Framework), U2F • FIDO2 - Evoluzioni rispetto a FIDO: supporto al protocollo WebAuthn e CTAP (Client to Authenticator Protocol) • Esempi di implementazione nei browser moderni e nei dispositivi hardware (e.g., YubiKey).	• Identità digitale e protocolli standard (e.g., SAML, OAuth 2.0, OpenID Connect) • Principi dell'identità decentralizzata • Uso della blockchain per la gestione sicura e autonoma dell'identità.	• Firme elettroniche semplici (SES), avanzate (AES), e qualificate (QES) • Documenti informatici	• Certificati digitali e CA • Gestione della revoca

ARTICOLAZIONE DEL CORSO

MODULO 6 (2 ORE) Formati Firma	**MODULO 7 (2 ORE)** Validazione Temporale	**MODULO 8 (4 ORE)** Dispositivo qualificato di firma e Firma Remota	**LABORATORIO (16 ORE)**
• Formati standard per la firma digitale (CADES, PADES, XADES) • Confronti tra i formati • Scenari applicativi e vantaggi specifici di ciascun formato	• Importanza della validazione temporale nelle firme digitali • Funzionamento di un Time Stamping Authority (TSA).	• Compliance normativa	• Esercitazione su protocolli di autenticazione federata (SAML2 e Open-ID Connect) e SSI. Sessioni pratiche per sviluppatori sull'integrazione di soluzioni di identità digitale (SAML SSO, OpenID Connect, OAuth2.0, WebAuthn).

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Crittografia e applicazioni

DESCRIZIONE CORSO

L'obiettivo del modulo è fornire le conoscenze di base relative alla crittografia e alla sua applicazione ai servizi di sicurezza.

ARGOMENTI

Funzioni one-way e trap-door; Ciphers; Cifrari simmetrici e a chiave pubblica; Principi di confusione e diffusione; Crittografia classica; Attacchi e criptoanalisi; Modelli di attacco; Known Ciphertext Attack; Known Plaintext Attack; Chosen Plaintext Attack; Chosen Ciphertext Attack; Cifrari a blocchi e cifrari a flusso; Rete di Feistel; Data Encryption Standard (DES); Vulnerabilità di DES; composizione di funzioni di cifratura e meet in the middle attack; Triple DES; Blowfish; AES; Modalità di funzionamento della cifratura a blocchi; ECB; CBC; Cipher feedback; OFB; Counter; Pseudo and True Random Number Generators (PRNG and TRNG); Stream Ciphers; Hash crittografici; SHA1 - SHA-256; Attacco del compleanno; Schemi crittografici a chiave pubblica; RSA; Malleability di RSA; Vulnerabilità di RSA; Crittografia probabilistica; OAEP RSA; Curve ellittiche; Autenticazione dei messaggi basata su crittografia simmetrica e a chiave pubblica; Autenticazione dei messaggi basata su hash crittografici (MAC); Prefisso segreto; Postfisso segreto; HMAC; Schemi crittografici a chiave pubblica e firma digitale; Blind signature; Algoritmo Diffie-Hellman e scambio di chiavi; Approcci basati su KDC (Key Distribution Center); Approcci basati su PKI X.509. Applicazioni della crittografia per il web sicuro: TLS. Sicurezza al livello rete: IP sec e VPN.

TARGET

- Imprese e Pubbliche amministrazioni in particolare se appartenenti al perimetro. Studenti di Master e Dottorato.
- Personale IT per imprese e PA
- Studenti di master e dottorati nel settore IT con interesse verso cybersecurity.

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE) Cifrari Simmetrici	**MODULO 2 (8 ORE)** Cifrari a chiave pubblica	**MODULO 3 (2 ORE)** Cifrari a flusso	**MODULO 4 (6 ORE)** Hash Crittografici	**MODULO 5 (4 ORE)** Autenticazione di messaggi
• Cifrari a Blocchi e a Flusso • Rete di Feistel • Data Encryption Standard (DES) • Advanced Encryption Standard (AES) • Modalità di Funzionamento della Cifratura a Blocchi	• RSA (Rivest-Shamir-Adleman) • Curve Ellittiche (ECC - Elliptic Curve Cryptography) • Introduzione e vantaggi rispetto a RSA • Applicazioni nei sistemi moderni (e.g., TLS)	• Differenze tra cifratura a blocchi e a flusso • Esempi di stream ciphers (RC4, Salsa20) • Applicazioni in contesti pratici	• Proprietà degli Hash Crittografici (Unicità, irreversibilità, e dipendenza dai dati) • SHA (Secure Hash Algorithm)/ SHA-1 e SHA-256 • Implicazioni per la sicurezza dei sistemi	• Autenticazione Basata su Crittografia Simmetrica e Asimmetrica • MAC (Message Authentication Code) • Autenticazione Basata su Hash: Generazione e verifica di codici di autenticazione

ARTICOLAZIONE DEL CORSO

MODULO 6 (2 ORE)
Primitive di firma digitale

- Schemi Crittografici a Chiave Pubblica e Firma Digitale
- Applicazioni legali e nei sistemi digitali

MODULO 7 (2 ORE)
Metodi per lo scambio delle chiavi

- Concetto di "key exchange"
- Scambio delle chiavi asimmetriche e simmetriche
- Certificati digitali e infrastruttura a chiave pubblica (PKI)
- Autenticazione e firma digitale

MODULO 8 (4 ORE)
Modalità di esecuzione dei cifrari a blocchi

- Introduzione ai cifrari a blocchi
- ECB (Electronic Codebook)
- CBC (Cipher Block Chaining)
- CFB (Cipher Feedback)
- OFB (Output Feedback)
- CTR (Counter Mode)

MODULO 9
(4 ORE)

- Applicazioni della crittografia per la sicurezza web e IP

LABORATORIO (16 ORE)
Esercitazioni pratiche con software e tool crittografici e con i protocolli TLS e IPsec. Utilizzo pratico di GPG.

- Cifrari e Hash: Python (PyCryptodome, cryptography), Java (BouncyCastle), OpenSSL
- CrypTool per simulazioni
- Attacchi e Criptoanalisi; John the Ripper, Hashcat per attacchi su hash;
- Burp Suite, OWASP ZAP per test di vulnerabilità;
- PKI e Certificati: OpenSSL, Keytool per generare chiavi e certificati X.509;
- Certbot per TLS;
- Firme Digitali e Autenticazione: Python cryptography, OpenSSL per RSA, HMAC, ECDSA;
- Sicurezza di Rete e Web: Wireshark per analisi TLS;
- OpenVPN, StrongSwan per VPN/IPsec

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

La sicurezza dei dati e dei servizi nella trasformazione digitale

DESCRIZIONE CORSO

Questo modulo affronta i temi relativi ai rischi introdotti dalla digitalizzazione dei processi, con particolare riferimento alla sicurezza dei dati e dei servizi. Dopo aver discusso le principali novità apportate dalla trasformazione digitali verranno introdotti i rischi di cybersicurezza connessi. Per ciascuno di questi saranno illustrate le principali best practice, e relative tecnologie, oggi disponibile per mitigarne l'impatto.

ARGOMENTI

Panoramica sulla trasformazione digitale, impatti sui processi e sui servizi aziendali
Concetti chiave di cybersicurezza: minacce, vulnerabilità e obiettivi di protezione
Ruolo della cybersicurezza nei processi di digitalizzazione
Tipologie principali di attacchi: phishing, ransomware, etc.
Tecnologie per la protezione dei dati sensibili: cifratura, gestione degli accessi e controllo
Compliance normativa: GDPR e altre normative rilevanti
Best practice per la protezione della privacy in contesti digitalizzati
Tecnologie per la protezione dei sistemi: firewall, VPN, segmentazione delle reti, etc.
Modelli di sicurezza per il cloud computing e l'IoT
Pianificazione della risposta agli incidenti
Business Continuity e Disaster Recovery
Gestione delle crisi e comunicazione interna ed esterna durante un incidente

TARGET

- Imprese e pubbliche amministrazioni
- In generale tutto il personale impattato dai processi di trasformazione digitale
- Particolarmente di interesse per il personale con funzioni manageriali
- Di interesse per neolaureati di discipline non tecniche che intendono formarsi sui temi generali della cybersecurity prima dell'ingresso nel mondo del lavoro

ARTICOLAZIONE DEL CORSO

MODULO 1 (10 ORE)	MODULO 2 (8 ORE)	MODULO 3 (10 ORE)	MODULO 4 (10 ORE)	MODULO 5 (10 ORE)	LABORATORIO (16 ORE)

• Panoramica sulla trasformazione digitale, impatti sui processi e sui servizi aziendali	• Introduzione al Risk Management nella Cybersecurity
	  • Definizioni e concetti chiave
	  • Analisi degli impatti sui processi e sui servizi aziendali
	  • Strategie di mitigazione: prevenzione, protezione, rilevamento e risposta
		• Compliance normativa: GDPR e altre normative rilevanti
		• Best practice per la protezione della privacy in contesti digitalizzati
		• Tecnologie per la protezione dei dati sensibili: cifratura, gestione degli accessi e controllo
			• Tipologie principali di attacchi: phishing, ransomware, etc.
			• Tecnologie per la protezione dei sistemi: firewall, VPN, segmentazione delle reti, etc.
			• Pianificazione della risposta agli incidenti
			• Business Continuity e Disaster Recovery
			• Gestione delle crisi e comunicazione interna ed esterna durante un incidente
				• Modelli di sicurezza per il cloud computing e l'IoT	• Simulazione di un attacco (e.g. phishing) e pianificazione della risposta per consentire ai partecipanti di riconoscere segnali di compromissione, rispondere all'incidente e attuare misure di contenimento e recupero.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Privacy e sicurezza nella condivisione e gestione dei dati in scenari emergenti

DESCRIZIONE CORSO

Il modulo fornisce una panoramica di problematiche, rischi e soluzioni di particolare rilievo per la protezione dei dati in scenari emergenti nei quali coloro che operano in realtà pubbliche e private o come professionisti si confrontano con crescente frequenza. Tali contesti includono la condivisione, la pubblicazione, l'analisi, la gestione e l'archiviazione di dati nel rispetto della loro privacy e sicurezza. Legislazioni e regolamentazione per la protezione di dati impongono restrizioni che limitano l'uso dei dati, e gli individui, così come le aziende, chiedono il rispetto dei loro requisiti di protezione e la garanzia di un controllo effettivo dei loro dati.

ARGOMENTI

Concetti di privacy e anonymity. Problematiche inerenti la protezione dei dati; Aspetti normativi; Requisiti e Politiche; Approcci alle protezione dei dati (ad es. anonimizzazione, pseudonimizzazione); Apprendimento delle tecniche e metriche di protezione (ad es. k-anonymity, l-diversity, differential privacy); Protezione dei dati in scenari emergenti (ad es. AI, Smart Cities, Cloud); Privacy in contesti AI (ad es. Machine Learning); Sicurezza e privacy dei dati in contesti di outsourcing e distribuiti (ad es. Cloud, IoT, Fog/edge computing).

TARGET

- Imprese e pubbliche amministrazioni
- Dipendenti e professionisti coinvolti nel trattamento dei dati, sia in ambito informatico che in ambito amministrativo, gestionale come anche in altre funzioni

ARTICOLAZIONE DEL CORSO

MODULO 1 (12 ORE)
Sicurezza e privacy dei dati

- Concetti di privacy e anonymity;
- Problematiche inerenti la protezione dei dati;
- Aspetti normativi e standard di riferimento.
- Requisiti
- Politiche
- Introduzione a misure tecniche quali ad es. anonimizzazione e pseudonimizzazione

MODULO 2 (16 ORE)
Approfondimento delle tecniche e metriche di protezione:

- k-anonymity,
- l-diversity;
- Differential privacy.

MODULO 3 (12 ORE)
Protezione dei dati in scenari emergenti:

- Analisi rischi in scenari quali ad es. AI, Smart Cities, Cloud;
- Approfondimento riguardante la Privacy in contesti AI (ad es. Machine Learning);
- Sicurezza e privacy dei dati in contesti di outsourcing e distribuiti (ad es. Cloud, IoT, Fog/edge computing).

LABORATORIO (16 ORE)

- Esercitazioni pratiche volte ad analizzare esempi e casi di studio relativamente all'applicazione dei concetti sviluppati per valutare i rischi di compromissione della privacy e l'applicazione di misure e tecniche di protezione dei dati.
- AI e sicurezza dei dati
- Cloud/Fog/Edge Computing

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Common Criteria for Information Technology Security Evaluation

DESCRIZIONE CORSO

Pagina seguente

DESCRIZIONE CORSO

Il modulo offre una panoramica approfondita sullo standard internazionale per la valutazione della sicurezza dei sistemi IT, con particolare attenzione agli aspetti teorici e pratici del framework. Vengono introdotti i concetti fondamentali, analizzando termini essenziali come Target of Evaluation (TOE), Security Functional Requirements (SFRs) e Security Assurance Requirements (SARs). Viene quindi spiegata la struttura del framework e come questa si applica nei diversi contesti di valutazione. Un focus specifico è dedicato al Protection Profile (PP), ossia il documento che definisce i requisiti di sicurezza generici per una categoria di prodotti, evidenziandone l'importanza e il processo di creazione. Il modulo quindi approfondisce la definizione e il ruolo del Target of Evaluation, l'insieme specifico di funzioni di sicurezza e tecnologie sottoposte a valutazione. Attraverso esempi pratici, i partecipanti imparano a identificare le caratteristiche principali del TOE e come documentarle efficacemente.

Una parte significativa del programma riguarda il processo di valutazione stesso, spiegando le sue fasi principali: dalla pianificazione iniziale, passando per la verifica tecnica, fino alla certificazione ufficiale. Vengono analizzati i ruoli e le responsabilità di tutti gli attori coinvolti, inclusi sviluppatori, valutatori e organismi di certificazione.

Infine, il corso fornisce strumenti pratici per applicare i Common Criteria in contesti reali, preparando i partecipanti a sviluppare, valutare o certificare prodotti in linea con i requisiti dello standard, con l'obiettivo finale di garantire sicurezza, affidabilità e conformità normativa.

Il modulo è organizzato su due parti da seguire a distanza da 20 ore ciascuno per un totale di 40 ore più 16 ore di attività di laboratorio in presenza.

ARGOMENTI

- ISO e i principali standard internazionali collegati ai Common Criteria;
- Target of Evaluation, Security Target e Protection Profile;
- CAP e TOE composto;
- Valutazione Assurance Continuity;
- Schemi di valutazione nazionali e europei e EUCC.

TARGET

- laboratori di valutazione, inseriti nello Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione ai fini della tutela delle informazioni classificate concernenti la sicurezza interna e esterna dello Stato" (DPCM del 11/4/2002) gestito dalla PCM, nello "Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art.10c1 del DL n.10/2002" (DPCM del 30/10/2003) gestito da OCSI, o in quello del Perimetro di Sicurezza Cibernetica Nazionale (D.Lgs del 21.09.2019, n. 105) gestito da ACN;
- aziende che si vogliono inserire nel mercato per fornire prodotti e sistemi ICT e che intendono certificarli. Personale specializzato è essenziale affinché sia in grado di guidare il processo di sviluppo di prodotti o sistemi e di integrazione degli stessi affinché la qualità delle misure di sicurezza sia tale da superare agevolmente superare i test che una valutazione ai fini della certificazione di sicurezza richiede.

ARTICOLAZIONE DEL CORSO

MODULO INTRODUTTIVO (20 ORE)	MODULO AVANZATO (20 ORE)	LABORATORIO (16 ORE)
• Introduzione generale • La valutazione e la certificazione • Termini tecnici di base (TOE, PP, SFR, SAR, EAL/CAP, VA&PT) • Schemi nazionali, europei e accordi multinazionali • Perimetro Sicurezza Nazionale Cibernetica (PSNC) • Accreditamento laboratori	• Termini specifici dei CC e struttura documenti • Struttura dei documenti • Principali SFR • Svolgimento valutazione a EAL1 e EAL2 e differenze • Rapporto Finale di Valutazione (RFV)	• L'obiettivo è prendere confidenza con gli strumenti del II volume dei Common Criteria sulle SFR al fine di scrivere i documenti a supporto dei prodotti/sistemi sviluppati o integrati e del III volume dei Common Criteria sulle SARsistemi ICT; svolgere piccole attività di valutazione a livello EAL1 e a EAL2 con l'impiego del CEM. • Modulo esercitativo Ore Approfondimento, esempi ed esercizi di scrittura di ST/PP (CC Vol. II e IV)

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Framework e Standard open per Cyber Risk Assessment

DESCRZIONE CORSO

Il modulo presenta alcuni dei principali metodi open per l'assessment (non trattamento) dei rischi cyber, dal modello NIST all'approccio europeo di ENISA, fino allo standard ISO/IEC 27001:2022. Il modulo si compone di una prima parte teorica e di una seconda parte orientata ad analizzare molteplici contesti applicativi sia in ambito IT sia in ambito OT. Il modulo è organizzato su due parti da seguire a distanza: il primo teorico di 16 ore; il secondo pratico da 24 ore per un totale di 40 ore.

ARGOMENTI

Cyber risk assessment del NIST; Cyber risk assessment di ENISA anche per PMI; Cyber risk assessment dello standard ISO/IEC 27001:2022; Almeno due casi applicativi in ambito IT; Un caso applicativo in ambito OT industriale; Un caso applicativo in ambito OT civile (es., smart city)

TARGET

- Personale aziendale e della PA di organizzazioni del perimetro nazionale, della NIS2 e di DORA.
- Studenti di master e dottorato.
- Personale di informatica e ingegneria informatica ovvero di altri aree gestionali, economiche e tecnologiche

ARTICOLAZIONE DEL CORSO

MODULO 1 (16 ORE)
Contesto e concetti base

- Evoluzione normativa (L90, NIS2, DORA) e Panorama delle minacce Cyber
- Probabilità, Rischio e Impatto
- Metriche e metodologia di analisi del rischio
- Analisi dei rischi e Strategie di sicurezza
- Cyber Risk Assessment
  - 1. Cyber risk assessment del NIST
  - 2. Cyber risk assessment di ENISA anche per PMI
  - 3. Cyber risk assessment dello standard ISO/IEC 27001:2022

MODULO 2 (24 ORE)
Use cases applicativi in ambito IT

- Un caso applicativo in ambito OT industriale
- Un caso applicativo in ambito OT civile (es., smart city)

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Framework e Standard commerciali per Cyber Risk Assessment

DESCRIZIONE CORSO

Il modulo presenta due dei principali metodi commerciali per l'assessment (non trattamento) dei rischi cyber. Il modulo si compone di una prima parte teorica e di una seconda parte orientata ad analizzare molteplici contesti applicativi. Il modulo è di 24 ore da seguire a distanza, in cui vi è una parte teorica di 8 ore e una seconda di casi applicativi di 16 ore.

ARGOMENTI

I due metodi da prendere in considerazione sono a libera scelta dell'RTI così come l'organizzazione dei contenuti. Si suggerisce di presentare ciascun metodo in 4 ore di lezione teorica e di dedicare 8 ore per ciascun metodo ai contesti applicativi. Si può anche ipotizzare di considerare uno stesso contesto a cui si applicano i due metodi.

TARGET

- Personale aziendale e della PA di organizzazioni del perimetro nazionale, della NIS2 e di DORA.
- Studenti di master e dottorato.
- Personale di informatica e ingegneria informatica ovvero di altri aree gestionali, economiche e tecnologiche

ARTICOLAZIONE DEL CORSO

MODULO 1 (16 ORE)
Cyber risk assessment

- Descrizione del tool 1 di risk assessment/metodologie
- Descrizione del tool 2 di risk assessment/metodologie
- Almeno due casi applicativi in ambito IT

MODULO 2 (24 ORE)
Use cases applicativi in ambito IT

- Un caso applicativo in altri ambiti
- Guida all'utilizzo pratico degli strumenti

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Orchestratori distribuiti e applicazioni "Cloud Native"

DESCRIZIONE CORSO

Il corso offre una panoramica sugli aspetti operativi e di sicurezza dell'orchestratore Kubernetes e le caratteristiche delle applicazioni cloud native. Il modulo si divide in tre parti: la prima della durata di 8 ore illustra l'architettura e le scelte progettuali dietro all'orchestratore, la seconda della durata di 20 ore coinvolgerá invece delle lezioni pratiche sull'installazione, operazione, manutenzione sia di applicativi che dell'orchestratore stesso. Il terzo modulo di 12 ore approfondisce le tematiche di sicurezza, tra cui la gestione dei segreti, la gestione della rete, le pratiche di osservabilità e la simulazione e il rilevamento di potenziali attacchi.

ARGOMENTI

- Architettura di Kubernetes, nodi, stato distribuito, modello a Pod, networking model; installazione e manutenzione di Kubernetes in ambienti baremetal, controllori integrati, service discovery, gestione traffico nord-sud, operatori, gestori di pacchetti per Kubernetes; gestione dei segreti, policy di rete, monitoraggio, logging, auditing, detection di movimenti laterali (pivot) ed evasione dalle sandbox.

TARGET

- Aziende di medie e grandi dimensioni che stanno effettuando una transizione verso architetture cloud native
- Società di consulenza IT che necessitano di formare il proprio personale sulle tecnologie container
- Startup tecnologiche che intendono scalare le proprie infrastrutture
- System integrator che devono gestire deployment complessi per i propri clienti
- Il corso è rivolto a professionisti IT, DevOps engineer, system administrator e sviluppatori software che desiderano acquisire competenze approfondite su Kubernetes e le architetture cloud native.

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE)	MODULO 2 (20 ORE)	MODULO 3 (12 ORE)	LABORATORIO (16 ORE)
• Architettura di Kubernetes, nodi, stato distribuito, modello a Pod, networking model.	• Installazione e manutenzione di Kubernetes in ambienti baremetal, controllori integrati, service discovery, gestione traffico nord-sud, operatori, gestori di pacchetti per Kubernetes	• Gestione dei segreti, policy di rete, monitoraggio, logging, auditing, detection di movimenti laterali (pivot) ed evasione dalle sandbox.	• Tutti i contenuti del modulo due si terranno sotto forma di esercitazioni guidate all'interno di macchine virtuali, permettendo agli allievi di fare esperienza pratica con le tecnologie prese in esame.

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Digital Sovereignty: Beyond tensions of data protection and cybersecurity

DESCRIZIONE CORSO

Il modulo intende approfondire i punti di maggiore tensione tra la governance e disciplina dei dati, sia personali che non personali, e la cybersicurezza. Il modulo si divide in tre parti. Nella prima sono individuati i profili tecnici della digital sovereignty. Nella seconda parte si analizzeranno i profili di connessione tra la disciplina dei dati personali e la cybersicurezza, soprattutto relativamente agli aspetti problematici della gestione e notifica dei data breach e delle notifiche cybersicurezza. La terza parte affronta i problemi collegati alla gestione della compliance alle norme NIS2 (DLGS 138/2024) e Legge 90/2024.

ARGOMENTI

Digital sovereignty (data sovereignty and trust models; confidentiality and compliance of computations); Analisi di casi studio in materia di databreach; Disciplina delle notifiche in materia di data breach e notifiche cybersecurity; La gestione della compliance NIS 2; Cenni alla compliance DORA.

TARGET

- PA tenute alla compliance NIS 2 o DORA.
- Aziende nazionali non tenute alle norme perimetro ma a NIS 2 o DORA
- Studenti master e dottorato
- Personale della PA, personale di aziene e professionisti che hanno già interesse al tema cyber e lavorano già nel mondo della protezione dei dati.

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE)	MODULO 2 (20 ORE)	MODULO 3 (12 ORE)	LABORATORIO
• Digital sovereignty • Data sovereignty and trust models; • Confidentiality and compliance of computations	• Analisi di casi studio in materia di databreach. • Disciplina delle notifiche in materia di data breach e notifiche cybersecurity	• La gestione della compliance NIS 2 • Cenni alla compliance DORA	• Il modulo si terrà sotto forma di lezioni che partiranno da casi studio, modello Harvard Business.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Sicurezza e privacy nei dispositivi mobili

DESCRIZIONE CORSO

Il modulo ha lo scopo di fornire le conoscenze di base per la comprensione, l'analisi e la gestione della sicurezza e della privacy sui dispositivi mobili. Per raggiungere questo obiettivo, il modulo introduce dapprima le caratteristiche principali dei sistemi operativi mobili, con un particolare focus su Android, e i processi di sviluppo delle app, per poi indagare i principali problemi di sicureza e privacy del mondo mobile nonché le tecniche allo stato dell'arte per la loro analisi e risoluzione.

ARGOMENTI

Ecosistema Mobile; Sicurezza & Privacy applicazioni mobile; Metodologie statiche e dinamiche per il VA/PT; Resilienza & Offuscamento; Malware

ARTICOLAZIONE DEL CORSO

MODULO 1 (6 ORE) Ecosistema Mobile

- Panoramica sull'ecosistema mobile
- Analisi delle architetture di Android e iOS
- Approfondimento sul sistema operativo Android
- Modello di sviluppo delle app Android e iOS

MODULO 2 (6 ORE) Sicurezza & Privacy applicazioni mobile

- Concetti di rischio, vulnerabilità, superfici di attacco
- Vulnerabilità e attacchi al sistema operativo e alle app
- Tecniche di profilazione dell'utente e del dispositivo mobile
- Attacchi alla privacy dell'utente

MODULO 3 (18 ORE) Metodologie statiche e dinamiche per il VA/PT

- Analisi statica di applicazioni Android e iOS
- Analisi dinamica di applicazioni Android e iOS

MODULO 4 (5 ORE) Resilienza & Offuscamento

- Attacchi di repackaging e tecniche di anti-repackaging
- Tecniche di offuscamento del bytecode e del codice nativo

MODULO 5 (5 ORE) Malware

- Panoramica mobile malware
- Realizzazione e analisi di malware mobile (basi)

ARTICOLAZIONE DEL CORSO

LABORATORIO (16 ORE)

- Analisi statica e dinamica di app Android reali con metodologie e tool allo stato dell'arte (8h)
- Protezione di una app vera dal repackaging tramite l'utilizzo di tecniche di anti-repackaging e offuscamento (4h)
- Implementazione di tecniche di anonimizzazione su un'app (4h)
- Analisi statica e dinamica di app Android reali con metodologie e tool allo stato dell'arte (8h)
- Protezione di una app vera dal repackaging tramite l'utilizzo di tecniche di anti-repackaging e offuscamento (4h)
- Implementazione di tecniche di anonimizzazione su un'app (4h)

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Aspetti di sicurezza nei dispositivi embedded

DESCRIZIONE CORSO

Il modulo affronta i principali aspetti di sicurezza legati ai dispositivi embedded, con un focus su hardware e software utilizzati in applicazioni critiche. Verranno esplorati attacchi e contromisure specifici per l'ambiente embedded, con laboratori pratici per consolidare le conoscenze teoriche. Il modulo ha come obiettivi: (i) comprendere i principi di sicurezza nei sistemi embedded, (ii) Identificare vulnerabilità hardware e software specifiche dei dispositivi embedded (iii) applicare tecniche di protezione contro attacchi mirati a piattaforme embedded (iii) sviluppare competenze pratiche in analisi e mitigazione delle minacce.

ARGOMENTI

Introduzione alla Sicurezza nei Sistemi Embedded; Architetture e Modelli di attacco; Sicurezza Hardware; Sicurezza del Software Embedded; Comunicazioni Sicure; Tendenze e Case Study

ARTICOLAZIONE DEL CORSO

MODULO 1 (10 ORE) Introduzione alla Sicurezza nei Sistemi Embedded	**MODULO 2 (10 ORE)** Architetture e Modelli di attacco	**MODULO 3 (10 ORE)** Sicurezza Hardware	**MODULO 4 (5 ORE)** Sicurezza del Software Embedded	**MODULO 5 (5 ORE)** Comunicazioni Sicure

• Differenze tra sicurezza nei sistemi embedded e nei sistemi generici.
• Principi di sicurezza: confidenzialità, integrità, disponibilità.
• Minacce specifiche: attacchi fisici, attacchi software e vulnerabilità del firmware
	• Architetture hardware di dispositivi embedded (SoC, MCU, FPGA).
	• Modelli di attacco (Threat Models) e analisi di rischio.
	• Introduzione a TrustZone, SGX e altre tecnologie per sicurezza
		• Attacchi a livello hardware:
		  • Side-channel attacks (DPA, SPA).
		  • Fault injection (laser, glitching).
		• Contromisure hardware:
		  • Randomizzazione.
		  • Tecniche di masking e DPA countermeasures
			• Buffer overflow e mitigazioni.
			• Sicurezza del firmware:
			  • Tecniche di cifratura e autenticazione.
			  • Secure Boot e aggiornamenti sicuri.
			  • Utilizzo di strumenti come Binwalk per analisi firmware
				• Protocolli crittografici per IoT ed embedded (TLS/DTLS, MQTT)
				• Implementazione di chiavi crittografiche sicure.
				• Vulnerabilità nei protocolli wireless (ZigBee, Bluetooth).

ARTICOLAZIONE DEL CORSO

LABORATORIO (16 ORE)

- Analisi di firmware: Decodifica e reverse engineering con Binwalk e Ghidra
- Side-channel attack: Simulazione e rilevazione di attacchi DPA su hardware demo.
- Secure Boot: Implementazione di un sistema di avvio sicuro con microcontrollori.
- Simulazione di attacchi wireless: Analisi della sicurezza di ZigBee o Bluetooth.
- Testing hardware: Identificazione di vulnerabilità con fault injection su FPGA

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Aspetti di sicurezza e relative normative nel mondo automotive

DESCRIZIONE CORSO

Il modulo fornisce una panoramica completa sulle normative di sicurezza nell'industria automobilistica, con particolare attenzione agli standard funzionali e di cybersecurity. L'obiettivo è di preparare i partecipanti ad affrontare le sfide tecniche e normative necessarie per progettare e certificare veicoli sicuri secondo le regolamentazioni globali.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARGOMENTI

Introduzione alle Normative Automotive; Sicurezza Funzionale - ISO 26262; Cybersecurity nei Veicoli - ISO/SAE 21434; Certificazioni e Conformità

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

ARTICOLAZIONE DEL CORSO

MODULO 1 (8 ORE)
Introduzione alle Normative Automotive

- Concetti base di sicurezza in ambito automotive
- Panoramica delle normative principali:
  - ISO 26262 (Functional Safety)
  - ISO/SAE 21434 (Cybersecurity)
  - UNECE WP.29 (Regolamento per la cybersecurity e l'aggiornamento software)

MODULO 2 (16 ORE)
Sicurezza Funzionale - ISO 26262

- Principi di sicurezza funzionale:
  - ASIL (Automotive Safety Integrity Level).
  - Hazard and Risk Analysis (HARA).
- Ciclo di vita della sicurezza (Safety Lifecycle):
  - Concetti di progettazione sicura
  - Validazione e verifica
  - Processi di testing e rilascio

MODULO 3 (12 ORE)
Cybersecurity nei Veicoli - ISO/SAE 21434

- Minacce alla cybersecurity dei veicoli connessi
- Cybersecurity lifecycle:
  - TARA (Threat Analysis and Risk Assessment).
  - Progettazione sicura di sistemi elettronici.
  - Impatti del regolamento UNECE WP.29 e CSMS (Cybersecurity Management System)

MODULO 4 (4 ORE)
Certificazioni e Conformità

- Preparazione e gestione degli audit.
- Redazione della documentazione tecnica:
  - Safety Case
  - Cybersecurity Case

LABORATORIO (16 ORE)
Laboratorio di Hazard and Risk Analysis (HARA)

- Identificazione dei rischi per un sistema ADAS
- Laboratorio di TARA: Valutazione delle minacce cybersecurity in un'architettura CAN bus
- Validazione e Verifica: Analisi di test funzionali basati su ISO 26262
- Redazione della Documentazione: Creazione di un Safety Case per un componente automobilistico.

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE