CYBER INNOVATION NETWORK: DALLA VALIDAZIONE ALLA VISIONE

Brochure Completa

Indice

Cyber Innovation Network | Portfolio di startup finanziate

I3P

Quantum cybersecurity to ensure data and communications

Embedded systems designed to accelerate development and integration while ensuring software security

Real-time monitoring of IoT devices, advanced threat detection, and regulatory compliance

Satellite data protection to safeguard against hacker attacks on critical infrastructures

Scientifica

Unbreakable digital identities through voice and biometric recognition

Data authenticity certification through forensic methodology

Plug-and-play blackbox for cybersecurity

Solution to enhance the security of EV charging stations and OT and IIoT devices

Nana Bianca

Automate the compliance process with current regulations through AI and ML to mitigate vulnerabilities

End-to-end automation of compliance with traceable evidence and immutable audit trail that reduces audit costs and time

Hardware products for cybersecurity in OT, IoT, and automotive environments

3D gaming platform for cybersecurity awareness focused on major threats


i3P
INCUBATORE
POLITECNICO DI TORINO
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA AEDIFICAT
NCC
CYBERSECURITY NATIONAL
COORDINATION CENTRE
ITALY

levelQuantum
THE QUANTUM SECURITY COMPANY

info@levelquantum.it
www.levelquantum.eu

Head office: Milan, Italy
Year of establishment: 2022
Supported by: i3P
CEO: Magdalena Stobinska
Team: 4

Target sectors: Cybersecurity, IoT
Turnover and Business Volume: n/a
Obtained funding: 150.000 €
Funding need: 500.000 €
Supported by ACN: Yes

Value proposition

levelQuantum provides unbreakable, quantum-based cybersecurity with real-time threat detection and secure key exchange over any distance, protecting critical communications for defense and high-value industries.

Solution and Technology

Solution: quantum-based key distribution system (quantum terminals) that guarantees unbreakable data security and real-time intrusion detection for critical communications.

Technology: patented device-independent QKD technology which uses quantum entanglement to generate encryption keys without transmission, ensuring absolute security even against quantum-computer attacks.

Business Model

levelQuantum operates a dual business model combining hardware sales and recurring service revenues. It sells quantum cryptographic terminals with integrated software to governments, defense, and critical industries, while offering ongoing support, system updates, and customization. This approach builds long-term partnerships and scalable growth through high-value, dual-use cybersecurity solutions.

Emerging Disruptive Technologies

Quantum Cryptography	Quantum Entanglement	Device-Independent QKD	Post-Quantum Security	Photonic Communicaitons	Quantum Randomness
Real-time intrusion detection	Cloud-Native Architecture	Zero-Trust Architecture	Dual-Use Cybersecurity	Critical Infrastructure Protection	Quantum Internet

mulini

info@mulini.eu

www.mulini.eu

Head office: Turin, Italy
Year of establishment: 2024
Supported by: I3P
CEO: Vanessa Carioggia
Team: 6

Target sectors: Cybersecurity, IoT
Turnover and Business Volume: n/a
Obtained funding: 150.000 €
Funding need: 500.000 €
Supported by ACN: Yes

Value proposition

Mulini provides an advanced solution for automated regulatory compliance verification in IoT environments. In a context where European regulations such as the Cyber Resilience Act (CRA), NIS2, and GDPR impose strict requirements, the platform enables manufacturers, assessors, and public administrations to avoid costly penalties. The solution is also designed for high-risk environments, such as hospitals, smart cities, and industrial infrastructures, offering continuous monitoring, threat detection, and real-time compliance assurance.

Solution and Technology

Solution: CertifIoT monitors IoT device compliance with worldwide regulations (CRA, GDPR, JC-star), ensuring security and transparency. FORMA Box detects anomalies and controls non-essential destinations, protecting devices and critical infrastructure. MEDibox secures digital hospitals, ensuring compliant use of connected medical devices and safeguarding patient data.

Technology: Mulini provides a platform for automated IoT security and regulatory compliance, combining continuous monitoring, vulnerability detection, and AI-driven compliance assessment. Its offline, modular architecture ensures data privacy, operational control, and scalability across diverse IoT environments, helping organizations reduce risks and meet evolving security and privacy regulations.

Business Model

Mulini operates on a license-based business model, offering its software solutions through annual product licenses. This approach ensures predictable recurring revenue streams while providing clients with continuous access to updates, maintenance, and technical support. Target Customers: Vendors: IoT device manufacturers and system integrators who require automated compliance and security validation for their products. Assessors: Independent security and compliance assessment organizations. Public Administrations: Government bodies and regulatory agencies can adopt Mulini's solutions to support oversight, certification, and audit processes.

Emerging Disruptive Technologies

IoT	Data Science	Machine and Deep Learning	DevSecOps	Knowledge representation and reasoning	Business process management

OSMIUM

info@osmium.solutions

www.osmium.solutions

Head office: Turin, italy

Year of establishment: 2023

Supported by: I3P

CEO: Juan José Grosso

Team: 10

Target sectors: Aerospace, Defence and Automotive

Turnover and Business Volume: 700.000 € (2025)

Obtained funding: Bootstrapped + ESA & National Funding

Funding need: Looking for venture customers/ clients

Supported by ACN: Yes

Value proposition

Resilience of Embedded Systems and Communications.

Solution and Technology

Solution: Osmium OS, an all-European, secure embedded Linux solution that simplifies development for teams with limited cybersecurity expertise, allowing savings of up to 75%, providing pre-packaged security configurations (kernel/user-level) and tools for guided system tuning (TweakControl) and security testing using ANSSI and CIS frameworks (RiftHound). Supports real-time applications (HyperSync) and ensures lifecycle security with OTA updates (ModularTweak) and a HW root of trust (BastionHSM). Compliance includes ISO/SAE 21434, UNECE WP.29.

Technology: Yocto, Cgroups, SELinux, RAUC, NFTables, React.

Business Model

OSMIUM has different sources of revenue.
In the case of Osmium OS, it will be offered on a tiered subscription model designed to scale with customer needs: Starter, Basic, Advanced and Corporate.
Revenue comes from these bundled features, advanced tools, and expert services, ensuring flexibility to and capturing value from startups to large enterprises.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Embedded Systems Security	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

SYNCHROPAL
timing and synchronization

info@synchropal.com

www.synchropal.com

Head office: Alba (CN), Italy
Year of establishment: 2022
Supported by: I3P
CEO: Ibrahim Osmani
Team: 9

Target sectors: Drones, eVTOL UAM, U-space, security.
Turnover and Business Volume: n/a
Obtained funding: 3.050.000 €
Funding need: 2.000.000 €
Supported by ACN: Yes

Value proposition

Secure drone positioning with multi-source validation and server-based processing. TechFlight detects spoofing and jamming, ensuring flight integrity and continuity through advanced multilateration algorithms.

Solution and Technology

Solution: Secure drone positioning with real-time spoofing and jamming detection, ensuring continuous navigation even in the event of a GNSS attack.

Technology: Integration of authenticated GNSS, ADS-B, and server-based processing with advanced multilateration to validate flight position and integrity in real time.

Business Model

B2B solutions with integration, retrofit, or greenfield deployment for drones and eVTOL UAM. The Standard model performs local multi-source validation with anti-spoofing/jamming alerts and flight continuity. The Premium model adds server-based multilateration for increased accuracy, cooperative surveillance, and support for critical U-space operations. Scalable services are provided for operators, integrators, and autonomous platform manufacturers.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

scientifica

scientifica

hystriXEC

antonio@hystr-x.com

www.hystr-x.com

Head office: Pisa, Italy
Year of establishment: 2024
Supported by: Scientifica
CEO: Antonio La Marra
Team: 2

Target sector: Mobility, finance, energy, people
Turnover and Business Volume: 30.000 €
Obtained funding: 95.000 € (grant)
Funding need: 500.000 €
Supported by ACN: Yes

Value proposition

Hystrix provides a simple, affordable, and customizable solution specifically designed to enhance the security of both EV charging stations and a broad range of OT and IIoT devices. This directly addresses the growing concerns around cyberattacks in critical infrastructure and connected industrial environments.

Solution and Technology

Solution: the solution is a comprehensive device security platform that incorporates both software and hardware components. This holistic approach suggests a robust and integrated defense mechanism, aiming to protect devices from various angles.

Technology: advanced attack and anomaly detection, indicating an ability to identify and respond to novel threats that haven't been previously encountered. The platform also offers certified logs and modular authorization, allowing machine MFA (Multi-Factor Authentication) support.

Business Model

levelQuantum operates a dual business model combining hardware sales and recurring service revenues. It sells quantum cryptographic terminals with integrated software to governments, defense, and critical industries, while offering ongoing support, system updates, and customization. This approach builds long-term partnerships and scalable growth through high-value, dual-use cybersecurity solutions.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

scientifica

TrueScreen

fabio@truescreen.app

www.truescreen.io./it

Head office: Bologna, Italy
Year of establishment: 2021
Supported by: Scientifica
CEO: Fabio Ugolini
Team: 15

Target sectors: legal, industrial, logistics, infrastructure
Turnover and Business Volume: 700.000 €
Obtained funding: 2.400.000 €
Funding need: 5.000.000 €
Supported by ACN: Yes

Value proposition

TrueScreen is the only cybersecurity platform for the acquisition, signature, and management of indisputable digital data, ensuring authenticity, immutability, and legal validity through a forensic methodology.

Solution and Technology

Solution: TrueScreen provides an end-to-end secure data management system enabling the acquisition, certification, and notarization of digital content (photos, videos, emails, documents) with full legal value. Its services include certified emails, document signing, data notarization, and forensic reports.

Technology: Patented forensic offline environment for data acquisition, analysis, and certification; integration via API, SDK, and Web Portal; digital seal and timestamp issued by a certifying body; compliance with eIDAS, AGID, CAD, ISO 27037 standards.

Business Model

TrueScreen operates under a B2B SaaS model, offering:

- Subscription plans for enterprises using its platform for certified data acquisition, document signing, and digital notarization.
- Pay-per-use options for specific certified transactions (e.g., forensic reports or certified emails).
- White-label and API integration services for corporations seeking to embed TrueScreen's forensic certification technology into their existing workflows.
- Custom enterprise solutions for organizations requiring branded apps, tailored forensic processes, or regulatory compliance tools.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

scientifica

voiceme

mauro.ferri@voiceme.id

www.voiceme.id

Head office: Milan, Italy

Year of establishment: 2021

Supported by: Scientifica

CEO: Mauro Ferri

Team: 6

Target sectors: Banking and Fintech, Insurance

Turnover and Business Volume: 70.000 €

Obtained funding: 560.000 €

Funding need: 600.000 €

Supported by ACN: Yes

Value proposition

VoiceMe generates inviolable digital identities through advanced voice andbiometric recognition, transforming brand–customer interactions into secure,seamless, and password-free digital experiences.

Solution and Technology

Solution: VoiceMe is a multimodal authentication platform that verifies users through voiceprints, facial biometrics, liveness detection, and device validation. It integrates five patented modules: VoiceKey, VoiceAccess, VoicePay, VoiceSign, and VoiceOTP, to enable secure access, payments, and document signing. The solution is deepfake- and data breach–resistant, ensuring fast (3-second) and seamless verification.

Technology: Proprietary patented voice biometric technology and AI-driven verification engine with KYC integration. Supports SDKs for iOS, Android, and Web, cloud or on-premise deployment, and white-label mobile apps.

Business Model

VoiceMe operates under a B2B SaaS and licensing model, offering:

- Subscription-based access to its voice identity platform
- Licensing of SDKs and APIs for enterprises integrating biometric authentication in theirsystems
- White-label and enterprise solutions for banks, telcos, and large corporates
- Pay-per-use transactions for authentication, digital signing, or payment authorization

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

scientifica

zadig™

c.persurich@bitcorp.it

www.bitcorp.it/it/zadig

Head office: Milan, Italy

Year of establishment: 2023

Supported by: Scientifica

CEO: Christian Persurich

Team: 12

Target sectors: finance, industry, healthcare, defense, and public administration, where **data sovereignty** and **operational resilience** are critical.

Turnover and Business Volume: n/a

Obtained funding: 50.000 €

Funding need: 2.000.000 €

Supported by ACN: Yes

Value proposition

ZADIG democratizes advanced cybersecurity for organizations that prioritize data sovereignty, pairing transparency with automation. A modular XDR platform designed for lightweight, energy-efficient AI models, enabling users to own their data, customize detection, and stay resilient.

Solution and Technology

Solution: ZADIG XDR delivers real-time monitoring, automated threat response, and multi-source data integration for holistic cyber protection. Fully customizable and deployable within users' own IT environments, it ensures data sovereignty and transparency.

Technology: Energy-efficient proprietary AI models analyze network behavior, while machine learning predicts threats and continuous learning enables adaptive defense. Future releases will integrate blockchain-based security protocols and quantum-resistant algorithms to strengthen integrity and resilience.

Business Model

ZADIG operates on a recurring software licensing model (SaaS), complemented by technical assistance packages and modular add-on services. Sales are delivered through direct channels and authorized partners, ensuring tailored integration, local deployment options, and ongoing support.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**


nana
bianca
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA AEDIFICAT
NCC
CYBERSECURITY NATIONAL
COORDINATION CENTRE
ITALY

r.troiani@aigarage.it

https://aigarage.it

Head office: Milan, Italy
Year of establishment: 2024
Supported by: Nana Bianca
CEO: Roberto Troiani
Team: 6

Target sectors: Finance, Industrial
Turnover and Business Volume: 120.000 € [2025]
Obtained funding: 50.000 €
Funding need: 300.000 €
Supported by ACN: Yes

Value proposition

End-to-end solution for managing third-party cyber risk in compliance across all major European regulatory frameworks such as DORA, NIS2

Solution and Technology

Solution: AI enabled solution, composed by modules third party risk assessment, audit, monitoring, Register of Information (ROI), incident reporting providing real-time risk scoring, regulatory reporting and a collaboration environment among third parties and security, compliance, legal and procurement teams. AI plays a crucial role to increase usability and simplify the process.

Technology: SaaS solution hosted in data centers within the European Union, with production environments on Amazon Web Services (AWS)

Business Model

SaaS subscription platform, with pricing based on the number of suppliers/contracts monitored and the modules activated
Revenue comes from annual licenses plus optional professional services
Go-to-market combines direct sales and a partner channel (system integrators, SOCs, resellers, and white-label agreements).

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

info@frameworksecurity.it

www.frameworksecurity.it

Head office: Florence, Italy

Year of establishment: 2024

Supported by: Nana Bianca

CEO: Giovanni Ronconi

Team: 2 + 8 consultant

Target sectors: Finance/Banking & Insurance; PA, Golden Power, FCNDP perimeter plus mid/large enterprise

Turnover and Business Volume: 80–150.000 **€** / yearly per tenant (range 40–400.000 **€** second scope/add-on).

Obtained funding: 50.000 €

Funding need: 500.000 €

Supported by ACN: Yes

Value proposition

End-to-end compliance automation (ISO/NIS2/DORA/GDPR/PCI) with traceable evidence and immutable audit trail (hash + notarization + legal timestamp), reducing audit costs/times and non-compliance risks, supported by dashboards and reporting, in a unified GRC + security + BI platform, extendable with vertical packages and flexible deployment (multi-tenant SaaS or on-prem/hybrid).

Solution and Technology

Solution: End-to-end GRC platform with agentless discovery (endpoint/cloud/OT), log/API ingestion (WinRM/SSH/Syslog/NetFlow), ECS/STIX normalization, correlation + ML, multi-framework scoring (ISO/NIS2/DORA/GDPR/PCI), orchestrated remediation, forensic audit trail (hash+blockchain+eIDAS), real-time BI/dashboard and AI/NLP reporting. Extendable modules for vertical packages (DORA, PCI, OT/ICS), multi-tenant SaaS, and on-prem/hybrid option for regulated clients.

Technology: Containerized microservices on an orchestrator; event-driven bus for ingestion/processing; backend workers for ingestion, normalization, correlation, scoring, remediation; API gateway with REST/GraphQL endpoints; separate storage: document database for metadata, object storage for evidence/dumps, search/analytics engine for queries and BI; CI/CD pipeline with lint/test/build and progressive deployment (canary/blue-green); unified observability (logs/metrics/tracing) and defined operational SLOs.

Business Model

Multi-tenant SaaS with Trial/Pro/Enterprise plans and on-prem/hybrid option for regulated clients; pricing per tenant/year + vertical add-ons (DORA, PCI, ISO/NIS2, GDPR, etc.) and OT/ICS packs. Target ticket €80–150k/year (range €40–400k depending on scope and add-ons), professional services for accelerated onboarding/PoC - GRC services, optional modules (PAM/IR/... integration, premium AI reports), 24/7 premium support. GTM PoC-led and partnerships in Finance/PA/Healthcare/Energy.

Emerging Disruptive Technologies

Data Science	**Trusted Execution Technology**	**Machine and Deep Learning**	**Distributed Ledger Technology**	**Business process management**	**Zero Trust & mTLS**	**DevSecOps**	**GenAI**

giuseppe.compare@mindstormsecurity.com

www.mindstormsecurity.com

Head office: Barcellona Pozzo di Gotto (ME), Italy

Year of establishment: 2024

Supported by: Nana Bianca

CEO: Giuseppe Compare

Team: 4 partner + collaborators

Target sectors: Cybersecurity, OT/IoT Security, Automotive Security,Education & Training

Turnover and Business Volume: 200.000 €

Obtained funding: 50.000 € Cybershield Program

Funding need: Hardware development, product industrialisation, AI/Quantum research

Supported by ACN: Yes

Value proposition

Mindstorm enables organizations to move from occasional hardware and firmware testing to a standardized, repeatable and defensible process over time, with continuous updates that reduce cyber risk and simplify compliance with regulations such as NIS2 and IEC 62443

Solution and Technology

Mindstorm develops a proprietary technology platform for hardware penetration testing and firmware analysis across IoT, OT and embedded systems. Macobox integrates tools, procedures and audit-ready reporting into a structured and repeatable methodology. The Macobox platform is the first tool capable of automatically interacting with hardware devices through its integrated software tools and built-in AI agent. The cloud scanner module complements this by automating static firmware analysis, unpacking components, identifying architectures, and highlighting potential weaknesses, while providing an intuitive interface to navigate and compare results.

Business Model

Mindstorm operates a hybrid model based on hardware, licenses and recurring revenues. Macobox is sold or rented with an annual license that includes updates, support and continuous alignment with the operational standard. The platform is designed to scale through partners, collaborations and trained client teams, enabling operational activities such as penetration testing and training to be externalized without increasing internal costs. Mindstorm retains control over technology, standards, certifications and continuous updates, while direct services remain focused on complex and high-value strategic projects

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

SECURE QUEST

info@securequest.it

www.securequest.it

Head office: Turin, Italy

Year of establishment: 2024

Supported by: Nana Bianca

CEO: Alessandro Curioni

Team: 3

Target sectors: Enterprises, critical infrastructure, banking & insurance, fashion, public administration

Turnover and Business Volume: -

Obtained funding: 210.000 €

Funding need: n/a

Supported by ACN: Yes

Value proposition

Transforming the human factor from the weakest link into the first line of defense for organizations, through a training experience that shifts individuals from passive recipients to active participants, enabling stronger retention of key concepts with effectiveness surpassing any other learning approach.

Solution and Technology

Solution: CyberNemesis is a 3D cybersecurity awareness gaming platform featuring interactive mini-games, decision-making exercises, realistic scenarios, and guided simulations focused on the main threats users face. To keep engagement consistently high, a storytelling framework connects all game levels. The platform can be customized to meet specific client needs (e.g., courses on banking anti–money laundering regulations).

Technology: Cloud architecture on Microsoft Azure based on a proprietary platform, featuring a generative AI system that guides users throughout the training journey. Integrated with services such as Photon, Agora, and Ready Player Me.

Business Model

B2B e B2B2B Business Model: annual/three-year licenses. Direct sales to large enterprises, with a go-to-market model through distributors and resellers to also penetrate the Italian SME market.

Emerging Disruptive Technologies

IoT	**DevSecOps**	**Mobile 5G**	**HPC**	**Machine and Deep Learning**	**ICS**
Knowledge representation and reasoning	**HCI**	**Data Science**	**Trusted Execution Technology**	**Distributed Ledger Technology**	**Business process management**

PROGETTI DI DOTTORATO FINANZIATI

XL CICLO

XL CICLO | Dottorandi ACN

Sapienza Università di Roma

Adversarially robust binary similarity models for vulnerability detection

SPoND: Security and privacy of networks of drones

YOSO: Secure Multi-Party Computation

Università degli Studi di Padova

Every Signal Tells a Story: A New Approach to Wireless Security

Using Mechanistic Interpretability to Craft Jailbreaks Faster

Collaborative autonomous vehicle security

LUISS

Attacchi e sicurezza nei foundation models

Resilienza cibernetica nelle catene di approvvigionamento: modelli avanzati per la business continuity e il disaster recovery

Tor Vergata Università degli Studi di Roma

Security testing in 5G systems & beyond

Infrastructural Security for 5G: Multi-level methodologies

UCBM

Soluzioni di cybersecurity per infrastrutture critiche

Security of medical data

Università degli Studi Mediterranea di Reggio Calabria

SECTREID: Secure TRaceble Entity Identification

Università degli Studi dell'Insubria

KNOWLEDGE GRAPHS: Secure and Privacy-Preserving Sharing

unibz

Privacy-aware virtual knowledge graphs over heterogeneous Web APIs

Alma Mater Studiorum Università di Bologna

Modellazione degli attacchi ai sistemi di controllo industriali e metodi per la loro identificazione e rilevazione

Università della Calabria

ICSlure: A High-Interaction Honeynet for ICS

Sant'Anna Scuola Universitaria Superiore Pisa

Metodi di difesa contro attacchi avversari a modelli neurali nel mondo reale

Metodi di difesa contro attacchi avversari a modelli neurali nel mondo reale

Dottorando: Stefano Bianchettin
Supervisore: Prof. Giorgio Buttazzo
stefano.bianchettin@santannapisa.it

Università: Scuola Superiore Sant'Anna di Pisa
Denominazione del corso di dottorato: Emerging Digital Technologies
PhD cycle: XL

Value proposition

- Sicurezza dell'AI in tempo reale
- Robustezza ai perturbazioni avversarie
- Difesa in scenari realistici

Descrizione

Abstract: Il progetto sviluppa metodi efficienti per la rilevazione e mitigazione di attacchi avversari su modelli di AI, anche in scenari black-box e distribuiti, migliorandone robustezza e sicurezza in tempo reale.

Potenziali campi di applicazione del progetto: Sistemi a guida autonoma, Robotica, Visione artificiale, AI su cloud

Aree dell'Agenda

Sicurezza dei Dati e Privacy	**Gestione delle Minacce Cibernetiche**
Sicurezza delle Infrastrutture Digitali	Aspetti della Società
Sicurezza del Software e delle Piattaforme	Aspetti di Governo

Emerging Disruptive Technologies

IoT	General-purpose AI	Knowledge representation & reasoning	Satellite systems	**Robotics and autonomous systems**	HPC	Quantum technologies	
Zero-trust architecture	HCI	Distributed Ledger Technology	5G and beyond mobile networks	OT	**Virtualization and cloud**	Mobile devices	
DevSecOps	Hardware-based security	Virtual reality technologies	Business process management	Data Science	**Machine Learning and Deep Learning**		

Every Signal Tells a Story: A New Approach to Wireless Security

Dottorando: Luca Bonaventura

Supervisore: Prof. Stefano Tomasin
luca.bonaventura@phd.unipd.it

Università: Università degli Studi di Padova

Denominazione del corso di dottorato: Ingegneria delle telecomunicazioni

Ciclo di dottorato: XL

Value proposition

A lightweight authentication solution that lowers cost and power consumption while strengthening security for 6G and IoT ecosystems.

Descrizione

Abstract: Channel knowledge maps based physical layer authentication is an innovative security approach that uses the unique radio characteristics of the wireless environment to verify device identity. By learning how signals naturally behave, this technology enables authentication without relying on heavy cryptography.

Potenziali campi di applicazione del progetto: It is particularly well suited for future 6G networks and IoT, offering scalable, energy-efficient, and resilient protection.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

Using Mechanistic Interpretability to Craft Jailbreaks Faster

Dottorando: Matteo Gioele Collu

Supervisore: Prof. Roberto Confalonieri

matteogioele.collu@phd.unipd.it

Università: Università degli Studi di Padova

Denominazione del corso di dottorato: Brain, Mind and Computer Science

Ciclo di dottorato: XL

Value proposition

Accelerare l'individuazione di jailbreak white-box attraverso la mechanistic interpretability per consentire valutazioni di sicurezza dei sistemi di IA più rapide e rigorose.

Descrizione

Presentiamo un approccio guidato dall'interpretabilità per migliorare l'efficienza nella generazione di jailbreak nei large language models. Invece di valutare i prompt candidati tramite le probabilità di output, come avviene in metodi come AutoDAN, utilizziamo segnali meccanicistici derivati dagli hidden states del modello. In particolare, definiamo delle "regioni di rifiuto" nello spazio delle attivazioni e ottimizziamo i prompt sulla base della probabilità che le attivazioni interne evitino tali regioni. Questo fornisce uno score di fitness anticipato per aggirare il comportamento di rifiuto, permettendo una scoperta più rapida dei jailbreak.

Potenziali campi di applicazione del progetto: Sicurezza dei LLMs, Red Teaming, Mechanistic Interpretability

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

Attacchi e sicurezza nei foundation models

Dottorando: Miro Confalone
Supervisore: Prof. ssa Irene Finocchi
mconfalone@luiss.it

Università: Luiss Guido Carli Università di Roma
Denominazione del corso di dottorato: Cybersecurity
PhD cycle: XL

Value proposition

Il progetto mira a rendere i Foundation Models affidabili, sicuri e utilizzabili in contesti critici, affrontando in modo sistematico le loro vulnerabilità intrinseche.

Descrizione

I Foundation Models (FM) sono modelli di machine learning estremamente versatili alla base di un'ampia gamma di applicazioni, tra cui riconoscimento delle immagini, diagnosi medica, ma anche il vasto ambito dell'AI generativa con la produzione di testi, immagini e video. Utilizzano sofisticate tecniche di deep learning, sono addestrati su un vasto corpus di dati e si contraddistinguono per una grande dimensione e complessità. Tali caratteristiche li rendono tuttavia particolarmente vulnerabili a varie tipologie di attacchi e minacce alla sicurezza.

Potenziali campi di applicazione del progetto: Agentic AI, modellazione di fenomeni complessi, supporto alle decisioni politiche, monitoraggio di infrastrutture critiche, supporto ai cittadini nei servizi offerti dalla Pubblica Amminstrazine

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

SPoND: Security and privacy of networks of drones

Dottorando: Matteo Cornacchia

Supervisore: Prof. Riccardo Lazzeretti
cornacchia@diag.uniroma1.it

Università: Sapienza Università di Roma / LUISS

Denominazione del corso di dottorato: Cybersecurity

Ciclo di dottorato: XL

Value proposition

- Esplorare vettori di attacco originali contro lo stato dell'arte
- Proporre soluzioni efficaci e facilmente applicabili su vari hardware
- Supportare l'utilizzo di sistemi di volo autonomo su larga scala

Descrizione

Abstract: Il progetto SPoND si concentra principalmente sull'offrire soluzioni pratiche per migliorare il grado di maturità degli sciami di droni e la resilienza ad attacchi esterni, con enfasi sui sistemi di volo autonomo o assistito e sulla coordinazione di più veicoli indipendenti .

Potenziali campi di applicazione del progetto: Sistemi autonomi, IoT, Crittografia e data privacy, Sviluppo e testing di firmware sicuro, Sistemi di controllo VR e AR.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

Resilienza cibernetica nelle catene di approvvigionamento: modelli avanzati per la business continuity e il disaster recovery

Dottorando: Alessandra Di Giacomo
Supervisore: Prof. Paolo Spagnoletti
adigiacomo@luiss.it

Università: Luiss Guido Carli
Denominazione del corso di dottorato: Diritto e Impresa
PhD cycle: XL

Value proposition

Paradigma di auditing avanzato basato su sistemi di IA agentica per il monitoraggio continuo e risk-based della compliance normativa, con benefici in termini di governance dei dati, gestione dei rischi di terze parti e resilienza degli ecosistemi digitali interconnessi.

Descrizione

Abstract: La pressione normativa in materia di privacy e sicurezza dei dati rende inadeguati i tradizionali approcci di audit, basati su controlli manuali e periodici. Le regolamentazioni europee (GDPR, NIS2) richiedono modelli di compliance continuativi ed estesi all'intero ecosistema delle terze parti. Lo studio analizza il potenziale dell'IA agentica nei processi di audit, come leva per la transizione verso paradigmi predittivi, continui e autoadattivi.

Potenziali campi di applicazione del progetto: Settori ad alta complessità regolatoria (finanza, sanità, energia, telecomunicazioni, trasporti), PMI con limitate risorse specialistiche, Pubbliche Amministrazioni e Autorità di vigilanza.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- **Aspetti della Società**
- Sicurezza del Software e delle Piattaforme
- **Aspetti di Governo**

Emerging Disruptive Technologies

- IoT
- **General-purpose AI**
- **Knowledge representation & reasoning**
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- **Business process management**
- Data Science
- **Machine Learning and Deep Learning**

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Security testing in 5G systems & beyond

Dottorando: Matteo Fanfarillo
Supervisore: Prof. Giuseppe Bianchi
matteo.fanfarillo@students.uniroma2.eu

Università: Roma Tor Vergata
Denominazione del corso di dottorato: Ingegneria Elettronica
Ciclo di dottorato: XL

Value proposition

- Rendere l'utente finale consapevole del funzionamento delle applicazioni del 5G (come l'eSIM e il relativo provisioning).
- Garantire sicurezza all'utente finale.

Descrizione

Il progetto propone un approccio integrato al security testing nelle infrastrutture 5G e non solo, con lo scopo di affrontare la crescente complessità delle reti, l'integrazione di accessi radio non affidabili e l'aumento della superficie di attacco. Partendo dalle metodologie standard, il lavoro mira ad ampliarle con tecniche aggiuntive come fuzzing dei protocolli, analisi delle configurazioni e crawling, includendo anche aspetti implementativi specifici del 5G. Un ambito di particolare interesse del progetto di ricerca è l'ecosistema eSIM.

Aree dell'Agenda

- **Sicurezza dei Dati e Privacy**
- **Gestione delle Minacce Cibernetiche**
- **Sicurezza delle Infrastrutture Digitali**
- **Aspetti della Società**
- **Sicurezza del Software e delle Piattaforme**
- **Aspetti di Governo**

Emerging Disruptive Technologies

- **IoT**
- **General-purpose AI**
- **Knowledge representation & reasoning**
- **Satellite systems**
- **Robotics and autonomous systems**
- **HPC**
- **Quantum technologies**
- **Zero-trust architecture**
- **HCI**
- **Distributed Ledger Technology**
- **5G and beyond mobile networks**
- **OT**
- **Virtualization and cloud**
- **Mobile devices**
- **DevSecOps**
- **Hardware-based security**
- **Virtual reality technologies**
- **Business process management**
- **Data Science**
- **Machine Learning and Deep Learning**

SAPIENZA UNIVERSITÀ DI ROMA

Adversarially robust binary similarity models for vulnerability detection

PhD student: Anna Paola Giancaspro
Supervisor: Prof. Giuseppe Antonio di Luna
annapaola.giancaspro@uniroma1.it

University: Roma La Sapienza
Name of the doctoral course : Cybersecurity
Doctoral cycle: XL

Value proposition

- First systematic framework for adversarial robustness
- Improve baseline accuracy without retraining and reducing attack success rates
- Establishes reproducible benchmarks for adversarial robustness assessment

Descrizione

Abstract: Binary similarity models determine whether two binary functions originate from the same source code but are vulnerable to adversarial perturbations, preserving functionality while misleading detection. With no validated defenses available, this research enhances models performance implementing re-ranking techniques and improves robustness via defensive mechanisms, establishing a novel framework for trustworthy binary similarity.

Potential fields of application: Vulnerability detection, malware phylogeny analysis, code clone detection for security auditing, and reverse engineering support for IoT and cross-platform systems.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- **Gestione delle Minacce Cibernetiche**
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- **Sicurezza del Software e delle Piattaforme**
- Aspetti di Governo

Emerging Disruptive Technologies

- **IoT**
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- **Machine Learning and Deep Learning**

Modellazione degli attacchi ai sistemi di controllo industriali e metodi per la loro identificazione e rilevazione

Dottorando: Antonio Iacobelli

Supervisore: Prof. Marco Prandini
antonio.iacobelli@unibo.it

Università: Alma Mater Studiorum Bologna

Denominazione del corso di dottorato: : Computer science and engineering

Ciclo di dottorato: XL

Value proposition

Framework ibrido per la protezione dei PLC che combina rilevamento adattivo e verifica formale, colmando il divario tra detection data-driven e garanzie di correttezza. Il progetto mira a migliorare la resilienza dei sistemi ICS contro attacchi silenti e manomissioni della logica di controllo.

Descrizione

Il progetto ha come obiettivo lo sviluppo di un framework per la protezione della logica di controllo dei controllori logici programmabili (PLC), dispositivi chiave nei sistemi di controllo industriale (ICS), integrando tre approcci complementari: machine learning, analisi formale e analisi dinamica. Il lavoro include la creazione e la pubblicazione di un dataset di attacchi industriali per la validazione e la ricerca scientifica.

Potenziali campi di applicazione: Sicurezza delle infrastrutture critiche e dei processi di Industria 4.0.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

SECTREID: SEcure TRaceble Entity Identification

Dottorando: Carmen Licciardi

Supervisore: Prof. Francesco Buccafurri

carmen.licciardi@unirc.it

Università: Università Mediterranea di Reggio Calabria

Denominazione del corso di dottorato: Ingegneria dell'Informazione

PhD cycle: XL

Value proposition

- Service-level prevention of vishing and spoofing
- Standardization of digital identity wallets and new business models
- Hardening 2F authentication with backward-compatible deployment
- Security enhancements for the national digital identity system (SPID)

Descrizione

The project focuses on the study and improvement of authentication mechanisms for digital identity systems, with the aim of strengthening their security in real-world usage scenarios. In particular, the work addresses the analysis and evolution of the authentication models defined by SPID and eIDAS, proposing solutions that are compatible with existing standards. The project also includes the design of privacy-preserving mechanisms for digital identity management, with specific focus on Self-Sovereign Identity models.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

Infrastructural Security for 5G: Multi-level methodologies

Dottorando: Edoardo Manenti

Supervisore: Prof. Francesco Quaglia

edoardo.manenti@uniroma2.it

Università: Roma Tor Vergata

Denominazione del corso di dottorato: : Computer science, control and geoinformation

Ciclo di dottorato: XL

Value proposition

Il progetto punta a rafforzare la resilienza del Core 5G virtualizzato tramite una difesa multi-livello che combina il monitoraggio granulare del kernel con meccanismi di monitoraggio ed enforcement attivo a livello hypervisor, garantendo la continuità dei servizi critici anche in caso di insider threats o attacchi nation-state con privilegi elevati.

Descrizione

Il progetto propone un approccio integrato alla protezione delle infrastrutture SDN/NFV nel 5G per contrastare l'aumento della superficie di attacco nei contesti virtualizzati. Il lavoro mira a garantire l'integrità dei dati e dei processi tramite soluzioni di monitoraggio operanti nel kernel e metodologie di rilevazione proattiva delle minacce. In parallelo, la ricerca introduce capacità di monitoraggio ed enforcement di security policy a livello hypervisor, rendendo l'infrastruttura "security-aware" e capace di validare l'esecuzione dei servizi in modo trasparente e resiliente alla compromissione dei sistemi ospiti.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

KNOWLEDGE GRAPHS
Secure and Privacy-Preserving Sharing

PhD student: Quan Nguyen Thanh
Supervisor: Prof. Elena Ferrari
qnguyenthanh@uninsubria.it

University: University of Insubria
Name of the doctoral course : Computer Science and Mathematics of Computation
Doctoral cycle: XL

Value proposition

The platform enables trustworthy knowledge graph sharing among mutually untrusted parties by combining personalized privacy protection with cryptographically verifiable enforcement, without sacrificing semantic utility or requiring a trusted central authority.

Description

Abstract: Knowledge graphs can enable rich data sharing but also raise serious privacy risks due to sensitive attributes and relationships. Therefore, we propose a decentralized data market platform that combines personalized anonymization with cryptographic verification to enable verifiable, privacy-preserving knowledge graph sharing without relying on trusted platform operators. The platform can ensure accountable data sharing and verifiable enforcement of data owners' privacy requirements in open and untrusted environments.

Potential fields of application: Enterprise Knowledge Management and Data Markets, Data Analytics and Research, Self-Sovereign Data, Privacy Compliance.

Aree dell'Agenda

- **Sicurezza dei Dati e Privacy**
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- **Aspetti della Società**
- Sicurezza del Software e delle Piattaforme
- **Aspetti di Governo**

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- **Knowledge representation & reasoning**
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- **Zero-trust architecture**
- HCI
- **Distributed Ledger Technology**
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- **Data Science**
- Machine Learning and Deep Learning

Privacy-aware virtual knowledge graphs over heterogeneous Web APIs

Dottorando: Albulen Pano
Supervisore: Dr. Davide Lanti
albulen.pano@uniroma1.it

Università: Liberà Universita di Bozen-Bolzano
Denominazione del corso di dottorato: Dottorato Nazionale in Intelligenza Artificiale
Ciclo di dottorato: XL

Value proposition

Controlled access to heterogeneous data sources via Virtual Knowledge Graphs (VKGs) to provide users with a high level representation of the data, possibly stored behind web APIs.

Description

Abstract: VKGs provide a lightweight ontology-based approach to query heterogeneous data sources. Access Pattern Constraints (APCs) enforce mandatory input parameters to access certain resources. We want to combine VKGs and APCs in order to prevent unauthorized access to data without losing the capability of optimizing query planning, or even in the presence of sources that are Web APIs.

Potenziali campi di applicazione del progetto: Any domain handling sensitive information e.g. medicine, finance, education.

Aree dell'Agenda

- **Sicurezza dei Dati e Privacy**
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- **Knowledge representation & reasoning**
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

FONDAZIONE POLICLINICO UNIVERSITARIO CAMPUS BIO-MEDICO

Soluzioni di cybersecurity per infrastrutture critiche

Dottorando: Stefano Perone
Supervisore: Dott. Riccardo Croce
s.perone@unicampus.it

Università: Campus Bio-Medico di Roma
Denominazione del corso di dottorato: Bioingegneria, Scienze Applicate e Sistemi Intelligenti
PhD cycle: XL

Value proposition

Il progetto presenta un approccio olistico che integra la gestione dinamica del rischio per infrastrutture critiche con una piattaforma AI pensata per la risposta agli incidenti nelle PMI, colmando il divario di competenze tecniche e ottimizzando le strategie di difesa.

Descrizione

Abstract: Il progetto sviluppa due soluzioni avanzate di cybersecurity per infrastrutture critiche: DYNAPLAN e PACY. DYNAPLAN ottimizza la difesa degli asset industriali utilizzando metriche temporali e reti bayesiane dinamiche per analizzare la probabilità di exploitation delle vulnerabilità nel tempo e ridurre il rischio cyber rispetto ai modelli statici. Contemporaneamente, PACY punta a porsi come strumento ausiliario per la sicurezza operativa nelle PMI attraverso una piattaforma AI multi-agente che automatizza il triage degli incidenti, l'analisi OSINT e la reportistica normativa.

Potenziali campi di applicazione del progetto: DYNAPLAN trova applicazione nella difesa delle infrastrutture critiche e industriali, ottimizzando la mitigazione del rischio su asset strategici come i PLC. PACY si rivolge invece alle PMI, automatizzando la gestione operativa degli incidenti e garantendo la conformità a normative come il GDPR e la NIS2.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

ICSlure: A High-Interaction Honeynet for ICS

Dottorando: Francesco Aurelio Pironti
Supervisore: Prof. Angelo Furfaro
francesco.pironti@unical.it

Università: Università della Calabria
Denominazione del corso di dottorato: ICT
PhD cycle: XL

Value proposition

ICSlure fornisce una piattaforma low-cost, high-fidelity e modulare per lo studio delle minacce ICS reali, superando i limiti dei tradizionali honeypot a bassa interazione.

Descrizione

Abstract: A differenza dei tradizionali honeypot software, la piattaforma combina PLC fisici reali con simulatori di impianto basati su modelli fisici, elevando il livello di realismo e riducendo il rischio di fingerprinting da parte degli attaccanti.

Potenziali campi di applicazione del progetto: Threat Intelligence per ICS, Testing di sicurezza e hardening, Simulazioni realistiche di scenari di Disaster Recovery

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

FONDAZIONE POLICLINICO UNIVERSITARIO CAMPUS BIO-MEDICO

Security of medical data

Dottorando: Ludovica Pompilio

Supervisore: Prof. Paolo Soda

ludovica.pompilio@unicampus.it

Università: Campus Bio-Medico di Roma

Denominazione del corso di dottorato: National PhD in Health and Life Sciences

PhD cycle: XL

Descrizione

Abstract: Il progetto si propone di garantire l'integrità e la privacy dei dati medici, focalizzandosi su due aspetti principali: la rilevazione delle manipolazioni avversarie nelle immagini mediche e la protezione contro inferenze malevoli nei modelli generativi utilizzati per la creazione di dati sintetici.

Potenziali campi di applicazione del progetto:

- Rafforzamento della sicurezza dei modelli AI per l'analisi di immagini mediche.
- Generazione di dati sintetici privacy-preserving, utilizzabili per l'addestramento di modelli AI e per supportare il processo decisionale clinico, offrendo una visione più completa del paziente.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

UNIVERSITÀ DEGLI STUDI DI PADOVA

Collaborative autonomous vehicle security

Dottorando: Giulio Umbrella
Supervisore: Prof. Mauro Conti
giulio.umbrella@phd.unipd.it

Università : Università degli studi di Padova
Denominazione del corso di dottorato: BMCS
Ciclo di dottorato: XL

Value proposition

Improve the security of how drones share and use sensory perception in autonomous decision-making systems.

Description

The goal of the project is to provide security guarantees in the emerging field of collaboration between autonomous entities. Sensory sharing improves perception and decision-making but introduces security challenges.

- Guarantees secure collaboration
- Develops new perceptual models
- Creates a pipeline for real world application
- Implements a virtual reality application

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

YOSO
Secure Multi-Party Computation

Dottorando: Leonardo Ventura
Supervisore: Prof. Daniele Venturi
leonardo.ventura@uniroma1.it

Università: Sapienza Università di Roma
Denominazione del corso di dottorato: Cybersecurity
PhD cycle: XL

Value proposition

Aumentare la sicurezza delle comunicazioni durante operazioni critiche mediante crittografia basata su Multi-Party Computation (MPC).
Questo consente di proteggere dati e decisioni senza dipendere dalla fiducia in una singola parte.

Descrizione

Abstract: Uno sciame di droni mappa aree sensibili proteggendo i dati critici: con Private Set Intersection (PSI) ogni dispositivo condivide solo le informazioni necessarie, preservando la riservatezza di infrastrutture, asset industriali e zone a accesso limitato.

Potenziali campi di applicazione del progetto: Scenari che richiedono massima riservatezza e anonimato dei dati condivisi: difesa e sicurezza pubblica, protezione di infrastrutture critiche, contesti d'emergenza.

Aree dell'Agenda

- Sicurezza dei Dati e Privacy
- Gestione delle Minacce Cibernetiche
- Sicurezza delle Infrastrutture Digitali
- Aspetti della Società
- Sicurezza del Software e delle Piattaforme
- Aspetti di Governo

Emerging Disruptive Technologies

- IoT
- General-purpose AI
- Knowledge representation & reasoning
- Satellite systems
- Robotics and autonomous systems
- HPC
- Quantum technologies
- Zero-trust architecture
- HCI
- Distributed Ledger Technology
- 5G and beyond mobile networks
- OT
- Virtualization and cloud
- Mobile devices
- DevSecOps
- Hardware-based security
- Virtual reality technologies
- Business process management
- Data Science
- Machine Learning and Deep Learning

NCC

CYBERSECURITY NATIONAL
COORDINATION CENTRE

ITALY