Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Difendere il Futuro: Ricerca, Innovazione e Resilienza

Il contributo del Partenariato Esteso SERICS alla cybersicurezza del Paese: risultati scientifici, nuove visioni e soluzioni alle maggiori sfide.

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

RICERCA SCIENTIFICA, SICUREZZA E RESILIENZA PER IL SISTEMA DIGITALE DEL PAESE

Attraverso la formazione, il Trasferimento Tecnologico
e la diffusione della cultura della cybersicurezza,
la Fondazione SERICS lavora per creare un ecosistema
digitale più innovativo, resiliente e consapevole.

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

INDICE

PREFAZIONE

Questo volume è rivolto a decisori politici, imprese, pubbliche amministrazioni e a tutti coloro che, a vario titolo, sono impegnati nella costruzione di un cyberspazio più sicuro, più giusto e più affidabile. L'invito è a considerare i risultati qui presentati non come un punto di arrivo, ma come l'inizio di un percorso condiviso verso un'Italia e un'Europa digitalmente resilienti, in cui la sicurezza sia un diritto per tutti e un fattore abilitante per lo sviluppo sostenibile e inclusivo della nostra società.

Ringrazio i redattori, i contributori e tutti coloro che hanno reso possibile questo progetto: che la lettura di queste pagine ispiri nuovi percorsi e collaborazioni, e offra utili elementi di orientamento per chiunque voglia partecipare al futuro della ricerca, della sicurezza e della libertà digitale in Italia.

Nel febbraio 2022, con il Piano Nazionale di Ripresa e Resilienza, l'Italia ha compiuto una scelta strategica di grande portata: investire nella costruzione di un ecosistema nazionale di eccellenza per la ricerca e l'innovazione in cybersicurezza. Nasceva così il Partenariato Esteso PE 14 - SERICS (Security and Rights in the CyberSpace), un'iniziativa senza precedenti che ha riunito le migliori competenze accademiche, scientifiche e industriali del Paese attorno a una missione comune: rafforzare la capacità dell'Italia di affrontare le sfide della sicurezza digitale in un mondo sempre più interconnesso e vulnerabile.

I Partenariati Estesi, promossi dal Ministero dell'Università e della Ricerca (MUR) con l'avviso D.D. n. 341 del 15 marzo 2022, rappresentano uno degli strumenti più innovativi del PNRR per la ricerca: aggregazioni ampie e multidisciplinari, capaci di mobilitare competenze complementari su tematiche di rilevanza strategica nazionale. Nel quadro complessivo sono stati selezionati 14 temi prioritari che coprono aree cruciali per lo sviluppo sostenibile, la competitività e la resilienza del Paese: dall'intelligenza artificiale alle energie, dalla salute alle telecomunicazioni, fino alla cybersecurity.

SERICS si distingue in questo panorama per l'ampiezza della visione e per la capacità di integrare dimensioni tecnologiche, giuridiche, sociali ed economiche della cybersicurezza, superando la tradizionale frammentazione disciplinare. Il progetto non si configura come un semplice programma di ricerca, ma come un autentico ecosistema nazionale: oltre un centinaio di partner tra università, enti di ricerca e imprese, coordinati dalla Fondazione SERICS, hanno lavorato per quasi tre anni attraverso una struttura di governance hub & spoke, in cui l'hub coordina le attività complessive e dieci spoke tematici declinano le sfide più urgenti e complesse della sicurezza cibernetica.

Dagli aspetti umani, sociali e legali alla lotta contro la disinformazione; dalle tecniche avanzate di attacco e difesa alla sicurezza dei sistemi operativi e della virtualizzazione; dalla crittografia post-quantistica alla protezione delle infrastrutture critiche; dalla gestione del rischio alla governance dei dati nell'era dell'intelligenza artificiale: SERICS ha costruito ponti tra ricerca fondamentale e applicazione concreta, promuovendo un modello in cui la salvaguardia delle infrastrutture e dei dati procede di pari passo con la tutela delle libertà individuali e collettive.

I numeri testimoniano l'impatto di questa iniziativa: oltre 1500 pubblicazioni scientifiche in riviste e conferenze internazionali, decine di prototipi e piattaforme tecnologiche sviluppate, nuove vulnerabilità scoperte con risonanza globale, brevetti depositati, spin-off avviati, collaborazioni strutturate con le principali autorità nazionali. Ma ciò che rende SERICS davvero distintivo non è solo la quantità dei risultati, bensì la loro qualità e, soprattutto, la capacità di

A cura di

VINCENZO LOIA

Presidente Fondazione

tradurre la ricerca in impatto concreto per il sistema-Paese. La presente raccolta di contributi documenta questo percorso straordinario con un obiettivo duplice. Da una parte, far emergere con chiarezza e rigore i risultati scientifici, tecnologici e operativi raggiunti nei vari ambiti di intervento. Dall'altra, offrire una visione integrata delle sfide future, indicando traiettorie di ricerca e applicazione che possano guidare le politiche nazionali e le strategie delle istituzioni, delle imprese e del mondo accademico.

Il valore aggiunto di SERICS risiede proprio in questo approccio olistico. La cybersicurezza è considerata non più una questione puramente tecnica, ma un bene comune che coinvolge diritti fondamentali, sostenibilità economica, resilienza sociale e competitività nazionale. Ogni progetto, ogni risultato presentato in questo volume, è stato concepito come un tassello di un ecosistema più ampio, destinato a generare valore duraturo per cittadini, imprese, pubbliche amministrazioni e istituzioni. Guardando al futuro, la sfida sarà consolidare e far crescere questo ecosistema, trasformandolo in un asset strategico permanente per il Paese. Le minacce non si fermano: dall'avvento del calcolo quantistico all'intelligenza artificiale generativa, dalla protezione di infrastrutture sempre più interconnesse alla gestione della sovranità digitale in un contesto geopolitico complesso. Ma la solida base di competenze, collaborazioni e risultati costruita attraverso SERICS rappresenta il miglior punto di partenza per affrontare con successo le sfide di domani.

Questo volume è rivolto a decisori politici, imprese, pubbliche amministrazioni e a tutti coloro che, a vario titolo, sono impegnati nella costruzione di un cyberspazio più sicuro, più giusto e più affidabile. L'invito è a considerare i risultati qui presentati non come un punto di arrivo, ma come l'inizio di un percorso condiviso verso un'Italia e un'Europa digitalmente resilienti, in cui la sicurezza sia un diritto per tutti e un fattore abilitante per lo sviluppo sostenibile e inclusivo della nostra società.

Ringrazio i redattori, i contributori e tutti coloro che hanno reso possibile questo progetto: che la lettura di queste pagine ispiri nuovi percorsi e collaborazioni, e offra utili elementi di orientamento per chiunque voglia partecipare al futuro della ricerca, della sicurezza e della libertà digitale in Italia

INTRODUZIONE

A cura di

ALESSANDRO ARMANDO

Presidente Comitato Scientifico

ROCCO DE NICOLA

Vicepresidente Fondazione

La sicurezza digitale come sfida strategica nazionale

Attacchi informatici sempre più sofisticati, campagne di disinformazione su larga scala, minacce ibride che combinano dimensioni fisiche e digitali, crisi della fiducia nelle infrastrutture critiche e nei sistemi di comunicazione: questi sono soltanto alcuni degli scenari che mettono alla prova la resilienza del nostro Paese e dell'Europa intera. La cybersicurezza è ormai diventata un elemento fondamentale per garantire la protezione dei diritti fondamentali dei cittadini, la continuità dei servizi essenziali e la competitività del sistema-paese nel panorama globale.

Nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), il Ministero dell'Università e della Ricerca ha indetto un bando per la selezione di quattordici Partenariati Estesi come nuovi strumenti di politica della ricerca, concepiti per superare la frammentazione degli interventi, favorire la collaborazione strutturata tra università, enti di ricerca e industria e concentrare risorse su grandi sfide di rilevanza strategica per il Paese. La cybersicurezza è stata individuata come uno di questi ambiti prioritari, per il suo impatto diretto sulla sovranità digitale, sulla sicurezza nazionale e sulla tutela dei diritti fondamentali.

In questo contesto, nasceva la proposta di costituzione del partenariato esteso SERICS, coordinata dall'Università di Salerno, su impulso del Cybersecurity National Lab del Consorzio Interuniversitario Nazionale per l'Informatica (CINI). Facendo leva su un patrimonio consolidato di competenze scientifiche e su una lunga esperienza di coordinamento tra università ed enti di ricerca, il Laboratorio ha favorito la convergenza verso una proposta unitaria in linea con le priorità strategiche del PNRR. La proposta, articolata in dieci spoke tematici, affrontava in maniera coordinata e sistemica le principali sfide della sicurezza cibernetica, dall'hardware al software, dalla protezione delle infrastrutture critiche alla tutela dei diritti digitali, dall'intelligenza artificiale alle dinamiche sociali legate alla disinformazione. A valle del processo di selezione dei quattordici Partenariati Estesi, che ha visto la proposta SERICS tra quelle ammesse al finanziamento, è stata istituita la Fondazione SERICS, con sede presso l'Università di Salerno.

Un ecosistema di eccellenze per la sicurezza del cyberspazio

L'approccio multidisciplinare e integrato è uno degli elementi distintivi di SERICS: non rispondere alle minacce con soluzioni tecniche isolate, ma costruire una visione olistica della cybersicurezza come bene comune, capace di coniugare dimensioni tecnologiche, giuridiche, economiche e sociali.

Un elemento chiave di questo percorso di apertura e trasferimento è rappresentato dalle Open Call, uno strumento previsto sin dalla progettazione del Partenariato per ampliare l'impatto di SERICS oltre il perimetro dei partner fondatori e favorire l'integrazione nel progetto dell'intero ecosistema nazionale della ricerca in cybersicurezza. Le Open Call hanno consentito di finanziare progetti di

ricerca e innovazione proposti da soggetti esterni al Partenariato – università, enti di ricerca, startup, PMI e altri attori dell'ecosistema – selezionati attraverso procedure competitive basate su criteri di eccellenza scientifica, rilevanza industriale e coerenza con gli obiettivi strategici di SERICS.

SERICS ha visto la partecipazione di oltre un centinaio di soggetti tra università, enti pubblici di ricerca e partner industriali, mobilitando competenze diverse e complementari su tutto il territorio nazionale. I numeri testimoniano l'ampiezza dell'iniziativa: decine di progetti di ricerca avviati, centinaia di ricercatori coinvolti, migliaia di ore di formazione specialistica erogate, nuove piattaforme tecnologiche sviluppate e già sperimentate sul campo. Questa massa critica ha permesso di affrontare in maniera sistemica le vulnerabilità del cyberspazio e di individuare soluzioni trasferibili verso imprese, pubbliche amministrazioni e cittadini. Gli spoke del progetto riflettono questa visione ampia e articolata.

Lo Spoke 1 ha esplorato gli aspetti umani, sociali e legali della cybersicurezza, riconoscendo che uno spazio digitale sicuro è innanzitutto quello in cui sono garantiti i diritti di ciascuno e in cui i comportamenti umani sono adeguatamente considerati nella progettazione dei sistemi di protezione. Sono stati sviluppati framework regolatori, modelli di governance e strumenti formativi per supportare imprese e pubblica amministrazione nella compliance e nella protezione dei diritti fondamentali.

Lo Spoke 2 ha affrontato le sfide poste dalla disinformazione e dalle fake news, fenomeni che erodono la fiducia collettiva e minacciano la resilienza informativa della società. Con un arsenale tecnologico avanzato che include piattaforme di monitoraggio basate su AI, strumenti per il rilevamento di deepfake e modelli per l'analisi della credibilità delle fonti, questo spoke ha prodotto un innovativo SIEM per la Sicurezza Cognitiva, che estende i principi della cybersecurity alla protezione dell'ecosistema informativo.

Lo Spoke 3 ha concentrato l'attenzione sugli attacchi e le difese, sviluppando tecniche avanzate per rilevare e contrastare minacce sempre più sofisticate. La ricerca ha prodotto strumenti basati su deep learning e large language models per la rilevazione di vulnerabilità nel software, l'analisi di malware e la protezione dei sistemi di IA stessi da possibili manipolazioni. Particolarmente significativo è lo sviluppo della libreria open-source SecML-Torch, divenuta un riferimento per la comunità scientifica internazionale nella valutazione della sicurezza degli algoritmi di machine learning.

Lo Spoke 4 si è dedicato alla sicurezza dei sistemi operativi e della virtualizzazione, elementi fondamentali per la protezione delle architetture cloud-native e delle reti 5G, sviluppando cyber range elastici e digital twin di complesse infrastrutture cyber-fisiche che hanno permesso scoperte di grande impatto, come le vulnerabilità nel sistema anticollisione aereo TCAS, riconosciute a livello internazionale.

Lo Spoke 5 ha affrontato la crittografia e la sicurezza dei sistemi distribuiti, con particolare attenzione all'identità digitale, producendo soluzioni innovative per la protezione dalle truffe telefoniche e schemi di crittografia post-quantistica..

Lo Spoke 6 ha affrontato il divario tra modelli teorici e implementazioni reali nella sicurezza del software, sviluppando strumenti per la verifica formale di sistemi embedded e per il rilevamento di phishing basato su LLM.

Lo Spoke 7 si è concentrato sulla protezione delle infrastrutture critiche, scoprendo nuove vulnerabilità micro-architetturali della famiglia Spectre con impatto su milioni di dispositivi e sviluppando soluzioni per la sicurezza di sistemi cyber-fisici nei settori energetico, dei trasporti e della sanità.

Lo Spoke 8 ha esplorato la dimensione della governance e ha sviluppato metodologie innovative per la gestione del rischio cyber, modelli di contagio finanziario in caso di attacchi sistemici e piattaforme per la risposta automatica agli incidenti.

Lo Spoke 9 si è concentrato sullo sviluppo di soluzioni tecnologiche e metodologiche per garantire sicurezza, fiducia e resilienza nei processi di digitalizzazione inclusi i settori strategici come finanza, pubblica amministrazione, sanità e comunicazioni quantistiche.

Lo Spoke 10 ha affrontato le sfide legate alla gestione sicura e responsabile delle informazioni in un contesto di crescente digitalizzazione e diffusione di tecnologie come cloud e intelligenza artificiale con l'obiettivo di garantire privacy, controllo e conformità normativa lungo tutto il ciclo di vita dei dati, bilanciando sicurezza e funzionalità.

Dalla ricerca all'impatto: risultati concreti per il sistema-paese

Il valore di SERICS si misura non soltanto dai contributi scientifici prodotti ma soprattutto dalla capacità di trasformare le scoperte scientifiche in tecniche e strumenti per migliorare la resilienza del sistema-paese. SERICS ha interpretato la ricerca come strumento di impatto: generare conoscenza con l'obiettivo di trasformarla in competenze, strumenti, linee guida, iniziative imprenditoriali e policy.

Tra i risultati più significativi che testimoniano questa capacità di generare ricadute concrete si possono citare: la nascita del Centro Interuniversitario di Ricerca CybeRights, struttura permanente che garantirà continuità alle attività di ricerca sugli aspetti legali e sociali della cybersicurezza, trasformando un progetto a tempo determinato in un asset strategico per il sistema-paese; lo sviluppo di piattaforme avanzate per il monitoraggio della disinformazione online, alcune delle quali hanno già dato origine a iniziative imprenditoriali come lo spin-off basato sulla piattaforma IDA.

La scoperta di nuove vulnerabilità microarchitetturali nei processori moderni – tre nuovi vettori di attacco della famiglia Spectre – ha avuto un impatto globale, interessando decine di milioni di dispositivi e portando al rilascio di security bulletin ufficiali da parte di ARM e all'assegnazione di CVE. Nel settore delle infrastrutture critiche, la scoperta di vulnerabilità nel sistema TCAS per

la prevenzione delle collisioni aeree, realizzata utilizzando il cyber range ARTIC, è stata riconosciuta e divulgata ufficialmente dalla Cybersecurity and Infrastructure Security Agency (CISA) statunitense.

Sul fronte dell'identità digitale e della protezione dai crimini informatici, CallTrust rappresenta una soluzione innovativa per contrastare le truffe telefoniche basate su vishing e spoofing, integrabile in un modello federato conforme a eIDAS 2.0. Nel campo della crittografia, lo schema di firma digitale CROSS e altri contributi alla crittografia post-quantistica alimentano il dibattito internazionale sulla standardizzazione di algoritmi resistenti al calcolo quantistico.

Altri contributi includono strumenti avanzati per la protezione dei microservizi e l'implementazione di pratiche DevSecOps, metodologie per la sicurezza delle reti 5G e delle architetture O-RAN, framework per la gestione sicura dei dati in ambienti cloud distribuiti, e soluzioni per la protezione delle smart grid e dei sistemi di controllo industriale.

In ambito formativo e di sensibilizzazione, sono stati realizzati programmi innovativi come il CyberTour, un ciclo di nove incontri itineranti che ha diffuso la cultura della cybersicurezza in diverse città italiane, con un'attenzione particolare alle esigenze delle pubbliche amministrazioni e delle piccole e medie imprese. A supporto della diffusione della cultura digitale, l'Osservatorio CybeRights rende inoltre disponibili risorse formative in open access tra cui il Breviario giuridico della cybersicurezza.

La SERICS Cybersecurity Academy ha operato come strumento trasversale di valorizzazione delle competenze sviluppate dagli Spoke, con l'obiettivo di trasferire conoscenza specialistica verso professionisti, pubbliche amministrazioni e imprese. Coordinata dall'Hub e sviluppata in stretto raccordo con gli Spoke, che contribuiscono ai contenuti e alla docenza, l'Academy garantisce coerenza scientifica e aggiornamento continuo, in linea con la governance complessiva del Partenariato.

In parallelo, SERICS ha affiancato alla ricerca un servizio strutturato di trasferimento tecnologico per favorire il dialogo con le imprese e accompagnare l'evoluzione delle innovazioni verso il mercato, creando un continuum tra formazione, ricerca e innovazione orientata all'impatto. Attraverso percorsi multidisciplinari di supporto a team di ricerca, startup e spin-off – che integrano competenze in proprietà intellettuale, mentoring, analisi di mercato e advisory di business – il Partenariato ha promosso la valorizzazione dei risultati scientifici e la diffusione di una cultura imprenditoriale nella comunità della cybersicurezza.

Le collaborazioni strutturate o in via di strutturazione con le principali autorità nazionali in materia di cybersicurezza – ACN, AGID, Garante Privacy, AGCOM – garantiscono un costante dialogo tra il mondo della ricerca e le esigenze concrete del sistema-paese, facilitando la traduzione dei risultati scientifici in policy e strumenti operativi. Il coinvolgimento di partner industriali nella validazione delle soluzioni sviluppate rafforza ulteriormente il legame tra ricerca e applicazione.

Verso un futuro digitale resiliente e inclusivo

La forza di SERICS risiede nella capacità di agire come un moltiplicatore di valore, catalizzando competenze, generando sinergie e trasferendo conoscenza al sistema paese. Dalla creazione di spin-off e laboratori congiunti, al deposito di brevetti e domande di brevetto, fino all'istituzione di centri di ricerca permanenti, l'eredità di SERICS è destinata a perpetuarsi ben oltre la durata del progetto iniziale.

Guardando al futuro, la sfida consisterà nel consolidare questo ecosistema collaborativo e renderlo sempre più un asset strategico per il Paese, capace di coniugare sicurezza, innovazione e diritti in un mondo digitale in continua trasformazione. Le sfide non mancano: dall'avvento del calcolo quantistico alle nuove frontiere dell'intelligenza artificiale generativa, dalla protezione delle infrastrutture critiche sempre più interconnesse alla gestione della sovranità digitale in un contesto geopolitico complesso. La solida base di competenze e collaborazioni costruita attraverso SERICS rappresenta il miglior viatico per affrontarle con successo.

Questo booklet offre una sintesi dei principali risultati conseguiti, organizzati per spoke tematico. Ogni sezione presenta lo scenario di riferimento, le sfide affrontate, i risultati principali e un approfondimento su un risultato particolarmente significativo per esemplificare l'impatto concreto delle attività di ricerca. L'obiettivo è fornire a decisori politici, imprese, pubbliche amministrazioni e stakeholder una visione d'insieme delle potenzialità offerte dai risultati di SERICS, facilitando il dialogo e la collaborazione per tradurre la ricerca in innovazione e sicurezza per la società italiana ed europea.

Con questo spirito, la Fondazione SERICS invita tutti gli attori interessati – imprese innovative, pubbliche amministrazioni impegnate nella transizione digitale, investitori sensibili alla cybersecurity, partner internazionali – a unirsi in questo percorso collettivo verso un cyberspazio più sicuro, più giusto e più affidabile, in cui la tecnologia sia al servizio delle persone e la sicurezza digitale diventi un diritto per tutti e un fattore abilitante per lo sviluppo economico e sociale del nostro Paese.

LA FONDAZIONE

La Fondazione SERICS – Security and Rights in CyberSpace è un ente pubblico di ricerca nato come soggetto attuatore del Partenariato Esteso “Cybersecurity, nuove tecnologie e tutela dei diritti” nell’ambito del PNRR, con l’obiettivo di promuovere la ricerca scientifica e tecnologica sulla sicurezza informatica e i diritti digitali, sviluppare strategie innovative per affrontare le sfide del cyberspazio e rafforzare la resilienza del sistema-Paese.

La Fondazione si propone come piattaforma nazionale di riferimento per la cybersecurity, consolidandosi come struttura di ricerca e innovazione capace di integrare attività scientifiche, industriali e formative.

In questa direzione, offre percorsi di alta specializzazione attraverso la SERICS Cybersecurity Academy, realizza programmi di TrasferimentoTecnologico, sostiene l’imprenditorialità e promuove iniziative volte a diffondere conoscenza e consapevolezza sui temi della cybersicurezza.

Grazie a un partenariato accademico-industriale articolato in 10 Spoke tematici, SERICS adotta un approccio interdisciplinare che integra competenze tecniche, giuridiche e sociali per sviluppare soluzioni sostenibili e applicabili sia in ambito istituzionale che produttivo. Parallelamente, è impegnata in un’intensa attività di comunicazione e divulgazione, volta a favorire il dialogo tra esperti, istituzioni, imprese e cittadini e a costruire una massa critica di sensibilizzazione e competenza nel Paese.

KEY DATA:

23
SOCI TRA ENTI PUBBLICI E PRIVATI

54
PROGETTI FINANZIATI PER I BANDI A CASCATA

113
FINANZIAMENTO (MLN €)

27
PROGETTI DI RICERCA

43,8%
FINANZIAMENTI PER LE REGIONI DEL SUD ITALIA

684
RICERCATORI COINVOLTI

26%
FINANZIAMENTI PER BANDI DI RICERCA PER ENTI PUBBLICI

350
RICERCATORI STRUTTURATI

8%
FINANZIAMENTI PER BANDI DI INNOVAZIONE

134
NUOVI RICERCATORI

30%
RICERCATRICI

IL CONSIGLIO DI AMMINISTRAZIONE

La Governance della Fondazione assicura una direzione strategica solida e una gestione operativa trasparente ed efficiente.

Vincenzo Loia - Presidente
Nominato dall'Università degli Studi di Salerno

Marco Conti
Nominato dall'Assemblea generale
su designazione del CNR

Rocco De Nicola - Vicepresidente
Nominato dall'Assemblea generale su
designazione degli Enti pubblici di ricerca e delle
Scuole a Ordinamento Speciale che rivestono
la qualifica di membri fondatori

Giorgio Giacinto
Nominato dall'Assemblea generale su
designazione degli Enti pubblici di ricerca e
delle Scuole a Ordinamento Speciale
che rivestono la qualifica di membri fondatori

Alessandro Massa
Nominato dall'Assemblea generale su
designazione delle persone giuridiche di diritto
privato che rivestono la qualifica di membri
Fondatori

Angelo Ientile
Componente su designazione del M.U.R.

IL COMITATO SCIENTIFICO

Il Comitato Scientifico è composto da esperti del mondo accademico e della ricerca pubblica, con competenze di alto livello nei campi della cybersicurezza, dei diritti digitali e dell'innovazione tecnologica.

Per le Università statali e non statali

Alessandro Armando - Presidente Comitato Scientifico
per l'Università degli Studi di Genova

Francesco Buccafurri
per l'Università della Calabria

Danilo Caivano
per l'Università degli studi di Bari "Aldo Moro"

Michele Colajanni
per l'Università degli studi di Bologna "Alma Mater Studiorum"

Stefano Di Carlo
per il Politecnico di Torino

Giuseppe Fenza
per l'Università degli studi di Salerno

Riccardo Focardi
per l'Università degli studi di Venezia "Cà Foscari"

Davide Maiorca
per l'Università degli studi di Cagliari

Leonardo Querzoni
per l'Università degli studi di Roma "La Sapienza"

Pierangela Samarati
per l'Università degli studi di Milano

Andrea Simoncini
per l'Università degli studi di Firenze

Per gli enti pubblici di ricerca e degli atenei e delle scuole a ordinamento speciale

Giuseppe Bianchi
per il Consorzio Nazionale interuniversitario per le Telecomunicazioni CNIT

Alessandro Biondi
per Sant'Anna Scuola Universitaria Superiore Pisa

Gabriele Costa
per la Scuola IMT Alti Studi Lucca

Elena Ferrari
per il Consorzio Nazionale interuniversitario per l'Informatica (CINI)

Fabio Martinelli
per il Consiglio Nazionale delle Ricerche (CNR)

Silvio Ranise
per la Fondazione Bruno Kessler

Marina Settembre
per la Fondazione Ugo Bordoni

I SOCI

La Fondazione, costituita grazie all'impegno dei suoi soci fondatori, collabora con numerosi enti e istituzioni accademiche e industriali, formando un partenariato esteso tra pubblico e privato, capace di affrontare le sfide della sicurezza informatica.

Università e Istituti speciali

Università degli Studi di Salerno
Politecnico di Torino
Università degli Studi di Bari Aldo Moro
Alma Mater Studiorum Università di Bologna
UNICA Università degli Studi di Cagliari
Università della Calabria
Università degli Studi Firenze
Università di Genova
Università degli Studi di Milano
Sapienza Università di Roma
Università Ca'Foscari Venezia
IMT Scuola Alti Studi Lucca
Sant'Anna Scuola Universitaria Superiore Pisa

Enti di Ricerca

cini consorzio interuniversitario nazionale per l'informatica
cnit consorzio nazionale interuniversitario per le telecomunicazioni
Consiglio Nazionale delle Ricerche
Fondazione Bruno Kessler
FUB Fondazione Ugo Bordoni Ricerca e Innovazione

Aziende

eni
Fincantieri
Intesa Sanpaolo
Leonardo
Telsy A TIM Enterprise Brand

LE STRUTTURE AUSILIARIE

Advisory Board

Prof. Rocco De Nicola - Presidente
con delega del Presidente del Consiglio di Amministrazione

Dott. Gianluca Ignagni
Capo di Gabinetto ACN – Agenzia per la Cybersicurezza Nazionale

Gen. Isp. Capo Giuseppe Lupoli
Direzione ARMAEREO – Segretariato Generale della Difesa/DNA

Gen. C.A. Stefano Mannino
Presidente CASD – Centro Alti Studi Difesa / Scuola Superiore Universitaria

Dott. Agostino Santoni
Vice presidente CISCO South Europe

Dott. Filippo Trifiletti
Direttore Generale ACCREDIA – L'Ente Italiano di Accreditamento

Innovation Board

Ing. Daniele Alì
Responsabile Cyber Centre of Excellence, FINCANTIERI

Dott. Roberto Barbieri
Responsabile Global Cyber Defence & Operations, ENI

Prof.ssa Paola Girdinio
Centro di competenza START 4.0

Dott. Luca Iuliano
Direttore Engineering, TELSY

Prof. Leonardo Querzoni - Presidente
Centro di competenza CYBER 4.0

Dott. Fabio Ugoste
Information Security Officer, Gruppo INTESA SANPAOLO

Ing. Gianluca Vannuccini
Direttore Sistemi Informativi, Regione Toscana

10 SPOKE

10 Spoke, ciascuno dedicato al coordinamento di aree tematiche specifiche, che promuovono la ricerca e l'innovazione nei diversi settori della cybersecurity.

SPOKE 1 — **Aspetti umani, sociali e legali**

SPOKE 2 — **Disinformazione e Fake News**

SPOKE 3 — **Attacchi e difese**

SPOKE 4 — **Sicurezza dei Sistemi Operativi e della Virtualizzazione**

SPOKE 5 — **Crittografia e sicurezza dei sistemi distribuiti**

SPOKE 6

Sicurezza del software e delle piattaforme

SPOKE 7

Sicurezza delle infrastrutture

SPOKE 8

Gestione del rischio e governance

SPOKE 9

Mettere in sicurezza la trasformazione digitale

SPOKE 10

Governance e protezione dei dati

Spoke

Aspetti umani, sociali e legali

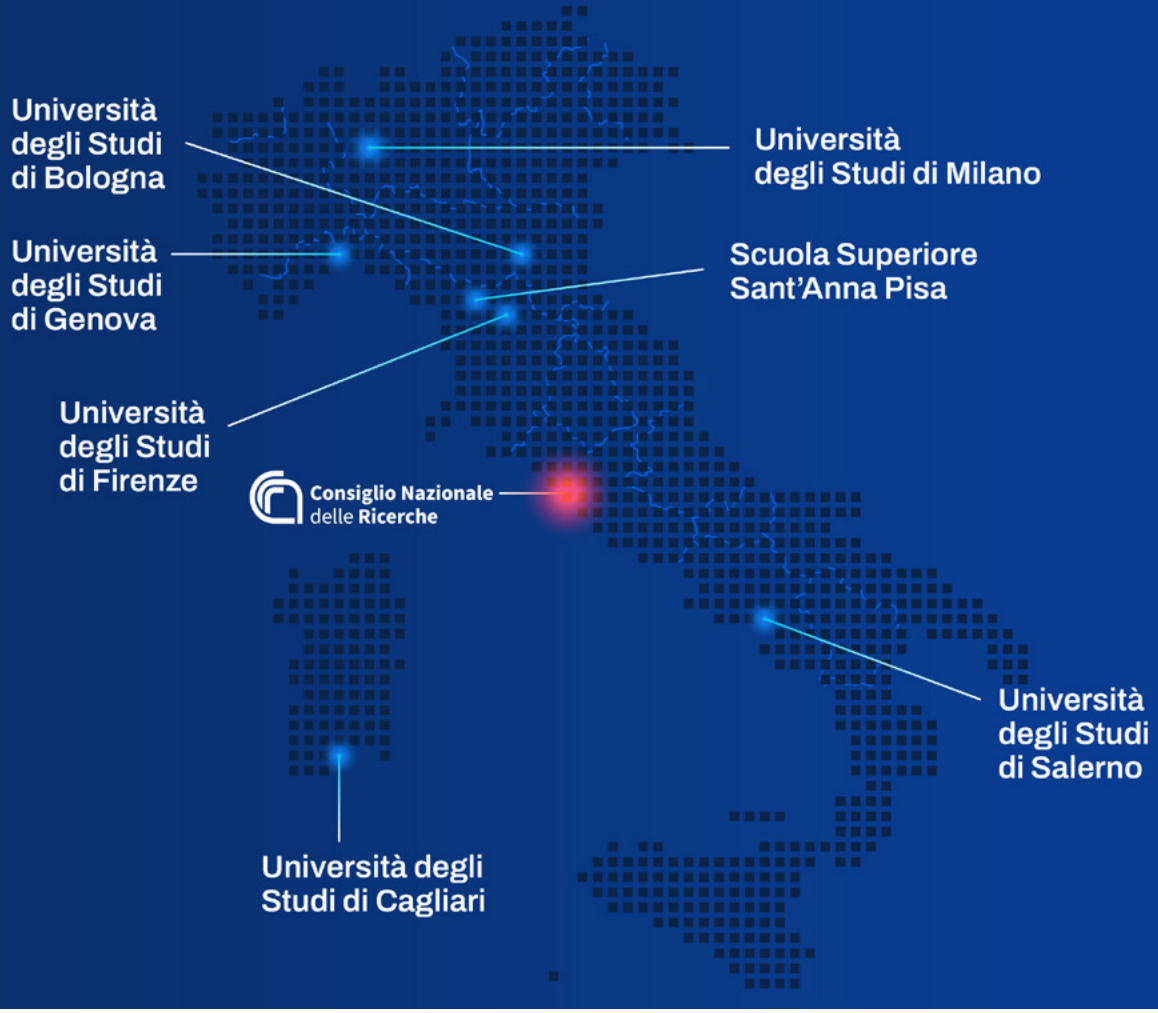
1

Coordinatore

Fabio Martinelli
Consiglio Nazionale delle Ricerche

Consiglio Nazionale delle Ricerche

Nel quadro generale dei cambiamenti che stanno interessando la nostra società e in particolare l'ambito della sicurezza e la risposta agli attacchi informatici, diviene imprescindibile affrontare la sfida della costruzione di un cyberspazio affidabile, unendo sistemi tecnologici robusti a comportamenti umani appropriati, convinti che uno spazio digitale sicuro è, innanzitutto, quello in cui sono garantiti i diritti fondamentali di ciascuno. Partendo dalla constatazione che le tradizionali misure di sicurezza e fiducia non sono più sufficienti in un contesto in cui mondo fisico e digitale si compenetrano, risulta particolarmente importante la prospettiva di una trattazione da parte di esperti con prospettive diverse (giuridiche, sociologiche, pedagogiche e tecnologiche) per definire un approccio olistico e interdisciplinare. Con l'obiettivo di contribuire all'implementazione e alla valutazione di nuove politiche di cybersicurezza che superino le misure già sperimentate, la ricerca ha voluto rafforzare la capacità di prevedere e affrontare i rischi di una società della sorveglianza, espandendo le frontiere legali in armonia con l'innovazione tecnologica. I progetti hanno integrato le competenze legali e tecnologiche, ottenendo risultati a favore del progresso scientifico e della capacità di quest'ultimo di indurre cambiamenti positivi nella società. Lo schema di lavoro adottato identifica e gestisce i problemi legali, sociali, etici e tecnici della cybersicurezza in modo interconnesso, riconoscendo che la protezione dei diritti in una società digitalizzata richiede una comprensione completa delle vulnerabilità umane, dei quadri normativi e delle capacità tecnologiche.



Progetti

CYBERIGHTS: Law and regulation for a better-safe Cyberspace

PI: ANDREA SIMONCINI, UNIVERSITÀ DEGLI STUDI DI FIRENZE

DiSe: Digital Sovereignty

PI: FABIO MARTINELLI, CONSIGLIO NAZIONALE DELLE RICERCHE

Spoke 1

SFIDE

Il Progetto CybeRights. *Law, regulation and policy for a better-safe cyberspace* ha affrontato una serie di sfide complesse per costruire un cyberspazio più sicuro e giusto. Le attività si sono concentrate su quattro ambiti principali, che rappresentano settori cruciali del nostro tempo. La prima riguarda la definizione di diritti, regole e tassonomie per nuove forme di co-regolamentazione, capaci di raccogliere anche le esigenze della semplificazione normativa e, dunque, essenziali per la governance di un ecosistema digitale in rapida evoluzione, sia nel contesto nazionale che in quello sovranazionale e internazionale. La seconda concerne l'analisi delle questioni legali ed etiche legate alla protezione dei diritti fondamentali in un contesto tecnologico in continua espansione, con particolare attenzione alle dinamiche dell'intelligenza artificiale (IA), della disinformazione e alle evoluzioni dei diritti digitali e politici. La terza sfida è stata lo sviluppo di modelli di apprendimento e formazione continua sulle questioni legali della cybersicurezza, per colmare il divario di competenze tra professionisti del diritto e della tecnologia, sia in ambito pubblico che privato, con particolare riguardo a due settori chiave come quello della pubblica amministrazione e delle piccole e medie imprese. La quarta sfida ha esplorato gli aspetti penalistici e geopolitici, considerati quali elementi cruciali per una nuova strategia nazionale di prevenzione e repressione dei crimini informatici. Il progetto Digital Sovereignty (DiSe) ha investigato un ulteriore ambito quale la sovranità digitale, analizzando le implicazioni legali e di sicurezza di tecnologie emergenti digitali, ed è stato supportato tramite Open Call dal progetto *Enforcement and Monitoring of Data Sovereignty policies* (EMDAS) della università Federico II di Napoli.

In particolare, una prima sfida affrontata è stata la possibilità di analizzare le normative sulla sovranità digitale per definire direttamente i requisiti di cybersecurity per sistemi tecnologici. Sono state sviluppate tecniche per l'interpretazione e la traduzione semi-automatica delle policy e sono stati studiati gli aspetti socio-economici legati alla condivisione dei dati. Altra sfida consiste nello sviluppare soluzioni per la sovranità digitale in particolare per la protezione dei dati. Questo include la creazione di modelli per la gestione della fiducia, dell'identità e del controllo sull'uso dei dati, la raccolta di dati affidabili per l'IA sicura nella gestione delle minacce informatiche (quali il malware come ransomware). Una ulteriore sfida è stata l'identificazione di metodologie per lo sviluppo di sistemi sicuri e in grado di valutare dinamicamente il livello di rischio. Si mira a garantire la confidenzialità dei calcoli in ambienti distribuiti, a creare tecnologie sicure e usabili, e a validare le soluzioni in laboratorio, in particolare nei settori dell'energia e dei trasporti.

PRINCIPALI RISULTATI

Il Progetto CybeRights è stato guidato dall'Università di Firenze in collaborazione con altre cinque Università (in particolare, in qualità di WP Leader, l'Università degli Studi di Milano "Statale" e la Scuola Superiore Sant'Anna di Pisa) e con il CNR (Istituto di Informatica Giuridica e Sistemi Giudiziari, IGSG). Attraverso l'Open Call hanno contribuito alla definizione degli obiettivi e alla realizzazione dei risultati altre nove Università riunite nel progetto HARD-DISC. *Human Centered approach and regulatory dimension in developing an interoperable and secure cyberspace*, guidato dall'Università di Roma Tre.

I risultati principali ottenuti dal Progetto dimostrano l'efficacia del suo approccio olistico, con un impatto che si estende dalla comunità scientifica fino a quella dei professionisti e dei cittadini. I deliverable si possono raggruppare secondo quattro principali aree tematiche:

- **Regolazione e governance**. È stata creata una matrice di lavoro che mappa e sistematizza la legislazione e il ruolo assegnato alle istituzioni nella protezione del cyberspazio, anche in contesti diversi da quello europeo. Sono stati prodotti report tecnici sulla trasformazione del diritto internazionale ed europeo in materia di cybersicurezza, sull'applicazione del principio di "security-by-design" all'AI e sulla regolamentazione di rischio e disinformazione, anche in ottica comparata.
- **Diritti fondamentali ed etica**. Il progetto ha fornito un'architettura concettuale dei diritti fondamentali nel cyberspazio, con la redazione di report tecnici che propongono un nuovo vocabolario e rimedi pratici. Sono state analizzate le dinamiche di e-government ed e-democracy, la protezione dei dati personali in contesti transfrontalieri, le questioni di sicurezza nel settore sanitario e la gestione del rischio cyber per la proprietà intellettuale. Questi risultati contribuiscono a una comprensione effettiva dei diritti e delle loro dinamiche, specie sotto il profilo della realizzazione del principio di uguaglianza, in una società digitalizzata.
- **Formazione e sviluppo di competenze**. Il progetto ha risposto al bisogno di nuove figure professionali con competenze pluridisciplinari. Sono stati elaborati piani di nuovi moduli formativi sulla cybersicurezza per enti pubblici e privati, con specifici focus sulla compliance per la Pubblica Amministrazione e per le PMI. L'attivazione di Osservatori congiunti per la valutazione dell'impatto delle regolamentazioni a livello locale e regionale sottolinea l'impegno verso la formazione e il supporto concreto sul territorio.
- **Aspetti penalistici e geopolitici**. Un'importante area di ricerca ha prodotto report sulla prevenzione e repressione dei crimini informatici a livello nazionale, europeo e internazionale, accompagnato da specifiche analisi dedicate ai profili criminologici delle nuove vulnerabilità e delle indagini digitali. Ulteriori studi hanno esaminato l'evoluzione dei concetti di cyber-warfare e il regime giuridico applicabile alle operazioni ostili, fornendo un quadro strategico cruciale per la sicurezza nazionale e la diplomazia internazionale.

L'analisi dei risultati di CybeRights rivela un chiaro percorso che dalla conoscenza teorica si traduce in applicazioni pratiche con un forte orientamento all'azione e alla risoluzione dei problemi. Ad esempio, il report sulla protezione dei diritti in ambito sanitario o quello sulla

cyber-compliance per le Pubbliche amministrazioni non sono solo studi, ma guide operative che affrontano problematiche reali e di vitale importanza. L'analisi dei risultati di CybeRights rivela un chiaro percorso che dalla conoscenza teorica si traduce in applicazioni pratiche con un forte orientamento all'azione e alla risoluzione dei problemi. Ad esempio, il report sulla protezione dei diritti in ambito sanitario o quello sulla cyber-compliance per le Pubbliche amministrazioni non sono solo studi, ma guide operative che affrontano problematiche reali e di vitale importanza.

Questa trasformazione della ricerca in strumenti applicabili è un punto di forza fondamentale del progetto. L'istituzione di Osservatori congiunti con autorità e agenzie a livello nazionali (ACN, AGCOM, Garante per la Protezione dei Dati Personali e AGID) ed enti pubblici territoriali e non (Regioni, Comuni, altre Università e Centri di Ricerca) rappresenta l'impegno a tradurre le scoperte teoriche in analisi di impatto concrete e misurabili. Il progetto ha creato le infrastrutture necessarie per un'analisi continua delle dinamiche regolatorie e del loro impatto. Questa caratteristica rende i risultati di CybeRights non solo interessanti per la comunità scientifica, ma direttamente utilizzabili da imprese, pubbliche amministrazioni e decisori politici.

Sotto questo punto di vista possono essere menzionati due risultati particolarmente importanti che hanno avuto riscontri già significativi: l'**Osservatorio CybeRights** e il CyberTour. L'Osservatorio CybeRights fornisce informazioni chiare e comprensibili alla collettività sulle norme relative ad alcuni domini sensibili del processo di innovazione tecnologica. L'Osservatorio offre, inoltre, materiali liberi e gratuiti per la formazione in materia di cultura digitale ed educazione alla cittadinanza digitale. Tra questi il Breviario giuridico della cybersicurezza, uno strumento teorico-pratico utile per orientarsi nella complessa regolazione in materia. Costruito per voci e disponibile anche in un volume in open acces, il Breviario può essere un valido ausilio per le attività educative e formative, necessarie per accrescere il grado di consapevolezza dei rischi che si corrono nello spazio digitale. Con l'obiettivo di garantire una disseminazione agile di elementi di cybersecurity in collaborazione con la SERICS Academy, è stato attivato il **CyberTour**, articolato in nove incontri di una giornata ciascuno, e strutturato in una prima parte di carattere generale, nel corso della mattina, e in una speciale, nel pomeriggio, specificamente dedicata alle pubbliche amministrazioni e alle piccole e medie imprese.

Per il progetto DiSe, guidato dal CNR, si sono ottenuti una serie di risultati significativi quali:

- Studio per la gestione semi-automatica delle politiche di sicurezza e per la protezione dei dati e comparazione delle politiche di sicurezza su cloud in EU e US;
- Analisi sociale ed economica della gestione dei dati con particolare riguardo al settore della cybersecurity nel settore energetico;
- Strumenti avanzati per l'analisi collaborativa e distribuita in ambiente sicuro e rispettoso della privacy tramite tecniche di data usage control ed applicazione nel settore automotive;
- Strumenti avanzati di rilevazione di minacce ransomware tramite soluzioni di explainable AI;
- Sistemi di analisi del rischio dinamici e per l'identificazione di contromisure ottimali, in particolare nel settore energetico;
- Metodologie per integrare gli aspetti di sicurezza informatica e la qualità dei sistemi (Quality 5.0).

Tramite alcuni di questi servizi è stato rafforzato l'osservatorio per la cybersecurity **cybersecurityosservatorio.it.** In particolare, in cooperazione con PID ed il centro di competenza Start 4.0, è stato messo a disposizione un servizio di self assessment sulla postura di sicurezza delle PMI che ha portato all'analisi di migliaia di società in Italia.

IN EVIDENZA

Il risultato più significativo e a lungo termine del Progetto CybeRights è la nascita del **Centro Interuniversitario di Ricerca CybeRights**, le cui attività saranno articolate in quattro assi principali: ricerca, didattica e formazione d'eccellenza, consulenza al settore pubblico e privato nelle forme del trasferimento tecnologico e del public engagement e divulgazione.

Questa iniziativa rappresenta un'evoluzione fondamentale, trasformando un progetto a tempo determinato in una struttura permanente. Le attività del Centro si focalizzeranno, attraverso una prospettiva non solo giuridica, ma anche economica, sociale e politica, su temi come la valutazione di impatto della Direttiva NIS2, la regolamentazione delle tecnologie quantistiche, la sicurezza delle operazioni spaziali e la criminalità informatica. La sua struttura, modellata sulle quattro aree della ricerca originaria (regolazione, diritti, formazione e aspetti penalistici e geopolitici), assicura una continuità di visione e un impatto duraturo, facendo del Centro un asset strategico per il sistema-Paese e un punto di riferimento per l'innovazione.

Questa mossa strategica trasforma il progetto in un moltiplicatore di valore. L'iniziativa non è un'azione isolata, ma il punto di partenza per una piattaforma di collaborazione che continuerà a generare conoscenza, formazione e impatto per anni a venire.

Questa rete di eccellenze accademiche e di ricerca è stata ulteriormente rafforzata da una forte partnership con le Autorità e le Agenzie italiane (in particolare attraverso la Convenzione Quadro conclusa con AGCOM e la stretta collaborazione su numerosi progetti, a partire dallo sviluppo di regulatory sandboxes, con ACN) che operano nel campo della sicurezza informatica, garantendo così un costante dialogo tra il mondo della ricerca e le esigenze concrete del sistema-Paese.

Spoke

Disinformazione e Fake News

2

Coordinatore

Vincenzo Loia
Università degli Studi di Salerno

UNIVERSITÀ DEGLI STUDI DI SALERNO

La trasformazione digitale e l'accesso ubiquo all'informazione hanno reso la società più vulnerabile a disinformazione e manipolazione. L'attuale ecosistema comunicativo, dominato da contenuti istantanei diffusi sui social, privilegia la velocità rispetto all'affidabilità. Le minacce non riguardano solo notizie false, ma includono tecniche di manipolazione cognitiva basate su bias psicologici, strategie persuasive e algoritmi di raccomandazione. L'avvento dell'AI generativa ha amplificato i rischi, producendo testi, immagini, video e audio sintetici sempre più realistici e difficili da distinguere, alimentando deepfake, prove falsificate e propaganda a costi minimi ma con impatti economici e sociali rilevanti. A ciò si aggiunge l'uso coordinato di bot, troll e reti di account che amplificano messaggi, polarizzano il dibattito e mascherano l'origine di campagne organizzate, favorendo fenomeni come astroturfing, inauthentic coordinated behavior e creazione artificiale di consenso. Parallelamente, anche i sistemi di rilevazione basati su AI e machine learning diventano bersaglio di attacchi adversariali, che ne minano l'affidabilità e aprono scenari critici per la sicurezza informativa e la fiducia istituzionale. In questo quadro complesso, lo scenario dello Spoke 2 si colloca all'intersezione tra tecnologia, società e sicurezza, con l'obiettivo di contrastare minacce sistemiche che erodono resilienza informativa e fiducia collettiva.

Progetti

DETERRENCE: DEcision supporT SystEm foR cybeR intelligENCE

PI: MAURIZIO TESCONI, CONSIGLIO NAZIONALE DELLE RICERCHE

FF4ALL: Detection of Deep Fake Media and Life-Long Media Authentication

PI: ROCCO DE NICOLA, SCUOLA IMT ALTI STUDI LUCCA

HUMANE: Holistic sUpports against inforMAtioN disordEr

PI: FABRIZIO SILVESTRI, SAPIENZA UNIVERSITÀ DI ROMA

IDA: Information Disorder Awareness

PI: VINCENZO LOIA, UNIVERSITÀ DEGLI STUDI DI SALERNO

Spoke 2

SFIDE

I partner dello Spoke 2 hanno affrontato la complessità delle minacce informative, tra disinformazione e fake news, puntando a rafforzare la fiducia dei cittadini nei media e nelle istituzioni. I progetti hanno condiviso sfide comuni, affrontate con approcci sinergici, richiedendo un ecosistema tecnologico e metodologico avanzato, efficace, sostenibile e centrato sull'utente esperto e sui processi decisionali.

Una prima sfida riguarda l'affidabilità delle fonti e la veridicità dei contenuti. L'analisi automatica di notizie, post e media richiede modelli capaci di distinguere narrazioni genuine da tentativi orchestrati di disinformazione. L'integrazione di strumenti OSINT, tecniche semantiche, e explainable AI è stata centrale per costruire pipeline robuste di verifica e reputazione.

Un secondo gruppo di sfide affrontate ha riguardato la modellazione delle dinamiche sociali nei contesti digitali. Polarizzazione, coordinamento tra account, tossicità e ruolo di utenti influenti sono stati analizzati tramite modelli computazionali, simulazioni e osservazioni su Twitter, Telegram e Reddit. Queste analisi hanno consentito di rilevare segnali precoci di campagne di disinformazione e di sviluppare metodologie non solo di debunking, ma anche di prebunking, anticipando l'impatto delle narrazioni manipolative.

Sul piano tecnologico, una sfida cruciale ha riguardato la rilevazione e l'attribuzione di contenuti sintetici (deepfake), divenuti via via più sofisticati. Da un lato, i progetti hanno perseguito approcci di tipo passive detection, analizzando contenuti multimediali e audio per stabilirne l'autenticità e distinguere i contenuti genuini da quelli manipolati. Dall'altro lato, è stata condotta un'analisi preliminare volta a individuare, per ciascun contenuto, una specifica impronta (fingerprint), con l'intento di attribuire la provenienza a uno specifico generatore di immagini o modello.

Un'ulteriore sfida è stata l'adattabilità dei modelli a contesti nuovi o non supervisionati. L'uso di mixture-of-experts, few-shot e federated learning ha permesso di esplorare approcci scalabili e privacy-preserving in scenari dinamici e decentralizzati. L'eterogeneità di fonti, formati e linguaggi ha reso necessarie soluzioni multimodali e multilingue.

Parallelamente per affrontare un noto nodo critico, ossia il bias algoritmico nei modelli generativi e nei sistemi di raccomandazione, è stato necessario sviluppare strumenti per l'audit dei bias, valutare implicazioni socio-politiche e giuridiche e promuovere strategie che considerino la dimensione etica e istituzionale. Inoltre, è emersa la sfida di garantire trasparenza e robustezza dei sistemi: i modelli devono offrire risultati accurati, rendere interpretabili i processi decisionali e resistere a manipolazioni, errori di generalizzazione e condizioni operative impreviste, sfruttando tecniche di AI ed Explainable AI.

Infine, in ottica monitoraggio e mitigazione ci si è concentrati sull'interazione tra esseri umani e sistemi intelligenti. L'approccio human-in-the-loop è stato integrato per migliorare l'accuratezza dei modelli e coinvolgere attivamente esperti, giornalisti, decisori e cittadini nella comprensione dei rischi e nell'attivazione di contromisure.

PRINCIPALI RISULTATI

IDA – Information Disorder Awareness:

- **CVES (Cognitive Vulnerability Exploitation Score)**.Metodologia per stimare in anticipo con un indicatore dedicato il rischio di manipolazione di eventi reali . Per il metodo, è stata depositata domanda di brevetto.
- **IDA (Information Disorder Awareness)**. Piattaforma per il monitoraggio e l'analisi della disinformazione online, basata su AI e data mining. Rileva segnali di disinformazione, ne traccia la diffusione e valuta il rischio, fornendo dashboard interattive. Ad oggi, è alla base di uno spin-off attualmente in fase di costituzione.
- **Claim Verification Tool**. Prototipo di metodologia che implementa un'architettura di Retrieval Augmented Generation per verificare la veridicità delle affermazioni online in due fasi: recupero da fonti affidabili e successiva conferma o smentita.
- **Propaganda Detection Tool**. Prototipo che individua tecniche di propaganda nei testi, usando AI e strumenti di spiegabilità (xAI) per comprendere e validare le decisioni dei modelli.
- **MSCS (Multifactorial Source Credibility Score)**. Metodologia per il calcolo di un indicatore di credibilità dei siti web considerando vari fattori (es. bias, pubblicità, ecc.), la cui verifica ha mostrato punteggi coerenti con valutazioni umane esperte (es. NewsGuard).
- **Multimodal Manipulation Detection**. Soluzione che integra computer vision e audio forensics per individuare contenuti alterati, combinando stima della posa, incongruenze biometriche e fingerprinting dei generatori di contenuti sintetici.

Deterrence – DEcision supporT SystEm foR cybeR intelligENCE:

- **MERMAID**. Framework basato su un approccio mixture of experts, in cui i modelli più adatti sono selezionati dinamicamente e una procedura di merging consente di ridurre il numero complessivo di modelli e preservare specializzazione e adattabilità.
- **Temporal Dynamics**. Metodologia di analisi della dinamicità del comportamento coordinato online con rete multilivello. Mostra comunità spesso instabili, utenti che seguono archetipi fissi e contenuti e struttura influenzano l'adesione.
- **Rilevamento automatico di minacce ibride online**. Metodologie scalabili per rilevare interferenze e manipolazioni informative cross-piattaforma (FIMI). La validazione ha rivelato campagne pro-disinformazione e media russi.
- **MIPD, Entity Framing, PolyNarrative**. Corpora multilingue e multilabel per lo studio di disinformazione,

tecniche manipolative, framing delle entità e narrazioni su guerra e clima.

- **Adversarial Magnification**. Tecniche di super-risoluzione usate come attacco adversariale per ingannare i deepfake detector. Minime modifiche visive hanno una forte influenza sulla precisione dei sistemi.
- **Opinion Dynamics**. Metodo per identificare configurazioni che generano posizioni estreme, analizzando la polarizzazione e il ruolo della centralità dei nodi.
- **M3DUSA**. Framework multimodale che combina testo, immagini e strutture sociali con strategie di fusione flessibili. I test su dataset reali mostrano superiorità rispetto ai modelli tradizionali.

HUMANE – Holistic sUpports against inforMAtioN disordEr:

- **Modelli teorici**. L'Università di Roma "La Sapienza" ha studiato la diffusione dell'informazione tramite modelli di dinamica delle opinioni, con focus su polarizzazione politica e teorie del complotto. Ha inoltre condotto analisi su iper-grafi e complessi simpliciali per valutarne la capacità descrittiva di contenuti informativi e disinformativi.
- **Attacchi e difese**. L'Università di Roma "La Sapienza" ha analizzato la vulnerabilità di classificatori ad attacchi di data poisoning, mostrando che modelli largamente usati in letteratura possono essere manipolati alterando i dati di addestramento. Un caso di studio ha riguardato l'impatto di un attacco su classificatori di commenti misogini su Reddit. Parallelamente è stato sviluppato DanteLLM, modello linguistico di grandi dimensioni per l'italiano, che rappresenta un passo verso sistemi NLP più robusti. L'Università degli Studi di Milano ha analizzato il fenomeno del disordine informativo on-line e le caratteristiche degli strumenti tecnologici atti a intercettarlo e contrastarlo da una prospettiva giuridica con particolare attenzione ai settori sanitario e della sicurezza nazionale ed al bilanciamento dei diritti coinvolti elaborando modelli e indicazioni operative per supportare le Istituzioni.
- **Analisi applicative**. Il CNR ha creato un framework NLP per l'analisi del sentiment nelle fake news e modelli per lo studio della diffusione della disinformazione sui social. Con IMT e UniRoma1 ha contribuito a metodi automatizzati per valutare l'attendibilità delle fonti online. L'Università Ca' Foscari di Venezia ha analizzato l'impatto della disinformazione in vari domini digitali e avviato lo sviluppo di misure correttive basate su dataset annotati e aggiornati.

FF4ALL – Detection of Deep Fake Media and Life-Long Media Authentication:

- **Dataset pubblici**. Sono stati creati e rilasciati dataset unici per dimensione e varietà, tra cui WILD (20.000 immagini da 20 generatori), TrueFake (600.000 immagini reali e sintetiche) e VideoDiffusion (3.000 video da modelli di diffusione). Queste risorse costituiscono dei solidi benchmark per testare la robustezza dei sistemi.
- **Framework per Deepfake Detection and Attribution**. Sono stati sviluppati framework multimodali per attribuire i contenuti ai generatori di origine, sfruttando caratteristiche visive, biometriche e acustiche. Tecniche basate su geometria 3D dei volti, mixture of experts e architetture transformer hanno migliorato le prestazioni in scenari reali e compressi.
- **Metodi per Explainability e Robustezza**. Sono stati introdotti metodi training-free e soluzioni di explainable AI per rendere interpretabili i processi decisionali. Le prestazioni sono state valutate contro manipolazioni e attacchi avversari, evidenziando resilienza e criticità dei modelli.
- **Soluzioni per Protezione Attiva e Firme Digitali**. Sono state proposte tecniche di fingerprinting e watermarking già in fase di generazione, oltre a firme crittografiche che restano valide al ritaglio dell'immagine. Esplorate anche applicazioni in cloud ed edge computing, con focus su sicurezza e interoperabilità.

IN EVIDENZA

Il risultato più significativo è la realizzazione di sistema per il monitoraggio dell'Information Disorder che adotta standard e framework di settore come STIX e DISARM e impiega modelli di intelligenza artificiale avanzata, combinando competenze, dati e tecnologie. La soluzione si propone come un SIEM (Security Information and Event Management) dedicato alla Sicurezza Cognitiva. Questa soluzione estende la protezione non solo all'ambito informativo e cognitivo, ma anche al dominio del contrasto alla disinformazione online, dove oggi si sviluppano molte delle minacce più sofisticate. Il flusso di lavoro consente all'analista di definire argomenti di interesse e indicatori di compromissione, il sistema processa, arricchisce, aggrega osservabili acquisiti dai social e dal web e li restituisce in una forma consultabile da analisti del settore, a vantaggio di un monitoraggio interattivo ed intelligente del disordine informativo e potenzialmente di supporto a imprese, istituzioni e media. La soluzione combina diversi servizi innovativi: l'analisi dell'affidabilità delle fonti, veridicità e genuinità dei contenuti testuali e multimediali; l'individuazione di campagne coordinate; moduli avanzati di autenticazione e attribuzione di contenuti sintetici, come testo generato e deepfake audio-visivi.

Il valore aggiunto è duplice: da un lato, la possibilità di quantificare e anticipare gli effetti di campagne manipolative, dall'altro, la capacità di restituire ai decisori strumenti trasparenti, basati su IA spiegabile, per interpretare in tempo reale fenomeni complessi. Attualmente la piattaforma è in fase di valutazione da parte dei partner industriali del progetto.

Spoke

Attacchi e difese

3

Coordinatore

Giorgio Giacinto
Università degli Studi di Cagliari

La crescente digitalizzazione è causa di un incremento della superficie di attacco che a sua volta determina un incremento della varietà degli attacchi, sia dal punto di vista delle tecniche utilizzate, sia dal punto di vista della sequenza dei passi che l'attaccante deve compiere per raggiungere l'obiettivo finale. Le tecniche di attacco sfruttano diverse vulnerabilità, da quelle caratteristiche degli esseri umani legate alla naturale tendenza a fidarsi, a quelle caratteristiche dei dispositivi fisici, della rete di comunicazione e del software dovute a errori di progettazione o implementazione, o legate alla complessità delle interazioni fra sistemi. La complessità degli attacchi è molto variabile, e spesso include tecniche sofisticate sviluppate per rendere le attività malevole nascoste e dissimulate per sfuggire alla sorveglianza da parte dei sistemi automatici di sicurezza. Il filo comune che unisce le diverse tecniche di attacco è la loro capacità di risultare invisibili sia agli strumenti tecnologici, sia agli esperti umani. Le tecniche di intelligenza artificiale (IA) da diversi anni costituiscono una soluzione efficace per la progettazione di sistemi per la rilevazione e contenimento di attacchi informatici. Da un lato, vi è la necessità di aggiornare continuamente i sistemi di difesa in risposta all'evoluzione delle minacce. Dall'altro, occorre proteggere e irrobustire i sistemi di IA diventati essi stessi bersaglio degli attaccanti.

Progetti

COVERT: In searCh Of eVidence of stEalth cybeR Threats

PI: GIORGIO GIACINTO, UNIVERSITÀ DEGLI STUDI DI CAGLIARI

GERONIMO: GEneralized Real-time On-line National Internet MOnitoring Infrastructure

PI: FRANCESCO PALMIERI, UNIVERSITÀ DEGLI STUDI DI SALERNO

SOS_AI: Science and engineering Of Security of Artificial Intelligence

PI: FABIO ROLI, UNIVERSITÀ DEGLI STUDI DI GENOVA

CSS: Cyber Social Security

PI: DANILO CAIVANO, UNIVERSITÀ DEGLI STUDI BARI ALDO MORO

Spoke 3

SFIDE

Quattro progetti hanno affrontato le sfide dello scenario di riferimento. Il progetto **COVERT (In searCh Of eVidence of stEalth cybeR Threats)** è focalizzato sullo studio e analisi degli attacchi che usano tecniche sofisticate per nascondere le azioni malevole, sfruttando le caratteristiche dei linguaggi di programmazione, o attraverso la dissimulazione dei contenuti malevoli in contenuti digitali apparentemente innocui, o ancora modificando il comportamento di un programma a seconda dell'ambiente di esecuzione. Per costruire strumenti efficaci di rilevazione degli attacchi sono stati sviluppati approcci basati su tecniche di IA che consentono di elaborare un numero molto elevato di misure che individuano anche i più deboli segnali di potenziali attività malevole. Gli approcci basati su IA hanno consentito al progetto **GERONIMO (GEneralized Real-time On-line National Internet Monitoring)** di sviluppare strumenti di rilevazione di anomalie, attacchi e attività malevole attraverso analisi del traffico di rete a diversi livelli di granularità. Il numero crescente di dispositivi connessi alla rete, che spesso generano traffico di rete anonimizzato e crittografato, richiede un'accurata selezione delle caratteristiche del traffico di rete da monitorare e lo sviluppo di approcci di machine learning specializzati.

Il progetto **CSS (Cyber Social Security)** affronta rischi digitali non solo come minacce tecniche, ma come fenomeni che hanno impatti sociali, politici e culturali, richiedendo la reinterpretazione delle funzioni di Prevenzione, Rilevazione e Risposta. L'evoluzione delle minacce impone approcci multidisciplinari per la gestione del rischio, articolati lungo quattro direttrici: "tecnologica", con l'uso dell'IA per il rilevamento e la mitigazione di *hate speech, deepfake, cyberbullying*, violenze digitali e disinformazione; "etico-sociale", bilanciando libertà di espressione e prevenzione, riducendo i bias e proteggendo i soggetti vulnerabili; "normativa", considerando i vari framework sulla sicurezza e protezione dei dati e dei sistemi come GDPR, NIS2, AI Act e Cybersecurity Act; "operativa e organizzativa", attraverso governance e cooperazione tra esperti, istituzioni, aziende e società civile.

Il progetto **SOS AI (Science and engineering Of Security of Artificial Intelligence)** ha affrontato due sfide aperte in modo integrato. La rifondazione dei fondamenti teorici dell'IA per applicazioni di cyber-sicurezza, e la sicurezza degli strumenti basati sull'IA e dei sistemi potenziati dall'IA. Difatti, i fondamenti teorici dell'IA non sono stati pensati considerando applicazioni dove attaccanti intelligenti mirino a sovvertire intenzionalmente il processo di apprendimento e di decisione di un sistema basato sull'IA e l'IA rischia di diventare l'anello più debole della catena della sicurezza informatica. La sfida affrontata è stata quella di sviluppare nuove soluzioni algoritmiche e strumenti software per la progettazione sicura di strumenti basati sull'IA.

PRINCIPALI **RISULTATI**

All'interno del progetto COVERT i principali risultati possono essere riassunti nei seguenti punti

- Sviluppo di tecniche basate su *deep learning* e *large language models* per la rilevazione di vulnerabilità nel codice sorgente e per analisi di altre tipologie di minacce informatiche come attacchi di tipo DoS, *stego-malware*, e *malware* per dispositivi Android.
- Sviluppo di uno strumento software per l'analisi di macro all'interno di documenti Microsoft Office finalizzato alla produzione di un rapporto relativo alle potenziali azioni malevole
- Individuazione di vulnerabilità in alcuni sistemi operativi nella implementazione della gestione della memoria principale con tecniche ASLR.
- Valutazione formale e sperimentale della robustezza degli strumenti per l'analisi statica del codice binario quando sono utilizzate tecniche di offuscamento e di packing e sviluppo di nuove tecniche specializzate per superarne le limitazioni.
- Individuazione di vulnerabilità in template engine usati nello sviluppo di applicazioni web, e nelle implementazioni del protocollo HTTP/3 che possono dare origine a nuove minacce informatiche.
- Sviluppo di strumenti avanzati per la Cyber Threat Intelligence attraverso l'integrazione di OSINT all'interno di SIEM, lo sviluppo di IDS con tecniche innovative di machine learning, la creazione di attack graphs, e l'integrazione di informazioni non strutturate attraverso l'uso di large language models.
- Analisi delle minacce a sistemi di controllo industriale attraverso la modellazione dei sistemi di controllo e attraverso l'analisi del traffico di rete con tecniche di machine learning.

All'interno del progetto GERONIMO sono stati sviluppati:

- Sistemi basati sul paradigma del federated learning finalizzati alla correlazione di traffico generato da diversi dispositivi a scopo di rilevazione di attacchi o classificazione dei flussi di traffico. Il sistema TinyIDS è un IDS progettato per essere installato su dispositivi con ridotte capacità computazionali, basato sulla distribuzione TinyML che implementa tecniche di machine learning che possono essere eseguite su microcontrollori. L'analisi del traffico in reti di sensori wireless (WSN) ha consentito lo sviluppo di un modello epidemiologico della propagazione del malware.
- Sono stati inoltre sviluppati diversi approcci basati su ML e DNN, nonché su tecniche avanzate di feature selection, per l'*anomaly detection* su serie temporali riferibili a traffico di rete.
- Una metodologia per garantire la riservatezza negli approcci di federated learning, utilizzati per la correlazione di diversi flussi di traffico, attraverso l'utilizzo di crittografia omomorfica. Il sistema è stato progettato per essere resiliente ad attacchi di tipo *adversarial learning*.
- Una metodologia di deanonimizzazione basata sulla correlazione di diversi flussi finalizzata a rilevare le mi-

nacce informatiche che si propagano attraverso traffico anonimizzato e crittografato.

Il progetto Cyber Social Security (CSS) ha sviluppato metodi e strumenti multidisciplinari per la gestione del rischio cyber-social, articolata in due dimensioni: orizzontale e verticale.

La dimensione orizzontale comprende i seguenti ambiti chiave:

- Cyberbullying, molestie digitali tramite messaggi offensivi, esclusione o diffusione di contenuti umilianti.
- Abusi e violenze contro i minorenni mediante la produzione, diffusione o fruizione di materiali e l'adescamento online.
- Violenza contro il partner e violenza di genere attraverso minacce e molestie veicolate sul digitale con attività di stalking o revenge porn o esercitando il controllo a distanza, ad esempio geolocalizzando la vittima.
- Cyberterrorismo: adattamento del terrorismo classico al cyberspazio, usato per attacchi, propaganda, reclutamento.
- Diffusione di contenuti multimediali di incitamento all'odio e disinformazione con finalità manipolativa all'interno del contesto sociale e politico.
- Interconnessione tra sicurezza fisica e digitale in contesti urbani.
- Utela della privacy e diritti, contrasto a sorveglianza di massa e discriminazione algoritmica.

La dimensione verticale si articola nelle tre unità operative di sicurezza:

- Rilevazione, per identificare e prevedere eventi sociali significativi nel cyberspazio.
- Risposta, per definire nuovi protocolli di intervento e cooperazione.
- Prevenzione, per ridefinire processi di censimento e mitigazione degli incidenti alla luce delle nuove risorse critiche.

Negli ambiti del progetto SOS AI, i risultati relativi alla sfida sulla "rifondazione dei fondamenti teorici dell'IA per applicazioni di cyber-sicurezza" possono essere così riassunti:

- Sviluppo della libreria software *SecML-Torch* per la valutazione della sicurezza di algoritmi di IA (https://secml-torch.readthedocs.io/) e per la difesa di strumenti di IA utilizzati nella "multimedia forensics".
- Sviluppo di metodi per la spiegazione ed interpretazione degli algoritmi IA al fine di valutarne la sicurezza e proporre adeguate misure di mitigazione degli attacchi, con specifica applicazione alla rilevazione di "Windows PE malware".
- Sviluppo di una nuova classe di "boosted tree ensembles" per applicazioni con dati tabulari, come quelli medici, che unisce elevate prestazioni a una robustezza superiore, formalmente dimostrata e verificabile in modo estremamente efficiente.

Fra i principali **risultati relativi alla sfida sulla "sicurezza degli strumenti basati sull'IA e dei sistemi potenziati dall'IA":**

- Sviluppo di attacchi contro sistemi di visione basati su IA a bordo di autoveicoli e loro test in ambiente reale, e di tecniche di difesa ed attacco a sistemi cyber-fisici che utilizzano moduli basati su IA.
- Sviluppo di strumenti tecnologici per la valutazione della conformità alla legislazione dello European AI Act dei sistemi basati su IA.
- Creazione del laboratorio congiunto sAIfer Lab (Joint Lab on Safety and Security of AI, https://www.saiferlab.ai) da parte di due partner del progetto SOS AI, le Università di Cagliari e di Genova.

IN EVIDENZA

Nei progetti realizzati, grande enfasi è stata posta sulla robustezza delle tecniche di *machine e deep learning* nei confronti di attacchi che mirano a ridurre l'efficacia in diversi contesti applicativi. Le tecniche sviluppate consentono ad aziende e pubbliche amministrazioni di progettare sistemi di Intelligenza Artificiale robusti ed efficaci, e contribuiscono a costituire un nucleo solido di strumenti per verificarne l'adeguatezza dei sistemi di IA adottati rispetto a requisiti funzionali e normativi. Il progetto SOS AI ha sistematizzato numerosi scenari di attacco sia da un punto di vista metodologico, sia attraverso la creazione della libreria open-source SecML-Torch che viene continuamente arricchita di nuovi moduli grazie ai contributi provenienti dalla comunità. La libreria consente di evidenziare le debolezze e vulnerabilità di un sistema di machine learning rispetto a numerosi scenari di attacco e fornisce al progettista un utile riscontro per rendere il sistema robusto. Questo risultato consente di progettare strumenti di *machine* learning e *deep learning* in grado di rilevare attacchi informatici caratterizzati da una sempre maggiore complessità e sofisticazione.

Spoke 4

Sicurezza dei Sistemi Operativi e della Virtualizzazione

Coordinatore

Alessandro Armando
Università degli Studi di Genova

Università di Genova

La crescente adozione di tecnologie di **cloudificazione** e **virtualizzazione** sta trasformando in profondità le infrastrutture critiche. Piattaforme un tempo gestite come sistemi isolati e verticali oggi convergono in un continuum distribuito che integra risorse di calcolo e di comunicazione, orchestrate con paradigmi cloud-native. La progressiva fusione tra computing e networking produce architetture flessibili e scalabili, però esposte a nuove superfici di rischio.

Un esempio emblematico è rappresentato dalla cloudificazione del 5G: funzioni tradizionalmente radicate nell'hardware vengono smaterializzate e ridistribuite in forma di microservizi, integrando in modo trasparente la parte radio con il core di rete. Questo approccio permette di abilitare servizi mission critical, edge computing e network slicing, creando un tessuto infrastrutturale in grado di adattarsi dinamicamente alla domanda. La natura distribuita e virtualizzata di tali ambienti porta però con sé complessità senza precedenti. La resilienza diventa un requisito fondante: i sistemi devono continuare a funzionare anche in presenza di guasti o attacchi mirati. L'integrazione fra cloud, edge e core radio apre nuovi scenari di sperimentazione, in cui la sicurezza non può essere pensata come un'aggiunta, ma deve essere incorporata nativamente nel ciclo di vita delle applicazioni. La capacità di automatizzare, orchestrare e monitorare in tempo reale ambienti eterogenei rappresenta oggi la base su cui costruire la sicurezza delle infrastrutture critiche del futuro.

Progetti

SecCo: Securing Containers

PI: LUCA VERDERAME, UNIVERSITÀ DEGLI STUDI DI GENOVA

5Gsec: Security in 5G and beyond

PI: RAFFAELE BOLLA, UNIVERSITÀ DEGLI STUDI DI GENOVA

ARTIC: Affordable, Reusable and Truly Interoperable Cyber ranges

PI: ENRICO RUSSO, UNIVERSITÀ DEGLI STUDI DI GENOVA

Spoke 4

SFIDE

Il passaggio a infrastrutture virtualizzate, distribuite e **cloud-native** genera una molteplicità di sfide interconnesse. Una delle più rilevanti è la resilienza: i sistemi devono mantenere livelli di servizio accettabili anche sotto attacco o in condizioni di guasto, garantendo continuità operativa in scenari estremamente dinamici. Parallelamente, cresce la necessità di governare ecosistemi eterogenei composti da **microservizi**, componenti legacy e nuovi moduli cloud-native, ciascuno con cicli di aggiornamento e requisiti diversi. La complessità della virtualizzazione introduce specifici problemi di sicurezza: la condivisione delle risorse hardware e l'orchestrazione multi-tenant aumentano i punti d'ingresso per possibili compromissioni. Inoltre, la superficie d'attacco si estende a più livelli, dal radio access network al core virtualizzato, passando per le piattaforme edge e gli apparati utente. Gli aggressori possono posizionarsi in punti diversi della rete — terminali compromessi, componenti legacy, interfacce radio esposte — sfruttando la natura distribuita per mascherare attività malevole.

In questo contesto, testare le contromisure di sicurezza senza interrompere l'operatività è un obiettivo difficile da raggiungere. Per questo diventano cruciali strumenti come i digital twin e i cyber range, capaci di riprodurre fedelmente infrastrutture complesse e di permettere la sperimentazione sicura di scenari di attacco e difesa. Anche i microservizi, pur abilitando scalabilità e agilità, introducono nuove criticità: il loro rapido ciclo di vita, le interdipendenze e le comunicazioni interne aprono vettori di attacco difficili da monitorare con strumenti tradizionali.

Per affrontare efficacemente queste sfide, la sicurezza deve essere integrata lungo l'intero ciclo di vita applicativo, dalle fasi di design e sviluppo fino al rilascio e al runtime. Questo significa non limitarsi a controlli ex post, ma adottare un approccio preventivo, con verifiche sistematiche e continue che accompagnano ogni fase del processo. In questa prospettiva si colloca il paradigma **DevSecOps**, che traduce l'idea di "security by design" in pratiche operative: controlli statici e dinamici del codice, scansione automatica di dipendenze e container, validazione delle configurazioni rispetto a policy dichiarative e, in produzione, monitoraggio continuo e enforcement delle regole. Attraverso automazione e feedback costante, DevSecOps riduce la finestra di esposizione, rafforza la resilienza e rende la protezione una caratteristica nativa dei sistemi cloud-native.

PROGETTO SECCO

Il progetto ha posto al centro la sicurezza dei microservizi e dei flussi DevSecOps. Sono stati sviluppati moduli di hardening integrati nelle pipeline di sviluppo, con l'obiettivo di introdurre controlli statici e dinamici già durante la fase di rilascio. Sono state inoltre definite politiche di sicurezza per i container, basate su linguaggi formali estesi per esprimere regole di accesso e controllo dei flussi informativi, e ne è stata verificata la correttezza tramite strumenti di analisi formale.

Sul piano del rilevamento delle minacce, sono state sviluppate numerose tecniche innovative:

- Una metodologia di security-by-design per costruire microservizi secondo le più avanzate strategie di protezione dell'applicazione e dei dati da essa gestiti;
- Tecniche per rilevare individuare fenomeni di **cryptojacking** e campagne di furto di risorse su larga scala;
- Una tassonomia dei canali nascosti utile a progettare meccanismi di contrasto durante il monitoraggio a runtime;
- Sistemi per la rilevazione di anomalie nelle comunicazioni cifrate TLS 1.3, integrati con strumenti di osservazione Kubernetes.

Sono stati inoltre condotti esperimenti su attacchi DoS a microservizi containerizzati, sviluppati modelli basati su *transformer* e *autoencoder* per il rilevamento di minacce e rilasciati strumenti di automazione per l'orchestrazione edge/cloud, con l'obiettivo di abilitare deployment scalabili e sicuri.

PROGETTO 5GSEC

Il progetto ha indagato la sicurezza del 5G e delle reti di nuova generazione, con risultati distribuiti lungo più dimensioni.

Nell'ambito della privacy e sicurezza del 5G, il tool 5Gmap è stato esteso per supportare architetture NSA, test di attach basati su TMSI e verifiche di esposizione di IMSI/IMEI, rilevando anomalie in reti reali. Sono stati sviluppati testbed avanzati per attacchi di localizzazione, come overshadowing angolare e meaconing a pieno frame, sfruttando hardware FPGA per simulazioni ad alta precisione. Parallelamente, la piattaforma ScasDK ha consolidato il proprio ruolo per il testing di conformità SCAS, con riconoscimento da parte di autorità nazionali.

La ricerca ha esplorato le minacce avversarie in O-RAN, mostrando come xApp e rApp possano essere vulnerabili a evasion, poisoning e input manipolati. Sono state realizzate difese a runtime e benchmark di robustezza. Sul fronte fisico, sono stati studiati attacchi di jamming RF e sviluppati modelli di mitigazione coordinata tra dApp e xApp.

Risultati significativi riguardano anche la propagazione del malware nei network slicing: testbed di emulazione hanno dimostrato che difendere un singolo slice non è sufficiente, e che le dinamiche di secondo ordine possono amplificare instabilità se le difese non sono correttamente calibrate.

Il progetto ha inoltre prodotto:

- Un digital twin per test sicuri delle configurazioni BGP, strumenti per il rilevamento distribuito di hijacking, e dashboard per la valutazione del rischio presso IXPs;
- Studi di security assurance su funzioni 5G (UDM) nell'ambito NESAS/SECAM;
- Metodologie per il rilevamento di jamming selettivo in IoT LoRaWAN e soluzioni basate su gateway intelligenti e infrastrutture virtualizzate;

- Benchmark dei tool di runtime protection per container 5G (Falco e soluzioni commerciali), con estensione a orchestratori NFVCL e modelli AI addestrati su traffico realistico;
- Un testbed per Mission Critical Services in scenari OTA, che ha portato anche a proposte di modifica degli standard 3GPP;
- Prototipi radio per contrastare jamming e incrementare la privacy, unitamente a studi sull'integrazione di crittografia post-quantum nelle interfacce O-RAN;
- L'estensione della piattaforma Arkime per il parsing di traffico 5G e la proposta di un framework di intercettazione basato su key escrow, capace di bilanciare privacy e conformità normativa.

PROGETTO **ARTIC**

ARTIC ha sviluppato e reso disponibile alla comunità un framework open source per cyber range che supera le architetture tradizionali adottando i paradigmi cloud-native. Il framework consente di realizzare cyber range elastici, cioè capaci di adattarsi sia a piccole organizzazioni con risorse limitate, sia a esercitazioni di grande scala su infrastrutture complesse.

L'elasticità del framework è un valore aggiunto importante per la formazione, consentendo la realizzazione di sessioni hands-on con facilità e rapidità. Il progetto ha posto in evidenza anche il ruolo crescente dei cyber range nel testing di apparati e soluzioni tecnologiche, dove è essenziale poter ricreare con precisione ambienti complessi, protocolli, configurazioni, processi fisici e sensori, fino a includere componenti hardware. Sono stati ricreati sistemi cyber-fisici di notevole complessità, con particolare riferimento ai domini marittimo e avionico.

- Nel settore marittimo è stato sviluppato e rilasciato MaCySTe (Maritime Cyber Security Testbed), una versione specializzata del framework che ha supportato lo sviluppo di attività di ricerca su scenari realistici, sperimentare nuovi attacchi, valutare la resilienza e proporre contromisure dedicate.
- In ambito avionico il framework è stato integrato con sistemi di software defined radio, consentendo di effettuare test in sicurezza su sottosistemi che utilizzano comunicazioni in radiofrequenza e che possono essere esposti ad attacchi wireless. In particolare è stato possibile simulare il Traffic Collision Avoidance System (TCAS), un sistema di bordo che previene collisioni aeree fornendo istruzioni ai piloti.

Questi risultati hanno ricevuto una validazione concreta anche in ambito industriale, grazie all'utilizzo diretto da parte dei partner industriali del progetto, rafforzando ulteriormente la rilevanza del framework per il testing di sistemi cyber-fisici complessi.

Il framework è stato inoltre utilizzato come piattaforma per honeypot avanzati e sandbox complesse consentendo di analizzare come malware o advanced persistent threats possano muoversi e propagarsi in un'architettura reale.

SINERGIE TRA I PROGETTI

Le attività dei tre progetti mostrano un'elevata complementarità. Le soluzioni di hardening e monitoraggio sviluppate in SECCO trovano naturale applicazione negli ambienti 5G studiati in 5GSEC. Le minacce avanzate esplorate in 5GSEC possono essere riprodotte e studiate nei cyber range e digital twin offerti da ARTIC, consentendo la validazione sperimentale in ambienti sicuri.

Questa interazione apre la strada a un ciclo virtuoso: SECCO fornisce meccanismi di protezione integrabili nei flussi DevSecOps, 5GSEC offre casi d'uso realistici e altamente critici nel dominio delle telecomunicazioni, ARTIC mette a disposizione la capacità di simulare e validare gli scenari in ambienti controllati. Insieme, i progetti creano un ecosistema capace di rafforzare la sicurezza delle infrastrutture cloud-native e delle reti mobili di nuova generazione, con impatti diretti sulla protezione delle infrastrutture critiche europee.

IN **EVIDENZA**

Attacchi al sistema anti-collisione aereo

Utilizzando il cyber-range ARTIC è stato possibile simulare con elevata precisione, ma in ambiente controllato, il funzionamento del sistema Traffic Collision Avoidance System (TCAS) e nuove tecniche di attacco contro di esso. Le simulazioni condotte hanno mostrato che un attaccante a terra, con strumentazione relativamente accessibile, può introdurre falsi segnali radar, facendo credere all'aereo che ci siano ostacoli inesistenti o nascondendo invece minacce reali. In pratica, l'attaccante può spingere il pilota a compiere manovre inutili o addirittura pericolose.

Questa scoperta, oltre a essere stata ripresa dai media internazionali, ha portato al riconoscimento ufficiale di due nuove vulnerabilità (CVE-2024-9310 e CVE-2024-11166) da parte della Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti e a un miglioramento della sicurezza del controllo del traffico aereo internazionale.

Spoke 5

Crittografia e sicurezza dei sistemi distribuiti

Coordinatore

Francesco Buccafurri
Università Mediterranea di Reggio Calabria

UNIVERSITÀ DELLA CALABRIA

La protezione dei sistemi distribuiti e l'evoluzione della crittografia si collocano in uno scenario caratterizzato da complessità crescente e trasformazioni rapide. La necessità di garantire solidità teorica e affidabilità dei protocolli crittografici è resa più pressante dall'emergere di nuove tecniche di attacco e dall'impatto potenziale della computazione quantistica, che impongono soluzioni innovative e capacità di governare la transizione. In stretta connessione, l'identità digitale rappresenta una sfida cruciale: la gestione sicura di autenticazione, tracciabilità e accountability solleva questioni di interoperabilità, scalabilità e tutela della privacy, con implicazioni decisive per infrastrutture, servizi e sistemi economici.

Parallelamente, le Distributed Ledger Technologies e la blockchain aprono scenari rilevanti: da un lato pongono interrogativi di sicurezza, efficienza e sostenibilità, dall'altro offrono applicazioni in contesti complessi, nei quali trasparenza e verificabilità sono requisiti indispensabili. In questo quadro, identificazione e tracciabilità assumono un ruolo strategico, configurandosi come elementi basilari della sicurezza dei sistemi distribuiti e come leve di sviluppo per domini di rilevanza nazionale e internazionale. La sovrapposizione tra approcci teorici e prospettive applicative diventa così il terreno su cui costruire soluzioni capaci di trasformare sfide globali in opportunità di innovazione e rafforzamento della fiducia digitale.

Progetti

STRIDE: Project Secure and TRaceable Identities in Distributed Environments

PI: FRANCESCO BUCCAFURRI, UNIVERSITÀ MEDITERRANEA DI REGGIO CALABRIA

Spoke 5

SFIDE

Il progetto STRIDE (Secure and TRaceable Identities in Distributed Environments), ha affrontato sfide che riflettono la complessità dell'identificazione e della tracciabilità, anche in scenari ibridi che intrecciano dimensione fisica e virtuale. Un focus specifico è stato quello dell'identità digitale, considerata nelle sue diverse declinazioni e analizzata nelle forme tradizionali e anonime. La difficoltà di coniugare riconoscibilità, privacy e tracciabilità ha richiesto lo sviluppo di soluzioni nuove, capaci di garantire protezione dell'utente e accountability dei sistemi. In questo contesto è cresciuto l'interesse verso i modelli di **Self-Sovereign Identity**, che pongono al centro l'individuo e la gestione autonoma delle informazioni personali, ma che sollevano interrogativi complessi su interoperabilità, sostenibilità e governance delle infrastrutture.

Un'altra sfida cruciale ha riguardato blockchain, identificazione e tracciabilità. Le **tecnologie DLT** offrono strumenti potenti per sicurezza, trasparenza e decentralizzazione, ma debbono confrontarsi con problematiche relative a scalabilità, affidabilità dei meccanismi di consenso, sicurezza degli smart contract e reale applicabilità in contesti industriali e nazionali. Governance e fiducia rimangono punti delicati per la diffusione di queste tecnologie. Grande attenzione è stata rivolta alla crittografia per autenticazione e controllo degli accessi, un settore reso complesso dall'evoluzione degli attacchi e dalla prospettiva del calcolo quantistico. Lo sviluppo di protocolli sicuri e scalabili è stato prioritario, insieme alla necessità di coniugare rigore teorico e bisogni concreti provenienti dall'industria, come l'accesso sicuro ai servizi finanziari o la protezione delle infrastrutture critiche. Un'altra area innovativa ha riguardato scenari ibridi, in cui mondo virtuale e fisico convivono. Qui l'adozione di **Physical Unclonable Functions** è apparsa promettente per rafforzare i sistemi di autenticazione hardware e prevenire la clonazione dei dispositivi, pur con sfide legate a affidabilità, economicità e integrazione con architetture distribuite.

Infine, il progetto ha affrontato la questione più ampia del ruolo dell'identità nell'era del cyberspazio, un contesto in cui dimensioni tecnologiche, sociali ed economiche si intrecciano. L'identificazione e la tracciabilità digitale sono state quindi considerate non solo strumenti tecnici, ma paradigmi per interpretare la sicurezza di sistemi complessi e distribuiti. Queste sfide hanno mostrato la necessità di un approccio multiprospettico, fondato sulla combinazione di visioni diverse, che spaziano dalla ricerca fondamentale all'applicazione in scenari reali. La sinergia ha permesso di trasformare criticità scientifiche e operative in risultati concreti, delineando soluzioni trasferibili verso domini di interesse strategico, con impatti duraturi a livello nazionale ed europeo.

PRINCIPALI **RISULTATI**

Il progetto STRIDE (Secure and TRaceable Identities in Distributed Environments), ha prodotto risultati significativi che affrontano in modo concreto le problematiche di identificazione e tracciabilità digitale nei sistemi distribuiti. Più in dettaglio, i risultati conseguiti dallo Spoke 5 coprono in modo sinergico diverse sfide: dall'identità digitale alla crittografia avanzata, dall'autenticazione distribuita alla sicurezza hardware, dalle applicazioni blockchain alla protezione dell'IoT. Alcuni risultati hanno carattere fortemente applicativo e trasferibile, altri rappresentano contributi di frontiera alla ricerca internazionale. Questa varietà mostra come lo Spoke abbia saputo integrare approcci teorici, prototipi e casi d'uso concreti, producendo soluzioni con impatti rilevanti per la comunità scientifica, l'industria e le istituzioni, e rafforzando il ruolo del Paese in ambiti strategici per la sicurezza digitale.

Identità digitale e Self-Sovereign Identity (SSI).

Un asse portante del progetto ha riguardato la sperimentazione di modelli avanzati di identità digitale basati su Self-Sovereign Identity, sviluppati e validati all'interno dello Spoke. L'obiettivo è stato mettere al centro l'utente, consentendogli di gestire in autonomia le proprie credenziali e di condividere solo le informazioni strettamente necessarie, in linea con le normative europee e con le esigenze di interoperabilità. Un risultato significativo è stato l'integrazione di questo approccio nella piattaforma TreC Salute, che ha dimostrato come l'adozione di SSI possa rafforzare fiducia, privacy e usabilità nei servizi sanitari digitali. La ricerca ha inoltre affrontato il problema del controllo dell'accesso combinato con il paradigma SSI e quello della revoca delle Verifiable Credentials, proponendo un nuovo protocollo basato su Anonymous Hierarchical Identity-Based Encryption che consente una revoca temporale e flessibile senza compromettere la privacy dell'utente. Un ulteriore contributo è arrivato dalla formalizzazione delle politiche di autenticazione federata: lo studio ha mostrato come sistemi apparentemente sicuri possano diventare vulnerabili quando interagiscono, e ha proposto un nuovo protocollo SSI-based per garantire coerenza e sicurezza nelle federazioni.

Autenticazione e accountability nei sistemi distribuiti.

Un filone distinto ha affrontato i meccanismi di autenticazione e tracciabilità in scenari di comunicazione. CallTrust è un sistema federato ideato per contrastare la combinazione di attacchi di tipo spoofing dell'ID del chiamante o di dirottamento delle chiamate in uscita con tecniche di vishing. CallTrust riduce il rischio di truffe telefoniche, problema di grande rilevanza sociale ed economica basandosi su un modello di trust federato e conforme a eIDAS 2.0.

Crittografia e controllo accessi.

Lo Spoke ha sviluppato strumenti e metodologie crittografiche per la protezione dei dati e la gestione sicura degli accessi in scenari distribuiti. CryptoAC, un prototipo open-source di Cryptographic Access Control, dimostra come sia possibile garantire protezione end-to-end in architetture cloud-native a microservizi e in scenari zero-trust, coniugando sicurezza ed efficienza. A questo

risultato si affianca la progettazione di una metodologia e di un sistema per il penetration testing di protocolli crittografici, concepito per valutare in modo sistematico la robustezza delle soluzioni e identificarne tempestivamente eventuali vulnerabilità.

Crittografia post-quantistica.

L'avvento del calcolo quantistico ha reso prioritario sviluppare algoritmi resistenti a futuri attacchi. In questa direzione si colloca CROSS, uno schema di firma digitale basato su codici che unisce efficienza e sicurezza, distinguendosi come alternativa competitiva rispetto agli algoritmi in corso di standardizzazione. Accanto a CROSS, i partner dello Spoke hanno contribuito a nuove primitive come le ring signature post-quantum e MiRitH, uno schema basato sul problema MinRank, ampliando il ventaglio di soluzioni crittografiche per rafforzare la resilienza delle infrastrutture digitali e alimentando il dibattito internazionale sulla standardizzazione della crittografia post-quantistica.

PUF e autenticazione hardware.

In scenari ibridi, in cui mondo fisico e digitale si intrecciano, è stato sviluppato un innovativo approccio alle Physical Unclonable Functions (PUF) basato su tecniche ottiche multilivello. Queste soluzioni sfruttano la variabilità intrinseca dei materiali per garantire meccanismi di autenticazione hardware non clonabili, con potenziale applicazione in diversi scenari concreti. Alla ricerca sulle PUF ottiche si affiancano studi su PUF quantistiche e implementazioni leggere, che aprono la strada a una nuova generazione di strumenti di autenticazione radicati nella fisicità dei dispositivi.

Blockchain e DLT.

È stato sviluppato un linguaggio grafico per descrivere le supply chain, da cui generare automaticamente smart contract, interfacce e policy di accesso, aumentando tracciabilità, trasparenza e sicurezza nei processi industriali. È stato inoltre introdotto il concetto di Non-Fungible Mutable Tokens (NFMTs), evoluzione degli NFT classici, i cui attributi possono essere aggiornati in modo controllato tramite regole di accesso basate sugli attributi: un modello innovativo per certificare asset digitali e fisici in scenari dinamici. Lo Spoke ha anche contribuito a protocolli di interoperabilità tra blockchain, prerequisito essenziale per l'adozione concreta di approcci basati su blockchain, e ha esplorato l'uso di intelligenza artificiale per individuare e spiegare vulnerabilità negli smart contract, rendendo più affidabili e sicure le applicazioni distribuite.

Sicurezza IoT e scenari distribuiti.

La protezione degli oggetti connessi è stata affrontata con REPLIOT, uno strumento per il testing automatico delle vulnerabilità a replay attack nei dispositivi IoT. Grazie al suo approccio scalabile e automatizzato, REPLIOT consente di individuare rapidamente debolezze e supportare i produttori nella fase di sviluppo. Questo risultato si inserisce in un più ampio filone di strumenti di red-teaming automatico per l'IoT, integrato da intrusion detection avanzata e da PUF per dispositivi a basso costo, con l'obiettivo di rafforzare la resilienza complessiva dei sistemi distribuiti.

IN EVIDENZA

Le truffe telefoniche basate su *vishing*, spesso con falsificazione dell'ID del chiamante (*spoofing*), rappresentano oggi una delle frodi più diffuse. I cittadini sono le vittime, ma le conseguenze ricadono anche su banche, imprese e altre organizzazioni che si trovano ad affrontare costi di rimborso, perdita di fiducia e danni reputazionali. Al tempo stesso, queste realtà hanno la necessità di comunicare via telefono con milioni di utenti, ma i sistemi attuali non offrono adeguata protezione. Dal "Rapporto sulle operazioni di pagamento fraudolente in Italia nel 2° semestre 2024" pubblicato da Banca d'Italia, emerge che le frodi da manipolazione del pagatore sono in preoccupante e continua crescita.

CallTrust è una soluzione innovativa che consente di autenticare in tempo reale le chiamate tra utenti e servizi "certificati" (banche, PA, assicurazioni, ecc.). Il sistema si basa su credenziali digitali pubblicate dai servizi stessi, in grado di attestare l'autenticità della chiamata. L'approccio proposto funziona sia su reti telefoniche tradizionali sia su reti VoIP, senza richiedere modifiche all'infrastruttura. Un elemento distintivo di CallTrust è la sua integrazione in un modello federato, conforme a eIDAS 2.0, che permette di attuare la protezione in maniera interoperabile anche a livello transfrontaliero. Queste caratteristiche rendono CallTrust di interesse per banche, organizzazioni di diverso tipo, ma anche per governi e istituzioni impegnati a rafforzare la fiducia nelle comunicazioni digitali.

Spoke

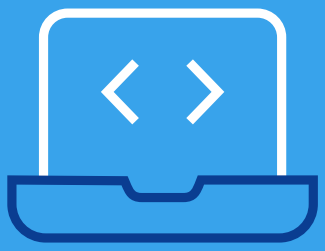
Sicurezza del software e delle piattaforme

6

Coordinatore

Riccardo Focardi
Università Ca' Foscari di Venezia

Università Ca'Foscari Venezia



La trasformazione digitale richiede che la sicurezza del software e delle infrastrutture sia garantita, per tutelare la fiducia dei cittadini, la resilienza delle imprese e la protezione dei servizi critici. In questo contesto, la sfida non è solo prevenire attacchi informatici, ma anche colmare il divario tra modelli matematici di sicurezza e implementazioni concrete, spesso fonte di vulnerabilità. I sistemi complessi per la gestione dell'identità digitale, le piattaforme blockchain, le architetture embedded e i sistemi OT/ICS evidenziano come anche software formalmente corretto possa essere attaccato in modi non previsti dai modelli teorici. Diventa quindi fondamentale integrare metodologie formali, prototipi sperimentali, simulazioni realistiche e validazioni empiriche al fine di aumentare la sicurezza dei sistemi reali, garantendo un impatto tangibile sulle infrastrutture digitali e sull'uso quotidiano delle tecnologie da parte di cittadini, imprese e pubbliche amministrazioni.

Questo approccio integrato comprende strumenti automatizzati, linguaggi di policy avanzati, analizzatori statici, tecniche di machine learning spiegabile e framework per la verifica continua della sicurezza, promuovendo una cultura di protezione attiva e consapevole e contribuendo a consolidare l'affidabilità dei sistemi digitali in settori critici e strategici.

Progetti

SCAI: Supply Chain Attack Avoidance

PI: FLAMINIA LUCCIO, UNIVERSITÀ CA'FOSCARI DI VENEZIA

SWOPS: Securing softWare frOm first PrincipleS

PI: GABRIELE COSTA, SCUOLA IMT ALTI STUDI LUCCA

Spoke 6

SFIDE

Le sfide affrontate dai progetti di ricerca dello spoke riflettono la complessità crescente dei sistemi digitali contemporanei e l'esigenza di garantire sicurezza, affidabilità e fiducia nelle infrastrutture critiche, nei dispositivi embedded e nelle applicazioni distribuite. Una prima sfida fondamentale riguarda il divario tra modelli teorici e implementazioni reali. Gli strumenti di verifica formale permettono di dimostrare matematicamente la correttezza e la sicurezza di un sistema, ma spesso la complessità del software e dell'hardware reale introduce discrepanze che possono essere sfruttate da attaccanti sofisticati. La difficoltà è quindi progettare metodi in grado di collegare modelli astratti a comportamenti concreti, fornendo garanzie affidabili anche in scenari operativi reali.

Un'altra sfida cruciale è la protezione dei dati, anche quelli personali relativi all'identità digitale dei cittadini. Garantire che i protocolli crittografici siano implementati correttamente e che eventuali vulnerabilità siano rapidamente individuate richiede un approccio integrato, che combini analisi formale, test sperimentali e collaborazione con enti pubblici e sviluppatori software. In parallelo, la crescente digitalizzazione delle infrastrutture industriali e dei sistemi OT/ICS comporta la necessità di proteggere impianti fisici da attacchi informatici, dove anche piccoli errori nel software possono avere conseguenze gravi sul funzionamento di reti elettriche, impianti idrici o catene di produzione.

La diffusione di blockchain, smart contracts e architetture decentralizzate introduce ulteriori sfide. Questi sistemi richiedono analisi sofisticate per rilevare comportamenti non deterministici, invocazioni non autorizzate o vulnerabilità cross-chain, garantendo sicurezza e affidabilità in un contesto in cui le transazioni hanno effetti economici reali.

In ambito machine learning e intelligenza artificiale, le sfide riguardano sia la sicurezza dei modelli sia la loro spiegabilità. È fondamentale comprendere come i sistemi di rilevamento malware o i modelli di classificazione automatica prendano decisioni, rendendo trasparente il processo e permettendo agli analisti di fidarsi dei risultati. Inoltre, l'uso di tecniche di federated learning per rilevare malware nascosto in applicazioni mobili richiede approcci innovativi per preservare la privacy e l'efficacia del modello.

Il contesto delle infrastrutture cloud-edge e serverless comporta sfide legate alla gestione di risorse distribuite, sicurezza dei dati e ottimizzazione delle prestazioni, mentre la definizione e l'applicazione di policy di accesso dinamiche in sistemi distribuiti rappresenta un problema complesso, poiché occorre coordinare regole complesse tra più nodi senza introdurre falle di sicurezza.

Infine, il rapido sviluppo di strumenti di AI generativa e la crescente automazione nei test del software sollevano nuove sfide in termini di robustezza, affidabilità e valutazione comparativa dei modelli. Tutte queste problematiche richiedono una combinazione di ricerca teorica, sviluppo di prototipi e collaborazione interuniversitaria e industriale, integrando conoscenze multidisciplinari per affrontare la sicurezza digitale in modo olistico.

PRINCIPALI RISULTATI

- **ALVIE: ridurre il divario tra modelli e sistemi reali**. ALVIE rappresenta un prototipo innovativo per ridurre il divario tra modelli e implementazioni reali di sistemi embedded. Interagendo direttamente con l'hardware, il sistema estrae un modello comportamentale reale e lo analizza in relazione a possibili minacce. Questo approccio permette di individuare sia attacchi noti che vulnerabilità nuove, fornendo un metodo sistematico per verificare e certificare la sicurezza di microprocessori embedded utilizzati, ad esempio, in ambito smart city. Il progetto europeo CCAT, che inizierà a gennaio 2026, estenderà l'uso di ALVIE a nuove architetture, per aumentarne l'usabilità anche per utenti non specialisti. È stata attivata una nuova collaborazione con il Politecnico di Torino, sempre nell'ambito del partenariato SERICS, che ha lo scopo di esplorare l'applicabilità di ALVIE alle estensioni crittografiche dell'architettura RISC-V, aprendo la strada a verifiche formali di nuova generazione per architetture open-source.
- **APOLLO: rilevazione phishing tramite LLM**. APOLLO è uno strumento basato su GPT-4o per rilevare email di phishing e generare messaggi esplicativi che aiutino gli utenti a comprendere il rischio. APOLLO integra una pipeline di Large Language Models per produrre spiegazioni che migliorano la comprensione e la fiducia degli utenti. In studi controllati su larga scala (N = 750), il sistema ha mostrato prestazioni eccezionali (fino al 99% di accuratezza nella classificazione) e ha ridotto la suscettibilità al phishing. L'approccio combina tecniche di explainable AI con valutazioni comportamentali degli utenti, permettendo di produrre avvisi adattivi e scalabili. La validazione ha coinvolto anche collaborazioni con altri centri accademici internazionali.
- **Protezione delle infrastrutture critiche OT/ICS**. Per i sistemi industriali e le infrastrutture critiche, sono stati sviluppati framework avanzati di offuscazione per PLC, in grado di rendere più difficile la comprensione dei processi fisici da parte degli attaccanti. Parallelamente, sono stati realizzati algoritmi di monitoraggio distribuito basati sulla logica formale CyTL, capaci di rilevare anomalie e attacchi DDoS, aumentando la resilienza e la continuità operativa di impianti complessi. Questi strumenti permettono di combinare la specifica qualitativa del comportamento con misure quantitative, come tempi e quantità di dati, per garantire sicurezza sia locale che globale delle infrastrutture.
- **Blockchain e smart contracts**. La sicurezza degli smart contracts è stata notevolmente migliorata grazie a strumenti di analisi statica basati su abstract interpretation, come LiSA e GoLiSA. Tali strumenti identificano comportamenti non deterministici e invocazioni non affidabili nei contratti Go e nelle applicazioni decentralizzate. AlgoMove, invece, consente di utilizzare il linguaggio Move all'interno della piattaforma Algorand, combinando le proprietà di sicurezza di Move

con la versatilità di Algorand. Questi prototipi hanno permesso di verificare cross-chain smart contracts, riducendo rischi di frodi e comportamenti imprevisti nelle blockchain pubbliche e private.

- **Machine learning e individuazione del malware**. Sono stati sviluppati approcci avanzati per migliorare la trasparenza e l'affidabilità dei modelli di sicurezza basati su ML. In particolare, la explainability nei sistemi di rilevamento di malware Android è stata potenziata mediante l'analisi dei grafi delle chiamate a funzione. Sono stati condotti studi comparativi tra modelli LLM come GPT e BERT per il vulnerability scoring, evidenziando le differenze tra le capacità generative e la comprensione bidirezionale del testo. Parallelamente, sistemi federati di rilevazione di stegomalware consentono di individuare dati nascosti nelle icone delle app senza condividere direttamente dati sensibili, rispettando le normative sulla privacy.
- **Performance vs sicurezza nei sistemi cloud-edge e FaaS**. FlexiPlace permette di distribuire applicazioni multi-servizio su infrastrutture cloud-edge tenendo conto non solo delle funzionalità, ma anche della sicurezza, della disponibilità dei nodi, della latenza, della banda e dell'impatto ambientale. WasteLess è un framework che ottimizza in modo predittivo il provisioning in ambienti FaaS, bilanciando costi, prestazioni e sicurezza, con risparmi significativi rispetto a strategie manuali o self-adaptive. Questi strumenti, sviluppati all'interno del partenariato SERICS, mostrano come, in scenari reali con limiti computazionali, si renda necessario un equilibrio tra disponibilità delle risorse e sicurezza, garantendo sistemi sicuri ma al contempo funzionali e utilizzabili.
- **Policy e controllo degli accessi**. I linguaggi Bart, OWSM e Strobilus, sviluppati nell'ambito del partenariato SERICS, permettono di specificare politiche di accesso dinamiche e collaborative in sistemi distribuiti e architetture a microservizi. Questi strumenti formalizzano regole complesse e ne consentono l'applicazione automatica, migliorando la sicurezza delle infrastrutture enterprise e pubbliche. Bart, ad esempio, permette lo scambio controllato di accesso a risorse tra più parti, garantendo la correttezza operativa senza intervento umano.
- **Generative AI e testing.** Per aumentare l'affidabilità e la sicurezza dei sistemi AI, sono stati sviluppati benchmark per la generazione di input di test tramite modelli generativi e tecniche di search-based fuzz testing. L'analisi comparativa di diverse architetture ha evidenziato come modelli più sofisticati producano un numero maggiore di input validi e in grado di provocare errori, specialmente in dataset complessi. Garantire l'affidabilità e la sicurezza dei sistemi AI contribuisce direttamente a rendere più sicuri anche il software e le piattaforme su cui operano, rafforzando l'intera infrastruttura digitale.

IN EVIDENZA

ALVIE è un prototipo innovativo sviluppato dall'Università Ca' Foscari di Venezia per verificare la sicurezza di sistemi embedded come l'architettura Sancus. A differenza degli strumenti formali tradizionali, che spesso forniscono garanzie teoriche difficili da applicare al mondo reale, ALVIE interagisce direttamente con l'hardware per costruire un modello comportamentale concreto del sistema. Analizzando questo modello secondo scenari di minaccia definiti, ALVIE è in grado di identificare attacchi noti e nuove vulnerabilità, producendo al contempo una stima precisa della probabilità che il sistema sia sicuro. Il prototipo è stato scelto per il progetto europeo CCAT, con l'obiettivo di estenderne l'uso a diverse architetture embedded e renderlo accessibile anche a non esperti. In collaborazione con il Politecnico di Torino, sempre nell'ambito del partenariato SERICS, stiamo studiando come applicare ALVIE allo studio della sicurezza delle estensioni crittografiche dell'architettura RISC-V, dimostrando come strumenti avanzati di analisi possano ridurre concretamente il divario tra teoria e implementazione reale, aumentando la fiducia nella sicurezza del software e dei dispositivi.

Spoke

Sicurezza delle infrastrutture

7

Coordinatore

Stefano Di Carlo
Politecnico di Torino

Politecnico di Torino

Le infrastrutture critiche costituiscono il cuore pulsante di una società moderna: distribuzione di energia elettrica e gas, reti idriche, trasporti, sanità e telecomunicazioni sono servizi essenziali senza i quali la vita quotidiana e l'economia non potrebbero funzionare. La loro crescente digitalizzazione, spinta dall'adozione di tecnologie IoT, edge computing e sistemi basati su intelligenza artificiale (IA), ha migliorato efficienza e capacità di controllo, ma al prezzo di un aumento significativo della superficie d'attacco. In questo contesto, la sicurezza non può limitarsi alla sola protezione dei dati, ma deve garantire la continuità del servizio e la resilienza operativa, elementi imprescindibili per infrastrutture che devono funzionare senza interruzioni.Questa tensione richiede uno sforzo per affrontare nuove problematiche. Sistemi complessi, distribuiti e fortemente interconnessi, che includono dispositivi legacy difficili da aggiornare, convivono con tecnologie di nuova generazione. La presenza simultanea di componenti Information Technology (IT), cioè i sistemi informatici tradizionali, di Operational Technology (OT), cioè i sistemi di controllo e automazione industriale, e di Internet of Things (IoT) espone le infrastrutture a minacce avanzate e persistenti, capaci di compromettere non solo la disponibilità dei servizi ma anche la sicurezza fisica delle persone. Inoltre, la dimensione geopolitica e strategica degli attacchi cibernetici alle infrastrutture critiche rende la protezione di questi sistemi una priorità nazionale ed europea. In questo scenario la ricerca svolge un ruolo fondamentale nell'analizzare vulnerabilità specifiche, sviluppare strumenti innovativi per la prevenzione, il rilevamento e la risposta agli attacchi, e definire metodologie che rafforzino la fiducia e l'affidabilità delle tecnologie digitali nei contesti più sensibili per la collettività.

Progetti

SANDSTORM: Secure AND Safe infrasTructures fOR cps in the compute continuuM

PI: ERNESTO SANCHEZ, POLITECNICO DI TORINO

SCAR: Securing the third millennium's cyber-CARs

PI: ILARIA MATTEUCCI, CONSIGLIO NAZIONALE DELLE RICERCHE

SCS: Smart-Grid Cyber-physical Security

PI: MARIO MARCHESE, UNIVERSITÀ DEGLI STUDI DI GENOVA

Eraclito

PI: NICOLÒ MAUNERO, CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA

Spoke 7

SFIDE

I rogetti dello Spoke 7 hanno affrontato un insieme articolato di sfide che derivano dalla natura complessa, interconnessa e spesso legacy delle infrastrutture critiche.

Tra queste:

- **Protezione di sistemi eterogenei**. La coesistenza di componenti di Information Technology (IT), Operational Technology (OT) e Internet of Things (IoT) richiede approcci integrati di sicurezza che tengano conto sia delle reti di calcolo sia dei dispositivi di campo, spesso vincolati da risorse limitate.
- **Gestione di minacce avanzate e persistenti (APT)**.Gli attacchi diretti alle infrastrutture critiche sono sempre più mirati e sofisticati, capaci di sfruttare vulnerabilità multiple lungo la supply chain. È stato necessario sviluppare tecniche di rilevamento tempestivo, anche mediante l'uso di IA e machine learning.
- **Resilienza e continuità operativa**. A differenza di altri domini IT, un'interruzione nei servizi critici può avere conseguenze immediate su cittadini e imprese. La sfida è stata progettare strategie di difesa che preservino l'operatività anche in caso di compromissione parziale.
- **Compatibilità con sistemi legacy**. Molti impianti operano con tecnologie non aggiornabili o prive di patch di sicurezza. I progetti hanno dovuto individuare soluzioni che non richiedano interventi invasivi, privilegiando tecniche di monitoraggio non intrusive.
- **Affidabilità dei modelli IA**. L'integrazione di algoritmi intelligenti per il rilevamento delle anomalie solleva interrogativi sulla loro robustezza a guasti hardware e attacchi avversariali. È stato quindi necessario sviluppare metodologie di validazione e testing specifiche per ambienti critici.
- **Sicurezza automotive**. I veicoli moderni, sempre più connessi e autonomi, sono essi stessi infrastrutture critiche mobili. I progetti hanno affrontato la protezione di architetture elettroniche e software automotive da attacchi che potrebbero compromettere la sicurezza stradale e la fiducia degli utenti.
- **Sicurezza dell'hardware**. Per lungo tempo considerata un aspetto secondario, la protezione a livello di microarchitettura e di dispositivi fisici è oggi cruciale. Sono stati esplorati approcci per rilevare vulnerabilità hardware, sviluppare contromisure a guasti intenzionali e garantire l'integrità della piattaforma di calcolo.
- **Risposta coordinata agli incidenti**. Data la natura distribuita delle infrastrutture, è fondamentale disporre di meccanismi di condivisione delle informazioni e orchestrazione degli interventi, anche tra diversi stakeholder pubblici e privati.
- **Conformità normativa e governance**. Le soluzioni sviluppate devono rispettare regolamenti nazionali ed europei (es. NIS2), armonizzando requisiti legali con esigenze tecniche.

Queste sfide hanno guidato la definizione delle metodologie e degli strumenti elaborati nei progetti, che spaziano dal monitoraggio proattivo alla risposta automatizzata, dall'analisi della resilienza cibernetica fino alla formazione di operatori specializzati, preparando così il terreno per i risultati concreti che seguono.

PRINCIPALI **RISULTATI**

I risultati ottenuti dai progetti sono qui presentati organizzati per iniziativa e, all'interno di ciascun progetto, per le principali sotto-tematiche affrontate.

Progetto SANDSTORM

Obiettivo principale del progetto è la realizzazione di un'architettura di calcolo aperta e sicura basata sul processore RISC-V, coprendo l'intero stack – dall'hardware fino ai framework di AI e agli strumenti di progettazione. SANDSTORM rappresenta un primo passo verso l'indipendenza tecnologica italiana dalle soluzioni chiuse estere, in linea con la European Processor Initiative (EPI) e con l'ambizione di rendere l'Italia protagonista nel futuro mercato RISC-V. I principali risultati di questo progetto sono stati:

- **Architetture e sicurezza hardware**. È stato potenziato una CPU CVA6 RISC-V con un acceleratore crittografico capace di eseguire operazioni crittografiche a 64 bit ad alta velocità. In parallelo, è stata proposta una metodologia di verifica di attacchi side-channel a livello RTL, validata con misure su FPGA.
- **Vulnerabilità microarchitetturali**. Sono stati scoperti tre nuovi vettori di attacco della famiglia Spectre che sfruttano meccanismi hardware poco documentati. Queste scoperte hanno già portato alla segnalazione di vulnerabilità a livello industriale (CVE-2024-10929) e avranno impatti su decine di milioni di dispositivi, inclusi i nuovi chip AMD/Xilinx Versal.
- **Mixed-criticality systems**. Sono stati proposti metodi per garantire l'isolamento degli acceleratori hardware in sistemi embedded eterogenei basati su RISC-V, inclusi meccanismi per isolare le transazioni su bus avviate da acceleratori su FPGA-SoC.
- **AI robustness**. È stata progettata una tassonomia e un benchmark standardizzato per le tecniche di Adversarial Pruning (AP), reso pubblico per valutazioni robuste e riproducibili.

Progetto SCAR

Il progetto affronta la **cybersecurity nei veicoli stradali**, considerando componenti hardware, software, aspetti sociali e regolatori. L'obiettivo è rafforzare la sicurezza sia intra-veicolare (reti interne come il CAN bus) sia extra-veicolare (comunicazioni V2X con infrastrutture di trasporto).I principali risultati di questo progetto sono stati:

- **Intrusion Detection Systems (IDS)**. Sviluppo di IDS hardware per riconoscere attacchi sulla rete intra-veicolare CAN e sistemi software di anomaly detection su ROS.
- **Protocollo di autenticazione V2X**. Progettato e ve-

rificato formalmente un protocollo di autenticazione multi-fattore e multi-canale (MFA) per comunicazioni V2X, basato su challenge-response e sull'utilizzo di un canale fisico per l'autenticazione. Il protocollo è stato implementato e testato su strada e il suo potenziale trasferimento al settore industriale è già oggetto di valutazione.

- **Threat intelligence**. È stato sviluppato un approccio innovativo di cyber threat intelligence che sfrutta modelli di AI generativa per analizzare grandi quantità di dati provenienti dai social media. L'obiettivo è identificare precocemente trend, potenziali minacce e attività malevole che possono avere un impatto sul dominio automotive.
- **Zero Trust Software Defined Vehicle (ZT-SDV)**. Concettualizzato un nuovo paradigma che applica il principio "never trust, always verify" ai veicoli software-defined, trattando ogni componente come non affidabile fino a prova contraria. L'approccio combina TEEs, virtualizzazione, containerizzazione, attestazioni crittografiche e micro-segmentation, consentendo l'installazione sicura di app di terze parti e l'esecuzione verificabile di moduli software dinamici tramite WebAssembly (WASM) su ARM TrustZone.

Progetto Eraclito

Il progetto mira a innovare il processo di valutazione del rischio cyber superando approcci manuali e frammentati, introducendo strumenti e modelli avanzati per automatizzare correlazioni, identificare rischi e valutare gli impatti a livello tecnologico, organizzativo e legale. I principali risultati di questo progetto sono stati:

- **Modello ontologico del rischio**. Sviluppo di un modello per rappresentare e integrare informazioni su utenti, infrastrutture e conseguenze, abilitando viste multidimensionali personalizzate per i diversi stakeholder.
- **Collegamento tra rischi tecnologici e impatti legali**. Correlazione tra principi di sicurezza informatica (confidenzialità, integrità, disponibilità) e conseguenze sui diritti fondamentali delle persone.
- **Strumenti prototipali basati su AI e ontologie**. Sviluppo di tool che sfruttano regole inferenziali e LLM per automatizzare fasi cruciali quali il threat modeling, la correlazione di minacce e contromisure, e la catalogazione delle vulnerabilità. Ciò permette strategie di cybersecurity adattive e dinamiche.

Progetto (SCS)

Il progetto SCS affronta il tema della sicurezza cibernetica e fisica delle smart grid, con un focus particolare sulle comunità energetiche e sui sistemi di accumulo distribuiti. L'obiettivo è garantire un monitoraggio accurato e la resilienza delle infrastrutture energetiche contro minacce informatiche e anomalie operative. I principali risultati di questo progetto sono stati:

- **Algoritmo di anomaly detection**. Sviluppo di un metodo basato su autoencoder e physics-informed neural networks che integra leggi fisiche nei modelli di AI, consentendo un monitoraggio più affidabile delle risorse energetiche distribuite.
- **Dataset BESS-Set**. Creazione di un dataset per la cybersecurity dei sistemi di accumulo a batterie, già pubblicato e messo a disposizione della comunità scientifica e industriale.
- **Framework IEC 62443**. Definizione di un approccio secure-by-design per le comunità energetiche, conforme agli standard internazionali di sicurezza industriale.
- **Strumenti di monitoraggio industriale**. Sviluppo di un framework per il deployment di tool di cybersecurity negli ambienti industriali.
- **Analisi di impatto degli attacchi**. Valutazione delle conseguenze di attacchi cibernetici contro comunità energetiche, reti di distribuzione e stazioni di ricarica per veicoli elettrici, evidenziando vulnerabilità e strategie di mitigazione.

IN EVIDENZA

Uno dei risultati più significativi riguarda la scoperta di nuove vulnerabilità microarchitetturali nei moderni microprocessori, legate alla gestione della *branch prediction*. Lo studio, svolto dalla Scuola Superiore Sant'Anna nell'ambito del progetto SANDSTORM ha mostrato che meccanismi hardware poco documentati, introdotti per migliorare le prestazioni dei microprocessori (come il Bias-Free Branch Prediction e la Branch History Speculation), possono essere sfruttati per costruire nuovi attacchi della famiglia Spectre, capaci di aggirare le difese oggi considerate standard. I ricercatori hanno individuato tre nuovi vettori di attacco — BiasScope, Spectre-BSE e Spectre-BHS — e realizzato un dimostratore pratico (Chimera) che, sfruttando Spectre-BHS, è stato in grado di estrarre dati dal kernel Linux a velocità superiori a 24 kbit/s, pur con tutte le mitigazioni attive. L'impatto di questa scoperta è enorme: sono interessate varie famiglie di processori e decine di milioni di dispositivi. Per citare un caso emblematico, tutti i nuovi chip Versal di AMD/Xilinx risultano vulnerabili. ARM ha già rilasciato un security bulletin ufficiale per Spectre-BSE e BiasScope, distribuito patch per il kernel Linux e assegnato la vulnerabilità CVE-2024-10929. Sebbene ARM abbia stimato un rischio di exploitation basso, la ricerca ha dimostrato la possibilità di eseguire attacchi completi e funzionanti, capaci di compromettere un sistema reale. Inoltre, un ulteriore CVE è in corso di rilascio per Spectre-BHS e Chimera, a testimonianza della rilevanza della scoperta. Questo risultato evidenzia come la sicurezza dell'hardware, per lungo tempo sottovalutata, rappresenti oggi un punto nevralgico per la protezione delle infrastrutture critiche e dei servizi digitali. Allo stesso tempo, fornisce alla comunità scientifica e ai produttori indicazioni preziose per rafforzare la resilienza delle piattaforme di calcolo, contribuendo a innalzare in modo significativo il livello di protezione dell'ecosistema digitale europeo.

Spoke

Gestione del rischio e governance

8

Coordinatore

Michele Colajanni
Alma Master Studiorum -
Università di Bologna

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

La trasformazione digitale ha portato allo sviluppo di ecosistemi sempre più complessi, in cui molteplici elementi digitali, interagendo con sistemi cyber-fisici, supportano il funzionamento dei servizi produttivi e civili di tutti gli stati. L'adozione di tecnologie sempre più sofisticate, dal cloud all'edge computing e all'intelligenza artificiale (IA), apre nuove opportunità, ma genera al contempo rischi cyber crescenti. Poiché gli ecosistemi digitali non sono isolati, un attacco informatico può produrre effetti a cascata sul piano industriale, finanziario e sociale, innescando rischi sistemici che mettono in discussione la resilienza complessiva delle società contemporanee. In questo contesto, la cybersicurezza non riguarda più solo la protezione tecnica dei sistemi, ma diventa un tema che coinvolge l'intero spettro delle politiche, della regolazione, dei diritti fondamentali e delle relazioni economiche globali.

Diventa pertanto importante porsi all''incrocio di queste sfide e sviluppare strumenti di analisi e modelli di prevenzione del rischio per rafforzare lo sviluppo sicuro dei sistemi, proporre metodologie per la gestione del rischio in settori critici, esplorare l'impatto delle politiche europee sulla cybersecurity, mirando a formare nuove competenze di gestione del rischio cyber per cittadini, tecnici ed esperti legali e politici.

Progetti

EcoCyber: Risk management for future cyber-physical ecosystems

PI: MICHELE COLAJANNI, ALMA MASTER STUDIORUM - UNIVERSITÀ DI BOLOGNA

PROTECT-IT: imPROving The rEsilience to Cyberattacks of distributed ICT InfrastrucTures

PI: ANTONIO LIOY, POLITECNICO DI TORINO

Spoke 8

SFIDE

La complessità dello scenario attuale pone numerose sfide, sia di natura tecnica sia gestionale e regolatoria.

- **Prevedere e modellare minacce emergenti**. La fase di progettazione dei sistemi deve includere strumenti per anticipare possibili attacchi. Estensioni di framework esistenti, arricchiti con pattern di attacco e profili avversari, permettono di simulare percorsi di attacco e probabilità di successo degli aggressori, fornendo una base scientifica per confrontare la sicurezza di architetture e identificare vulnerabilità critiche.
- **Gestire i rischi sistemici e finanziari**. Un attacco cyber non colpisce solo il singolo nodo, ma può propagarsi attraverso reti interbancarie o catene industriali, amplificando i danni. Servono modelli di contagio del rischio cyber in grado di integrare dimensioni economiche e digitali, insieme a strategie di mitigazione che combinino strumenti finanziari e assicurativi, allocazione ottimale degli investimenti in sicurezza e approcci difensivi innovativi, quali cyber-deception, zero-trust e il reinforcement learning applicato ai controlli di stabilità.
- **Proteggere l'industria 4.0 e i sistemi di automazione**. Gli Industrial Automation Control Systems sono al centro della trasformazione digitale, ma restano esposti a vulnerabilità critiche. La sfida è integrare metodologie di valutazione del rischio conformi a standard internazionali, includendo il coinvolgimento degli asset owner, la gestione della complessità crescente e l'adozione di contromisure su misura, come mostrato dal caso studio in un impianto a turbina a gas.
- **Sviluppare tecnologie resilienti per sistemi IoT**. La diffusione di dispositivi embedded e IoT richiede capacità di monitoraggio in tempo reale, rilevamento di anomalie e difesa da attacchi avanzati. Vi sarebbe la necessità di sviluppare stack hardware-software basati su architetture aperte, integrando remote attestation, intrusion detection e dataset sperimentali. Una sfida centrale resta l'orchestrazione sicura dei servizi di rete, attraverso l'integrazione di paradigmi di virtualizzazione SDN finora separati.
- **Integrare diritto, politiche e società**. La regolazione europea (es., Cyber Resilience Act, NIS2) ridefinisce ruoli e responsabilità di imprese e istituzioni. Ciò comporta tensioni tra sicurezza nazionale, mercato unico e tutela dei diritti civili che andranno affrontate a livello tecnico, giuridico e politico.
- **Diffondere consapevolezza e inclusione**. Una sfida cruciale è anche culturale: vi è la necessità di aumentare la consapevolezza dei cittadini, sviluppare competenze digitali e promuovere il gender balance nelle carriere tecnologiche. Solo un approccio integrato potrà garantire un ecosistema cyber-fisico realmente resiliente e democratico.

PRINCIPALI **RISULTATI**

Il progetto **Ecocyber** ha prodotto risultati significativi su tre piani complementari – tecnico, modellistico e regolatorio – che insieme contribuiscono a rafforzare la sicurezza degli ecosistemi digitali e cyber-fisici. Il progetto è partito dai rischi e dalla sicurezza dei singoli componenti, sviluppando e sperimentando strategie di monitoraggio e rilevamento di anomalie per sistemi embedded e IoT conducendo campagne sperimentali e producendo dataset e software e sviluppando un nuovo modello per garantire l'orchestrazione sicura di servizi in rete attraverso l'integrazione tra tecniche evolute di gestione, finora confinate a domini separati (SDN, Data Plane Programmability, Choreographic Programming). È stato inoltre sviluppato uno stack per un'architettura in grado di garantire l'esecuzione integra e confinata di codice, basata su componenti aperti RISC-V, OpenTitan, tecniche di remote attestation e con lo sviluppo di nuovi elementi per il kernel Linux. Sono state validate tecniche per il rilevamento in tempo reale di istruzioni malevoli su processori RISC-V e per l'analisi dell'affidabilità dei Physical Unclonable Function in presenza di guasti e stress ambientali. I metodi formali di verifica sono stati estesi a sistemi distribuiti data-intensive.

Il progetto si è poi orientato alle componenti sistemiche integrate. Nell'ambito degli Industrial Automation Control Systems, è stata proposta una metodologia di risk assessment allineata allo standard ISA/IEC 62443 ZCR 5, che integra gestione della complessità, contromisure specifiche, coinvolgimento degli asset owner e tool di supporto. L'efficacia è stata dimostrata attraverso un caso di studio in una centrale a turbina a gas. E' stata condotto anche una ricerca su un'architettura ibrida di cyber-robust Machine Learning, con l'obiettivo di valutare l'efficienza di modelli di neural networks per supervised e unsupervised learning che siano interpretabili e robusti contro rischi avversariali, mediante metodi della meccanica statistica e quantistica. Sono state sviluppate metodologie innovative per valutare e rafforzare la cybersecurity in domini critici. Sono stati applicati modelli di digital twin a infrastrutture industriali e modelli quantitativi per rilevare rischi cyber e analizzare le barriere umane nella risposta agli incidenti. Nei sistemi critici, sono stati progettati classificatori resilienti basati su machine learning con strategie di rifiuto dell'output per evitare decisioni insicure. Sono stati proposti modelli e metodi innovativi di zero trust e machine learning per il settore Industrial IoT oltre a modelli innovativi di deception basati su digital twin.

Nel dominio delle smart city, sono stati sperimentati framework basati su blockchain per il monitoraggio sicuro e la valutazione delle prestazioni degli smart contract in scenari IoT safety-critical. Nella componente modellistica, è stata proposta un'estensione del framework ADVISE Meta applicandola a un sistema di supervisione del trasporto pubblico. Tale estensione ha consentito di valutare le probabilità di successo degli avversari, i percorsi d'attacco, condurre analisi di sensitività, confrontare architetture e identificare componenti vulnerabili. Sono stati, infine, presentati modelli di cyber e financial risk contagion, insieme a strategie di mitigazione che includono strumenti finanziari progettati per rafforzare la sta-

bilità sistemica; allocazione ottimale degli investimenti in cybersecurity sui nodi della rete, sfruttando cyber-deception e security game theory; meccanismi di controllo finanziario basati su reinforcement learning.

Il progetto EcoCyber ha anche affrontato i rischi cyber in ambito giuridico e politologico producendo risultati significativi nella valutazione e nell'applicazione dei quadri normativi europei in materia di gestione del rischio cyber e del loro impatto su standard e politiche globali, relazioni economiche e rapporti tra cybersicurezza, sicurezza nazionale e sorveglianza. La ricerca ha portato anche alla realizzazione della Guida Interattiva EU Cyber Resilience Act, che offre un ausilio su come questa norma opererà nella pratica per operatori economici, consulenti legali ed esperti tecnici. Infine, sono stati approfonditi i rischi connessi alla gestione dei dati da parte delle forze dell'ordine, evidenziando le tensioni tra sicurezza, privacy e diritti civili. I membri del progetto Ecocyber hanno organizzato e collaborato a numerose iniziative di sensibilizzazione alla cybersicurezza e di formazione all'educazione digitale, anche con riferimento al gender balance.

Il progetto **PROTECT-IT** ha studiato le minacce di Internet combinando una rete distribuita di sensori con tecniche di IA, configurazione automatica delle difese e rilevamento in tempo reale di attacchi. È stata realizzata un'infrastruttura per raccogliere e condividere dati sul traffico sospetto osservato da telescopi di rete e honeypot, sviluppando metodi di apprendimento automatico capaci di riconoscere schemi nascosti, trasferire conoscenza tra reti, catturare l'evoluzione temporale dei fenomeni e integrare informazioni eterogenee. Questi approcci sono stati utilizzati per individuare attività anomale e nuove minacce, e per costruire modelli più spiegabili e trasparenti, sottolineando al contempo i limiti e i rischi di scorciatoie poco affidabili.

La piattaforma distribuita è oggi aperta ad altri partner che ospitano nodi di raccolta e utilizzano i dati per sviluppare e testare algoritmi. Su questa rete, sono stati sviluppati due servizi di protezione: REACT-VEREFOO, un meccanismo automatico di reazione che riconfigura i firewall per bloccare attacchi mantenendo i servizi essenziali, con elevate garanzie di correttezza e rapidità; un sistema per identificare in tempo reale attacchi verso nodi di rete (basandosi su root-of trust per piattaforme x86 e RISC-V). Genera report periodici sullo stato software dei nodi, analizzati da un Verificatore esterno, per rilevare modifiche o software non autorizzato e reagire (es. isolamento del nODO).

IN EVIDENZA

Il progetto ha sviluppato una piattaforma capace di identificare nuove tipologie di rischi cyber, reagire automaticamente in modo affidabile e assicurare che le infrastrutture di rete non vengano compromesse da software malevolo.

Per la fase di osservazione, è stata realizzata un'infrastruttura distribuita che raccoglie e condivide dati sul traffico sospetto osservato da telescopi di rete e honeypot, aumentando la visibilità su attività malevole provenienti dal cyberspazio. Su tali dati sono stati sviluppati algoritmi di IA capaci di riconoscere schemi nascosti, trasferire conoscenza tra reti diverse, catturare l'evoluzione temporale degli attacchi e integrare fonti eterogenee.

Queste tecniche hanno consentito di individuare attività anomale e nuove minacce, con particolare attenzione a modelli spiegabili e trasparenti. Allo stesso tempo, è stato dimostrato come l'uso di IA vada affrontato con cautela, perché i modelli possono a volte basarsi su scorciatoie poco affidabili. Per la fase di reazione, è stato progettato e realizzato un meccanismo di difesa autonoma in grado di riconfigurare dinamicamente i firewall di rete in risposta agli attacchi, anche grazie a iniziative di cyber deception basate su SDN e digital twin. Parallelamente, è stato sviluppato un sistema basato su *root-of-trust* che consente di monitorare in tempo reale l'integrità del software eseguito sui nodi di rete. Questa componente è cruciale per prevenire che un attaccante comprometta direttamente i router o altri dispositivi della rete al fine di eludere le contromisure adottate.

Spoke

Mettere in sicurezza la trasformazione digitale

9

Coordinatore

Leonardo Querzoni
Sapienza Università di Roma

La trasformazione digitale dei processi, a tutti i livelli della società moderna, porta con sé grandi opportunità, ma anche rischi che minano fiducia, resilienza e sostenibilità di prodotti e servizi. In questo contesto, la sicurezza non può essere vista come un semplice vincolo tecnico; si tratta piuttosto di una condizione abilitante per soluzioni digitali affidabili, interoperabili, efficaci. Lo scenario attuale presenta sfide fortemente eterogenee. Nel settore finanziario, l'uso crescente di distributed ledger technologies (DLT) e smart contracts apre a mercati più trasparenti, ma espone a rischi di manipolazione, scalabilità e frodi. Nelle pubbliche amministrazioni in fase di digitalizzazione, la protezione dei dati e la gestione sicura delle identità diventano cruciali per tutelare privacy e diritti dei cittadini, limitando abusi e accessi non autorizzati. Nell'ambito sanitario, la crescita della medicina a distanza amplia la superficie d'attacco: dispositivi medici e reti di sensori compromessi possono incidere direttamente sulla salute dei pazienti e sulla continuità del servizio, oltre a mettere a rischio la sicurezza dei dati personali.

Tecnologie emergenti come la quantum key distribution (QKD) promettono livelli di protezione elevati, ma pongono ancora sfide legate a integrazione e robustezza operativa che ne impediscono una immediata adozione. Rendere sicuri questi ambiti significa rafforzare la fiducia nei processi di trasformazione digitale e garantire che l'innovazione possa tradursi in servizi essenziali, resilienti e sostenibili per la società.

Progetti

ReQuS: Network for ultra-secure quantum communications

PI: ALESSANDRO ZAVATTA, CONSIGLIO NAZIONALE DELLE RICERCHE

SPEGO: Security and Privacy of E-Government

PI: MAURO CONTI, SAPIENZA UNIVERSITÀ DI ROMA

SmartDeFi: Smart Decentralized Finance

PI: DANIELE VENTURI, SAPIENZA UNIVERSITÀ DI ROMA

SuReCare: Secure Remote Healthcare for a Better Future

PI: LEONARDO QUERZONI, SAPIENZA UNIVERSITÀ DI ROMA

Spoke 9

SFIDE

Le sfide trasversali affrontate riflettono le esigenze di sicurezza dei principali settori coinvolti nella trasformazione digitale. Le attività di ricerca dello spoke si sono concentrate su queste sfide per riuscire a proporre soluzioni direttamente applicabili nei contesti di riferimento.

- **Threshold cryptography**: è una tecnica crittografica in cui un'operazione segreta (come la decrittazione o la firma) può essere eseguita solo se almeno un numero minimo prestabilito (threshold) di partecipanti collabora, senza che nessuno di essi possieda da solo l'intero segreto. Si tratta di una tecnologia destinata a diventare cruciale nei processi digitali per sostituire punti singoli di vulnerabilità con schemi distribuiti e collaborativi. Le sfide principali emergono negli scenari dinamici, dove i partecipanti possono entrare o uscire dal sistema. Qui occorre gestire in modo sicuro la riconfigurazione delle chiavi e delle politiche di accesso senza un coordinatore fidato, mantenendo forward e backward secrecy, resilienza contro avversari adattivi e scalabilità nei processi di key generation e refresh distribuiti.
- **L'IA nella digitalizzazione della pubblica amministrazione**: l'intelligenza artificiale rappresenta senza alcun dubbio una rivoluzione tecnologica che già oggi sta trasformando in modo profondo l'uso quotidiano degli strumenti informatici. L'integrazione di tali tecnologie nei processi decisionali e burocratici delle pubbliche amministrazioni pone numerose sfide. Le principali difficoltà consistono nel progettare architetture basate su IA per automatizzare procedure, garantire la conformità normativa in materia di sicurezza e privacy, e assicurare la scalabilità del sistema riducendo l'impatto sulle risorse computazionali.
- **Sicurezza dei dispositivi remoti**: i dispositivi utilizzati negli ambiti del monitoraggio a distanza devono essere progettati in modo sicuro. Questo è particolarmente vero nel contesto della telemedicina. Servono nuovi approcci per garantire l'integrità del loro software e firmware, nonché modelli efficaci per gestire aggiornamenti tempestivi nel caso in cui nuove vulnerabilità vengano scoperte.
- **Coordinamento di infrastrutture eterogenee**: il controllo e la gestione di grandi quantità di dispositivi eterogenei richiedono algoritmi robusti, capaci di mantenere l'affidabilità del sistema anche in presenza di comportamenti avversi o malevoli.
- **Tutela dei dati sensibili**: le informazioni personali e sanitarie (PII e PHI), incluse quelle raccolte da dispositivi remoti, devono essere protette da accessi non autorizzati durante tutto il loro ciclo di vita, non solo in fase di trasmissione o archiviazione.
- **Gestione del rischio in ecosistemi complessi**: garantire la sicurezza di un ecosistema composto da dispositivi, software e servizi interconnessi richiede metodologie di gestione del rischio adeguate alla natura cibernetico-fisica del contesto. Tali approcci devono essere coerenti con le più recenti normative che favoriscono la trasformazione digitale in particolare nel settore sanitario.
- **Reti per Quantum Key Distribution (QKD)**: lo sviluppo di reti su scala metropolitana e inter-metropolitana capaci di supportare la QKD si scontra con alcune limitazioni tecniche che riducono la scalabilità di tale tecnologia.. Ulteriori sfide riguardano sostenibilità, costi e interoperabilità, nonché la definizione di modelli e procedure di test per verificarne prestazioni e applicabilità su larga scala.

PRINCIPALI **RISULTATI**

Lo Spoke 9 ha conseguito risultati significativi nei quattro ambiti progettuali, contribuendo all'avanzamento di soluzioni di sicurezza per scenari digitali complessi.

Nel progetto **SmartDeFi** sono stati sviluppati i seguenti contributi principali:

- **Crittografia Avanzata per la Privacy**: Sono state sviluppate nuove tecniche crittografiche per proteggere i dati in modi più flessibili. Questo include metodi per permettere accessi granulari ai dati cifrati (cifratura funzionale e predicate encryption), sistemi per garantire che i protocolli di sicurezza non possano essere manipolati da un avversario (non-malleabilità) e prove a conoscenza zero (SNARKs/prove di conoscenza parziale) più efficienti, utili anche per la privacy nei pagamenti elettronici.
- **Sicurezza e Vulnerabilità dell'Intelligenza Artificiale**: È stata condotta un'analisi approfondita dei rischi legati ai moderni sistemi di IA. Questo comprende lo studio di nuovi attacchi (come poisoning e attacchi adversarial) specifici per Graph Neural Networks (GNN) e sistemi di raccomandazione, e lo sviluppo di contromisure come il watermarking (inserimento di "marchi" nascosti) per proteggere la proprietà intellettuale dei modelli e sistemi per rilevare malware o ransomware.
- **Spiegabilità e Trasparenza dell'IA (XAI)**: Sono stati creati nuovi metodi per rendere le decisioni dei modelli di IA più comprensibili per gli esseri umani. Un focus particolare è sull'uso delle "spiegazioni controfattuali", che mostrano quali minimi cambiamenti nei dati di input avrebbero portato il modello a una decisione diversa.
- **Analisi delle Minacce in Blockchain e DeFi**: È stato studiato l'ecosistema della finanza decentralizzata (DeFi) e delle criptovalute per identificare e analizzare attività illecite o manipolative. Questo include l'individuazione e lo studio sistematico di bot automatici che manipolano il mercato (sniper bots), truffe come i rug pull, e pratiche ingannevoli come il wash trading (compravendite fittizie) nel mercato degli NFT.
- **Verifica e Ottimizzazione del Software Quantistico**: Sono stati proposti metodi per migliorare lo sviluppo e l'affidabilità dei programmi destinati ai computer quantistici. Questo include la creazione di linguaggi di programmazione di più alto livello (come Silq), lo sviluppo di tecniche per verificare automaticamente la correttezza dei circuiti quantistici e algoritmi per

ottimizzarli (ad esempio, riducendo il numero di porte logiche necessarie).

Nel progetto **SPeGO**, con **GoTMaT** sono stati ottenuti risultati concreti che possono essere utili per la pubblica amministrazione.

- È stato creato un dataset di provvedimenti per l'addestramento di modelli di IA, mediante un processo automatizzato di acquisizione, pulizia e strutturazione dei dati provenienti da interfacce ministeriali.
- È stata progettata e addestrata un'architettura basata su Large Language Models (LLM) e Retrieval-Augmented Generation (RAG) per automatizzare le procedure burocratiche dell'area 3 (Depenalizzazione). Sebbene ancora in fase di sviluppo su un caso specifico, l'approccio è potenzialmente adattabile a diversi contesti, con possibilità di estensione tramite procedure di fine-tuning mirate.

Nell'ambito del progetto SuReCare sono stati raggiunti i seguenti risultati:

- **Analisi della Sicurezza del Software a Basso Livello**: Sono state sviluppate tecniche avanzate per trovare vulnerabilità nel software analizzandone direttamente il codice binario (eseguibile). Questo include l'uso di modelli di intelligenza artificiale per interpretare cosa fa il codice e lo sviluppo di metodi di fuzzing (test automatici e intelligenti) più efficaci per scovare errori di gestione della memoria e altre falle di sicurezza.
- **Sviluppo e Valutazione del Federated Learning (FL)**: È stata studiata l'applicazione dell'apprendimento automatico distribuito, dove i dati non vengono centralizzati. Sono state create piattaforme (workbench) per testare e confrontare le prestazioni degli algoritmi di FL e metodi per generare set di dati "non-identici" (Non-IID) che simulano scenari realistici.
- **Sicurezza delle Tecnologie Emergenti**: È stata condotta un'analisi approfondita dei rischi specifici in nuovi ambiti tecnologici. Per i droni (UAV), sono stati valutati i sistemi di autenticazione e le difese contro attacchi (es. falsificazione del segnale GPS). Per la Realtà Virtuale ed Estesa (VR/XR), sono state identificate nuove minacce alla privacy, come la possibilità di estrarre conversazioni vocali analizzando i dati provenienti da sensori apparentemente innocui (es. accelerometri).
- **Ingegneria del Software per l'IA (MLOps e AutoML)**: È stata esaminata l'intersezione tra lo sviluppo software tradizionale e l'intelligenza artificiale. Sono stati valutati i benefici e i rischi di sicurezza del ciclo di vita dei modelli di machine learning (MLOps) e l'efficacia dell'uso dell'automazione (AutoML) e della qualità dei dati nei processi di ingegneria del software.
- **Governo della sicurezza**: Sono stati sviluppati framework di sicurezza, basati su solidi standard internazionali, che colgono le peculiarità del settore sanitario e propongono controlli di sicurezza e soluzioni adatte a soddisfare i criteri imposti dalle regolamentazioni vigenti.

Infine il progetto **ReQus** ha sviluppato il design di una rete inter-metropolitana per lo scambio quantistico di chiavi. Il progetto ha acquisito gli asset necessari per poter testare tale tecnologia in un deployment realistico, che accentua la complessità implementativa, soprattutto per le tratte su lunga distanza. Una parte di tale rete è stata oggetto di implementazione e su questa sono stati sviluppati test atti a valutarne le prestazioni.

Nel complesso, i risultati dei progetti dello Spoke 9 mostrano come l'integrazione di innovazione tecnologica, metodologica e normativa consenta di affrontare in modo olistico le sfide della trasformazione digitale, rafforzando la sicurezza in settori ad alto impatto sociale ed economico.

IN EVIDENZA

Uno dei risultati più impattanti è stato ottenuto dal progetto GoTMaT attraverso lo sviluppo di un prototipo per automatizzare la generazione dei provvedimenti di area 3 (Depenalizzazione) presso la Prefettura di Padova. Questo risultato mostra concretamente come le tecnologie di IA possano alleggerire il carico burocratico, velocizzando i processi e liberando risorse umane per attività a più alto valore aggiunto. Il sistema è progettato per funzionare interamente in locale, garantendo così pieno controllo e sicurezza nella gestione dei dati personali, un aspetto cruciale quando si lavora con informazioni sensibili. Parallelamente, è in fase di sperimentazione una versione che integra modelli "quantizzati": una scelta che permette di ridurre drasticamente il fabbisogno di potenza di calcolo, aumentando al tempo stesso portabilità e scalabilità. Grazie a questo approccio, la tecnologia sviluppata non si limita ad una applicazione al caso della Prefettura di Padova, ma diventa replicabile in altri uffici pubblici, aprendo la strada a una pubblica amministrazione più efficiente, sicura e vicina ai cittadini.

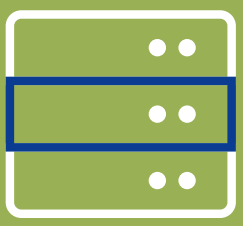
Spoke

Governance e protezione dei dati

10

Coordinatore

Pierangela Samarati
Università degli Studi di Milano



UNIVERSITÀ DEGLI STUDI DI MILANO

I progressi nel campo delle Tecnologie dell'Informazione e della Comunicazione (ICT) e la disponibilità di una varietà di collezioni di dati offrono l'opportunità di accedere facilmente ed elaborare un'enorme quantità di informazioni, ottenendo così una descrizione estremamente dettagliata del comportamento delle persone e delle attività delle organizzazioni. La disponibilità di queste collezioni di dati, insieme alla grande capacità delle moderne infrastrutture di rete e di calcolo, offre chiaramente importanti vantaggi agli utenti, alle organizzazioni e alla società in generale. La raccolta, condivisione e analisi dei dati, con il contributo di soggetti diversi, è infatti un grande fattore abilitante per una società sempre più evoluta digitalmente. Un chiaro ostacolo alla realizzazione di tale visione è rappresentato dalle preoccupazioni relative alla sicurezza e alla privacy. I dati possono essere sensibili o riservati e non essere quindi condivisibili apertamente.

Più in generale, i dati possono essere soggetti a restrizioni di accesso e utilizzo (comprese quelle derivanti dalle normative sulla protezione dei dati) e la loro riservatezza, nonché la loro integrità, dovrebbero essere garantite anche quando i dati sono memorizzati o processati da terze parti. Senza un'adeguata protezione dei dati esiste, infatti, un forte rischio di uso improprio, con minacce alla tutela della privacy dei cittadini e della riservatezza di aziende e istituzioni.

Progetti

DGDP: Data Governance and Data Protection

PI: PIERANGELA SAMARATI, UNIVERSITÀ DEGLI STUDI DI MILANO

Spoke 10

SFIDE

Per la piena realizzazione di una moderna società digitale è fondamentale fornire **soluzioni** efficaci per la **governance** e la **protezione dei dati**.

Questa sfida richiede lo sviluppo di soluzioni avanzate che consentano a diversi attori (ad es. individui, aziende e istituzioni) di **mantenere il controllo sui propri dati** in vari scenari di rilascio, condivisione e analisi delle informazioni.

Tali soluzioni devono permettere anche l'implementazione delle **restrizioni** dettate da legislazione e regolamentazioni sulla protezione dei dati (ad es., il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea) e mirare al **bilanciamento** fra la protezione dei dati da un lato e il mantenimento della funzionalità e utilità delle informazioni dall'altro.

Lo sviluppo di nuove soluzioni deve inoltre tenere conto delle caratteristiche specifiche che la gestione privata e sicura dei dati in scenari moderni ed emergenti presenta, consentendo, anche in tali contesti, la condivisione dei dati, l'analisi collaborativa e permettendo ai proprietari dei dati di mantenere il controllo.

L'evoluzione tecnologica ha reso agevolmente accessibili architetture distribuite di calcolo e memorizzazione dei dati. Le **architetture cloud** garantiscono flessibilità e economicità (rendendo la migrazione cloud una priorità per aziende ed enti pubblici), ma pongono problemi rilevanti in termini di protezione dei dati. Ad esempio, cresce il numero dei soggetti coinvolti nella gestione dei sistemi informativi che potrebbero accedere a informazioni riservate e le relazioni tra di essi diventano più articolate.

Per evitare che tali problemi possano posticipare o annullare i benefici offerti dal cloud, è necessario sviluppare soluzioni per la protezione dei dati che tengano conto della complessità di tali ambienti, al fine di consentire ai proprietari dei dati di mantenere il controllo sulle informazioni condivise.

Una ulteriore sfida è rappresentata dalle tecnologie emergenti, opportunità strategiche irrinunciabili per una società evoluta digitalmente (come testimonia il Regolamento Artificial Intelligence Act dell'Unione Europea). Tuttavia, queste tecnologie, in particolare i sistemi di **Machine Learning**, richiedendo l'accesso a grandi quantità di dati, enfatizzano i rischi legati alla condivisione delle informazioni.

Inoltre, tali tecnologie introducono vulnerabilità e problematiche nuove e peculiari. Sono quindi necessarie soluzioni di governo e protezione dei dati evolute, sviluppate per rispondere in modo specifico alla sfida rappresentata dalla diffusione dell'**Intelligenza Artificiale** (IA).

Infine, nel contesto attuale, una sfida è rappresentata anche dalla incrementata complessità delle interazioni tra i soggetti che hanno, con diversi ruoli, accesso ai dati condivisi richiedendo soluzioni innovative per la condivisione e l'utilizzo controllato dei dati.

PRINCIPALI **RISULTATI**

I ricercatori impegnati nello spoke hanno colto le sfide offerte dal contesto attuale adottando un approccio olistico, investigando diversi aspetti della governance e della protezione delle informazioni durante l'**intero ciclo di vita dei dati**.

Le attività di ricerca hanno interessato la definizione di soluzioni per la specifica di requisiti, modelli e politiche di protezione, inclusa la modellazione di dati e metadati per esprimere le proprietà che devono essere considerate per la regolamentazione dell'accesso e della condivisione. Le attività hanno inoltre interessato la definizione e lo sviluppo di tecniche innovative di protezione dei dati in considerazione anche delle garanzie di protezione e funzionalità richieste in diversi scenari.

Grazie a tale approccio, i ricercatori attivi nello spoke hanno contribuito allo sviluppo di soluzioni innovative di sanitizzazione e wrapping dei dati per consentirne la gestione privata e sicura in scenari moderni ed emergenti, abilitando la condivisione delle informazioni e l'analisi collaborativa, consentendo al contempo ai proprietari dei dati di mantenere il controllo. Tali soluzioni sono state sviluppate tenendo conto delle restrizioni all'uso dei dati derivanti da leggi e regolamenti sulla protezione dei dati e delle esigenze di aziende ed enti pubblici.

Con **più di 250 articoli scientifici pubblicati** in riviste e conferenze internazionali, il contributo dei partner impegnati nello spoke è stato ampio e articolato.

Un primo risultato raggiunto è stato il contributo fornito allo sviluppo di componenti essenziali per la gestione sicura e privata dei dati. Tale risultato ha riguardato la definizione di soluzioni per la **modellazione di dati e metadati** per esprimere le proprietà che devono essere considerate nella regolamentazione dell'accesso e della condivisione dei dati, per le relative **specifiche ontologiche** e **ragionamenti** correlati, e per l'identificazione e l'analisi dei requisiti di protezione. Un esempio è rappresentato dal sistema di estrazione della conoscenza basato sulla combinazione di modelli di embedding context-aware e tecniche di apprendimento zero-shot. Il sistema estrae progressivamente concetti rappresentativi dei diversi significati della terminologia utilizzata, un modello utilizzabile con l'obiettivo di estrarre concetti per la modellazione dei dati e la specifica dell'ontologia.

Un ulteriore risultato raggiunto dai partner dello spoke ha riguardato la definizione di soluzioni per supportare la specifica e l'applicazione di requisiti di protezione dei dati, attraverso linguaggi e modelli che consentono di esprimere e ragionare su tali requisiti, oltre a supportare la valutazione e l'amministrazione delle **politiche** di accesso ai dati. L'obiettivo è stato quello di offrire modelli flessibili, estensibili ed espressivi in grado di rappresentare i diversi requisiti di protezione dei dati.

L'area di maggior focalizzazione dello spoke ha riguardato la realizzazione di tecniche, caratterizzate in **wrapping** (reversibili) e **sanitizzazione** (irreversibili), per implementare la sicurezza e la privacy durante tutto il ciclo di vita dei dati. In particolare, sono state sviluppate soluzioni di wrapping che consentono, anche in ambienti cloud, la protezione dei dati nella loro memorizzazione

e analisi. Tali soluzioni innovative, sfruttando tecniche crittografiche, consentono di garantire al proprietario la **protezione delle informazioni in ambienti distribuiti**, ma allo stesso tempo consentono di salvaguardarne anche l'utilità funzionale. Inoltre, le soluzioni realizzate consentono al proprietario dei dati di mantenere il controllo, ad esempio fornendo la garanzia della cancellazione delle informazioni anche in ambienti distribuiti.

Le soluzioni sviluppate hanno inoltre incluso tecniche di sanitizzazione dei dati che offrono garanzie di privacy e confidenzialità misurate da opportune metriche, pur mantenendo l'utilità dei dati anche in scenari innovativi come quelli abilitati dall'IA. Ad esempio, nell'ambito dell'**addestramento** di **modelli di Machine Learning** sia supervisionati (classificazione) che non supervisionati (clustering), è stata realizzata una soluzione che, effettuando una opportuna riorganizzazione dei dati preliminarmente alla sanitizzazione, consente di soddisfare le garanzie di protezione richieste, riducendo al contempo gli impatti sull'utilità dei dati anonimizzati.

Grazie ai **bandi a cascata**, le attività di ricerca dei partner coinvolti nel progetto DGDP dello spoke hanno visto il contributo di ulteriori ricercatori oltre al già ampio network del partenariato esteso SERICS, grazie al progetto **SMIMI**. La ricerca si è concentrata sulla valutazione delle **tecnologie emergenti di gestione dei dati**, studiando l'applicazione della protezione a nuovi modelli di dati e moderne piattaforme di gestione su larga scala in scenari di collaborazione distribuiti e garantendo l'applicazione efficiente ed efficace (e quindi la scalabilità e applicabilità) delle misure di protezione, con l'obiettivo di ridurre l'impatto sulla funzionalità. Tali attività hanno portato ad avanzare la ricerca inerente alla protezione dei dati in ambiti cloud, Internet of Things, IA e Quantum Computing. Inoltre, in ambito **ricerca industriale** e sviluppo sperimentale, il bando Innovation Open Call ha consentito a una realtà privata del Mezzogiorno la realizzazione del progetto **Privacy-RAG**, riguardante lo sviluppo di tecniche innovative di protezione dei dati volte a mitigare le vulnerabilità di sistemi che sfruttano **Large Language Models** in modalità Retrieval Augmented Generation, sfruttando strumenti di Deep Learning e offuscamento dei dati.

IN EVIDENZA

L'utilizzo di architetture **cloud** offre molteplici opportunità: per la memorizzazione dei dati, per le componenti applicative, per la gestione end-to-end di interi processi.

La migrazione al Cloud è quindi una priorità per aziende ed enti pubblici.

Tuttavia, tali scenari richiedono soluzioni che consentano ai proprietari dei dati di mantenere il controllo.

La molteplicità degli scenari da gestire ha condotto alla realizzazione di una **famiglia di soluzioni modulari** implementando tecniche di wrapping e sanitizzazione.

Le soluzioni sviluppate permettono l'interrogazione di dati in scenari distribuiti che vedono il coinvolgimento di molteplici provider e permettono ai proprietari dei dati di collaborare consentendo a ciascuno un accesso selettivo e controllato alle informazioni.

Un'ulteriore soluzione riguarda il controllo dei dati in cloud, offrendo al proprietario del dato la garanzia della cancellazione delle informazioni anche in ambienti distribuiti.

I ricercatori impegnati nello spoke hanno inoltre sviluppato una soluzione basata su tecniche crittografiche per rimuovere vincoli di confidenzialità che ostacolano l'outsourcing in cloud di processi aziendali critici come gli Internal Controls and Audit.

Le soluzioni sviluppate permettono inoltre di garantire confidenzialità di informazioni sensibili o critiche in contesti di rilascio di dati e di **modelli IA**.

I risultati ottenuti sono stati presentati in riviste e conferenze primarie del settore in ambito internazionale.

ACADEMY

La SERICS Cybersecurity Academy è un progetto della Fondazione SERICS nato per rafforzare le competenze della popolazione in ambito cybersecurity, sovranità digitale e protezione dei dati. La missione dell'Academy è quella di promuovere una cultura della sicurezza informatica che possa coniugare tematiche connesse alla consapevolezza normativa e alla tutela dei diritti digitali. Tenendo conto dei fabbisogni aziendali sul territorio nazionale e delle linee guida di indirizzo elaborate dal settore pubblico, i corsi formativi progettati dall'Academy hanno l'obiettivo di rafforzare, integrare e creare nuove competenze per migliorare la sicurezza degli asset tecnologici e garantire la diffusione delle best practice nella gestione dei rischi informatici e nella tutela della sicurezza digitale, formando professionisti, ricercatori, decisori pubblici capaci di progettare, gestire e difendere infrastrutture, sistemi e dati complessi.
Al contempo, attraverso moduli formatividedicati al settore educativo e dell'istruzione primaria e secondaria, l'Academy si propone di promuovere una consapevolezza sulle opportunità e sui rischi informatici, favorendo la tutela dei più giovani.

Per rispondere a queste finalità, il progetto si articola in una pluralità di attività formative che integrano competenze tecniche e trasversali, con attenzione anche ai temi dell'imprenditorialità.

Tutte le attività previste dall'Academy sono gratuite per gli studenti in quanto realizzate nell'ambito del progetto della Fondazione SERICS.

LE ATTIVITÀ DELL'ACADEMY E I **RISULTATI RAGGIUNTI**

Rispettando e promuovendo le finalità di cui sopra, il **progetto SERICS Academy, nel suo primo anno di attività, prevedeva l'erogazione di più di 9000 ore di formazione gratuita**, da erogare entro la fine del 2025. Di seguito una descrizione sintetica delle attività dell'Academy e i risultati raggiunti.

Formazione specialistica per dipendenti e professionisti

- L'Academy offre percorsi altamente qualificati rivolti a dipendenti e professionisti, finalizzati a rispondere ai fabbisogni del mercato del lavoro attraverso l'acquisizione di competenze avanzate e l'adozione di soluzioni innovative. Attualmente l'Academy propone un catalogo composto da oltre 12 corsi, progettati ed erogati da docenti universitari ed esperti di settore, per un totale di oltre 6000 ore di formazione. I corsi sono erogati in modalità blended che prevede lezioni online e laboratori in presenza; inoltre, grazie all'attivazione di una piattaforma apposita è possibile frequentare le lezioni anche in modalità asincrona.

  Durante il primo periodo dell'iniziativa, l'Academy ha offerto corsi ad una molteplicità di professionisti e di dipendenti provenienti da circa 15 enti, sia del settore pubblico che privato, impiegati in diversi settori economico-professionali: ricerca, università, difesa, trasporti, ICT.

Promozione e supporto di scuole specialistiche di dottorato

- L'Academy ha contribuito all'erogazione, organizzazione e pianificazione di 12 scuole specialistiche di dottorato, realizzate interamente in presenza, con l'obiettivo di favorire lo scambio di conoscenze e la crescita scientifica a livello nazionale e internazionale, per un totale di più di 400 ore di formazione erogata. Le scuole hanno rappresentato un punto di incontro tra studenti e docenti provenienti da contesti accademici e professionali differenti, sia in Italia sia all'estero, creando un ambiente stimolante per la condivisione di esperienze, metodologie di ricerca e buone pratiche nel campo della cybersecurity. Le scuole sono state erogate nel periodo giugno-novembre 2025 e hanno riscontrato un grande interesse da parte degli studenti delle scuole di dottorato.

Promozione e supporto di master universitari

- Ad integrazione dell'offerta formativa proposta dagli atenei all'interno dei percorsi master di I e II livello, l'Academy offre moduli di approfondimento per gli studenti focalizzati sulla cybersecurity e sulla tutela dei diritti nel cyberspazio. Attualmente, sono stati erogati corsi in presenza presso due edizioni di master e sono disponibili sulla piattaforma dell'Academy moduli da fruire in modalità asincrona dedicati a diverse tematiche e aperti agli studenti dei corsi master, per un totale di più di 600 ore di formazione erogata.

Corsi di imprenditorialità per laureandi, neolaureati, dottorandi e neo dottorati

- Il percorso, dedicato a giovani in fase di inserimento nel mercato del lavoro, vuole essere uno strumento per supportarli in questa fase fornendo una comprensione completa del processo imprenditoriale, dalla definizione della vision e della strategia alla gestione delle risorse e dei rischi, con particolare attenzione all'integrazione delle tecnologie digitali e della sicurezza informatica nella governance aziendale.

  Gli obiettivi che si pone il corso sono orientati all'acquisizione di competenze utili per la realizzazione di un business plan in funzione della creazione d'impresa, nonché fornire conoscenze e competenze utili all'applicazione di tecniche e strumenti per la conduzione di un'impresa. Attualmente sono state erogate 4 edizioni del corso ed è ancora possibile iscriversi alle successive, per un totale di 480 ore di formazione, comprensiva di percorsi di apprendimento tramite attività di gaming.

Train the Trainers

I corsi di "formazione ai formatori" prevedono due tipologie di percorso diverse:

- Il primo percorso è dedicato agli insegnanti di scuola primaria e secondaria di primo grado con l'obiettivo di promuovere la conoscenza di competenze chiave e strategiche necessarie per rafforzare la consapevolezza e i rischi in rete. Il percorso ha l'obiettivo di supportare i docenti attraverso l'acquisizione di competenze, strumenti e metodologie utili per garantire un approccio alla rete più sicuro per gli studenti.
- Il secondo percorso si rivolge ad una platea di insegnanti, docenti, educatori, formatori, esperti ed operatori dell'apprendimento e si concentra sull'acquisizione di competenze e strumenti utili ad aumentare la propria consapevolezza sui temi della sicurezza informatica, dell'intelligenza artificiale e del diritto informatico. Il percorso ha l'obiettivo di far evolvere e consolidare le conoscenze sui temi della cybersecurity ed il rischio informatico offrendo strumenti e metodologie utili per poterle trasferire a soggetti con vulnerabilità e fragilità specifiche.

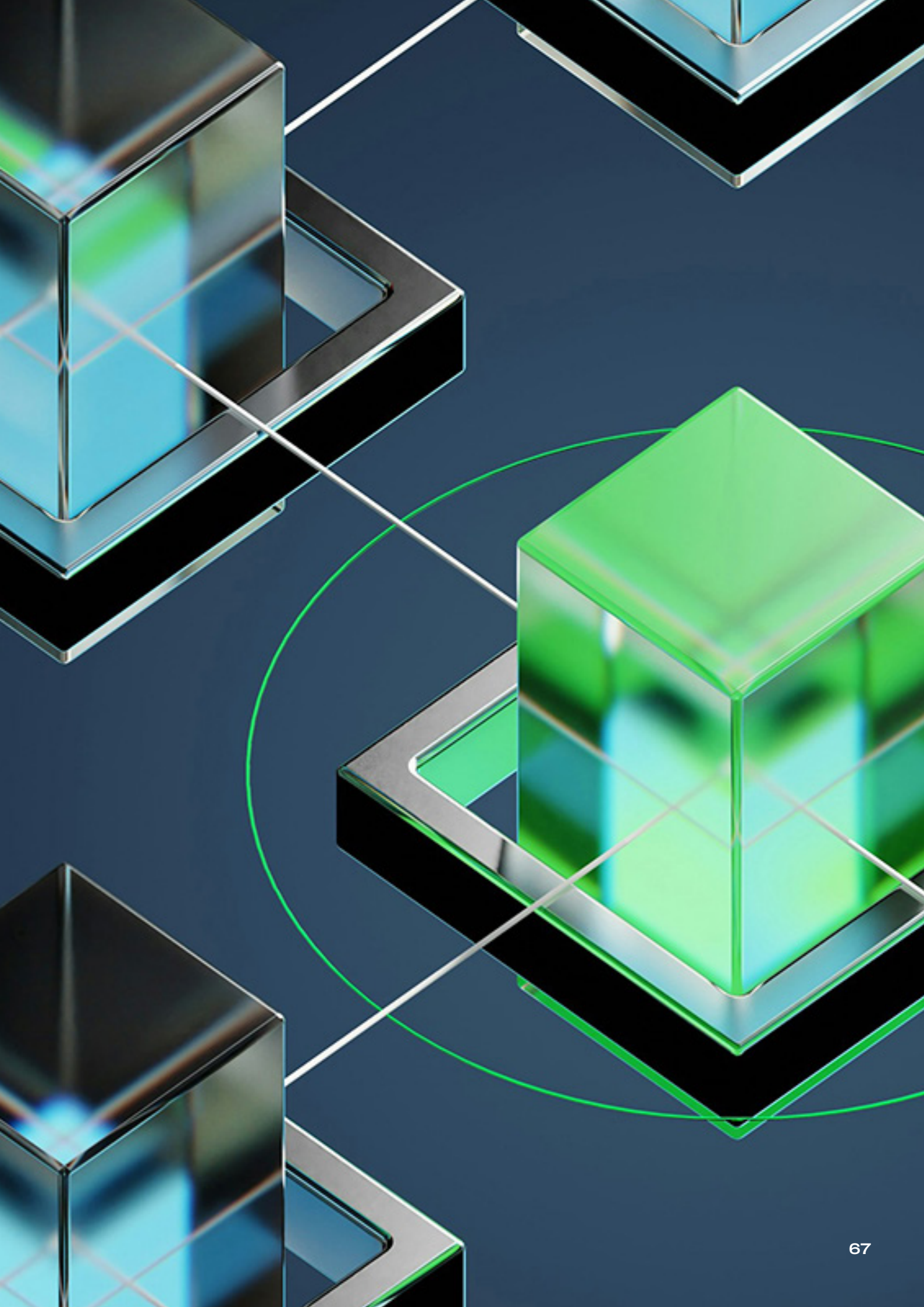
Ogni percorso ha coinvolto una platea di circa 150 partecipanti, per un totale di oltre 300 studenti complessivamente, ed è stato erogato alternando lezioni sincrone, in presenza presso alcune scuole ed attività da svolgere online, per un totale di 800 ore di formazione per ogni percorso.

TRASFERIMENTO TECNOLOGICO

Il servizio di trasferimento tecnologico sviluppato nell'ambito del Partenariato Esteso della Fondazione SERICS è stato concepito per favorire la contaminazione e la cooperazione tra ricerca e imprese. L'obiettivo è stimolare il passaggio delle innovazioni dal sistema della ricerca al tessuto produttivo, sostenere la nascita e lo sviluppo di startup e spin-off accademici, promuovere la scoperta di talenti e alimentare la cultura imprenditoriale all'interno della comunità italiana della cybersecurity.

Il modello di accompagnamento dei team di ricerca, degli spin off e delle startup ha adottato un approccio multidisciplinare: consulenti specializzati in proprietà intellettuale, mentor, esperti di mercato e advisor di business hanno contribuito a mettere a valore strumenti operativi di supporto concreti.

A questi si sono aggiunte opportunità di networking con partner industriali per la sperimentazione o la realizzazione di proof-of-concept, nonché contatti con investitori specializzati. Con l'approccio adottato è stato possibile offrire percorsi strutturati e coerenti con le dinamiche di mercato.



INIZIATIVE CONNESSE A **PROPRIETÀ INTELLETTUALE E BREVETTI**

Il servizio ha previsto due tipologie di analisi complementari: analisi di anteriorità e Freedom to Operate (FTO). Le prime hanno consentito di ricostruire lo stato dell'arte, mappare le soluzioni esistenti in diversi ambiti applicativi e individuare spazi tecnologici ancora inesplorati insieme ai driver emergenti. Le seconde hanno avuto l'obiettivo di verificare l'assenza di vincoli brevettuali che potessero ostacolare l'ingresso sul mercato di nuove tecnologie, considerando le specificità territoriali e settoriali.

Complessivamente sono state realizzate 30 analisi, riferite a molteplici ambiti della cybersecurity. Tra i temi approfonditi figurano la cognitive security, la cooperative driving, i sistemi di intrusion detection (IDS) e lo sviluppo di smart tag di tipo Hyper Physical Unclonable Function - (HPUF). È stata inoltre esplorata l'integrazione tra architetture di Software Defined Vehicles e paradigma Zero Trust, individuando le principali traiettorie di ricerca nel settore della mobilità intelligente.

Altri fronti di indagine hanno riguardato le tecnologie IMSI catcher per l'intercettazione dei segnali cellulari, l'uso dell'intelligenza artificiale nei penetration test, i nuovi metodi di watermarking per garantire l'integrità dei dati in ambito sanitario, la gestione dei dati degli account post-mortem, l'analisi e il rafforzamento dei protocolli di sicurezza delle infrastrutture critiche OT (per i sistemi di controllo e monitoraggio processi fisici, come quelli nei settori della produzione, dell'energia e dei trasporti.) per garantire la comunicazione in tempo reale tra dispositivi e l'affidabilità e la sicurezza dei processi industriali critici nella produzione industriale e PMI manifatturiere. Sono stati inoltre esaminati la protezione dei modelli di intelligenza artificiale integrati nei dispositivi in diversi ambiti applicativi, la salvaguardia dei contenuti social attraverso sistemi avanzati di watermarking.

PERCORSI DI ACCOMPAGNAMENTO E ADVISORING A TEAM DI RICERCA E START UP

Il programma di trasferimento tecnologico ha supportato 64 iniziative, tra idee progettuali, team di ricerca e imprese in fase di avvio. Fra queste, 28 iniziative - tra gruppi informali, startup e spin-off - hanno preso parte ad un percorso strutturato di accelerazione che ha combinato momenti di formazione con sessioni di mentorship. Tutte hanno ricevuto assistenza personalizzata.

Le iniziative accompagnate si concentrano su alcuni cluster tematici principali: sicurezza delle infrastrutture critiche e degli ambienti OT/IIoT, protezione dei modelli e dei dati in ambito AI, threat intelligence e gestione del rischio, mobilità connessa e software-defined vehicles, compliance dei sistemi aziendali alla direttiva NIS2 e AI Act e servizi per la pubblica amministrazione. Inoltre, sono stati seguiti progetti relativi all'integrità dei contenuti social, alla sicurezza dei dispositivi embedded, al cloud-edge e DevSecOps.

Nei contesti OT/IIoT emergono progetti che combinano monitoraggio di rete e rilevazione di anomalie per il settore manifatturiero, con l'obiettivo di ridurre tempi di fermo e superficie d'attacco lungo la filiera. Nella mobilità connessa si osservano soluzioni orientate alla sicurezza dei protocolli di autenticazione multi-fattore V2I.

Nel dominio telco si sono sviluppate iniziative dedicate alla protezione dell'identità e all'analisi del rischio derivante da tecniche di intercettazione della segnalazione mobile e all'analisi delle vulnerabilità delle eSim.

Il livello di maturità tecnologica dei team accompagnati risulta eterogeneo. La maggior parte delle iniziative riguarda attività collocate a cavallo tra la fase di ricerca di base e concettualizzazione e quella di sviluppo e validazione tecnologica. Alcune iniziative molto promettenti si trovano già nella fase di dimostrazione e utilizzo operativo.

La metodologia di accompagnamento è stata strutturata in sessioni di lavoro dedicate e momenti di brainstorming finalizzati a trasferire cultura d'impresa, sviluppare il pensiero critico sul potenziale commerciale delle soluzioni e far comprendere l'importanza della centralità del cliente, delle dinamiche competitive e della costruzione di un business model coerente.

I team sono stati guidati nell'identificazione del mercato di riferimento. L'approccio lean ha offerto un ciclo pragmatico Build–Measure–Learn, utile a ridurre il rischio e a validare rapidamente le ipotesi.

In chiave operativa sono stati condotti workshop individuali di co-progettazione, focalizzati sul Business Model. Sono stati realizzati cicli di design thinking facilitati da mentor senior, lavorando dal cuore della value proposition fino alla costruzione dei nove blocchi canonici del Business Model Canvas.

Accanto ai percorsi formativi e di mentorship, i gruppi di ricerca, le startup e gli spin off hanno potuto beneficiare dell'erogazione di servizi specialistici finalizzati al rafforzamento della proposta di business, alla verifica della fattibilità di mercato, alla realizzazione di Proof of Concept. Sono stati realizzati nel complesso 52 servizi di advisoring specialistico tra analisi di mercato, benchmarking, definizione di strategie go-to-market, ricerca investitori e partner per sperimentazioni in ambiente reale, scouting di opportunità di finanziamento e pianificazione economico-finanziaria.

ATTIVITÀ DI OPEN INNOVATION, SFIDE, SPERIMENTAZIONI, TRASFERIMENTO ALLE IMPRESE

In continuità con i percorsi di advisory e con il confronto avviato in seno all'Innovation Board quale luogo di incontro con i partner industriali e istituzionali, la Fondazione SERICS ha strutturato un programma di open innovation finalizzato a connettere i fabbisogni degli attori pubblici e privati con le capacità della comunità di ricerca, delle startup e degli spin-off dell'ecosistema.

In questo ambito è stata lanciata la Cybersecurity Technology Challenge finalizzata alla co-creazione di soluzioni

volte a preservare la sicurezza cibernetica delle istituzioni. Sviluppata in collaborazione con la Regione Toscana, la challenge riguarda, nello specifico, l'ottimizzazione delle configurazioni dei Web Application Firewall, l'impiego dell'intelligenza artificiale nella Cyber Threat Intelligence e lo sviluppo di metodologie di penetration testing a minimo impatto sui sistemi in produzione.

Parallelamente sono state avviate sei sfide di open innovation, progettate per far emergere ipotesi di soluzione agili e realizzabili in tempi brevi in risposta ai fabbisogni dei player industriali, per favorire meccanismi di collaborazione attiva tra il sistema produttivo e la comunità di ricerca. Le sfide, di fatto, ideate a partire da esigenze operative reali segnalate da grandi operatori nazionali, partner della Fondazione SERICS, mirano a favorire l'incontro tra domanda industriale e offerta di ricerca di alto livello, promuovendo un trasferimento tecnologico rapido e qualificato all'interno dell'ecosistema SERICS.

Partecipano alle sfide come "solver/solutori" team di ricerca (docenti, ricercatori, dottorandi e collaboratori di università e centri pubblici partner di SERICS) e spin-off accademici riconosciuti, mediante la formulazione di proposte (relazioni, presentazioni/slide, prototipi, POC, ecc.) relative alla soluzione del problema individuato, ai risultati attesi / realizzabilità (a 3 mesi, a lungo termine), alle modalità di gestione dei diritti IP (brevetti, know-how) impiegati.

Nel dettaglio le 6 sfide di Open Innovation affrontano criticità per la resilienza e la competitività in diversi ambitii:

- **Cybersecurity & Digital Transformation in Banking**: focalizzata sull'operatività cloud e mobile nel settore finanziario. Si cercano soluzioni di difesa automatizzata, strumenti di decision support spiegabili (per la governance del rischio), modelli per la rilevazione delle frodi cognitive e algoritmi di crittografia post-quantum.
- **Sicurezza Semplice**: L'obiettivo è ottimizzare la protezione di dati e transazioni nei servizi ad alto impatto (finanziari e logistici) garantendo una user experience rapida e trasparente. L'attenzione è posta sulla protezione di dati e transazioni, sui meccanismi di autenticazione e privacy semplificati, e sul contrasto alle frodi digitali e cognitive che manipolano psicologicamente i clienti.
- **Cybersecurity Marittima**: rilevamento delle anomalie di bordo: soluzioni innovative per la rilevazione tempestiva di comportamenti anomali e minacce cyber sui sistemi IT e OT di bordo nave, anche in contesti multi-nave e multi-flotta, con fonti eterogenee di dati del dominio marittimo, e modalità non invasive, compatibili con sistemi legacy e capaci di bilanciare precisione e tempestività.
- **Gestione intelligente delle vulnerabilità in ambito industriale**: L'obiettivo è ridurre l'impatto economico e operativo delle attività di mitigazione dei rischi su infrastrutture estese. La sfida è centrata sulla proposta di un algoritmo di prioritizzazione che bilanci in modo motivato il costo di intervento e il rischio residuo.
- **Gestione avanzata dei plugin dei browser aziendali**: la sfida mira a ridurre il rischio di incidenti di sicurezza causati dagli add-on dei browser usati da migliaia di dipendenti nel contesto di un grande operatore industriale. La soluzione deve permettere l'identificazione e categorizzazione dei plugin e l'abilitazione di sistemi di scansione, monitoraggio e rimozione selettiva.
- **Sicurezza sistemi industriali IoT**: Rivolta a grandi imprese operanti in settori industriali critici (energia, aerospazio, difesa). L'obiettivo è individuare soluzioni di cybersecurity modulari e scalabili per la protezione di sensori, attuatori e sistemi di automazione critici, garantendo interoperabilità e facilità di gestione in ambienti distribuiti e mission-critical.

RELAZIONE **ECOSISTEMICA**

Le attività di trasferimento tecnologico hanno contribuito a costruire un canale stabile di dialogo tra il sistema della ricerca e le imprese, generando tre effetti concreti. In primo luogo, la valorizzazione dei risultati prodotti dagli Spoke, con il loro riconoscimento come asset utili anche oltre l'ambito accademico. In secondo luogo, la traduzione dei progetti in soluzioni operative, capaci di rispondere a fabbisogni reali del mercato. Infine, l'apertura di spazi di co-sviluppo tecnologico e formativo all'interno dell'ecosistema nazionale dell'innovazione.

Questo approccio ha permesso di avviare sperimentazioni in ambienti reali di soluzioni inizialmente sviluppate in laboratorio, in linea con la terza missione universitaria, la tutela degli asset e l'orientamento al mercato. Lo sforzo progettuale e le relative azioni di trasferimento e sperimentazione intendono cambiare il paradigma nelle relazioni tra mondo della ricerca e sistema produttivo, abilitando nel medio termine, la ricerca scientifica come motore di innovazione applicata e propulsiva in una logica di sistema.

L'ecosistema SERICS in un'unica dashboard: esplorazione interattiva di progetti, partner e risultati.

RINGRAZIAMENTI

Si ringraziano l'ing. Luca Romanelli, Program Research Manager del Partenariato Esteso SERICS, la dottoressa Filomena Annarumma dell'Ufficio di Coordinamento attività per il PNRR dell'Università degli Studi di Salerno, e il team di supporto tecnico specialistico della Fondazione SERICS, composto da Vincenzo Aquino, Teresa Orza, Ilaria Polito e Silvia Salemi, per il prezioso contributo fornito, la professionalità e la costante collaborazione dimostrata nel corso dello sviluppo del progetto.

Un sentito ringraziamento è inoltre rivolto al Ministero dell'Università e della Ricerca per il sostegno, la disponibilità e la collaborazione che hanno reso possibile la realizzazione delle attività progettuali.