Allegato 2 – Thematic Areas for Spoke n. 4

Allegato Tecnico

Questo documento è strutturato in due parti. La prima parte (Parte I) fornisce una sintetica descrizione dei progetti scientifici già avviati in seno allo Spoke 4. La seconda parte (Parte II) descrive gli obiettivi scientifici che dovranno essere perseguiti dalle proposte progettuali oggetto del presente bando. La descrizione dei progetti scientifici descritti già attivati (Parte I) è intesa fornire il contesto in cui andranno a inserirsi le proposte progettuali oggetto del presente bando (Parte II).

La dotazione finanziaria e i requisiti finanziari della proposta suddivisi per Aree Tematiche sono riportati in Tabella 1.

Tabella 1 - Dotazione finanziaria e i requisiti finanziari

	Tematica	Dotazione Finanziaria	Costo minimo di ogni proposta progettuale	Costo massimo di ogni proposta progettuale	Di cui spesi nelle ragioni del mezzogiorno
a	Next Generation Cyber Ranges	€785,154	€628,123	€785,154	€0,00
b	Security of 5G	€1,413,431	€1,130,745	€1,413,431	€675,014
c	Security of Containerization Technologies	€1,237,329	€989,863	€1,237,329	€590,912
	TOTALE	**€3,435,914**	**€2,748,731**	**€3,435,914**	**€1,265,926**

Parte I – I progetti scientifici già attivati

Operating Systems (OS) and Virtualization Technologies (VT) are key enablers for existing and emerging computation and communication paradigms, namely cloud, fog, edge computing and 5G/6G. By leveraging the primitive security mechanisms provided by the hardware, OS and VT offer key security mechanisms and services (e.g., basic identity management and access control) upon which the security of applications, and henceforth of the whole cyberspace, is rooted. Spoke 4 is concerned with the development of high-level automated security services and innovative security assessment and assurance methodologies to support the secure-by-design development and verification of cloud, edge, and 5G applications. The effectiveness of the proposed techniques will be assessed by stress-testing them in simulated, yet highly realistic attack scenarios, safely run within a platform of federated Cyber Ranges.

Spoke 4 is coordinated by UNIGE and brings together several complementary initiatives to address the thematic line in its overall complexity. It relies on the implementation of the following project scopes (i.e., Ambiti Progettuali):

- Securing Containers (SecCo)
- Security in 5G and beyond (5Gsec)
- Affordable, Reusable and Truly Interoperable Cyber ranges (ARTIC)

SecCo focuses on supporting the secure development and deployment of containerized applications on distributed and heterogeneous environments. **5Gsec** addresses security in 5G interfaces and deployments, with specific emphasis on the security of software network functions. **ARTIC** aims to devise a framework for enhancing the capabilities and functionalities of current Cyber Ranges while ensuring their broader accessibility to a diverse range of organizations and users.

Spoke 4 launches Open Calls / Bando a Cascata to address certain tasks foreseen in each of the aforementioned project scopes. For each project scope, this document introduces the corresponding set of tasks that have to be managed by the participants with their proposals.

SecCo

Securing Containers

Abstract

The project aims at supporting the secure development and deployment of containerized applications on distributed and heterogeneous architectures. This will be achieved by extending and integrating existing

security assessment methodologies (e.g., SAST, DAST, and Code review) into the DevOps CI/CD pipeline. To this end, SecCo will develop a novel pipeline of new automatic security services, which will (i) prevent and reduce security vulnerabilities in the design, implementation, and deployment phases and (ii) identify and mitigate, at runtime, attempts to exploit them. SecCo will provide three main pipelined automatic security services granting, the (i) hardening of containers during the application development phase (the Hardening module), (ii) compliance verification of hardened containers with respect to some user-defined security policies to be granted to the microservice application executing on the containers' deployment (the Compliance Verification module), and the (iii) runtime monitoring of non-compliant containers when the microservice application executes in production (the Runtime Monitoring module). The SecCo pipeline will be implemented to be easily integrated into the different phases of the DevOps paradigm and applied to real container deployments containing complex microservice-based distributed applications.

Work Breakdown Structure

WP1 - Container Hardening

WP Description

The WP will define the enabling methodologies and tools to build a *Hardening module* able to output a set of secured containers - ready to host a microservice application - that are compliant with security best practices and the requirements of the CI/CD team. The hardening process includes threat modeling and vulnerability assessment (VA) of containers and the injection of security plugins to support security-critical operations (e.g., TLS communications and federated authentication).

- Task 1.1: Automated Vulnerability Assessment of Containers. UNIGE, CNR.
- Task 1.2: Building Secure-by-Design Containers. UNIGE, Open Call.

WP2 - Compliance Verification of Container Deployments

WP Description

The WP will focus on the design of a *Compliance Verification module.* This module receives a set of hardened containers (outputted from the Hardening module developed in WP1) and a security policy defined by the CI/CD team. The policy is related to the microservice application that is expected to be hosted and executed on the set of hardened containers. It defines a set of security constraints on the behavior of containers that must be satisfied to execute the application securely. The main challenge of the WP is defining proper formalisms to model the runtime behavior of containers, a specification language for the security policy as well as the corresponding analysis methodologies following a risk-based approach to automatically check the compliance of the containers' behavior with the provided security policy.

- Task 2.1 - Behavioral Models of Containers and Security Policy Specification Language. Open Call.
- Task 2.2 - Automatic Formal Verification of Container Models. FBK

WP3 - Runtime Monitoring

WP Description:

The WP will focus on defining methodologies and tools to build up a Runtime Monitoring module, whose aim is to verify the compliance of the executing containers with respect to the security policy defined in the context of WP2. In detail, this module aims at verifying whether non-compliant containers try to violate the security policy and checking the compliance of rules of the security policy that the Compliance Verification module cannot statically verify. Furthermore, the Runtime Monitoring module will also provide Anomaly Detection features (based on AI) to identify whether the container deployment may be the target of external attacks.

- Task 3.1 - Practical Runtime Monitoring for Container Deployments. FBK, CNR
- Task 3.2 - AI-based Anomaly Detection in the Container Ecosystem. CNR, UNISA, FBK
- Task 3.3 - Runtime Policies and Configuration Enforcement. Open Call.

WP4 - Service Implementation and Validation

WP Description

This WP will focus on the prototype implementation and integration of the three security modules constituting the SecCo pipeline, i.e., the Hardening module (from WP1), the Compliance Verification module (from WP2), and the Runtime Monitoring module (from WP3). Also, the WP will set up the appropriate testing environment to evaluate the SecCo pipeline on real-world microservice applications.

- Task 4.1 - Design and Implementation of the SecCo Service. Open Call.
- Task 4.2 - Validation and Performance Analysis. UNIGE, CNR, FBK, UNISA

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

ARTIC

Affordable, Reusable and Truly Interoperable Cyber ranges

Abstract

Cyber ranges (CRs) are strategic assets for cyber security. According to the European Cyber Security Organisation (ECSO), CRs can be used by a wide range of target users and for many purposes including cybersecurity education, test, and research. ECSO also indicates issues associated with CRs. Similarly, to Gartner, ECSO confirms the positive and rapid trend of CRs but emphasizes that they are generally affordable and available only to large enterprises. Moreover, they highlight that CRs are constantly evolving. They need to be continuously developed to support new cyber security domains, integrate new technologies, and exploit their capabilities in new applications. Finally, they focused on the strong requirement of enabling cooperation between multiple CRs. This project starts from the above issues and includes investigating new methods and mechanisms to address the following challenges. (i) Make CRs affordable to all organizations by reducing technology and personnel costs. Containerization and microservices will be applied to reduce technology costs and automated tasks, verification, and testing techniques for reducing human ones. (ii) Support new domains and cross-domain scenarios by studying and implementing needed assets, potential weaknesses and vulnerabilities, and specific attack and defense techniques. This activity will focus on critical infrastructures and novel threat models, e.g., adversarial attacks against systems based on AI and disinformation spreading. (iii) Support new enabling technologies and paradigms by leveraging the Digital Twins (DTs) paradigm. DTs are extensively used to create virtual replicas of physical assets, e.g., ICS environments, and run simulations without impacting operations. They can extend the capabilities of CRs, and this activity will focus on their integration. (iv) Identify new application areas by running honeypots for Industrial Control Systems (ICSs) and sandboxes. A CR infrastructure and supported scenarios will improve current honeypots and sandboxes by luring knowledgeable adversaries, detecting sophisticated attacks, and testing malicious software that can spread across systems. (v) Foster cooperation by introducing federation and interoperability. Promoting federation will require studying and integrating common standards of operation, and interoperability creating a technological infrastructure that groups multiple CRs to deliver a single simulation environment.

Work Breakdown Structure

WP1 - A framework for Cyber Ranges

WP Description

The WP will concentrate on the architectural aspect of cyber ranges and the components required to facilitate training and testing operations and their outcomes.

The first goal is exploring methodologies to reduce the significant Total Cost of Ownership (TCO) that affects current CRs. It will focus on (a) technology costs, i.e., costs for covering the ownership and complexity of the management infrastructure and the simulation environment and, (b) human costs, i.e., the need for specialized personnel involved in different teams. Furthermore, an objective will be to investigate technologies that can improve the capabilities of current CR implementations. In particular, this WP will examine how implementing the Digital Twin paradigm in CR can improve their outcomes by facilitating the creation of more realistic simulation scenarios.

- Task 1.1 - Techniques and tools for the design, verification, testing of scenarios and runtime injections (UNIGE, IMT, CINI, LEONARDO).
- Task 1.2 - Integrating capabilities of Digital Twins to emulate and simulate realistic scenarios (UNICAL, FINCANTIERI).
- Task 1.3 - Affordable orchestration and virtualization technologies (Open Call).

WP2 - New application domains and exploitation scenarios

WP Description

The WP will focus on the contents, namely scenarios, that cyber range can support and run. The first activity deals with being consistent w.r.t the massive increase in cyber threats and the growth of attack surfaces. In detail, the expansion includes new attacking techniques, e.g., adversarial attacks against systems based on artificial intelligence, and novel vectors and vulnerabilities involving different types of critical infrastructure, e.g., deployments of 5G facilities, and OT systems, e.g., ships. Similarly, CRs must evolve to create environments replicating these scenarios. To this aim, this WP will examine the peculiarities of each domain in terms of needed assets, potential weaknesses or vulnerabilities, and specific attack and defense techniques. Moreover, it will analyze if and how the core components of CRs, e.g., the orchestrator, the scoring system, or the teams' toolsets, need to be extended to support them. A second activity is focused on leveraging the realism of scenarios and isolation offered by CRs to explore new potential capabilities other than training and testing. In particular, this WP will consider the possibility of being used as an enhancing resource for an extensively used cyber defense tool: honeypots.

- Task 2.1 - AI tools for cybersecurity and AdvML (UNIGE).
- Task 2.2 - Fake news and disinformation campaigns scenarios (IMT).
- Task 2.3 - Hardware-based scenarios (CINI).

- Task 2.4 - Critical infrastructures-related scenarios (Open Call).

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

5Gsec

Security in 5G and beyond

Abstract

This project focuses on the security of 5G architecture and its evolution towards 6G, with a scope that covers security, privacy, and availability challenges across various domains of 5G architecture. These include the air interface, Multi-access Edge Computing, transport infrastructure, virtualized core network functions, and management and orchestration. The project combines long-term 6G-oriented research with short-term vulnerability assessments and security assurance for upcoming 5G deployments. It specifically covers emerging localization techniques, air interface assessment tools, secure integration of non-3GPP access technologies, protection against massive IoT botnet DDoS attacks, privacy threats posed by emerging wireless sensing technologies, security automation and orchestration, and more. The project also aims to assist decision-making bodies in Italy, who are expected to establish a certification scheme for 5G, by developing and evaluating different security assurance and testing schemes in realistic environments.

Work Breakdown Structure

WP1 - Air Interface and Access Network Security

WP Description

This WP encompasses security and privacy-related activities concerning the radio interface. The main focus is on 3GPP access technologies and their evolution towards 6G, as well as on the emerging privacy concerns caused by the widespread distribution of antennas and their environmental "sensing" capabilities. Moreover, owing to their widespread deployment and recent integration into the 5G architecture through the N3IWF (Non 3GPP Inter Working Function), the WP also covers non-3GPP systems, with an emphasis on the newly emerging LoraWAN technology.

- Task 1.1 - Platforms and methodologies for air interface security assessment (CNIT)
- Task 1.2 - Securing Multi-access IoT technology towards 5G Integration (UniRM1, UniCAL)
- Task 1.3 - Physical Layer threats and solutions towards 6G (Open Call).

WP2 - 5G infrastructure security

WP Description

This work package focuses on security enhancements and solutions for the non-radio components and technologies that form the basis of the 5G infrastructure, including edge and core systems and functions, as well as their management and orchestration. Special attention is given to the key features of 5G and beyond architecture, such as its new service-oriented architecture based on Network Functions Virtualization, support for network slicing, and emerging support for decentralized components like Multi-Access Edge Computing systems and access means, including non-terrestrial scenarios.

- Task 2.1 - Secure Orchestration and orchestration for security (UniGE, CNIT)
- Task 2.2 - Resilience and protection against 5G network disruption threats (UniSA)
- Task 2.3 - Security and trust in decentralized 5G scenarios (Open Call).

WP3 - Security assurance and monitoring in 5G deployments

WP Description:

The objective of this final work package is to focus on security monitoring and testing. The aim is to ensure that the security properties, which were assumed to be guaranteed during the design phase, are not compromised due to implementation issues or misconfigurations. Both the content and the methodologies for security testing will be addressed, which involves determining what to test and how to test it. Additionally, 5G-tailored monitoring platforms and novel testing means such as protocol fuzzing will be experimented on realistic 5G testbeds. We will further give special attention to integrating 5G-specific security tests into DevSecOps frameworks and developing security monitoring tools that are tailored to the unique characteristics of the 5G infrastructure. Finally, we aim to establish contacts with the Italian regulatory bodies responsible for creating a certification scheme for 5G, so as to provide technical feedback and lessons learned from realistic environments on testing methodologies and schemes that could meet the certification needs.

- Task 3.1 - 5G Security Assurance and Risk Assessment: gap analysis and extensions (FUB, Leonardo, CNIT)
- Task 3.2 - 5G Security testing platforms and methodologies (CNIT, FUB, Leonardo)
- Task 3.3 - 5G security Monitoring and Lawful Interception (Open Call).

Parte II – Obiettivi scientifici dei progetti oggetto del Bando

For each project scope (*Ambito Progettuale*) included in Spoke 4, the sections below provide a detailed breakdown of the tasks and their corresponding main objectives. The selected proposal must successfully complete the tasks outlined below, ensuring that the requirements and objectives of the project milestones are met.

Each proposal must focus on addressing a specific project scope. In the case of more than one partner participating in the same proposal for addressing the same project scope, each of them must clearly state their role, expected outcomes, and corresponding budget.

Additionally, the proposal must provide a plan of the activities over time by producing a GANTT chart including milestones in accordance with the overall project GANTT reported in Figure 1 and meeting the deadlines for documentation and software deliveries.

Project Scope: SecCo

Building Secure-by-Design Containers

This task will involve the definition of the pipeline to support the hardening of general-purpose containers to meet the technical and security features of the application (e.g., TLS communications, two-factor authentication, and encryption at-rest) provided by the CI/CD team and security best practices.

Main Objectives:

- Identification of a methodology to parse requirements provided by the CI/CD team;
- Support the definition of a set of security plugins to add plug-and-play security features inside containers (e.g., TLS and Encryption);
- Design of the patching techniques to customize general-purpose containers and provide hardened container templates;
- Support the definition and implementation of the Hardening Module and the included components;
- Ensure the soundness of the hardening pipeline executed by the module (i.e., from the requirement parsing to the release of the hardened template).

Behavioral Models of Containers and Security Policy Specification Language

This task aims at defining a sound and complete policy language for describing all the interesting security constraints of the security policy, as well as a formal modeling of the behavioral model of containers describing at least all the security-sensitive operations carried out by the containers.

Main Objectives

- Identify or define the appropriate policy language to describe security constraints on containers and ecosystems of containers, thereby collaborating with WP3 to include both static and dynamic rules;
- Define a model to describe behavioural models of containers describing at least all the security-sensitive operations carried out by single containers and their composition;
- Define a methodology to infer behavioural models from a single container and the composition of containers;
- Collaborate with Task 2.2 to define the Compliance Verification module and ensure the soundness of the entire approach (from policy definition to formal verification).

Runtime Policies and Configuration Enforcement

This task will focus on defining proper ways to write down, implement and enforce security policies to monitor the architecture of the Runtime Monitoring module defined in Task 3.1 and 3.2. The task also aims at defining non-disruptive countermeasures whenever the behavior of a container may violate the security policy.

Main Objectives

- Interact with WP2 to propose a security policy specification language that can define rules to be evaluated at runtime;
- Identify the appropriate methodologies and technologies to enforce security policies at runtime;
- Collaborate with Tasks 3.1 and 3.2 to define the Runtime Monitoring module;
- Define non-disruptive countermeasures to apply the containers and/or the environment to react to violations of the security policy;
- Support the implementation of the Runtime Monitoring module.

Design and Implementation of the SecCo Service

This task concerns the definition of the detailed specifications of the SecCo architecture. The architecture will specify the main functional building blocks of the SecCo modules, as well as the structuring relationships driving their integration. Then, the task will proceed with the PoC implementation of the three security modules and all the necessary configurations to integrate the SecCo modules in a DevOps pipeline.

Main Objectives

- Define the detailed specifications of the entire SecCo architecture;
- Select the appropriate technologies to implement the SecCo services;
- Implement the PoC of the SecCo services and all the required configurations to integrate them in the DevOps pipeline defined in Task 4.2 - Validation and Performance Analysis;
- Support the identification of relevant use cases to test the architecture and support the configuration of the required demo environments.

Project Scope: ARTIC

Affordable orchestration and virtualization technologies

The task deals with technological costs that affect TCO. In particular, it focuses on investigating the potential benefits that a microservices approach and containerization can bring to CR.

Main Objectives

- Contributing in the analysis of design patterns concerning microservices and containerization, which offer potential solutions for implementing the framework designed in Task 1.1;
- Assist project partners in the practical implementation of the PoC for the framework;
- Support in identifying pertinent use cases and scenario contents for testing components of the framework.

Critical infrastructures-related scenarios

This task revolves around Critical Infrastructures-related scenarios, aiming to utilize them in exploring a CR that can function as honeypots. By incorporating CR capabilities into honeypots, it becomes possible to leverage more complex and realistic infrastructures, lure knowledgeable attackers, and detect and study sophisticated attacks.

Main Objectives

- Examine and suggest enhancements to the framework to support techniques for attracting cybercriminals, e.g., adequate simulation of network traffic, physics-awareness, the possibility of code injection on the PLCs, or consistent PLC registers manipulations;
- Propose solutions for improving CR components to detect and isolate unexpected behaviors and obtaining the required evidence when utilized as a honeypot;
- Support in defining and implementing the scenario components for the use case.

Project Scope: 5Gsec

Physical Layer threats and solutions towards 6G

This call aims to extend 5Gsec's coverage of security solutions and protection techniques by seeking proposals that cover Physical Layer threats crucial for 6G evolution. Proposals should address advanced radio capabilities to enhance localization security in beyond 5G systems and explore cutting-edge technologies and techniques to counter potential threats in the evolving network landscape. This includes, but is not limited to, jamming, spoofing of localization signals, and relevant attack scenarios (rogue BS, overshadowing attacks, wormhole attacks, etc). Moreover, proposals should also address different threat models emerging when smart surfaces are integrated into the environment, thus encompassing the malicious control of smart surfaces by a threat actor. Innovative technologies and methodologies are advocated for creating intelligent surfaces that protect sensitive user data while facilitating seamless connectivity and communication in the emerging 6G environment. Finally, to guarantee trustworthiness of interactions at the physical level, we solicit research proposals that explore innovative techniques and technologies to authenticate users, devices, and data at the physical layer within 6G systems, taking into consideration the game-changing nature of smart surfaces on the physical layer.

Main objectives:

- Identify and analyze the threat surface involved in location security and reconfigurable smart surfaces in beyond 5G systems.
- Investigate cutting-edge technologies to detect and thwart attacks based on jamming, spoofing of localization signals (SRS, PRS), and rogue base stations. Propose solutions and methods for the integrity of localization signals and the hardening of location management.
- Explore innovative technologies and methodologies that leverage RIS' controllable nature to enhance user privacy while preventing threat actors from exploiting RIS for malicious purposes.
- Investigate how smart surfaces impact physical-level authentication, addressing authentication in scenarios of partially controllable channels. In these scenarios, the attacker may infer the channel configuration or perform more efficient attacks based on its partial knowledge.

Security in Decentralized 5G Scenarios.

The goal of this call is to expand the scope of 5Gsec's infrastructure security challenges, specifically addressing security issues emerging in decentralized scenarios. This includes Multi-access Edge Computing (MEC), non-terrestrial 5G RAN scenarios, and, more broadly, mechanisms capable of enhancing trust and security in unconventional distributed scenarios. Given the pivotal role of Edge computing, which brings computational power closer to users and devices, proposed applications should focus on security in Multi-Access Edge Computing environments. This encompasses designing means to secure and optimize resource allocation and segmentation within MEC environments. Furthermore, this call aims to encompass various scenarios,

including non-terrestrial ones, extending to other decentralized contexts like IoT networks, cloud continuum, satellite-based communication systems, etc. Proposals should concentrate on enhancing security and trust mechanisms in these diverse decentralized 5G scenarios, ensuring the resilience and reliability of these emerging technologies.

Main Objectives:

- Develop and evaluate dynamic resource allocation algorithms adaptable to varying workloads and demands in MEC environments, optimizing resource utilization while maintaining security requirements.
- Extend security orchestration models and frameworks to edge systems, integrating security mechanisms into MEC environments. Assess the applicability of AI and ML for MEC-based threat detection and resolution in real-time.
- Investigate techniques for Privacy-Preserving Edge Computing, enabling users to benefit from MEC advantages while maintaining data privacy and security.
- Explore how Non-Terrestrial Networks influence security protocols, developing methods for confidentiality, integrity, and availability that can withstand the unique challenges of space-based and aerial networks.
- Research and develop mechanisms to enhance the resilience of decentralized 5G networks against various types of attacks, including DDoS attacks and network disruptions.

5G security Monitoring and Lawful Interception

This call aims to complement 5Gsec's WP3 activities, so far focused on security assurance, with monitoring tools and security-focused monitoring solutions tailored to the unique characteristics of the 5G infrastructure. Indeed, unlike conventional internet traffic, 5G traffic is uniquely complex and dynamic. It encompasses a multitude of applications, services, and devices, and its characteristics are markedly different from traditional internet traffic. This is due to the introduction of network slicing, ultra-low latency, edge computing, massive IoT connectivity, and an array of novel use cases. In light of these transformative changes, proposals should address 5G traffic monitoring via specialized protocol parsers for 5G control protocols, adapters for 5G-specific interfaces, and high performance features for coping with real-time monitoring and ultra-high data rates. Moreover, we seek innovative approaches and solutions for 5G lawful interception, addressing the challenges posed by 5G networks, such as encryption, network slicing, and low latency, while ensuring compliance with legal requirements and privacy regulations. Advanced methods and technologies that enable efficient and effective lawful interception should also address decentralized settings.

Main objectives:

- Develop platforms for efficient data capture, protocol parsing, and protocol analysis on 5G core network interface;

- Design data analysis algorithms, also driven by AI/ML techniques, to determine traffic anomalies and detect threats;
- Develop algorithms and solutions for processing data collection from a multiplicity of vantage points, hence involving de-duplication, correlation, fusion, etc;
- Provide tools and solutions for encrypted traffic analysis;
- Develop data search/analytic tools to aid Law Enforcement Authorities in mining data and in extracting behavioral information from intercepted traffic, while ensuring legal compliance.