Federating cyber-ranges: the experience of the ECHO project

Marco Angelini, Massimiliano Tarquini

Abstract

Cybersecurity represents one of the major concerns of modern societies. The pervasiveuse of ICT technologies offers opportunities to improve human activities in several sectors, from smart automotive to digital healthcare; however, it also opens the way to new vulnerabilities and threats that can put at risk the correct behavior of those technologies, having consequences ranging from the information plane to the physical one.

In this context, the European Commission is trying to keep the pace, promoting its own cybersecurity strategy, with fundings allocated to research activities (e.g., H2020 framework) to develop new solutions.

Among technical aspects, one prominent topic is the need to provide better training technologies that can help in forming the interested actors (e.g., cybersecurity operators, decision-makers, etc.) on realistic simulated scenarios, ranging from pure technical skills to complex scenario simulations.

This short essay introduces the work carried out within the H2020 ECHO project (European network of Cybersecurity centres and competence Hub for innovation and Operations) by the Link Campus University team while building a common cybersecurity strategy for Europe, inside the framework of the European Cybersecurity Competence Center located in Bucharest.

To this purpose, ECHO project develops a marketplace of multi-sector services coming from multiple cyber ranges, the E-FCR (ECHO Federated Cyber Range. This paper gives an overview of the architecture of this solution, and highlights the effort in making it capable to federate different existing cyber-ranges technologies in providing training and simulation services in an unified way.

1. Next-generation cyber ranges

The first definition of a next-generation cyber range was coined by the European Cybersecurity Organization (ECSO), which defines a cyber range as:

"*a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organization's ICT [Information and Communication Technology], OT [Operational Technology], mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realization and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases*" [1].

Looking at existing state-of-the-art solutions for the cyber-range domain, several contributions exist in the scientific and technical literature that coped with providing solutions for cyber ranges. Yamin et al. [2] developed a taxonomy for cyber range systems focusing on architecture, scenarios, capabilities, roles, tools and evaluation criteria. The work is aimed at evaluating cyber ranges in accordance with

existing best practices and lessons learned from contemporary research. Ahmad et al. [3] presents EVA, a model for implementation of a hybrid cyber range based on a Water Supply System and capable of modeling different scenarios of application; on similar topic, Kavallieratos at al. [4] surveys cyber-physical testbeds to identify key features and a reference architecture for cyber-physical ranges. Rosenstein at el. [5] present the architecture for the Range-level Command & Control System (RangeC2) developed as part of the Johns Hopkins University Applied Physics Laboratory's implementation of the DARPA National Cyber Range (NCR) [6]. The authors claim as objectives the management of all range resources, the management of numerous concurrent experiments and the enforcement of each experiment's resource security and perimeter isolation. However, this proposal does not envision a federation but works on single, complex range. Peratikou et al. [7] discuss different solutions on how to federate cyber ranges. Their contribution however is very specific on the network interconnection, where they review technical contributions. Urias at al. [8] present a discussion on limitations and needs of future cyber ranges, listing among others Architectural Integration Testing, Automation and pre-configuration, Credential and Configuration management, Licensing when multiple ranges are connected together. Finally, Karjalainen and Kokkonen propose the concept of cyber arena [9], a next generation cyber range. In the paper they discuss elements that next generation ranges must have in order to better support modern training activities.

Compared to a traditional cyber range, a next-generation cyber range is a platform which can simulate ICT/OT environments and a set of integrated functionalities for more effective usage.

Cyber ranges can be used by different actors, serving sector-specific purposes. Among them we identify strategic decision-makers, security professionals, military agencies, educators, researchers, all having different skills and training needs.

They additional can provide different services to the identified actors, ranging from security testing, supporting research and development activities, helping in competence building, increase of cybersecurity posture and cyber-resilience, provide security education and awareness.

Cyber ranges, hence, offer a flexible solution that can meet multiple needs. The versatility and the wide spectrum of services make them worth further investigation, as a tool to rely upon to strengthen EU cybersecurity in the future.

In this scenario fit the contributions of the H2020 ECHO project. Its main goal is to strengthen the proactive cyber defense of the European Union, enhancing Europe's technological sovereignty through effective and efficient multi-sector and multi- domain collaboration. The project will develop a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents.

This goal is declined in a set of activities, covering:

1. ECHO Governance Model: Management of direction and engagement of partners
2. ECHO Multi-sector assessment framework: Transverse and inter-sector needs assessment and technology R&D roadmaps
3. ECHO Cyber skills Framework and training curriculum: Cyber skills reference model and associated curriculum
4. ECHO Security Certification Scheme: Development of sector specific security certification needs within EU Cybersecurity Certification Framework from ENISA
5. ECHO Federated Cyber Range: Advanced cyber simulation environment supporting training, R&D and certification
6. ECHO Early Warning System: Secured collaborative information sharing of cyber-relevant information

2. The ECHO Federated Cyber Range (E-FCR)

Focusing on activity five, the ECHO Federated Cyber Range (E-FCR) represents a complex system that interconnects existing cyber range capacities and capabilities. The overarching goal is to provide the end-user with an overview over different cyber ranges in terms of capabilities and capacities, with a second goal to build a marketplace of composable services starting from the federated ranges to foster their adoption and standardization. It allows the simulation of complex realities and inter-sector dependencies of an inter-sector scenario.

The E-FCR is built on a microservices architecture to develop the overall system as a collection of services that are highly maintainable and testable, loosely coupled, independently deployable, organized around business capabilities.

The microservice architecture enables the rapid, frequent, and reliable delivery of the E-FCR, while allowing the organizations involved in the project to evolve its technology stack.

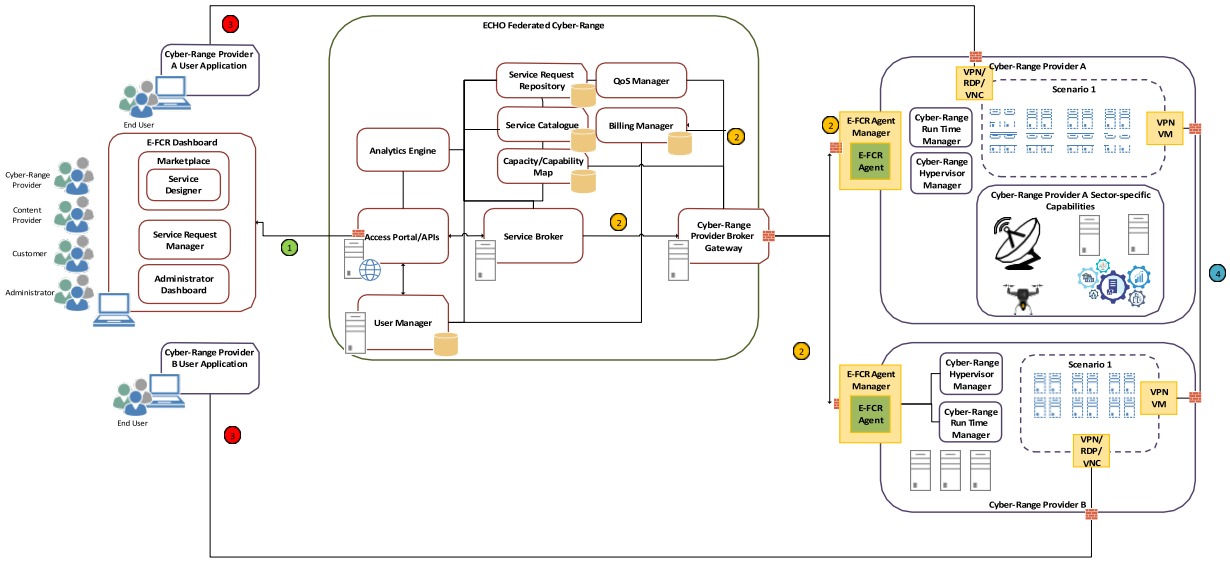

Figure 1: E-FCR high-level architecture

E-FCR consists of several components, each one developed independently by an organization. Some of them are related to general activity of the federation as a marketplace (**marketplace module**), like the **Billing Manager**, determining how much a customer should be charged for a given service; the **Quality of service manager**, monitoring the actual quality of the provided services, the **Service designer** for providing new services and the **User manager** for registering users and service providers.

Focusing instead on the sequence that allows to select a service, from the left to the right of the architecture visible in Figure 1.

- The **E-FCR Dashboard** is the main component in the client tier. It acts as a container for the different subcomponents that together build up the complete E-FCR user interface and it is the main entry point, from a user perspective, to the usage of the federation;
- The **Access Portal** represents the main entry point for the management part of the E-FCR. It acts as an API gateway and is responsible for routing a request to the correct component, ensuring that only authenticated requests are allowed to proceed;

- The **Capacity Capability Map** is essential for the E-FCR, since it manages all the capabilities and capacities of the interconnected cyber ranges. Two key features characterize the Capacity Capability Map component: first, it stores the capabilities and capacities of all cyber ranges interconnected to the Federation; secondly, it reserves the resources and capabilities for a current or future time to a customer in order to allow him to perform the requested service;
- The **Service Catalogue** is responsible for storing and making available the Services for the Marketplace (uploaded contents from Content Provider or Cyber Range Providers);
- The **Service Request Repository** is responsible for the user interface related to the overall management of service requests between end-users and cyber range providers. It ensures insight into the overall status and progress of a service request and facilitates the communication between the stakeholders of a service request;
- The **Service Broker** is mainly responsible for receiving submitted Cyber Range Service Requests from the Customer via the Service Request Repository. It is also devoted to pre-validate such requests (interrogating the Capacity/Capability Map component), preparing the Service order and the technical configuration for the Cyber Range Providers. The Service Broker may leverage machine learning in order to deal with the Service Requests in the most efficient way;
- The **Provider Broker Gateway** acts as a broker between cyber range platforms (represented by Agents)and E-FCR Mid-Tier components, such as Service Catalogue, Capacity Capability Map, and QoS Manager. It shields E-FCR components from the complexity of cyber ranges topology.
- The **Agent Manager**, that is a component deployed on each single cyber range, external to the federation, and that allows the intercommunication of each range with the federation through the Broker Gateway. The modularity of this component allows the deployment of multiple agents, each one developed for different services requiring different technologies (e.g. implemented in different programming languages), on the same cyber range and on the orchestration of the data they send and receive from the federation. In this way, the E-FCR allows to federate multiple ranges without imposing a common technology but remaining transparent to the specific technological choices that each provider chose for its range(s).

It is on those two final components that the work of Link Campus University focused the most as the component owner. The couple of Provider Broker Gateway and Agent Manager constitutes the linking point between the federation of cyber-ranges (the E-FCR platform) and the single ranges. This mechanism allows a loose coupling between the platform technology and the technology that each of the cyber-ranges to federate provide. Both components act in a coordinated way, and in particular an Agent Manager can even support the deployment of multiple agents, one for service or technology stacks of the cyber range to federate, allowing a centralized local management of the service exposed to the federation. These characteristics make the maintenance and future integration of new services modulable, where the integration of new services does not affect the existing ones.

The described components and their interconnection inside the federation allow a set of advantages in deploying the federation:

modularity/customizability, meaning that different versions of the federation can be deployed depending on the number of federated entities andon the scope of the training activities, where each of them is able to work in isolation and where differentcombinations of those components are possible. In this way, smaller entities could choose to federate just the technical parts of the simulation, leaving out, for example, the creation of customized services and or the QoS management. The proposed architecture responds to different needs, remaining upgradable in a second moment to its broader version.

technological transparency which is the capability of the Agent manager and Broker gateway components to accommodate for heterogeneous technology put on each single range, allowing to federate very different cyber ranges from their technological implementation. The effort to federate a range is reduced to simply developing the needed agent by implementing a simple API exposed by Agent Manager component.

reusability and sharing of best practices. Indeed, the architecture allows the sharing of very complex training scenarios to different stakeholders being part of the federation, ranging from Enterprises, Training centers, Research centers, university, and competition organizers. Components like Service Designer and Service Broker allow for composition of several services being delivered by different providers on different cyber-ranges, forming new services that are built on top of existing ones. This aspect helps sharing of best practices and excellences and allow the reusability of existing scenarios (already tested and reliable) to build more complex ones, improving their scalability and fostering the creation of an ecosystem of composed services (with related new business opportunities).

3. Conclusion

The E-FCR is currently in implementation and at the current state of development the E-FCR is implemented at version 3, reaching TRL8. The ECHO consortium is conducting testing activities on both efficacy and efficiency of the implemented federation, with an increasing number of federated ranges and demonstrating scenarios. More information can be found on the official ECHO project website [10].

References

[1] European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges: From Hype to Reality," *SWG 5.1 I Cyber Range Environments and Technical Exercises,* pp. 1-28, March 2020.

[2] M. M. Yamin, B. Katt and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security - https://doi.org/10.1016/j.cose.2019.101636,* vol. 88, no. 101636, 2020.

[3] S. Ahmad, N. Maunero and P. Prinetto, "EVA: A Hybrid Cyber Range," *ITASEC 2020 - Italian Conference on Cyber Security, Ancona (IT), February 4th-7th, 2020,* vol. 2597, pp. 12-23, 2020.

[4] G. Kavallieratos, S. K. Katsikas and V. Gkioulos, "Towards a Cyber-Physical Range.," *In Proceedings of the 5th on Cyber-Physical System Security Workshop (CPSS '19). Association for Computing Machinery, New York, NY, USA,* no. DOI:https://doi.org/10.1145/3327961.3329532, pp. 25-34, 2019.

[5] M. &. C. F. Rosenstein, "A Secure Architecture for the Range-Level Command and Control System of a National Cyber Range Testbed. In CSET.," 2012.

[6] DARPA, "The National Cyber Range: A National testbed for Critical security research," [Online]. Available: https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf.

[7] A. Peratikou, C. Louca, S. Shiaeles and S. Stavrou, "On Federated Cyber Range Network Interconnection," *International Networking Conference; INC 2020: Selected Papers from the*

12th InternationalNetworking Conference, Vols. Springer, Cham. https://doi.org/10.1007/978-3-030-64758-2_9, pp. 117-128.

[8] W. M. Stout, V. Urias, B. P. Van Leeuwen and H. W. Lin, "Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper.," *International Carnahan Conference on Security Technology (ICCST),* vol. doi: 10.1109/CCST.2018.8585460, pp. 1-5, 2018.

[9] M. Karjalainen and T. Kokkonen, "Comprehensive Cyber Arena; The Next Generation Cyber Range," *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* vol. doi: 10.1109/EuroSPW51379.2020.00011, pp. 11-16, 2020.

[10] H2020 ECHO project official website: https://echonetwork.eu/