Allegato Tecnico
SERICS
Spoke4 "Operating Systems and Virtualization Security"
Innovation Open Call

Avviso pubblico per la presentazione di proposte progettuali per la realizzazione di attività di ricerca industriale e sviluppo sperimentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 4 "Operating Systems and Virtualization Security" (UNIVERSITA' DEGLI STUDI DI GENOVA) ammesso a finanziamento con D.D. n. 1556 dell'11 ottobre 2022, registrato dalla Corte dei Conti il 04/11/2022 n. 2783 – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3 Creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base", finanziato dall'Unione europea – NextGenerationEU - Codice CUP D33C22001300002

Spoke 4 aims to establish a center of excellence on the security of Operating Systems (OS) and of the Virtualization Technologies (VT). OS and 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. The research activities carried out by Spoke 4 focus on 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.

Securing Containers (SecCo): 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.

Security in 5G and beyond (5Gsec): 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.

Affordable, Reusable and Truly Interoperable Cyber ranges (ARTIC): 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.

INNOVATION OPEN CALL

This innovation open call aims to select innovative projects capable of elevating the TRL (from 3-4 to 5-6) of selected research results and solutions currently under investigation in the aforementioned projects: SecCo, 5GSec, and ARTIC. Among the activities that can be funded by the call are pilot projects, demonstrators, and/or experiments. Proposed activities are expected to have a high degree of complementarity with (and/or leverage the results produced by) the research actions carried out in the SecCo, 5GSec, and/or ARTIC projects. The following research topics appear to align well with the call's goals (however, activities outside these topics are welcomed, as long as they are related to at least one of the Spoke projects). Proposals are not expected to cover all the following topics, but those covering multiple topics will be prioritized.

A1. DevSecOps CI/CD Services for Container Security. Develop a set of DevSecOps CI/CD services to enhance container security, evaluate security policies, and monitor container ecosystems in alignment with the SecCo project's architectural choices. The services must reach at least TRL 5 and shall prioritize the use and integration of state-of-the-art, preferably open-source security tools, shall support for OCI-

compatible security assessments with a specific focus on the Docker ecosystem, and must support the integration with leading version control platforms like GitHub and GitLab. Proposals that will release the services with an open-source software license (e.g., the GNU Affero General Public License version 3) will be prioritized.

A2. OS-Hardening Solutions for Virtualization Security. Develop and/or extend low-level OS-hardening solutions to enhance the security, observability, and monitoring capabilities of virtualization technology and hypervisors. Either HW-based approaches, leveraging Trusted Platform Modules (TPM), and purely software-based approaches such as Virtual Trusted Platform Modules (vTPM) or ad-hoc/innovative hardening solutions are in scope. Demonstrate robustness against VM/container escape attacks, providing improved isolation in multi-tenancy contexts. Proposals that will release the solution with an open-source software license (e.g., the GNU Affero General Public License version 3) will be prioritized.

A3. Industrial Case Scenario for SecCo Services. Demonstrate the effectiveness of the SecCo services through an industrial case scenario involving a microservice container ecosystem. The aim of this topic is to provide detailed functional and security requirements, all necessary configurations for using the SecCo services, and a description of the threat/vulnerability/attack scenarios for testing. The experimental phase must include the validation of the SecCo framework in terms of module efficiency, scalability, success rates in detecting and mitigating threats and attacks, and ease of integration with existing CI/CD pipelines.

B1. Security Assurance of 5G virtualized core networks. Using the ScasDK security assurance platform developed in 5Gsec, the proposal shall develop new test suites either implementing standard-based 3GPP SCAS tests for supplementary 5G core network, and/or designing custom tests, possibly covering also the underlying cloud infrastructures. Techniques should be further proposed to validate the test implementation and provide evidence for verifying the correctness of the runtime testing process. The usability and effectiveness of the developed test suites over Open Source 5G virtualized core networks should be preferably assessed on containerized 5G core networks deployed via Kubernetes. Proposals leveraging/extending insights from the SecCo projects are specifically encouraged.

B2. API Security in 5G Virtualized Core. Investigate and enhance API security within a 5G virtualized core environment, focusing on identifying vulnerabilities and implementing robust protection mechanisms. Assess the effectiveness of proposed solutions in mitigating common API security risks, leveraging insights from OWASP API security best practices, and explore techniques for runtime API monitoring and security posture evaluation. Proposals which, in addition to API security, also include activities focusing on the underlying cloud platform security will be prioritized.

B3. Network Function Security Enhancement through Decentralization. Explore the enhancement of network function security through decentralization and disaggregation strategies. Leverage offloading capabilities to dynamically deploy security-oriented functions/services across diverse hardware platforms, edge clouds, and smart NICs. Assess the effectiveness of the proposed strategies over network monitoring scenarios, traffic filtering, network segmentation, detection and isolation of critical functions. Adopt a moving target defense approach, promote solutions which permit the dynamic migration of security-oriented network functions across the network and diverse hardware platforms.

C1. Horizontal Scalability and Network Layer Control. Must enhance the horizontal scalability of the current Proof of Concept (PoC) implementation of the ARTIC Framework by integrating the Kubernetes platform. This scalability improvement will enable the framework to execute single scenarios across multiple hosts, as well as support multiple concurrent instances. It is crucial to maintain high availability for all components, with a Recovery Time Objective (RTO) of 60 seconds. Additionally, the network layer should be capable of supporting multiple, dynamically provisionable, and independent Layer2 networks. These networks should be managed by services operating from within the cluster itself, independent of the underlying infrastructure. Finally, the network layer should provide a way for external endpoints to be connected to such networks.

C2. Authentication Mechanisms and Graphical User Interface. Improve the ARTIC framework with the integration of authorization and authentication solutions by leveraging standardized and state-of-the-art protocols, such as OpenID Connect, User-Managed Access (UMA), and Google's Zanzibar architecture. It would also be beneficial to support the federation for these authentication and authorization facilities, for instance, by leveraging the draft OpenID Federation standards. For effective management and oversight, it is advisable to extend the framework with a graphical user interface that is accessible via a browser. This interface should provide administrators with information about the state of the framework components. Additionally, the user interface must facilitate the configuration, provisioning, and deprovisioning of scenarios. These scenarios should be discovered and stored within a repository in a standardized format to ensure consistency and reliability. Lastly, the graphical interface should provide users with access to situational awareness dashboards, offensive and defensive tools, and application consoles or GUIs, according to their level of privilege and role in the exercise. All software developed must be open-source, preferably licensed under the GNU Affero General Public License version 3.

C3. Training and testing scenario. Provide the implementation and documentation of a representative and realistic IT scenario that includes at least 32 hosts. It must be mainly based on Windows servers, ensuring support for Active Directory and Exchange servers, and clients. The scenario must be appropriately misconfigured to reproduce recent threats, vulnerabilities, and attacks. Provisioning of the scenario must start from golden images and software installation and configuration/misconfiguration must be automatically performed using state-of-the-art Infrastructure-as-Code solutions. Automation of attacks constitutes a preferred feature.