SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

Il Partenariato Esteso SERICS

Security and Rights in the Cyber Space

Alessandro Armando
Fondazione SERICS, Presidente Comitato Scientifico
CINI Cybersecurity National Lab, Direttore

Università di Genova

IMT SCUOLA ALTI STUDI LUCCA

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

PARTENARIATO ESTESO RELATIVO A

"Tematica 7. Cybersecurity, nuove tecnologie e tutela dei diritti"

- Soggetto attuatore: **Fondazione SERICS**
- Inizio: **1 Gennaio 2023**
- Durata: **3 anni**

— Avviso Pubblico per la presentazione di Proposte di intervento per la creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del PNRR, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU – Avviso nr. 341 del 15.3.2022.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

KEY DATA

300
Ricercatori Strutturati

126
Nuovi Ricercatori

114M€
Finanziamento

41,3%
di finanziamenti per le **regioni del Sud Italia**

34%
di finanziamenti per **Bandi di ricerca**

8%
di finanziamenti per **Bandi di innovazione**

5%
di finanziamenti per la **Cybersecurity Academy**

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

UNIVERSITÀ E ISTITUTI SPECIALI

UNIVERSITÀ DEGLI STUDI DI SALERNO

Università di Genova

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Università Ca'Foscari Venezia

SAPIENZA UNIVERSITÀ DI ROMA

UNIVERSITÀ DEGLI STUDI DI MILANO

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

UNIVERSITÀ DELLA CALABRIA

IMT SCUOLA ALTI STUDI LUCCA

UNIVERSITÀ DEGLI STUDI FIRENZE

Politecnico di Torino

Sant'Anna Scuola Universitaria Superiore Pisa

UNICA UNIVERSITÀ DEGLI STUDI DI CAGLIARI

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

ENTI DI RICERCA

cini consorzio interuniversitario nazionale per l'informatica

CYBERSECURITY NATIONAL LAB

Consiglio Nazionale delle Ricerche

cnit consorzio nazionale interuniversitario per le telecomunicazioni

FONDAZIONE BRUNO KESSLER

FUB Fondazione Ugo Bordoni Ricerca e Innovazione

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

AZIENDE

LEONARDO

FINCANTIERI

INTESA SANPAOLO

eni

Telsy

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

SERICS
THEMATIC AREAS

10
Aree Tematiche

27
Progetti di Ricerca

Ogni area tematica è gestita da uno "SPOKE"

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

SERICS THEMATIC AREAS SPOKE

SPOKE 1
Aspetti umani, sociali e legali
CNR

SPOKE 2
Disinformazione e fake news
UNISA

SPOKE 3
Attacchi e difese
UNICA

SPOKE 4
Sicurezza dei sistemi operativi e della visualizzazione
UNIGE

SPOKE 5
Crittografia e sicurezza dei sistemi distribuiti
UNICAL

SPOKE 6
Sicurezza del software e delle piattaforme
UNIVE

SPOKE 7
Sicurezza delle infrastrutture
POLITO

SPOKE 8
Gestione del rischio e governance
UNIBO

SPOKE 9
Mettere in sicurezza la trasformazione
UNIROMA

SPOKE 10
Governance e protezione dei dati
UNIMI

INNOVAZIONE

- Promuovere la migrazione dei risultati verso le aziende partner, nonché verso nuove imprese attraverso **bandi di innovazione aperti**, con l'obiettivo di aumentare il livello di maturità tecnologica (TRL) dei risultati della ricerca.
- **Facilitare l'accesso al mercato** delle soluzioni e dei servizi di Cybersecurity per le piccole e medie imprese (PMI) giovani.
- **Stimolare la creazione di start-up e spin-off**, nonché **la mobilitazione delle conoscenze innovative e dello spirito imprenditoriale** all'interno della comunità.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

CYBERSECURITY ACADEMY

- Formazione avanzata per dipendenti e professionisti su temi selezionati
- Supporto ai Scuole di Dottorato (scuole estive/invernali)
- Supporto ai Master Universitari
- Corsi di imprenditorialità su misura per studenti universitari, laureati, dottorandi e dottori di ricerca
- Formazione per formatori

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

CYBERSECURITY ACADEMY

- **Formazione avanzata per dipendenti e professionisti su temi selezionati**
- Supporto ai corsi di dottorato (scuole estive/invernali)
- Supporto ai master universitari
- Corsi di imprenditorialità su misura per studenti universitari, laureati, dottorandi e dottori di ricerca
- Formazione per formatori

Dettagli: https://www.serics.eu/academy

Cyber Threats & Defense

Difesa dagli attacchi avanzati, offuscati e evasivi
Metodologie e sistemi di Penetration Test e Intrusion Detection
Hardening di sistemi e servizi Linux
Log - Collezionamento, analisi e correlazione degli eventi
Contrastare la disinformazione: Strumenti e Tecniche per la gestione delle Minacce e dei Rischi

Software & System Security

Sicurezza del software: prevenzione delle vulnerabilità tramite programmazione sicura
Intelligenza Artificiale: progettazione sicura e robusta
Sicurezza e privacy nei dispositivi mobili
Aspetti di sicurezza nei dispositivi embedded
Aspetti di sicurezza e relative normative nel mondo automotive

Data Protection & Privacy

La sicurezza dei dati e dei servizi nella trasformazione digitale
Privacy e sicurezza nella condivisione e gestione dei dati in scenari emergenti
Digital Sovereignty: Beyond tensions of data protection and cybersecurity

Cryptography & Authentication

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

Risk Management & Evaluation Frameworks

Common Criteria for Information Technology Security Evaluation
Framework e Standard open per Cyber Risk Assessment
Framework e Standard commerciali per Cyber Risk Assessment

Security of Cloud & Emerging Technologies

Orchestratori distribuiti e applicazioni "Cloud Native"

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

Research Results
(a selection)

Spoke 4 - Security of OS and Virtualization

Project: ARTIC - Affordable, Reusable and Truly Interoperable Cyber Ranges

Goals:

- Framework for NextGen Cyber Ranges
- New application domains and exploitation scenarios

Partners:

- **Academic partners**: UniGE, UniCAL
- **School for advanced studies**: IMT Lucca
- **Consortium**: CINI
- **Industrial partners**: Leonardo, Fincantieri

Equipment and Infrastructure

- **High-performance computing nodes**: Proxmox cluster (384 CPUs, 1.97 TiB RAM, 74.77 TiB Storage) for running VMs and containers
- **Wireless security**: 10 software-defined radios (SDRs), 2 RFSoC, Signal Generator, Spectrum Analyzer, test enclosure, RF accessories, high-speed networking for integrating wireless-based systems
- **CPS security**: PLCs, microcontroller boards, and measurement tools to support realistic (and what-if) CPS scenarios
- **3D facilities**: 2 WS equipped with GPUs, 2 portable GPU in dedicated enclosures, used to integrate 3D simulators and to support high-fidelity simulation of electro-optical sensors

Key Achievements

Advanced cyber-physical scenario generation

- Supports both IT and OT systems, with simulated physical processes and hardware-in-the-loop capabilities
- Successfully validated by **uncovering real-world issues** in avionic, maritime, and mission-critical (MCx) systems
  - **2 CVEs** identified in the TCAS protocol, officially registered by CISA
  - Contributed to a **security update** of the **3GPP technical specification** (TS 33.180) for MCX authentication mechanisms (MCX Connect)

Key Achievements (continued)

Open source framework for next-generation cyber ranges

- Modular and flexible: supports both integration and full-range development
- Validated through training activities in cyber defence exercises: used in higher education settings for hands-on cybersecurity sessions

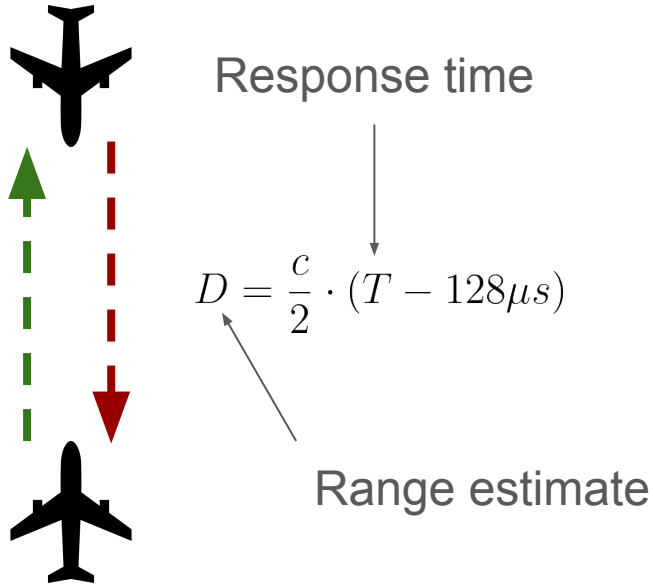
Open source testbed for Maritime cybersecurity “MaCySTe[1]”

- Validated use in research and industrial contexts, including Fincantieri and MSC Technologies

[1] G. Longo, A. Orlich, S. Musante, A. Merlo, **E. Russo**. MaCySTe: A virtual testbed for maritime cybersecurity. SoftwareX, 2023, 23, 101426. doi: 10.1016/j.softx.2023.101426 (https://github.com/CRACK-MCR/MaCySTe)

Zooming In: security analysis of TCAS

- A collision avoidance system used in aviation to prevent mid-air collisions through radio-based coordination
  - detects nearby aircraft, alerts on potential threats - Traffic Advisory (TA), resolves conflicts - Resolution Advisory (RA)
- Uses a insecure protocol but never exploited through a cyber attack using computer-based and SDR methods
  - estimates distance by measuring response delays compared w.r.t. a minuscule delay of 128 microseconds



Hijacking TCAS

- **Two attacks:**
  - TA and RA injections
  - simulating a fake ground station to send messages that disable the RA functionality of the TCAS system
- With commercial off-the-shelf (COTS) components (cost approx. €10,000)

TCAS Vulnerability Disclosure

- United Nations (UN)
- European Union Aviation Safety Agency (EASA)
- Federal Aviation Administration (FAA)
- 33rd Usenix Security Symposium[2] (August 2024)
- DEF CON 32 conference (August 2024)
- CISA ICS advisory[3]
  - CVE-2024-11166 (disable RAs): upgrading the equipment
  - CVE-2024-9310 (fake aircraft): no mitigation

[2] G. Longo, M. Strohmeier, E. Russo, A. Merlo, V. Lenders. 2024. On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS). In Proceeding of the 33rd Usenix Security Symposium (USENIX 2024)

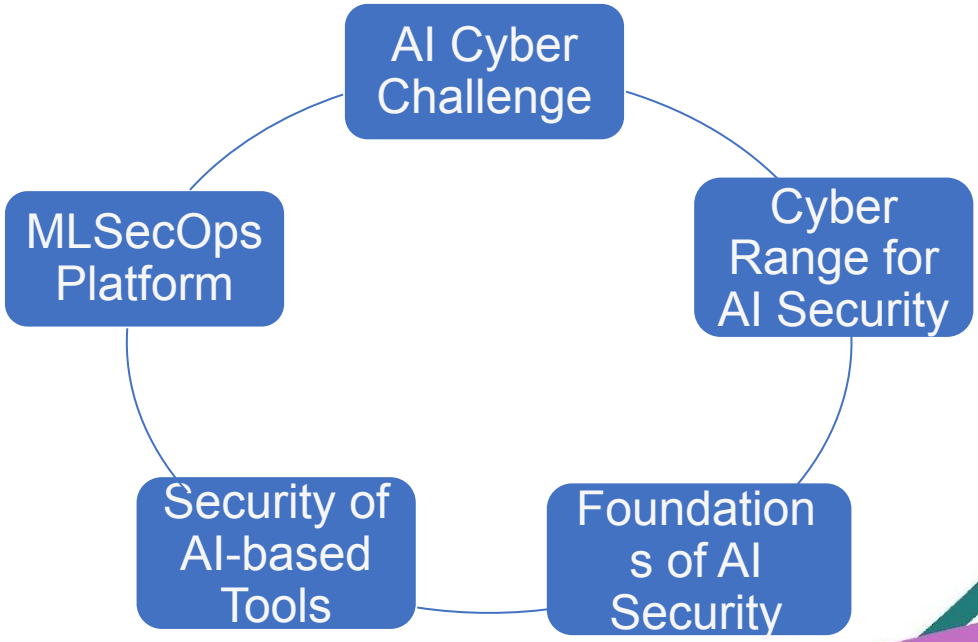
[3] https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-01

Spoke 3 - Attacks and Defences

Project: SOS AI - Science and engineering Of Security of Artificial Intelligence

Partners:

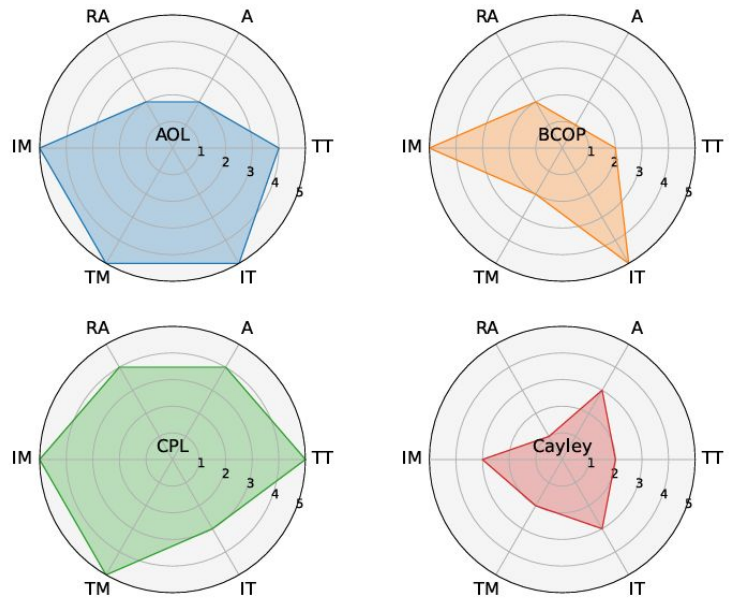
- **Academic partners**: UniCA, UniBA, UniCAL, UniGE, UniSA, UniRoma1, UniVE
- **School for advanced studies:** S. Anna Pisa
- **Research Entity**: CNR
- **Industrial partners**: ENI, Leonardo, Telsy



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

Advancements in Understanding Robust-by-Design Models

- **SSSA** focused on improving **certifiable robustness** by designing 1-Lipschitz neural networks using Lipschitz-bounded dense and convolutional layers.
- **Comprehensive comparison** of these methods, analyzing both **theoretical** aspects (e.g., complexity, memory) and **empirical** metrics (e.g., training time, accuracy, certifiable robustness).
- **Practical guidelines** to help users choose the most suitable approach based on the available resources.

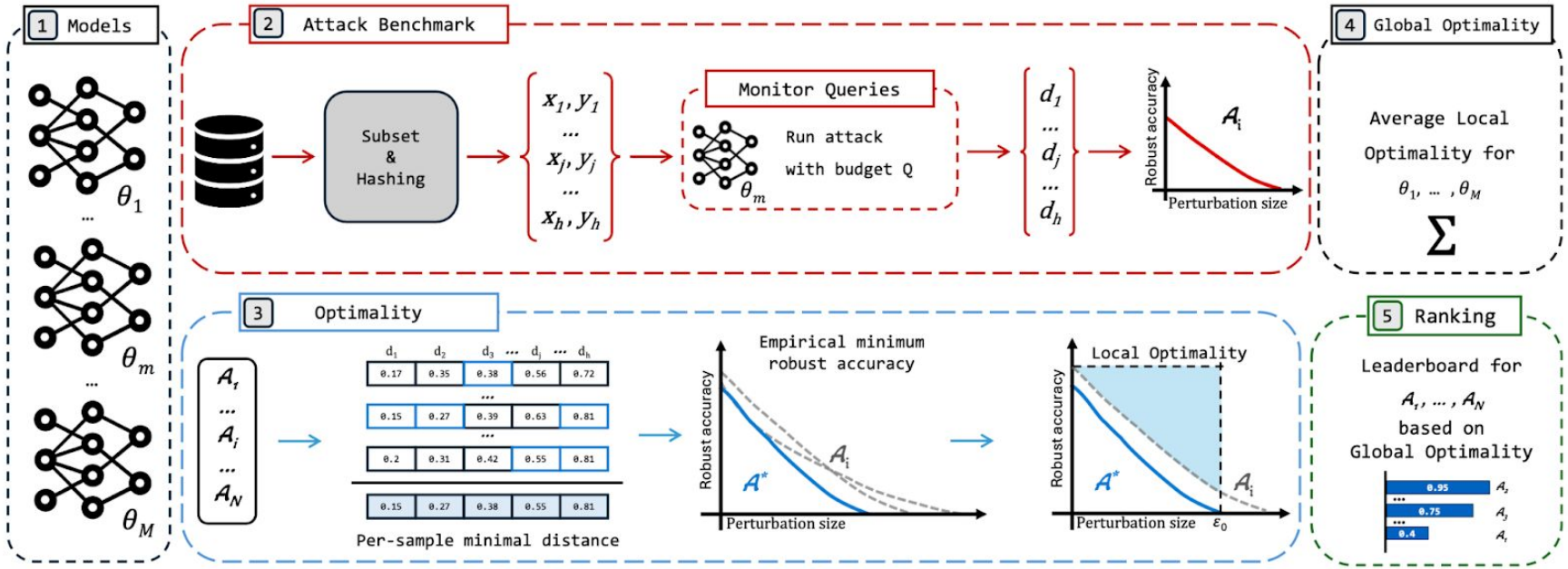


1. B. Prach, et al. "1-Lipschitz Layers Compared: Memory Speed and Certifiable Robustness," Proc. of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2024.

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

AI Security Evaluation with AttackBench

Goal: Identifying the most effective adversarial attacks for *robustness testing* and *proactive defense*.



- A novel optimality **metric** to rank attacks based on **effectiveness** and **efficiency**.
- Benchmarking **102 attacks** under consistent conditions to identify the most reliable threats.
- Revealing **bugs** and **inconsistencies** in **existing implementations**, improving attack reliability.
- *Open-source* framework with a public leaderboard to support ongoing security research.

Novel Methods for Robustness Evaluation

Goal: Develop novel, efficient, and **black-box adversarial attacks** to rigorously test model robustness and expose vulnerabilities overlooked by conventional attack strategies.

Contributions

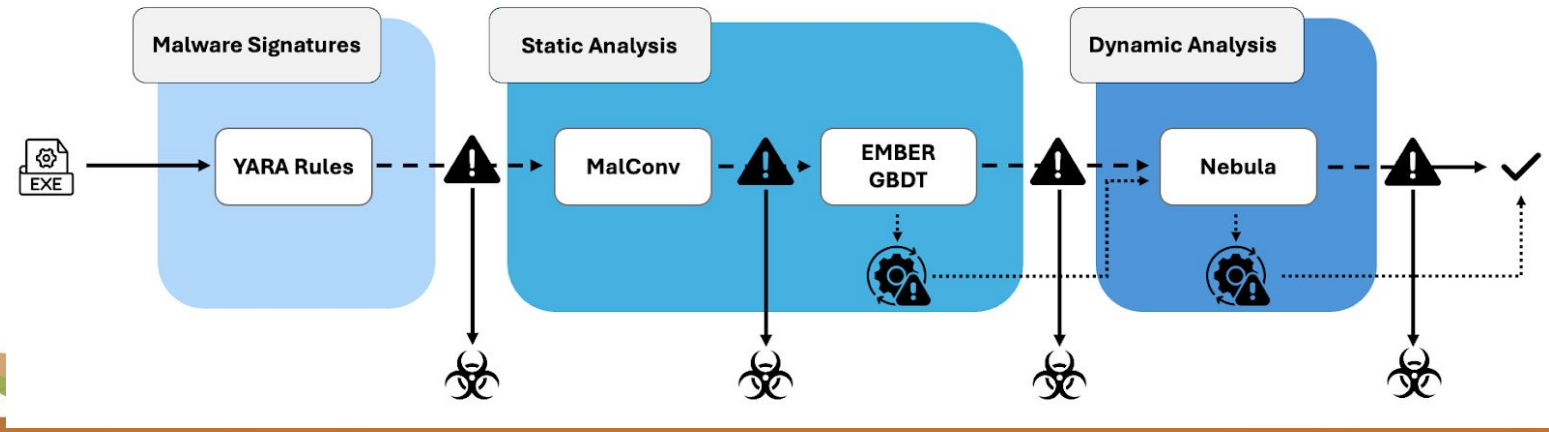
- A black-box attack against **Windows malware detectors** that relies only on model scores.
- Mathematical formulation with **theoretical guarantees**, ensuring reliability.
- **Outperforms state-of-the-art attacks** by requiring less content manipulation to evade detection.
- A **novel gradient-based attack** that efficiently optimizes sparse adversarial perturbations.
- **Outperforms existing sparse attacks** in success rate, perturbation size, and efficiency.
- Requires **no hyperparameter tuning**, enabling faster and more reliable robustness evaluations.

SLIFER: Investigating Performance and Robustness of Malware Detection Pipelines

Goal: reduce the gap with industrial technologies developed to **detect malware**, by analyzing the efficacy and robustness of Windows malware detector pipelines

Contributions:

- **Pre-processing errors** must be dealt with, which is ignored by most academic papers
- **Robustness to adversarial attacks** when an **attacker knows** only partially such a **pipeline**



Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
SERICS

SERICS THEMATIC AREAS SPOKE

SPOKE 1
Aspetti umani, sociali e legali
CNR

SPOKE 2
Disinformazione e fake news
UNISA

SPOKE 3
Attacchi e difese
UNICA

SPOKE 4
Sicurezza dei sistemi operativi e della visualizzazione
UNIGE

SPOKE 5
Crittografia e sicurezza dei sistemi distribuiti
UNICAL

SPOKE 6
Sicurezza del software e delle piattaforme
UNIVE

SPOKE 7
Sicurezza delle infrastrutture
POLITO

SPOKE 8
Gestione del rischio e governance
UNIBO

SPOKE 9
Mettere in sicurezza la trasformazione
UNIROMA

SPOKE 10
Governance e protezione dei dati
UNIMI

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

Alessandro Armando
Presidente Comitato Scientifico

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA