The SPIDER concept:

A Cyber Range as a Service platform

Christos Xenakis, Anna Angelogianni, Eleni Veroni
Department of Digital Systems
University of Piraeus
Piraeus, Greece

Neofytos Gerosavva, Vasileios Machamint
R&D Unit
EIGHT BELLS
Nicosia, Cyprus

Eirini Karapistoli, Matthias Ghering
Research & Innovation Department
Cyberlens
London, UK

Pierluigi Polvanesi, Angela Brignone
Product Development
Ericsson TEI
Genoa, Italy

Jeronimo Nunez Mendoza, Antonio Pastor
GCTIO- Network Innovation,
Telefonica I+D,
Madrid, Spain

Abstract— **The evolving cyber security threat landscape along with the extensive application of the 5G technology in various sectors brings together several cyber security concerns. To that extent, there is an apparent need for appropriate testing and training before the massive commercial deployment of 5G. The SPIDER platform proposes an innovative Cyber Range as a Service (CRaaS) platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges into a unified facility for (i) testing new security technologies, (ii) training modern cyber defenders in near real-world conditions, and (iii) supporting organizations and relevant stakeholders in making optimal cybersecurity investment decisions.**

Keywords— cybersecurity, cyber range, training

I. INTRODUCTION

The cyber security threat landscape is evolving, as the cyber-attacks are gradually becoming more sophisticated and the cybercrime perpetrators are getting more organized and the tools are automated [1]. Modern organizations need to heavily invest in cyber security technologies to proactively address the identified cyber risks, based on the characteristics of their infrastructure [2]. Moreover, a pragmatic and sustainable new approach is needed to better prepare network operators and service providers, with cyber defender training emerging as a strong candidate for achieving cybersecurity preparedness [3].

The EU funded SPIDER[1] project proposes an innovative Cyber Range as a Service (CRaaS) platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges with the most recent advances in telecommunications management and emulation. Apart from the network emulation, the SPIDER platform offers cyber security training capabilities for both experts and non-experts through gamification and serious games and moreover provides tools for cyber security econometric analysis.

[1] SPIDER Website https://spider-h2020.eu/

II. THE SPIDER CONCEPT

While many cyber security training platforms using a cyber-range already exist, only a few offer technology evaluation capabilities or training for the non-experts and none offers neither dedicated exercises for 5G training nor investment decision support. SPIDER will leverage on both traditional virtualization platforms as well as on more lightweight virtualization platforms based on containers and unikernels, giving particular attention to all the aspect related to performance isolation to virtualize the 5G functions.

SPIDER's basic objective is not only to provide the users with the capability of predicting the evolution of cyber-threats but moreover to analyze the associated economic impacts.

SPIDER's concept can be summed up on three major pillars:

- 5G Cyber Range Infrastructure and Supporting Technology (with a main focus on testing and assessment)
- 5G cybersecurity training in defending against advanced cyber-attacks both for cybersecurity experts and non-cybersecurity experts and
- 5G Risk Analysis and Cyber security Investment Decision Support, including econometric models.

A. 5G Cyber Range Infrastructure and Supporting Technology

Actors such as network operators, telecommunication, cloud infrastructure and software engineering providers etc will need a platform like SPIDER in order to test the security of their infrastructure as well as the effectiveness, and robustness of their cyber security defense technologies. SPIDER delivers an effective testbed for modelling, emulation and testing of network services, applications and security mechanisms as

well as a testbed for emulating network-wide attacks, forensic investigations, and tests that require a safe environment without the risk of proprietary data loss or adverse impact upon existing networks.

B. *5G cybersecurity training in defending against advanced cyber-attacks both for cybersecurity experts and non-cybersecurity experts*

SPIDER's Cyber Range as a Service (CRaaS) platform will take into account all relevant advancements and latest trends and will capitalize on current state of the art offering a synthetic, realistic and sophisticated war-gaming environment that will provide to the training users the ability of playing the part either of the attacker or the defender.

C. *5G Risk Analysis and Cyber security Investment Decision Support*

SPIDER will leverage advanced risks analysis and econometric models in order to provide more effective decision-making and faster cyber risk responding. SPIDER proposes the Continuous Risk Assessment Engine (CRAE) which allows a continuous evaluation of a company's cyber risks using the devised risk model templates. In addition, SPIDER incorporates and integrates well-known optimization techniques using Monte-Carlo simulation.

III. SPIDER ARCHITECTURE

The SPIDER architecture is comprised of 6 building blocks:

- the 5G virtualization platform for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;
- the network configuration and attacker emulation block, equipped with an Artificial Intelligence/Machine Learning-based engine, for modelling and emulation of network services, applications and security mechanisms;
- the administration platform, for the cyber range administrators to configure the training scenarios;
- the digital (simulation) gamified and serious game-based learning environment, leveraging on respective solutions for training experts and non-expert users;
- the risk analysis and cybersecurity economics block, which provides the forecast for the evolution of cyber-attacks and their associated economic impact;
- the monitoring and reporting layer, for the monitoring of the trainees' activity, and reporting the output of the SPIDER individual components.

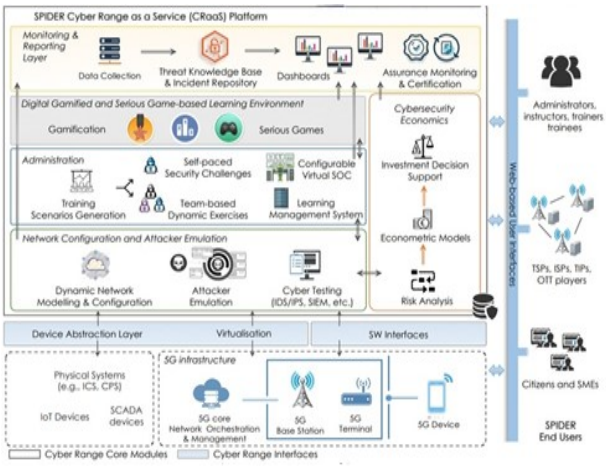

Figure 1: The SPIDER architecture

IV. SPIDER USE CASES

A. CYBERSECURITY TESTING

1) Cybersecurity Testing of 5G-ready applications and network services

The first use case focuses on representing the end-to-end network services through their entire lifecycle, and on the orchestration of 5G ready applications and network services. The goal is to validate SPIDER in terms of its ability to support testing, performance evaluation and security assessments of new security technologies.

2) Cybersecurity of Next Generation Mobile Core SBA

This pilot use case aims to develop and test the use of new cybersecurity tools based on machine learning which simulate adversarial techniques and tactics. The main aim is to address the new risks produced by the pervasive encryption in the 5G networks Control Plane (SBA).

B. 5G SECURITY TRAINING

1) 5G Security Training for Experts

SPIDER will be instrumental in rapidly equipping security professionals with the 5G security skills that will soon be required in the industry, in time for the global deployment of 5G, rather than after the first high-profile incident occurs in the wild.

2) 5G Security Training for Non-Experts

In this use case, the focus is not on the experts, but on the regular employees of 5G-oriented companies. The goal is to validate that the 5G security gamification solution results in real change and provide input to the exploitation of the solution after the project end.

C. CYBER INVESTMENT DECISION SUPPORT

The goal of this use case is to develop a decision support process integrated within the cyber range that can assist the relevant stakeholders to not only determining optimal investments to cybersecurity controls but also in taking the necessary steps to implement them.

V. CONCLUSION

This document presented the architecture and the use cases of the newly H2020 project SPIDER that aims to implement and provide a novel 5G cyber range platform.

REFERENCES

[1] Yamin, Muhammad & Katt, Basel & Gkioulos, Vasileios. (2019). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security. 88. 101636. 10.1016/j.cose.2019.101636.

[2] Why Funding for Cybersecurity Training Is Growing https://trainingindustry.com/blog/compliance/why-funding-for-cybersecurity-training-is-growing

[3] Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch-the cyber force. Alb. LJ Sci. & Tech., 18, 293.