A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services (SPIDER)

Neofytos Gerosavva[1], Manos Athanatos[2], Christoforos Ntantogian[3] , Christos Xenakis[3], Cristina Costa[4] , Alberto Mozo[5], Matthias Ghering[6] , Angela Brignone[7]

[1] EIGHT BELLS neofytos.gerosavva@8bellsresearch.com
[2] FORTH athanat@ics.forth.gr
[3]University of Piraeus (UPRC) {dadoyan,xenakis}@unipi.gr
[4]Fondazione Bruno Kessler (FBK) ccosta@fbk.eu
[5]Universidad Politécnica de Madrid (UPM) a.mozo@upm.es
[6]CYBERLENS matthias.ghering@cyberlens.eu
[7]ERICSSON angela.brignone@ericsson.com

URL : https://spider-h2020.eu/
Duration: 1st July 2019 – 30th June 2022 (36 months)

1 Summary of the project

1.1 Objectives

The vision of the H2020 funded project SPIDER (https://spider-h2020.eu/) is to deliver a next-generation, extensive, and replicable Cyber Range as a Service (CRaaS) platform for the telecommunications domain and its fifth-generation (5G). The proposed solution takes into account all relevant advancements and latest trends and capitalizes on the current state of the art offering a synthetic and sophisticated wargaming environment. Additionally, SPIDER features integrated tools for cyber testing including advanced emulation tools, novel training methods towards active learning as well as econometric models based on real-time emulation of modern cyber-attacks. Indeed, SPIDER's basic objective is not only to train professionals in 5G security but also to provide tools able to improve the user capability of predicting the evolution of cyber-threats and to analyse the associated economic impact and cost that is brought with the attack.

1.2 Expected tangible results

The main expected outputs of the project is the delivery of a cutting edge CRaaS platform able to offer to its intended users a digital gamified and serious game-based learning environment capable of training experts and non-experts. The envisioned platform represents also a serious gaming repository for sharing training material, as well as a realistic cybersecurity training infrastructure and brokerage facility for cybersecurity situation awareness, hands-on exercise experience and skills development in key cyber defence areas.

2 Summary of current project results

During the first 9 months of the project**,** the consortium partners conducted studies towards the analysis, collection, and extraction of SPIDER user requirements that the architecture development must address. A fundamental step during this preliminary work was to define the 5G cybersecurity threat landscape, and the related SPIDER actors, to outline the possible attack scenarios which the SPIDER's training platform should address. Based on these outputs, functional requirements have been extracted and grouped by the identified SPIDER actors, assigned a priority. Finally, functional requirements were mapped to non-functional requirements. In addition, and due to the lack of real data containing attacks for training purposes, SPIDER has investigated the application of Generative Adversarial Networks to the generation of synthetic network attacks. The use case analysis led to the definition of three pilot use case scenarios, described in the following:

A. CYBERSECURITY TESTING

A1. 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.

A2: Cybersecurity of Next Generation Mobile Core SBA

Here the objective is to develop and testing 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

B1: 5G Security Training for Experts

Experts will be trained on defending to potential threats using the SPIDER platform both in team or self-paced scenarios. Also, blue and red team exercises will be implemented and tested as there is an educational gap in the already existing platforms.

B2: 5G Security Training for Non-Experts

In this scenario, non-experts in cybersecurity will be introduced to cutting edge 5G technologies and its evolving cybersecurity landscape. The goal of this use case is to validate the 5G security gamification solution in realistic scenarios and provide input to the exploitation of the solution after the end of the project.

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.