UNIVERSITÀ DEGLI STUDI DI GENOVA
AREA RICERCA, TRASFERIMENTO TECNOLOGICO E TERZA MISSIONE
SERVIZIO RICERCA
SETTORE RICERCA NAZIONALE

IL RETTORE

Vista la Legge 9 maggio 1989, n. 168 - Istituzione del Ministero dell'Università e della ricerca scientifica e tecnologica e ss.mm.ii;

Visto lo Statuto dell'Università degli Studi di Genova;

Visto il Regolamento Generale di Ateneo;

Visto il Regolamento di Ateneo per l'Amministrazione, la Finanza e la Contabilità;

VISTA la legge 7 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" pubblicata sulla Gazzetta Ufficiale n. 192 del 18/08/1990 e s.m.i.;

VISTO il Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Disposizioni legislative in materia di documentazione amministrativa) e s.m.i.;

VISTO il Decreto Direttoriale MUR n. 341 del 15/03/2022 di emanazione di un Avviso pubblico per la presentazione di Proposte di intervento per la creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU";

VISTO il Decreto Direttoriale MUR n. 1556 dell'11 ottobre 2022 Codice identificativo PE00000014, Acronimo SERICS, Titolo "SEcurity and RIghts in the CyberSpace" (CUP D33C22001300002) registrato alla Corte dei Conti il 04/11/2023 n. 2783 e relativi allegati;

CONSIDERATO che l'Università degli Studi di Genova è leader dello Spoke 4, dal titolo "Operating Systems and Virtualization Security";

CONSIDERATO che gli Spoke possono emanare - nell'ambito dei limiti e con le modalità previste dall'Avviso - "bandi a cascata" finalizzati alla concessione di finanziamenti a soggetti esterni per attività coerenti con il progetto approvato;

VISTA la delibera della seduta del 20 dicembre 2023 con cui il Consiglio di Amministrazionedell'Università degli Studi di Genova ha approvato l'emanazione del bando a cascata per organismi di ricerca nell'ambito del Progetto SEcurity and RIghts in the CyberSpace (SERICS) - PNRR M4C2 per lo Spoke 4;

VISTO il Decreto del Direttore Generale n. 5418 del 14 novembre 2023 di nomina del Responsabile del Procedimento;

VISTO il Decreto del Rettore n. 11 del 8 gennaio 2024 di emanazione del Bando a cascata per il finanziamento di proposte di intervento per attività di ricerca svolte da Organismi di Ricerca nell'ambito del programma di ricerca PE "SEcurity and RIghts in the CyberSpace - SERICS", per lo Spoke 4 dal titolo "Operating Systems and Virtualization Security", nell'ambito del PNRR, Missione 4, Componente 2, Investimento 1.3 – finanziato

dall'Unione europea – NextGenerationEU (CUP D33C22001300002);

CONSIDERATO che alla data di scadenza per la presentazione delle proposte progettuali, fissata entro e non oltre il giorno 8 febbraio 2024, per la **Tematica A - NEXT GENERATION CYBER RANGES** era pervenuta a mezzo PEC all'indirizzo air3@pec.unige.it la seguente proposta in forma collaborativa:
PROPONENTE: Università degli studi di Verona - Prot. 8416 del 07.02.2024
TITOLO PROPOSTA: NoMeN - Novel Methodologies and Tools for Next Generation Cyber Ranges

TENUTO CONTO che la Responsabile del procedimento, Ing. Patrizia Cepollina, ha ritenuto ricevibile, ammissibile e conforme la proposta sopra citata;

CONSIDERATO che nel Bando è previsto che la valutazione di merito tecnico-scientifico dei progetti pervenuti sia affidata ad una Commissione composta da almeno tre esperti esterni al Partenariato, indipendenti e competenti dell'Area tematica dello Spoke;

VISTO l'estratto del Verbale della Riunione del 16 gennaio 2024 del Comitato Scientifico del programma di ricerca "SEcurity and RIghts in the CyberSpace - SERICS" che ha approvato e aggiornato la "Rosa di Candidati" per le Commissioni di Valutazione dei Bandi a cascata sul Programma SERICS;

VISTA la nota prot. 15152 del 28 febbraio 2024 con cui il Prof. Alessandro Armando, Responsabile Coordinatore Scientifico dello Spoke n. 4 "Sicurezza dei Sistemi Operativi e della Virtualizzazione" del Programma di ricerca PE SERICS ha proposto come componenti della Commissione di Valutazione i nominativi dei proff. Canini, Pellegrino e Viganò, scelti nell'ambito della Rosa dei candidati di cui sopra, in qualità di ricercatori indipendenti e di indubbio profilo internazionale, con grande esperienza sulla Cybersecurity e, più specificatamente, sui temi di ricerca sviluppati nello Spoke n. 4;

VISTO il D.R. n. 1042 del 29 febbraio 2024 con cui è stata nominata la Commissione di valutazione delle proposte pervenute in risposta al bando a cascata di cui al Decreto del Rettore n. 11 del 8 gennaio 2024, indicato nelle premesse del presente decreto;

ACQUISITO il verbale della Commissione di Valutazione della seduta del 4 aprile 2024 (Prot. 28145 del 08 aprile 2024);

VISTO il D.R. n. 1763 del 10 aprile 2024 con cui è stata approvata la graduatoria di merito per la Tematica A - NEXT GENERATION CYBER RANGES di cui al bando a cascata di cui al Decreto del Rettore n. 11 del 8 gennaio 2024, indicato nelle premesse del presente decreto;

TENUTO CONTO che in data 12 aprile 2024 è stata inviata all'Università degli Studi di Verona la comunicazione Prot. 30390 in cui si rendevano noti gli esiti della procedura e si richiedeva la documentazione propedeutica all'adozione del provvedimento di ammissione del finanziamento;

TENUTO CONTO che la documentazione, ricevuta dall'Università degli Studi di Genova con note prot. n. 36150 del 30 aprile 2024 e n. 38279 del 7 maggio 2024, è stata ritenuta conforme a quanto previsto nel bando a cascata di cui al Decreto del Rettore n. 11 del 8 gennaio 2024, indicato nelle premesse del presente decreto,

DECRETA

ART. 1

L'ammissione a finanziamento del progetto "NoMeN - Novel Methodologies and Tools for Next Generation Cyber Ranges" per la **Tematica A - NEXT GENERATION CYBER RANGES** con soggetto proponente Capofila

l'Università degli studi di Verona - come rappresentato negli Allegati B e C alla proposta presentata con domanda di partecipazione Prot. 8416 del 07.02.2024.

ART. 2

L'entità dell'agevolazione concessa, a fondo perduto, ammonta a 784.300 euro complessivi come rappresentati nell'allegato C alla proposta presentata con domanda di partecipazione Prot. 8416 del 07.02.2024. L'agevolazione è pari al 100% dei costi di progetto trattandosi di attività di ricerca fondamentale per Organismi di Ricerca. L'agevolazione è concessa a valere sui fondi PNRR - Programma "SEcurity and RIghts in the CyberSpace (SERICS)" Codice PE00000014 finanziato dalla Missione 4, Componente 2, Investimento 1.3, ai sensi del Decreto di concessione n. 1556 dell'11 ottobre 2022, registrato alla Corte dei Conti il 04/11/2023 n. 2783 iscritto al Bilancio di Ateneo sul progetto UGOV 100023-2022-AA-PNRR-SERICS_BANDI_A_CASCATA_DIP (CUP D33C22001300002).

ART. 3

Le attività, come indicate dettagliatamente nell'Allegato B alla domanda di finanziamento, dovranno essere avviate a partire dalla data di sottoscrizione del Contratto e concluse entro e non oltre il 22 novembre 2025 affinché siano rendicontate in tempo utile per consentire la chiusura del Programma PE SERICS il cui termine è attualmente previsto al 31 dicembre 2025.
Potrà essere valutata e concessa una sola proroga in presenza di ritardi dovuti a circostanze eccezionali e non dipendenti da scelte del Beneficiario esclusivamente nel caso in cui il MUR, a sua volta, proroghi il termine del Programma SERICS

ART. 4

Il presente atto sarà pubblicato sul sito UniGe https://unige.it/progetti-finanziati-dal-pnrr e sul sito https://serics.eu.
Il documento informatico originale sottoscritto con firma digitale sarà conservato presso l'Area Ricerca, Trasferimento Tecnologico e Terza Missione.

Allegati:
Allegato B – Proposta progettuale
Allegato C – Piano economico-finanziario

IL RETTORE
Prof. Federico DELFINO
(documento firmato digitalmente)

ALLEGATO B

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

PE00000014 PE7
"PNRR MUR - M4C2 - SERICS - SEcurity and RIghts in the CyberSpace (SERICS)"

SPOKE N. 4

Research proposal

Next Generation Cyber Ranges

NoMeN-
Novel Methodologies and Tools for Next Generation Cyber Ranges

Durata del progetto: 18 mesi

ROLE IN THE PROJECT	*NAME*	*SURNAME*	*INSTITUTION/ DEPARTMENT*	*QUALIFICATION*	*YOUNG (under 40 al 31.12.2023)*	*F/M*
Principal Investigator	*Massimo*	*Merro*	*UNIVR/Dip. di Informatica*	*Professore Ordinario*	*No*	*M*
co- Principal Investigator (PI)	*Alessio*	*Merlo*	*Centro Alti Studi per la Difesa*	*Professore Ordinario*	*No*	*M*
Membro di unità	*Ferdinando*	*Cicalese*	*UNIVR/Dip. Di Informatica*	*Professore Ordinario*	*No*	*M*
Membro di unità	*Roberto*	*Segala*	*UNIVR/Dip. di Informatica*	*Professore Ordinario*	*No*	*M*
Membro di unità	*Damiano*	*Carra*	*UNIVR/ Dip. Di Informatica*	*Professore Associato*	*No*	*M*
Membro di unità	*Matteo*	*Cristani*	*UNIVR/ Dip. Di Informatica*	*Professore Associato*	*No*	*M*

Membro di unità	*Giuditta*	*Franco*	*UNIVR/ Dip. di Informatica*	*Professoressa Associata*	*No*	*F*
Membro di unità	*Zsuzsanna*	*Liptak*	*UNIVR/ Dip. di Informatica*	*Professoressa Associata*	*No*	*F*
Membro di unità	*Isabella*	*Mastroeni*	*UNIVR/ Dip. di Informatica*	*Professoressa Associata*	*No*	*F*
Membro di unità	*Barbara*	*Oliboni*	*UNIVR/Dip. di Informatica*	*Professoressa Associata*	*No*	*F*
Membro di unità	*Federica Maria Francesca*	*Paci*	*UNIVR/ Dip.di Infomatica*	*Professoresa Associata*	*No*	*F*
Membro di unità	*Elisa*	*Quintarelli*	*UNIVR/ Dip. di Informatica*	*Professoressa Associata*	*No*	*F*
Membro di unità	*Daniela*	*Irrera*	*Centro Alti Studi per la Difesa*	*Professoressa Ordinaria*	*No*	*F*
Membro di unità	*Nicola*	*Colacino*	*Centro Alti Studi per la Difesa*	*Professore Associato*	*No*	*M*
Membro di unità	*Andrea*	*Bernardi*	*Centro Alti Studi per la Difesa*	*Professore Associato*	*No*	*M*
Membro di unità	*Davide*	*Verzotto*	*Centro Alti Studi per la Difesa*	*Ricercatore T.D. a*	*Si*	*M*
Membro di unità	*Carlo*	*Bongioanni*	*Centro Alti Studi per la Difesa*	*Ricercatore T.D. a*	*No*	*M*

ABSTRACT

L'attività di ricerca si propone di affrontare due obiettivi principali all'interno del progetto ARTIC, ovvero 1) lo studio, la selezione, e la definizione di tecnologie di virtualizzazione e containerizzazione per la realizzazione di Cyber Range che siano economici e scalabili e, 2) l'analisi e la definizione di nuovi verticali e use case per simulazioni ed esercitazioni basate su Cyber Range focalizzate sulla protezione delle infrastrutture critiche, con particolare di riferimento agli honeypot per sistemi di controllo industriali e alla rilevazione di attacchi in ambito OT basati su tecniche di intrusion detection.
Riguardo il primo obiettivo di ricerca, il progetto si propone di realizzare in primis uno studio esaustivo delle attuali tecniche di virtualizzazione e containerizzazione che siano utilizzabili per una facile ed efficiente realizzazione e manutenzione di Cyber Range. Inoltre, si propone di supportare sia l'implementazione delle stesse in un PoC di un CR, che la definizione di use case per il testing dello stesso PoC, al fine di valutare sperimentalmente l'efficacia delle tecnologie di virtualizzazione/containerizzazione selezionate.
Riguardo il secondo obiettivo, l'attività di ricerca si focalizzerà sulla definizione di nuovi verticali in ambito OT, con particolare riferimento ai sistemi di controllo industriali (Industrial Control Systems - ICS) che possano costituire nuovi scenari applicativi ed esercitativi per i Cyber Range. Nello specifico, la ricerca verterà sullo studio di ICS honeypot scalabili ed estendibili, nonché sulla definizione e realizzazione di sistemi di intrusion detection per sistemi OT integrabili all'interno di un Cyber Range. Infine, l'attività di ricerca si focalizzerà sul supporto alla definizione di ulteriori use case esercitativi interessanti per un Cyber Range, che coinvolgano in particolare la parte OT e, nello specifico, honeypot ICS e sistemi di intrusion detection.

PROPOSTA DI RICERCA
Sezione a. Stato dell'arte e obiettivi

Contesto e stato dell'arte:

I Cyber Range (CR) sono piattaforme emergenti per la generazione di diversi scenari virtuali che riproducano corrispondenti scenari reali al fine di svolgere su una infrastruttura virtualizzata attività critiche che non potrebbero essere replicate sulle controparti reali. A differenza dei Digital Twins [1], il principale utilizzo dei CR è attualmente a fini di training del personale, soprattutto in ambito cybersecurity [2], dove il CR replica quanto più fedelmente possibile, spesso in maniera automatica e verificata [3], strutture ICT realistiche, dove team di utenti possono simulare sessioni di attacco e difesa senza compromettere le strutture reali.

Seppur la tecnologia dei CR, e lo sviluppo degli stessi sia in continua evoluzione, la stessa è ancora limitata e i CR vengono spesso sviluppati e mantenuti da grossi player quali Cogent [4], Antisyphon [5], Cisco Talos [6], solo per citarne alcuni. Il principale problema che limita lo sviluppo dei CR "in the wild" è il costo che richiede, sia in termini economici per la realizzazione delle infrastrutture alla base dei CR, che di personale, per la manutenzione/gestione degli stessi durante le attività di training e simulative [7].

Tuttavia, negli ultimi anni lo sviluppo di tecnologie di virtualizzazione e containerizzazione promettenti come, ad esempio, Docker [8] ed i Linux Container (LXC) [9], e la definizione ed implementazione di software per la generazione e il deployment automatico di tali tecnologie (e.g., Docker Compose [10], Kubernetes [11]), forniscono un supporto per l'automatizzazione in fase di deployment e possono contribuire a semplificare la gestione da parte degli operatori umani.

Pertanto, è importante considerare l'utilizzo di queste soluzioni come "enabling technologies" per la realizzazione di futuri CR che siano economici e facilmente gestibili, in modo che possano scalare verso un utilizzo da parte di una sempre crescente mole di utenti.

Oltre alla realizzazione di un CR, un altro problema di ricerca è l'estensione delle modalità di utilizzo dei CR, oggi principalmente focalizzati solo su alcuni specifici aspetti delle infrastrutture informatiche, con un'attenzione particolare alle diverse interazioni IT che il sistema può avere con l'attaccante. In tale contesto, un utilizzo classico dei CR è la simulazione di scenari di tipo Capture-the-Flag su repliche di infrastrutture ICT reali, dove gruppi di studenti attaccano (Red Team) o difendono (Blue Team).

Tuttavia, le minacce informatiche stanno prendendo sempre più di mira i sistemi di controllo industriale (ICS) che spesso gestiscono infrastrutture critiche, come la distribuzione e la depurazione delle acque, la generazione e la distribuzione dell'energia elettrica, la generazione di energia nucleare, etc. Queste strutture sono state considerate per lungo tempo sicure perché difficilmente accessibili. Purtroppo, da quando le organizzazioni industriali hanno iniziato a connettere la loro rete di tecnologia operativa (OT) con le reti aziendali per migliorare l'efficienza aziendale e operativa, i sistemi di controllo industriale si sono ritrovati esposti ad una nuova categoria di attacchi, chiamati attacchi ciberfisici [12], nei quali violazioni della sicurezza nello spazio cyber (magari sfruttando vulnerabilità note IT) consentono l'accesso e quindi la manipolazione dei processi fisici produttivi (possibilmente sfruttando vulnerabilità OT). Questi attacchi, per loro natura, sono ben diversi dagli attacchi IT: l'obiettivo principale dell'attaccante non è in generale il dato, qualunque esso sia, ma la manipolazione del processo fisico target, manipolazione che dipende dalla natura del processo e che sicuramente richiede conoscenze adeguate per raggiungere i traguardi preposti dall'attaccante (non basta raggiungere un controllore, poi bisogna capire come modificare i suoi comandi per raggiungere l'effetto desiderato sul processo fisico gestito dal controllore).

Quindi una naturale estensione da considerare nell'ambito dei CR è la capacità di emulare le reti OT di sistemi industriali, insieme ai dispositivi ad esse connessi (PLC, RTU, HMI, etc) attraverso protocolli di rete industriali spesso privi di misure basilari di protezione come l'autenticazione della comunicazione. In tal senso, si rende necessaria la definizione di verticali specifici del contesto OT, dove poter simulare situazioni di attacco/difesa complessi, realistici ed attuali.

Al fine di studiare gli attacchi cyber-fisici contro ICS e i suoi dispositivi, negli ultimi anni sono stati proposti diversi honeypot industriali, comunemente chiamati ICS honeypot. Gli honeypot sono sistemi vulnerabili configurati dai difensori per fornire informazioni dettagliate sulle attività dell'aggressore e per difendersi o rallentare gli attacchi in corso. Lo sviluppo di honeypot industriali realistiche ed efficaci da integrarsi nei CR di prossima generazione rappresenta un contributo cruciale anche per: (i) l'esplorazione di possibili nuovi

vettori di attacco ciberfisici, (ii) sviluppare le tecniche di detection per individuare tali attacchi nel più breve lasso di tempo possibile; (iii) sviluppare delle tecniche di mitigazione per isolare o neutralizzare l'attività di agenti malevoli che hanno guadagnato accesso alla rete OT.

In breve, una honeypot è un sistema di sicurezza informatica che ospita ambienti virtuali in grado di emulare dispositivi hardware e software. Honeypot di diversa natura possono essere utilizzate per deviare l'attenzione dell'attaccante dal sistema reale e per studiare i modelli di attacco al fine di selezionare adeguate contromisure. Un sistema composto da due o più honeypot è chiamato honeynet. Negli ultimi anni, a seguito di numerosi attacchi cibefisici è cresciuto l'interesse verso lo sviluppo di honeypot per sistemi industriali, spesso chiamate ICS honeypot. Numerose ICS honeypot presenti in letteratura si basano su Conpot [13], una low-interaction honeypot open source. Conpot supporta diversi protocolli industriali, tra cui Modbus, S7comm, EtherNet/IP e BACnet, e protocolli di rete come HTTP, FTP, SNMP, IPMI e TFTP. A titolo di esempio, Pliatsios et al. [14] presentano un honeypot a bassa interazione che emula una centrale idroelettrica con dispositivo RTU in comunicazione con interfacce HMI reali e virtualizzate. Ferretti et al. [15] dispiegano una serie di honeypot che emulano il comportamento di diversi tipi di dispositivi e protocolli industriali.

Altre ICS honeypot si basano su Honeyd [16], una piattaforma open source per la creazione di honeypot a bassa interazione e scalabili. Honeyd consente la creazione di honeypot virtuali con l'eventuale integrazione di dispositivi fisici. A titolo di esempio, HoneyPLC [17] è un honeypot estensibile in grado di emulare un'ampia gamma di modelli di PLC. Conti et al. [18] estendono HoneyPLC con una simulazione semplificata del processo di trattamento dell'acqua. Di recente Lucchese et al. [19,20,21] hanno proposto HoneyICS, un honeypot physic-aware che consente la manipolazioni di registri delle PLC e attacchi MITM sul protocollo industriale Modbus/TCP. Tra gli honeypot ICS basati né su Conpot né su Honeyd, spicca il lavoro di Antonioli et al. [22] che simula una stazione di trattamento dell'acqua.

In generale, vista l'elevata esposizione ad attacchi esterni, le honeypot rappresentano una posizione privilegiata per la dislocazione di meccanismi di intrusion detection. Le tecniche standard di rilevamento delle intrusioni per gli ICS si basano su stime di stato per rilevare anomalie nei processi (vedi, ad esempio, [23]). Un'anomalia viene osservata se l'errore residuo supera una soglia predefinita. Tuttavia, poiché esistono varie fonti di rumore nei processi industriali, una soglia fissa tra misurazioni sensoriali normali e anomale è di solito difficile da trovare. Un approccio più efficiente si basa sulla verifica di invarianti di sistema [24]. Tali IDS utilizzano condizioni fisiche conosciute a priori e che devono valere per tutti gli stati raggiungibili dal sistema industriali. Tutti i valori fisici del processo osservati che violano queste regole vengono classificati come possibili intrusioni. IDS basati su invarianti possono essere trovati nelle versioni recenti del sistema di trattamento dell'acqua sicura (SWaT) [25] al centro di una serie di esercitazioni annuali di difesa cibernetica-fisica, note come "Critical Infrastructure Security Showdowns" (CISS) [26].

Obiettivi di ricerca:

Riguardo l'utilizzo di tecnologie di virtualizzazione/containerizzazione che possano rendere "affordable" i futuri CR, l'attività di ricerca del progetto si focalizza su tre obiettivi principali, da inquadrarsi nell'ambito del Task 1.3 del progetto ARTIC:

1. Studio e selezione di tecnologie di containerizzazione e virtualizzazione esistenti che supportino i requisiti ed i design patterns di un framework CR come definito nel Task 1.1. del progetto ARTIC che garantiscano tre requisiti, ovvero 1) affidabilità, 2) scalabilità e 4) un basso costo di realizzazione/gestione e mantenimento.
2. Supporto all'implementazione, integrazione e validazione in un PoC di CR delle tecnologie di containerizzazione e virtualizzazione selezionate nell'obiettivo 1. Lo scopo di questa attività è verificare l'effettiva garanzia dei tre requisiti definiti in precedenza nell'implementazione di un CR reale.
3. Supporto alla definizione di use case interessanti per il PoC sviluppato, che coinvolgano profusamente le tecnologie di containerizzazione/virtualizzazione, al fine di verificarne l'effettiva garanzia dei requisiti di economicità, scalabilità, e affidabilità su casi di studio realistici.

Per quanto concerne la definizione di nuovi scenari in ambito OT legati a infrastrutture critiche, l'attività di ricerca del progetto si focalizza, anche in questo caso, su tre obiettivi principali, da inquadrarsi nell'ambito del Task 2.4 del progetto ARTIC:

4. Studio e realizzazione di un prototipo di ICS honepot/honeynet integrabile in un CR con enfasi sull'emulazione dei dispositivi a livello OT, connessi attraverso protocolli industriali, come Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs). Verrà fornito anche un processo fisico (eventualmente simulato) governato dai controllori menzionati sopra. Questo consentirà all' ICS honeypot di fornire un feedback realistico e convincente nei confronti di attaccanti che tentano di modificare l'evoluzione a runtime di tale processo agendo sui controllori compromessi.
5. Sviluppo di tecnologie di intrusion detection a livello OT, sviluppate e raffinate all'interno della ICS honeypot, per riconoscere e catalogare tempestivamente tattiche, tecniche e procedure (TTPs) usate dall'attaccante a livello OT. Questi attacchi, se rilevati in infrastrutture reali, dovranno restare isolati all'interno di una sandbox, impedendo l'alterazione dell'infrastruttura reale. In nessuno caso l'attaccante dovrà aver accesso, e quindi aver modo di violare, il meccanismo di virtualizzazione (Docker containers) su cui si basa l'architettura della honeynet (vedi punto 1 del Task 1.3).
6. Supporto alla definizione di casi di studio realistici per CR, che coprano possibilmente diversi domini d'uso, che contengano al loro interno sia honeypot che sistemi di intrusion detection, al fine di verificarne l'efficacia, così come delineato ai punti 4 e 5, su un vettore di attacco che risulti quanto più ampio possibile.

Sezione b. Metodologia

Task 1.3: Affordable orchestration and virtualization

La realizzazione degli obiettivi 1, 2 e 3 descritti nella Sezione a. verrà effettuata attraverso i seguenti passi:

- Analisi sistematica delle tecnologie di virtualizzazione/containerizzazione disponibili e dello stato dell'arte della ricerca scientifica. Lo scopo dell'analisi tecnologica è la rilevazione delle tecniche attualmente allo stato dell'arte, il loro sviluppo, la dimensione della comunità e i principali utilizzi a supporto della realizzazione di prodotti commerciali (e.g., in ambito Cloud/DevOps). Verranno valutati gli aspetti tecnici e l'adattabilità ad un contesto CR, nonché il costo, il supporto e la estensibilità di tali soluzioni tecnologiche, al fine di determinare le migliori soluzioni disponibili al momento. L'analisi dello stato dell'arte della ricerca scientifica avrà lo scopo di rilevare eventuali estensioni future delle tecnologie, le nuove proposte ed il loro grado di realizzazione, per valutarne la futura adozione in ambito CR. L'output finale di questa attività sarà la definizione delle tecnologie alla base dell'implementazione del PoC del CR del progetto ARTIC.
- Supporto allo sviluppo, assieme ai corrispondenti partner, del PoC, in particolar modo in termini di configurazione delle tecnologie selezionate e monitoraggio dello stato di sviluppo e testing, in forte sinergia con i partner che si occuperanno dell'attività implementativa. L'attività comprenderà il dimensionamento delle tecnologie di virtualizzazione/containerizzazione, l'automazione del deployment delle stesse e la gestione di problematiche correlate alla fase di implementazione. Questo obiettivo sarà raggiunto al completamento di un PoC CR funzionante.
- La definizione degli use case si focalizzerà sulla costruzione di nuovi scenari IT che possano essere utilizzati per attività educative, e avverrà in sinergia con tutti i partner del WP 1 del progetto ARTIC. Tali use case dovranno avere requisiti di scalabilità dello scenario, in modo da verificare l'efficacia delle scelte architetturali adottate.

Task 2.4: Critical infrastructures-related scenarios

La realizzazione degli obiettivi 4, 5 e 6 descritti nella Sezione a. verrà invece effettuata attraverso i seguenti passi:

- Sviluppo e deployment su indirizzi IP usati in contesti industriali di un prototipo di ICS honeynet a livello OT che esponga dispostivi OT come PLCs, RTUs e HMIs connessi attraverso protocolli industriali. L'honeynet dovrà prevedere l'uso di un processo fisico (simulato o meno) governato dai controllori della honeynet stessa. Requisiti fondamentali saranno: (i) scalabilità della honeynet in termini di numero di dispositivi supportati; (ii) estensibilità, ovvero la capacità di inglobare nella honeynet dispositivi di marche e modelli diversi, in modalità emulata o fisica; l'estensibilità riguarderà anche la possibilità di adottare nella honeynet protocolli industriali diversi a seconda del

dominio d'uso e della dislocazione geografica del deployment; (iii) interazione accurata, sia in fase di fingerprinting, da parte dell'attaccante, che in fase del feedback ritornato all'attaccante qualora provi a manipolare il processo fisico del sistema; (iv) superficie di attacco, la honeypot dovrà esporre la massima superficie di attacco, possibilmente adottando dispositivi con vulnerabilità OT note; (v) in caso il processo fisico sia simulato, le simulazioni dovranno essere accurate ma allo stesso con un carico computazionale accettabile.

- I vari dispositivi della honeynet e la stessa rete industriale verrano equipaggiati con componenti software specializzato, che agiscono essenzialmente come sonde in grado di tracciare l'invocazione delle chiamate di sistema rilevanti insieme ai parametri associati. Le sonde dovranno identificare le sessioni aperte da un attaccante su un honeypot e una porta specifica. Una caratteristica chiave di tale sonda sarà quella di operare senza essere rilevata dall'agente malevolo. Nel nostro honeynet, le sonde raccoglieranno dati relativi all'accesso a ciascun dispositivo (PLC, RTU o HMI) e alla rete di controllo di supervisione. Tutte le informazioni raccolte dalle sonde verranno memorizzate in un archivio per ulteriori elaborazioni. Ciò include la lista degli attacchi mirati ad ogni honeypot, l'origine di tali attacchi e il tipo di malware utilizzato sono visualizzati. Inoltre, verrà sfruttato l'API Alienvault OTX per arricchire i dati raccolti con le TTP (Tactics, Techniques, and Procedures) di MITRE ATT&CK e utilizziamo l'API di VirusTotal per la classificazione e l'analisi di eventuali malware catturati. Il servizio fornirà una visualizzazione dei modelli di attacco rilevati in tempo reale, inclusi le porte e i servizi più frequentemente bersagliati, il numero totale di connessioni stabilite, la loro durata e il numero di attaccanti unici. Non ultimo, il meccanismo di intrusion detection cercherà di mettere in relazione interazioni malevole a livello OT con precedenti interazioni a livello IT.
- La definizione degli use case si focalizzerà sulla definizione di nuovi scenari di infrastrutture critiche che possano essere utilizzate per attività educative, e avverrà in sinergia con tutti i partner del WP 2 del progetto ARTIC. L'obiettivo è la definizione di almeno due use case di interesse, su due domini d'uso diverso, che possano essere utilizzati per attività di CTF sul PoC. Tali use case dovranno avere requisiti di scalabilità dello scenario, in modo da verificare l'efficacia delle scelte architetturali adottate.

Referenze:

[1] E. Russo, G. Costa, G. Longo, A. Armando, **A. Merlo**. "Lidite: a full-fledged and featherweight digital twin framework". In IEEE Transactions on Secure and Dependable Computing, 2023.

[2] E. Russo, G. Longo, M. Guerar, **A.Merlo**. "Cloud-Native Application Security Training and Testing with Cyber Ranges", Proc. of UCaml, 2023.

[3] E. Russo, G. Costa, A. Armando. "Building next generation cyber ranges with crack", in Computers & Security, 2020.

[4] Cogent Cyber Range. https://www.cogentcyberrange.com/

[5] AntiSyphon Cyber Range. https://www.antisyphontraining.com/cyber-range/

[6] Cisco Talos Cyber Range. https://talosintelligence.com/incident_response/cyberrange

[7] V. E. Urias, W. M. S. Stout, B. Van Leeuwen and H. Lin. "Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper". In International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, 2018

[8] M. Amit Potdar, D. G. Narayan, K. Shivaraj, M. M. Mulla. "Performance Evaluation of Docker Container and Virtual Machine" Procedia Computer Science, 2020.

[9] Á. Kovács. "Comparison of different Linux containers". In 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.

[10] M.H. Ibrahim, M. Sayagh, A. E. Hassan. "A study of how Docker Compose is used to compose multi-component systems. Empir Software Eng 26, 128 (2021).

[11] C. Carrión. "Kubernetes as a Standard Container Orchestrator - A Bibliometric Analysis". In Journal of Grid Computing 2022.

[12] R. Lanotte, **M. Merro**, A. Munteanu, L. Viganò. A Formal Approch to Physics-based Attacks in Cyber-physical Systems. ACM Trans. Priv. Secur. 23(1): 3:1-3:41, 2020

[13] L. Rist, J. Vestergaard, D. Haslinger, A. De Pasquale, and J. Smith. 2013. Conpot ICS/SCADA Honeypot. http://conpot.org/

[14] D. Pliatsios, P.G. Sarigiannidis, T. Liatifis, K. Rompolos, and I. Siniosoglou. 2019. A Novel and Interactive Industrial Control System Honeypot for Critical Grid Infrastructure. In IEEE CAMAD 1–6.

[15] P. Ferretti, M. Pogliani, and S. Zanero. 2019. Characterizing Background Noise in ICS Traffic Through a Set of Low Interaction Honeypots. In CPS-SPC. ACM.

[16] N. Provos. 2003. Honeyd: A Virtual Honeypot Daemon (Extended Abstract). DFN-CERT 2 (2003)

[17] E. López-Morales, C. Rubio, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G-H Ahn. 2020. HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems. ACM, 279–291.

[18] M. Conti, F. Trolese, and F. Turrin. 2022. ICSpot: A High-Interaction Honeypot for Industrial Control Systems. In ISNCC. IEEE, 1–4.

[19] M. Lucchese, F. Lupia, **M. Merro,** F. Paci, and N. Zannone, A. Furfaro. HoneyICS: A High-interaction, Physics-aware Honeynet for Industrial Control Systems. In ARES, ACM, 113:1-113-10, 2023.

[20] M. Lucchese, **M. Merro**, F. Paci, and N. Zannone. Towards a High-interaction, Physics-aware Honeynet for Industrial Control Systems. In SAC, ACM, 76-79, 2023.

[21] F. Lupia, M. Lucchese, **M. Merro** and N. Zannone. ICS Honeypot Interactions: A Latitudinal Study. In BigData 2023, IEEE, 3025-2034, 2023.

[22] D. Antonioli, A. Agrawal, and N.O. Tippenhauer. 2016. Towards High-Interaction Virtual ICS Honeypots-in-a-Box. In CPS-SPC. ACM, 13–22.

[23] A. A. Cardenas, S. Amin, Z-S. Lin, Y-L. Huang, C-Y. Huang, S. Sastry. Attacks against process control systems: risk assessment, detection and response. In AsiaCCS, pp. 355-366, 2011.

[24] S. Adepu, A. Mathur. Distributed attack Detection in a Water Treatment Plant: Method and Case Study. IEEE Trans. Dependable Secur. Compu. 18(1):86-99, 2021

[25] A. P. Mathur, N. O. Tippenhauer. SWaT: a water treatment testbed for research and training on ICS security. In CySWater@CPSWeek, 31-36, IEEE, 2016.

[26] F. Furtado, S. Shrivastava, A. Mathur, N. Goh. The Design of Cyber-Physical Exercises (CPXs). In CyCon, 348-366, IEEE, 2022.

Sezione c. Strumentazione e risorse disponibili

- Industrial Computer Engineering (ICE) Lab. Laboratorio con una linea di produzione industriale secondo i dettami dell'Industria 4.0 e focalizzata su didattica, formazione ed innovazione, attraverso diverse collaborazioni con aziende del territorio. Il laboratorio è stato finanziato dal progetto "Dipartimenti di Eccellenza 2018-2022", finanziato dal MUR, di cui ha usufruito il Dipartimento di Informatica di Verona.

Sezione d. Milestone, KPI e diagramma di GANTT

Task 1.3

- Milestone:
  - Riguardo gli obiettivi 1, 2 e 3, sono definite le seguenti milestone:
    - Milestone 1 (MS1) al M6: selezione delle tecnologie di containerizzazione/virtualizzazione da adottare nel PoC del CR ed eventuali indicazioni sulla loro configurazione e deployment nel PoC
    - Milestone 2 (MS2) al M14: validazione dell'implementazione e del deployment delle tecnologie di containerizzazione/virtualizzazione del PoC

- Milestone 3 (MS3) al M18: sintesi dell'insieme di use-case in ambito IT da eseguire sul PoC

- Deliverable:
  - D. 1.1. al M6: Documento contenente le tecnologie di containerizzazione/virtualizzazione selezionate per il PoC e le loro eventuali guidelines di configurazione
  - D.1.2. al M14: Relazione sull'utilizzo delle tecnologie selezionate nell'implementazione del PoC
  - D.1.3. al M18: Documento di sintesi sugli use-case IT definiti per il PoC

- KPI:
  - Sono definiti i seguenti KPI, collegati agli obiettivi 1, 2 e 3 e alle milestone definite in precedenza:
    - Pubblicazione "open access" dei risultati della ricerca svolta per gli obiettivi 1 e 2 in almeno *1 rivista internazionale di quartile massimo (Q1)*
    - Definizione e realizzazione di almeno due use case di interesse che possano essere utilizzati per attività di CTF sul PoC

Task 2.4

- Milestone:
  - Riguardo gli obiettivi 4, 5 e 6, sono definite le seguenti milestone:
    - Milestone 4 (MS4) al M8: analisi approfondita della letteratura esistente su ICS honeypot e progettazione, implementazione e deployment di una nuova ICS honeynet che soddisfi i requisiti menzionati sopra.
    - Milestone 5 (MS5) al M14: Sviluppo e validazione attraverso PoC attack delle tecnologie di intrusion detection all'interno della honeynet precedentemente indicate.
    - Milestone 6 (MS6) al M18: sintesi dell'insieme di use case in ambito OT da eseguire sul PoC.

- Deliverable:
  - D. 2.1. al M8: Documento contenente l'architettura e l'implementazione di un nuovo ICS honeynet già esportata su indirizzi IP realistici;
  - D.2.2. al M14: Relazione su uno studio latitudinale delle interazioni malevole raccolte dalla Honeynet esposta su Internet per un periodo di almeno 6 mesi;
  - D.2.3. al M18: Documento di sintesi sugli use-case OT definiti per il PoC.

- KPI:
  - Sono definiti i seguenti KPI, collegate agli obiettivi 4, 5 e 6 e alle milestone definire in precedenza:
    - Pubblicazione "open access" dei risultati della ricerca svolta per gli obiettivi 4 e 5 in almeno *1 pubblicazione su rivista internazionale di quartile massimo (Q1)*
    - Disseminazione dei risultati finali (con eventuale demo del PoC) in almeno un workshop tematico o conferenza di settore

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
Task 1.3																		
Obiettivo 1						MS1												
Obiettivo 2														MS2				
Obiettivo 3																		MS3
Task 2.4																		
Obiettivo 4								MS4										
Obiettivo 5														MS5				
Obiettivo 6																		MS6

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Appendice dell'Allegato B

Curriculum vitae dei membri delle unità di ricerca

Soggetto 1: Università degli Studi di Verona (UNIVR)

Composizione dell'unità di ricerca:

Massimo MERRO (**PI**), professore ordinario, ssd INF/01
ORCID: 0000-0002-1712-7492
PhD in Computer Science, Ecole Nationale Supérieure des Mines de Paris, France, 2000
CV: vedere il CV allegato in fondo alla presente.
h-index: 23 (Scopus), 25 (Scholar)
Citazioni: 1155 (Scopus), 1953 (Scholar)
Keywords: Cyber-Physical Systems Security, Formal Verification, Concurrency Theory.

Ferdinando CICALESE, professore ordinario, ssd INF/01
ORCID: 0000-0003-1652-0599
PhD in Computer Science, Università di Salerno, 2001
Laurea in Informatica, Università di Salerno, 1995
h-index: 15 (Scopus), 23 (Scholar)
Citazioni: 898 (Scopus), 1826 (Scholar)
Fellowships: EU Maric Curie (research training in 2004 e visiting professor 2009-2010)
Awards: Best paper ISAAC 2015; Sofia Kovalevskaja award; Best Italian PhD thesis in Theoretical Computer Science
Incarichi istituzionali: Coordinatore del Dottorato in Informatica (2022-); referente AQ per la Didattica del Dipartimento di Informatica (2020-2022)
Keywords: Algorithms, Error-correcting codes, Information Theory, Combinatorial search.

Roberto SEGALA, professore ordinario, ssd INF/01
ORCID: 0000-0001-5586-3362
PhD in Electrical Engineering and Computer Science, MIT, Boston, US, 1995
Master in Electrical Engineering and Computer Science, MIT, Boston, US, 1992
Diploma ordinario in Scienze dell'Informazione, Scuola Normale Superiore, Pisa, 1991
Laura con lode in Scienze dell'Informazione, Università degli Studi di Pisa, 1991
Fellowships: MIT, US, 1993
Editorial board: Information and Computation, 2011-
h-index: 28 (Scopus), 37 (Scholar)
Citazioni: 2351 (Scopus), 6770 (Scholar)
Incarichi istituzionali: Coordinatore del Dottorato in Informatica (2006-2009), Presidente del Collegio Didattico (2009-2012 e 2018-2021); Delegato del Rettore per l'Orientamento e l'e-learning (2006-2013)
Keywords: Hybrid systems, Security, Concurrency theory, probabilistic automata.

Damiano CARRA, professore associato, ssd ING-INF/05
ORCID: 0000-0002-3467-1166
PhD in Computer Science, Università di Trento, 2007
Master in Information Technology, Politecnico di Milano, 2000
Fellowships: EUROCOM Sophia-Antipolis (Apr 2007 – May 2008); INRIA Sophia Antipolis (June 2008 – Dec 2008)
h-index: 15 (Scopus), 19 (Scholar)
Citazioni: 566 (Scopus), 1040 (Scholar)
Incarichi istituzionali: Referente AQ per la Terza Missione (2022-)
Keywords: Big data, sistemi distribuiti.

Matteo CRISTANI, professore associato, ssd INF/01
ORCID: 0000-0001-5680-0080
PhD in Information Engineering, Università degli Studi di Padova, 1995
Laura con lode in Scienze dell'Informazione, Università di Milano, 1991
Fellowships: Università degli Studi di Padova, 1996-1997
h-index: 15 (Scopus), 18 (Scholar)
Citazioni: 761 (Scopus), 1269 (Scholar)
Keywords: Artificial intelligence, social computing.

Giuditta FRANCO, professoressa associata, ssd INF/01
ORCID: 0000-0003-1447-5253
PhD in Computer Science, University of Verona, 2006
Laurea in Matematica, Università degli Studi di Pisa, 2001
Fellowships: Leiden Institute of Advanced Computer Science (2006); University of South Florida (2007)
Editorial board: Open Computer Science (2018-)
h-index: 12 (Scopus), 14 (Scholar)
Citazioni: 513 (Scopus), 590 (Scholar)
Incarichi istituzionali: Referente AQ per il corso di laurea in Bioinformatica (2023-)
Keywords: Bioinformatics, DNA computing, Computational genomics.

Zsuzsanna LIPTAK, professoressa associata, ssd INF/01

ORCID: 0000-0002-3233-0691

PhD in Computer Science, Universitat Bielefeld, Germania, 2005

Master in Mathematics, Freie Universitat Berlin, Germania, 1999

Fellowships: Marie Curie IEF Fellow (2011) Technische Fakultät, Universität Bielefeld, Germania (2005-2009)

h-index: 14 (Scopus), 20 (Scholar)

Citazioni: 789 (Scopus), 1383 (Scholar)

Keywords: Algorithmic bioinformatics, string algorithms.

Isabella MASTROENI, professoressa associata, ssd INF/01

ORCID: 0000-0003-1213-636X

PhD in Informatica, Università di Verona, 2004

Laurea con lode in Informatica, Università di Verona, 2001

Fellowships: Kansas State University (2005 and 2006)

h-index: 14 (Scopus), 16 (Scholar)

Citazioni: 65 (Scopus), 1119 (Scholar)

Incarichi istituzionali: Referente AQ del corso di laurea in Informatica (2015-)

Keywords: Abstract interpretation, Noninterference, Information flow.

Federica Maria Francesca PACI, professoressa associata, ssd INF/01

ORCID: 0000-0003-3122-0236

PhD in Information Technology, Università di Milano, Italia 2008

Laurea con lode in Informatica, Università di Milano, 2004

Fellowships: Purdue University, West Lafayette, Indiana US (2008-2009); Università di Trento (2012-2015); University of Southampton (2015-2018)

h-index: 21 (Scopus), 28 (Scholar)

Citazioni: 1669 (Scopus), 3035 (Scholar)

Keywords: Access conrol, Security Risk Assessment, Privacy, Identity Managament.

Elisa QUINTARELLI, professoressa associata, ssd ING-INF/05

ORCID: 0000-0001-6092-6831

PhD in Information Technology, Università di Milano, 2002

Laurea con lode, Università degli Studi di Verona, 1998

Fellowships: Laboratoire d'Informatique de l'Ecole Polytechnique (LIX), Parigi, 2000

Awards: Premio Chorafas per la miglior tesi di Dottorato del Politecnico di Milano, 2002

h-index: 15 (Scopus), 22 (Scholar)

Citazioni: 1140 (Scopus), 2133 (Scholar)

Incarichi istituzionali: Referente AQ Didattica per il Dipartimento (2023-)

Keywords: Sistemi di raccomandazioni, Sistemi informativi orientati ai processi.

Barbara OLIBONI, professoressa associata, ssd INF/01

ORCID: 0000-0002-3233-0691

PhD in Computer Engineering, Politecnico di Milano, 2003

Laurea con lode in Informatica, Università degli Studi di Verona, 1998

h-index: 16 (Scopus), 20 (Scholar)

Citazioni: 904 (Scopus), 1137 (Scholar)

Incarichi istituzionali: Referente AQ del corso di LM in Ingegneria e Scienze Informatiche (2019-)

Keywords: Database, semistructured data.

Soggetto 2: Centro Alti Studi per la Difesa (CASD)

Composizione dell'unità di ricerca:

ALESSIO MERLO (**co-PI**), professore ordinario in ING-INF/05

- ORCID: 0000-0002-2272-2376
- CV: vedere il CV allegato in fondo alla presente.
- BIBLIOMETRICS:
  - h-index: 23 (Scopus), 30 (Scholar)
  - Citazioni: 1415 (Scopus), 2272 (Scholar)
  - KEYWORDS: Computer Security, Mobile Security.

DANIELA IRRERA, professore ordinario in SPS/04

- ORCID: 0000-0003-1572-2922
- EDUCATION
  - PhD in International Relations, Università di Catania, 2004
  - Laurea (quadriennale) in Scienza Politiche, Università di Messina, 1999
- FELLOWSHIPS
  - Gen.-Feb. 2009: Fulbright United States Institute on National Security - US Department of State; University of Delaware.
  - Nov. 2009: Centre Catholique International (Geneva); Université Libre de Bruxelles, Institute of European Studies.
  - Ott. – Dic. (Michaelmas Term) 2012: Department of Sociology, and Extra-Legal Governance Institute (ExLegi), University of Oxford.
  - Sett. - Ott. 2015: DAAD Fellow at Peace Research Institute Frankfurt.
  - Mag. 2016: EU Center of Excellence, University of Alberta, Canada.
  - Gen. - Feb. 2017: Erasmus Mundus Program MUNDUSMAPP, IBEI, Barcelona.
  - Lug.- Ago. 2019: Marie Curie Secondment H2020-Marie Sklodowska Curie Actions-RISE, "KANTINSA - Kant in South America" (Grant Agreement number: 777786), Universidade Federal de Santa Catarina, Florianopolis, Brazil.
  - Mag. 2023: University of Loughborough, Institute of Advanced Studies, Open Program Fellowship
- AWARDS
  - 2020: Premio per la simulazione del Game of Peace per le migliori pratiche europee di insegnamento the migliorino l'apprendimento degli studenti internazionali (progetto IMPACT).
- INSTITUTIONAL RESPONSIBILITIES
  - 2024-2026: Chair dell'European Consortium for Political Research ECPR
  - 2021-2023: Vicerettore per l'Institutional Erasmus Coordination
  - 2020- 2023: Vice-Coordinatore del programma di dottorato in Scienze Politiche, Università di Catania.
  - 2022-2023: Chair del programma MA in Global Politics and Euromediterranean Relations.
  - 2022-2023: Chair del comitato per l'ISA Robert W. & Jessie Cox Award (best paper per le Relazioni Internazionali).
  - 2014-2021: Vicedirettore del programma Erasmus, Università di Catania.
  - 2019-2021: Vicedirettore per la ricerca, Università di Catania.

    - 2019-2021: Chair dell'ECPR Standing on International Relations
    - 2019-2022: Presidente dell'European Peace Research Association (EuPRA).
    - 2018-2021: Segretario Generale dell'associazione italiana di scienze politiche (SISP).
    - 2020-2021: Membro del consiglio di governo dell'International Studies Association (ISA)
- PHD. COMMITEE MEMBERSHIP
    - Gen. 2023 – Candidato: Marcello Ciola (Université Paris-Est Sup et Université Catholique de Louvain)
    - Mag. 2023 – Candidato: Javier Ruipérez Canales (Università di Granada)
- RESEARCH KEYWORDS: Security studies, conflict studies.

NICOLA COLACINO, professore associato in IUS/13

- EDUCATION
    - Dottorato in International Order and Human Rights, Università di Roma Sapienza, 2004
    - Laurea in Giurisprudenza, 1998
- FELLOWSHIP
    - 3 affidamenti di docenza all'estero nel quadro del programma Erasmus+ (2 Università Di Tampere, 2019-2020, 1 Università di Brno, 2019)
- AWARDS
    - Premio CNR per la tesi di laurea
- INSTITUTIONAL RESPONSIBILITIES
    - Coordinatore del corso di laurea magistrale in relazioni internazionali (2019 – 2923), Unicusano.
    - Vicepresidente della commissione paritetica (2015 – 2021), Unicusano.
    - Presidente del gruppo del riesame nel corso di laurea in relazioni internazionali (2022 – 2023)
- RESEARCH KEYWORDS: International Security, International Environment Law

ANDREA BERNARDI, professore associato in SECSP/10

- ORCID: 0000-0003-2571-6817
- EDUCATION
    - Dottorato in Organizzazione e Risorse Umane Università di Milano Bicocca, 2009
    - Laurea in Economia, Università di Roma Tre, 2001
- FELLOWSHIPS
    - Erasmus+ Teaching Mobility Grant, 2018
    - Erasmus+ Organizational Mobility Grant, 2014
    - Research grant dall'University of Helsinki, 2009
    - Erasmus Teaching Staff Mobility Programm, 2003
- INSTITUTIONAL RESPONSIBILITIES
    - Erice International School of Diplomacy, membro dello steering committe dal 2024.
    - Membro del Data Management Committee, Oxford Brookes University
    - General Chair della 28th EAEPE Conference, 2016, Manchester.
    - Coordinatore del "International Relations and Exchange Programme", Manchester Metropolitan University School dal 2012 al 2016
    - Membro del comitato scientifico del Master in Economia, Diritto e Management, Università di Roma Tre, dal 2012 ad oggi.
- Membro dell'Occupational Health and Safety Committee, University of Nottingham.
- RESEARCH KEYWORDS: Wargaming Simulation, Cooperative Organizations.

DAVIDE VERZOTTO, Ricercatore a Tempo Determinato (a) in INF/01

- ORCID: 0000-0001-5152-4662
- EDUCATION
  - Dottorato in Ingegneria Informatica, Università of Padova, 2012
  - Laurea Magistrale in Ingegneria Informatica, magna cum laude, Università degli Studi di Padova, 2008.
- FELLOWSHIPS
  - 2019 – 2020 : Ricercatore di III livello, Istituto Scientifico Biomedico Euro Mediterraneo (ISBEM) - spin-off Università di Pisa e CNR di Pisa.
  - 2019: Visiting Professor di Sistemi di Elaborazione delle Informazioni, Università di Tunisi El Manar, Tunisia.
  - 2017-2018: Assegno di Ricerca in Informatica (INF/01), Dipartimento di Informatica, Università di Pisa.
  - 2015-2017: Research Fellow e Project Leader, A*STAR Genome Institute of Singapore, Singapore - in collaborazione con Procter & Gamble, USA.
  - 2012-2015: Postdoctoral Fellow, Agency for Science, Technology and Research (A*STAR) - Genome Institute of Singapore, Singapore.
  - 2010-2011: Visiting Scholar e Junior Specialist, Dipartimento di Computer Science & Engineering, Università della California, Riverside, USA.
- AWARDS
  - 2019: Best paper award alla conferenza DEXA-BIOKDD'19.
  - 2019: Programma di mobilità didattica come Visiting Professor di Sistemi di Elaborazione delle Informazioni (ING-INF/05), rilasciato dall'Università di Pisa con CUP 154F18000080005 e tenuto presso l'Università di Tunisi El Manar, Tunisia, nell'ambito del programma ERASMUS+ KA107 2018-20.
  - 2012, 2015 – Due Marie Curie–ERCIM "Alain Bensoussan" Career Development Enhancer fellowships (ABCDE), cofinanziati dalla Commissione Europea - ERCIM: European Research Consortium for Informatics and Mathematics; tasso di accettazione tipico: 7% su oltre 300 candidati.
  - 2015 – A*STAR GIS Early Career Researcher award.
  - 2013 – Premio “Città Impresa” per i migliori giovani talenti del Triveneto, in particolare nell'ambito del trasferimento della Ricerca.
  - 2011–12: Prestigioso premio "Veneto Giovani Ricerca Futuro", come miglior Giovane Ricercatore in ambito I.C.T. del Triveneto - organizzato dal Consorzio Veneto di Ricerca per i risultati ottenuti durante il Dottorato di Ricerca.
  - 2011: U.S. National Science Foundation (NSF) award.
  - 2010, 2011: Due prestigiosi grant individuali assegnati da parte della Fondazione Ing. Aldo Gini e dell'Università degli Studi di Padova.
- INSTITUTIONAL RESPONSIBILITIES
  - 2020: Coordinatore formale di network di Ricerca/PI in ambito "Trans-sectoral development of post-COVID-19 biosecurity and social interactions" (TRAPSE - Horizon 2020, MSCA). Partner: CNR (Italia; Coordinatore di Progetto); Cornell University, Weill Cornell Medicine e MIT (USA); Università Acibadem ed Epigenetiks A.S. (Turchia); Consorzio per il Trasferimento Tecnologico (C2T) e Find Your Doctor (FYD) S.r.l. (Italia); Università Politecnica di Madrid (Spagna); Università Sorbona e INSERM (Francia); Università Keio (Giappone); Institut Pasteur Korea (Corea del Sud); Consector Biro d.o.o. e Università di Zagabria (Croazia); Biolabtech Ltd. e NASU IMBG (Ucraina); Università Jagiellonian (Polonia); Università Abdelmalek Essaadi (Marocco).
  - 2020: Topic Editor stabile della rivista Algorithms (ambito: Informatica).
  - 2018-20 e 2019-21: Coordinatore di Progetto dei rispettivi programmi Erasmus+ KA107 tra l’Università di Pisa e l'Università di Tunisi El Manar, Tunisia.
  - 2018-19: Responsabile docenza universitaria "Knowledge Discovery Laboratory", M.S. in Information Systems Engineering, Università di Tunisi El Manar, Tunisia.

- 2018-19: Responsabile docenza universitaria "Data Mining Laboratory" (ING-INF/05), congiunta per L.M. in Computer Engineering, Università di Pisa e L.M. in Bionics Engineering, Scuola Superiore Sant'Anna.

- BIBLIOMETRICS
  - h-index: 7 (Scopus), 12 (Scholar)
  - Citazioni: 190 (Scopus), 449 (Scholar)
- RESEARCH KEYWORDS: Artificial Intelligence, Machine Learning.

CARLO BONGIOANNI, Ricercatore a Tempo Determinato (a) in ING-INF/03

- ORCID: 0000-0001-5537-5211
- EDUCATION
  - Dottorato in Telecomunicazioni, University di Roma Sapienza, 2010
  - Laurea Specialistica in Ingegneria delle Telecomunicazioni, 2006
- AWARDS
  - premio FRANCESCO CARASSA per il miglior lavoro nel settore "Elaborazione del segnale e Telerilevamento" nell'ambito della Riunione Annuale del Gruppo nazionale Telecomunicazioni e Teoria dell'Informazione – GTTI 2007 (Roma 18-20 Giugno 2007). Titolo del lavoro: "Passive radar prototypes for multifrequency target detection" (autori F. Colone, C. Bongioanni, A. Lauri, R. Cardinali, P. Lombardo)
  - Best student paper award per il seguente articolo: C. Bongioanni, F. Colone, P. Lombardo, "Performance Analysis of a Multi-Frequency FM Based Passive Bistatic Radar", IEEE Radar Conference 2008, Rome, Italy, May 26-30, 2008, pp. 1984-1989, ISSN: 1097-5659, ISBN: 978-1-4244-1538-0, doi: 10.1109/RADAR.2008.4720805
  - Best paper award per il seguente articolo: F. Colone, C. Bongioanni, P. Lombardo, "Experimental results for a Passive Forward Scatter Radar based on OFDM waveform of opportunity", 2021 21st International Radar Symposium (IRS 2021), pp. 1-10, doi: 10.23919/IRS51887.2021.9466219
- BIBLIOMETRICS
  - h-index: 15 (Scopus), 17 (Scholar)
  - Citazioni: 845 (Scopus), 1122 (Scholar)
- RESEARCH KEYWORDS: Network Simulation, Passive Radar.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Curriculum vitae del PI

- **PERSONAL INFORMATION**

MERRO, Massimo

ORCID: 0000-0002-1712-7492

Nato il

Nazionalità:

URL: profs.sci.univr.it/~merro/

- **EDUCATION**

2000 PhD con menzione "Très honorable avec félicitation du jury"
Ecole des Mines de Paris, Centre de Mathématiques Appliquées, Francia
Supervisor: Dr. Davide Sangiorgi

1996 Laurea con lode in Scienze dell'Informazione
Facoltà di Scienze MMFFN/ Dipartimento di Informatica
Università degli Studi di Pisa, Italia

- **CURRENT POSITION**

2018 – Professore di I fascia in Informatica (ssd: INF/01) presso il Dipartimento di Informatica dell'Università degli Studi di Verona, Italia.

- **PREVIOUS POSITIONS**

2006 – 2018 Professore di II fascia in Informatica (ssd: INF/01) presso il Dipartimento di Informatica dell'Università degli Studi di Verona, Italia.

2002 – 2006 Ricercatore in Informatica (ssd: INF/01) presso il Dipartimento di Informatica dell'Università degli Studi di Verona, Italia.

- **FELLOWSHIPS AND AWARDS**

2002 Research Fellow presso il "Laboratoire des Méthodes de Programmation, Institut d'Informatique Fondamentale, Faculté Informatique et Communications", Ecole Polytechnique Fédérale de Lausanne, Svizzera, sotto la supervisione del Prof. Uwe Nestmann (6 mesi, da maggio a ottobre)

2000 – 2002 Research Fellow presso la "School of Cognitive and Computing Science", University of Sussex, UK, sotto la supervisione del Prof. Matthew Hennessy (24 mesi)

1999 – 2000 EU Marie Curie TMR PhD scholarship (18 mesi)

1998 – 1999 INRIA PhD Scholarship (12 mesi)

1997 – 1998 Borsa CNR per l'estero (12 mesi)

2013 Best Paper Award alla conferenza COORDINATION 2013 per l'articolo "Modelling MAC-Layer Communications in Wireless Systems"

- **SUPERVISION OF GRADUATE STUDENTS AND POSTDOCTORAL FELLOWS (if applicable)**

2002 – 2023 4 Postdocs/ 3 student di PhD/ 25 Master Students
Dipartimento di Informatica, Università degli Studi di Verona, Italia.

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

- **INSTITUTIONAL RESPONSIBILITIES (if applicable)**

2016 – 2022 Coordinatore del Dottorato in Informatica di Verona

2019 – 2021 Co-delegato all'Internazionalizzazione dell'Università di Verona
2016 – 2019 Referente AQ del corso di LM in Ingegneria e Scienze Informatiche
2009 – 2022 Membro della Giunta del Consiglio di Dipartimento (escluso per gli anni 2016-2017)
2020 – 2022 Membro del Consiglio della Scuola di Dottorato di Ateneo
2016 – 2020 Membro del Consiglio della Scuola di Dottorato in Scienze Naturali e Ingegneristiche
2008 – 2011 Membro della Commissione Didattica del GRIN
2006 – 2012 Vicepresidente del Corso di Laurea in Informatica di Verona.

- **REVIEWING ACTIVITIES (if applicable)**

2014 – Editorial board di Frontiers in ICT, Computer and Network Security (Scopus)
2015- 2022 Editorial board di Open Computer Science (WoS and Scopus)
2014 - Editorial board di Mobile Information Systems (WoS and Scopus)
2002 – 2023 PC: VORTEX'22, FORTE'22, CYBER'22, CYBER'21, ITIA'20, ICTCS'19, EMSOFT'17, FORTE'16, ICALP'16 (track B), ICALP'15 (track C), ICALP'11 (track C), FCST'09, MeCBIC'08, CONCUR'06, EXPRESS'03, EXPRESS'02.
1998 – 2023 Reviewer: JACM, ACM TOPLAS, ACM TOPS, International Jounral of Critical Infrastructure Protection, Formal Aspects of Computing, Information and Computation, Theoretical Computer Science, Mathematical Structures in Computer Science, etc.
2000 – 2023 PhD committe reviewer: Dr. Stéèphane Micheloud, Dr. Fatemeh Ghassemi, Dr. Ian Cassar.

- **MAJOR COLLABORATIONS:**

  - Università dell'Insubria: Prof. Ruggero Lanotte e Prof. Simone Tini
  - Eindhoven University of Technology: Prof. Nicola Zannone
  - Harvard University: Gordon Mckay Prof. Stephen Chong
  - King's College London: Prof. Luca Viganò
  - Charlotte University: Dr. Jian Xiang
  - Università della Calabria: Dr. Francesco Lupia
  - KTH Stoccolma: Prof. Musard Balliu

- **5 RELEVANT PAPERS TO THE PROJECT:**

1. M. Lucchese, **M. Merro**, F. Paci, and N. Zannone. Towards a High-interaction, Physics-aware Honeynet for Industrial Control Systems. In SAC, ACM, 76-79, 2023.
2. M. Lucchese, F. Lupia, **M. Merro,** F. Paci, and N. Zannone, A. Furfaro. HoneyICS: A High-interaction, Physics-aware Honeynet for Industrial Control Systems. In ARES, ACM, 113:1-113-10, 2023.
3. F. Lupia, M. Lucchese, **M. Merro** and N. Zannone. ICS Honeypot Interactions: A Latitudinal Study. In BigData 2023, IEEE, 3025-2034, 2023.
4. R. Lanotte, **M. Merro**, A. Munteanu, L. Viganò. A Formal Approch to Physics-based Attacks in Cyber-physical Systems. ACM Trans. Priv. Secur. 23(1): 3:1-3:41, 2020
5. R. Lanotte, **M. Merro**, A. Munteanu. Industrial Control Systems Security via Runtime Enforcement. ACM Trans. Priv. Secur. 26(1): 4:1-4:41, 2023

Curriculum vitae del co-PI

INFORMAZIONI PERSONALI

MERLO, Alessio
ORCID: 0000-0002-2272-2376

Nazionalità

URL for web site: https://www.csec.it/people/alessio_merlo

- **EDUCATION**

2010 PhD in Informatica, Università degli Studi di Genova, Italia.
Supervisori: Vittoria Gianuzzi, Andrea Clematis, Angelo Corana

2006 Laurea Specialistica in Informatica, magna cum laude, Università degli Studi di Genova, Italia.

- **CURRENT POSITION(S)**

2023 – Professore Ordinario in Sistemi di Elaborazione dell'Informazione (ssd ING-INF/05)
Scuola di Studi Avanzati per la Difesa – Centro Alti Studi per la Difesa (CASD), Roma, Italia

- **PREVIOUS POSITIONS**

2020 – 2023 Professore Associato in Sistemi di Elaborazione dell'Informazione (ssd ING-INF/05)
DIBRIS - Università degli Studi di Genova

2017 – 2020 Ricercatore a T. D. di tipo b in Sistemi di Elaborazione dell'Informazione (ssd ING-INF/05)
DIBRIS - Università degli Studi di Genova

2014 – 2017 Ricercatore a T.D. di tipo a in Sistemi di Elaborazione dell'Informazione (ssd ING-INF/05)
DIBRIS - Università degli Studi di Genova

2011 – 2014 Ricercatore a t.d. (ex Moratti) in Sistemi di Elaborazione dell'Informazione (ssd ING-INF/05)
Università E-Campus, Novedrate (CO).

- **FELLOWSHIPS AND AWARDS**

2010 – 2011 Assegnista di ricerca (postDoc) presso il DIST, Università degli Studi di Genova

2009 – 2010 Assegnista di ricerca presso l'IEIIT-CNR, Genova.

2005 – 2006 Assegnista di ricerca presso l'IEIIT-CNR, Genova.

2022 – Best Paper Award alla conferenza ICST 2022 per l'articolo "IFRIT: Focused Testing through Deep Reinforcement Learning"

2021 – Best Artifact Award alla conferenza ACSAC 2021 per l'articolo "Repack Me If You Can: An Anti- Repackaging Solution Based on Android Virtualization"

2013 – Best Paper Award alla conferenza AINA 2013 per l'articolo "Energy Consumption Simulation of Different Distributed Intrusion Detection Approaches"

2012 – Best Paper Award alla conferenza MIST 2012 per l'articolo "Securing the Bring Your Own Device Policies"

2012 – Best Paper Award alla conferenza IFIP-SEC 2012 per l'articolo "Would you mind forking this process? A Denial of Service Attack on Android (and some countermeasures)"

- **SUPERVISION OF GRADUATE STUDENTS AND POSTDOCTORAL FELLOWS (if applicable)**

2014 – 2023 2 PhD
CASD – Centro Alti Studi per la Difesa

2014 – 2023 3 postDoc/ 13 studenti di PhD / 43 Tesi di Master
DIBRIS - Università degli Studi di Genova

- **ORGANISATION OF SCIENTIFIC MEETINGS**

2022 General Chair della 7th European Conference on Security & Privacy (EuroS&P 2022), 6-10 Giugno 2022, Genova.

2017 General Chair della 15th International Conference on High Performance Computing and Simulation (HPCS 2017), 17-21 luglio 2017, Genova.

- **INSTITUTIONAL RESPONSIBILITIES (if applicable)**

2024 – Membro dello Steering Committee dell'Erice International School on Science Diplomcy

2023 – Delegato del Rettore alla Cybersecurity, Centro Alti Studi per la Difesa, Roma.

2018 – 2022 Presidente del Master in "Cybersecurity and Critical Infrastructure Protection", Università degli Studi di Genova.

2020 – 2023 Membro della Comitato Tecnico Scientifico di CEDIA, Università degli Studi di Genova

2013 – 2023 Membro della Commissione Ricerca, DIBRIS - Università degli Studi di Genova

- **REVIEWING ACTIVITIES (if applicable)**

2010 – Membro del Program Committee di 74 conferenze internazionali con focus su argomenti di HPC e Cybersecurity. tra le quali IJCAI 2021- 24, SAC 2017 - 2023, e TrustCom 2019 – 2023

2010 – Revisore per 20 riviste internazionali tra cui Computers & Security. IEEE Transactions on Secure and Dependable Computing, Computer Networks, Future Generation Computer Systems.

2022 – Associate Editor del Journal Frontiers in Computer Science: Cybersecurity

2018 – 2023 Revisore di tesi di dottorato: Dr. Jennifer Bellizzi (University of Malta), Dr. Andrea Bisegna (Fondazione Bruno Kessler), Dr. Elham Arshad (Università di Trento), Maged Fathy Yuoussef Abdelaty (Università di Trento).

- **MEMBERSHIPS OF SCIENTIFIC SOCIETIES (if applicable)**

2006 – Membro dell'Institute for Electrical and Electronical Engineering, Senior Member dal 2022.
2006 – Membro dell'Association for Computing Machinery (ACM)

- **MAJOR COLLABORATIONS (if applicable)**

  - Università di Padova: Prof. Mauro Migliardi e Prof. Mauro Conti
  - Università di Salerno: Prof. Francesco Palmieri
  - IMATI-CNR: Dr. Luca Caviglione
  - Eurecom (Francia): Prof. Davide Balzarotti, Dott. Simone Aonzo
  - Università della Svizzera Italiana (Svizzera): Prof. Paolo Tonella
  - Università di Verona: Prof. Mariano Ceccato
  - Fondazione Bruno Kessler: Dott. Roberto Carbone
  - Università Mediterranea di Reggio Calabria: Prof. Francesco Buccafurri
  - Università di Trento: Prof. Silvio Ranise
  - Università di Roma Sapienza: Prof. Leonardo Querzoni, Dott. Daniele Cono D'Elia
  - Università di Tor Vergata: Prof. Giuseppe Bianchi
  - New York Institute of Technology: Prof. Paolo Gasti

  Tutte queste collaborazioni si sono focalizzato o si focalizzano su tematiche di Mobile Security, con uno specifico focus sul Security Testing, la malware analysis e la vulnerability analysis.

5 PAPERS RELEVANT TO THE PROJECT

- E. Russo, G. Costa, G. Longo, A. Armando, **A. Merlo**. "Lidite: a full-fledged and featherweight digital twin framework". In IEEE Transactions on Secure and Dependable Computing, 2023.
- E. Russo, G. Longo, M. Guerar, **A.Merlo**. "Cloud-Native Application Security Training and Testing with Cyber Ranges", Proc. of UCaml, 2023.
- L. Verderame, L. Caviglione, R. Carbone, **A. Merlo** "SecCo: Automated Services to Secure Containers in the DevOps Paradigm" in Proc. ACM RACS 2023.
- G. Benedetti, L. Verderame, **A. Merlo**. "Automatic Security Assessment of GitHub Action Workflows" in Proc. 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED'22), ACM CCS 2022.
- E. Russo, L. Verderame, **A. Merlo.** "Enabling Next-Generation Cyber Ranges with Mobile Components", in Proc. ICTSS 2020.

Appendix: All current grants and on-going and submitted grant applications of the PI and Co PI (Funding ID)

Mandatory information (does not count towards page limits)

Current grants (Please indicate "No funding" when applicable): No funding

ALLEGATO C - Budget personale costi standard

TABELLA COSTI PERSONALE STANDARD				COSTO DEL PERSONALE	TD
FASCIA DI COSTO /LIVELLO	**NUMERO SOGGETTI**	**COSTO ORARIO vedi nota**	**MONTE ORE**		
Basso	**2**	31 €	1625	50.375 €	
Medio	**10**	48 €	6125	294.000 €	
Alto	**5**	73 €	4625	337.625 €	
TOTALI	**17**		**12375**	**682.000 €**	

COSTO ORARIO: si deve far riferimento al Decreto Interministeriale n. 116 del 24/1/2018

Firma digitale del
Legale rappresentante del Proponente o Soggetto capofila

ALLEGATO C -Budget complessivo progetto

BUDGET DI PROGETTO	COSTO DEL PERSONALE	OVERHEAD	Costi per servizi di Consulenza Specialistica	Costi per licenze direttamente imputabili al progetto	Costi per materiali e attrezzature direttamente imputabili al progetto	Costi per altre tipologie di spese direttamente imputabili al progetto	COSTO TOTALE
Partecipante 1: Università degli Studi di Verona (UNIVR)	341.125,00 €	51.168,75 €					392.293,75 €
Partecipante 2: Centro Alti Studi per la Difesa (CASD)	340.875,00 €	51.131,25 €					392.006,25 €
Partecipante ….		0,00 €					0,00 €
Totale							784.300,00 €

Firma digitale del
Legale rappresentante del Proponente o Soggetto capofila

ALLEGATO C - quota Budget Mezzogiorno

BUDGET DI PROGETTO	COSTO DEL PERSONALE	OVERHEAD	Costi per servizi di Consulenza Specialistica	Costi per licenze direttamente imputabili al progetto	Costi per materiali e attrezzature direttamente imputabili al progetto	Costi per altre tipologie di spese direttamente imputabili al progetto	COSTO TOTALE MEZZOGIORNO
Partecipante 1: Università degli Studi di Verona (UNIVR)	0,00 €	0,00 €					0,00 €
Partecipante 2: Centro Alti Studi per la Difesa (CASD)	0,00 €	0,00 €					0,00 €
Partecipante	0,00 €	0,00 €					0,00 €
Totale							0,00 €

Firma digitale del
Legale rappresentante del Proponente o Soggetto capofila