SPIDER
5G CYBER RANGE

ABOUT SPIDER

SPIDER NEWSLETTER ISSUE #1

SPIDER is a 3-year Innovation Action (IA) from 2019 to 2022 funded under Horizon 2020 focusing on delivering an innovative Cyber Range as a Service platform that extends and combines the capabilities of existing telecommunication testbeds and cyber range into a unified facility for:

- testing new security technologies
- training modern cyber defenders near-real world conditions
- supporting organisations and relevant stakeholders in making optimal cybersecurity investment decisions

The SPIDER consortium is made up of 19 partners (industries, SMEs, research institutes and universities) coming from ten European countries: Greece, Italy, Spain, France, Cyprus, Romania, UK, Denmark, Switzerland, Bulgaria. ERICSSON acts as the project coordinator. SPIDER kicked-off on July 23-24, 2019 in Ericsson premises in Genoa (Italy).

VISION:

SPIDER aims to deliver a next-generation, extensive, and replicable cyber range platform for the telecommunications domain and its fifth generation (5G). The envisioned platform will be offering cybersecurity emulation, training and investment decision support. Towards this vision, it features integrated tools for cyber testing including advanced emulation tools, novel training methods based on active learning as well as econometric models based on real-time emulation of modern cyber-attacks. SPIDER supports both self-paced and team-based exercising. Moreover, SPIDER acts as a serious gaming repository for multiple stakeholders to share training material and maximize efficiency in delivering complex cyber exercises. The proposed cyber range model will be validated in five highly realistic pilot use case scenarios.

TABLE OF CONTENTS

PROJECT INFORMATION

SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
TYPE OF ACTION: Innovation Action (IA)
GRANT AGREEMENT ID: 833685
COORDINATOR: ERICSSON, Mr. Pierluigi Polvanesi, pierluigi.polvanesi@ericsson.com
START DATE: 1st July 2019
END DATE: 30th June 2022

Stay Tuned!

on all our latest news, developments, research & general information regarding the SPIDER project.

Follow us on:

https://twitter.com/spiderh2020_eu

https://www.facebook.com/SPIDER.H2020

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).

SPIDER ARCHITECTURE

SPIDER platform is comprised of 6 building blocks:

i. the 5G virtualisation platform for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

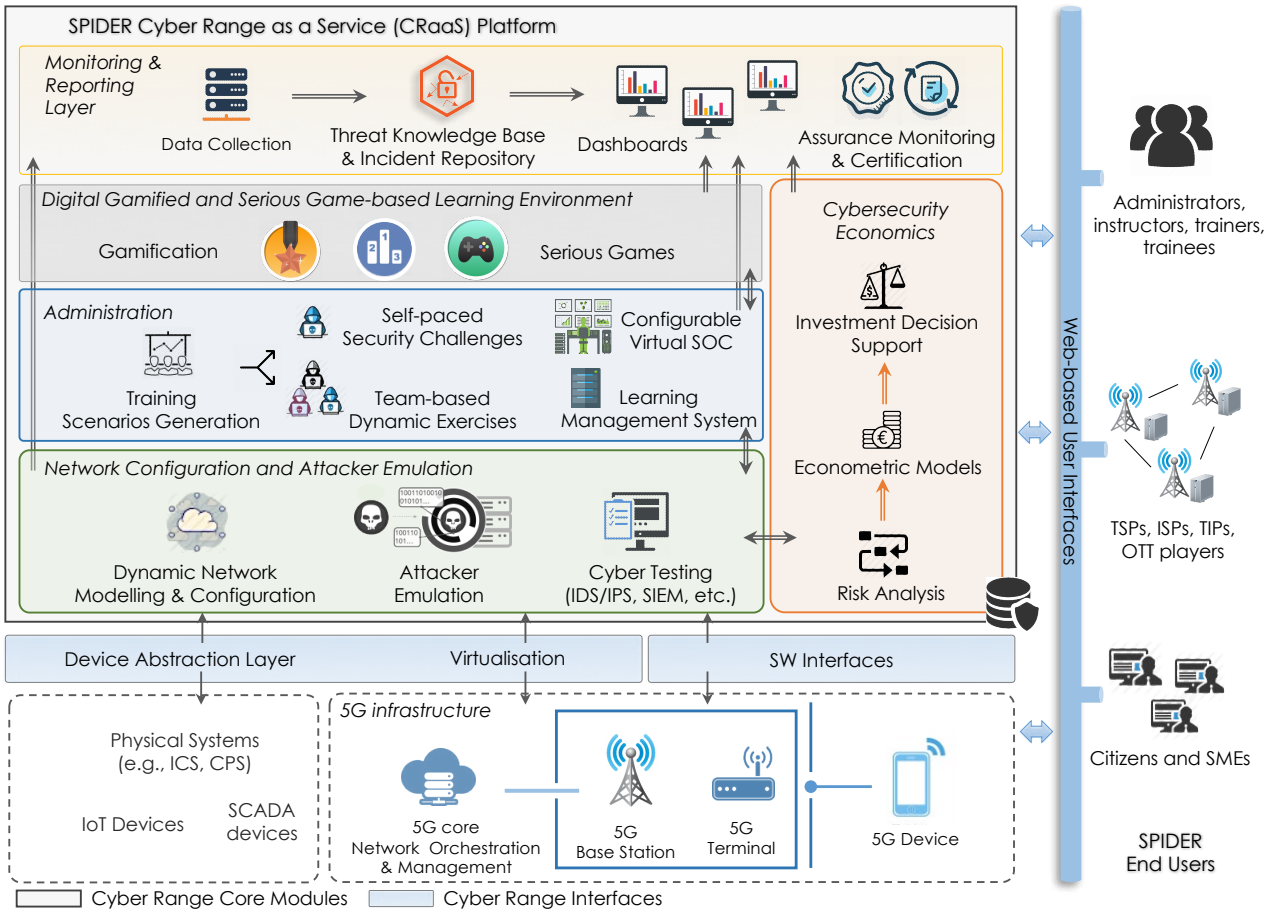
ii. the network configuration and attacker emulation block, equipped with an Artificial Intelligence/Machine Learning based engine, for modelling and emulation of network services, applications and security mechanisms;

iii. the administration platform, for the cyber range administrators to configure the training scenarios;

iv. the digital gamified and serious game-based learning environment, which is a simulation game framework leveraging on serious games and gamification solutions for training experts and non-expert users;

v. the risk analysis and cybersecurity economics block, which provides the forecast for the evolution of cyber-attacks and their associated economic impact;

vi. the monitoring and reporting layer, for the monitoring of the trainees' activity, and reporting the output of the SPIDER individual components.



The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER USE CASES

A. CYBERSECURITY TESTING

A1. Cybersecurity Testing of 5G-ready applications and network services

The first use case focuses on representing the end-to-end services for the overall lifecycle and orchestration of 5Gready 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. Particular emphasis is placed on the emulation of network-wide attacks, from rudimentary to highly complex.

A2: Cybersecurity of Next Generation Mobile Core SBA

Next Generation Core (NGC) applies Service Based Architecture (SBA) and Service Base Interfaces (SBI), defining a much more open relationship among the different control plane (NGC-CP) functions.Here the objective is to develop and testing the use of new cybersecurity tools based on machine learning to address the new risks produced by pervasive encryption in 5G networks Control plane (SBA).

B. 5G SECURITY TRAINING

B1: 5G Security Training for Experts

SPIDER will be instrumental in rapidly equipping security professionals with the 5G security skills required 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. These experts will be trained on defending to potential threats using the SPIDER platform both in team based or self-paced scenarios.

B2: 5G Security Training for Non-Experts

It has long been accepted in the security industry that experts and technical security measures cannot on their own protect organisations against cyber threats. Here, the focus is the cybersecurity non-experts that will be trained on cutting edge technologies and the evolving 5G cybersecurity landscape. The goal of this use case 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 validate the capabilities of the SPIDER modelling and emulation platform to forecast and estimate the impact of cyber-risks. Specifically, it will 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.

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER EVENTS

ETSI EXPERIENTIAL NETWORKED INTELLIGENCE INDUSTRY SPECIFICATION GROUP(ENI ISG)/ ETSI SECURITY WEEK

During the standardization meeting from ETSI Experiential Networked Intelligence Industry Specification Group (ENI ISG), at Aveiro (Portugal) on 9-11h July, partners from Telefonica introduced the SPIDER project and one of the use cases. Also SPIDER was presented from Telefonica during the ETSI security Week 2019 on 19th June at Sophia Antipolis, as part of the Artificial Intelligence & Securty Threat, in session 2: AI as an Attack and Defence Vector.

6th EAB. Cyber Meeting (Brussels)

Partners from University of Pireaus (UPRC), attended the 6th EAB. Cyber Meeting, organized by the European Security and Defence College (ESDC-https://esdc.europa.eu/) that took place in Brussels on 19/11/2019 where among other issues they also presented the SPIDER project.

The 6th NETWORK AND INFORMATION SECURITY (NIS'19)

The 6th Network and Information Security (NIS'19) Summer School, took place in Crete, Greece from 16 to 20 of September2019. This event, having a different "special theme" every year, is jointly organised by the European Union Agency for cybersecurity (ENISA) and the Foundation for Research and Technology – Hellas (FORTH). The theme for this year was "Security Challenges of Emerging Technologies". Towards this objective, ENISA and FORTH, brought together to this Summer School a distinguished faculty from around the world with the purpose to identify current trends, threats and opportunities against the background of recent advances on NIS measures and policies. The SPIDER project was included -among other projects in the event flyer that was disseminated in the NIS'19 summer-school and was enlisted among the event sponsors.

For more information please visit
https://nis-summer-school.enisa.europa.eu/

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER
5G CYBER RANGE

EVENTS & ACHIEVEMENTS

THE EUROPEAN CYBER SECURITY CHALLENGE 2020

The European Cyber Security Challenge 2020 (that is being organized by ENISA) kick of meeting took place on 13/2- 14/2/2020 in Vienna, Austria where UPRC partners had the opportunity to lobby with other participants and present the SPIDER project, and the related activities in regards to the evaluation of the platform from the Hellenic Cyber Security team. Additionally, the exploitation plans of the SPIDER platform for the ECSC were presented.

For more information please visit:
https://europeancybersecuritychallenge.eu/

SECURITY AND CYBERSECURITY HELIX EVENT

The Security and Cybersecurity Helix event was organized by the KIOS Research and Innovation Center of Excellence and Crowdhelix.This event took place at the University of Cyprus from 5- 6 of February 2020, and within the event context, EIGHT BELLS introduced SPIDER as a part of a presentation delivered regarding the company's portfolio of projects. This two-day meeting was a great opportunity to gather academia and businesses around common areas of interest. It was addressed at organisations specialised in security and Cybersecurity that are willing to collaborate and form consortia for Horizon 2020 calls. This event was attended by 30 researchers and industry representatives.

For more information please visit:
https://cybersecurity-helix-event-2020.b2match.io/

PROJECT ACHIEVEMENTS

In the first reporting period, the Project achieved to release an early set of results from 3 different WPs:

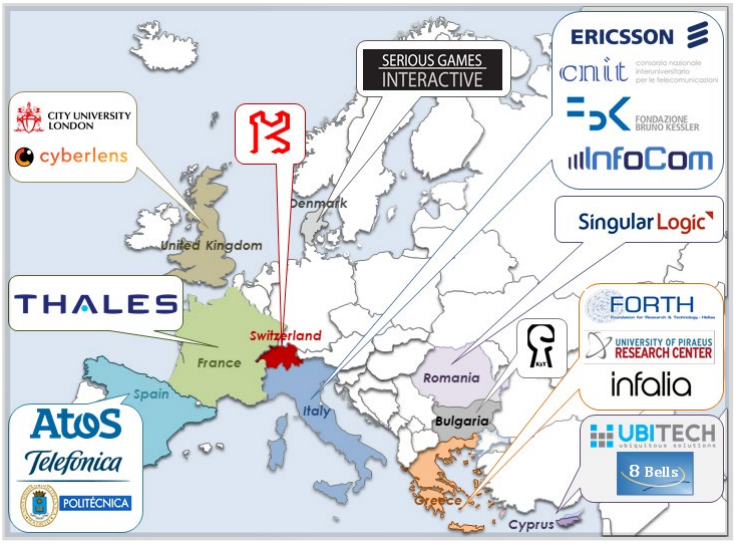
- as part of WP1 – Project Management, the project structure, the processes and the collaborations frameworks have been set-up to enable the Project to activate the work in the various WPs and Tasks
- the outcome of WP2 - Requirement Analysis, Architecture Definition & Pilot Use Cases has been the specification of the first round of user requirements, relying on high-level competence and expertise available internally from the partners that provided an effective level of contributions into the deliverable
- the WP8 – Dissemination, Communication and Exploitation of Results focused on the release of the Dissemination & Communication initial planning as a first step and started to track and coordinate the early dissemination activities that initiated thanks to a number of partners in the consortium.

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER
5G CYBER RANGE

WEBSITE & SOCIAL MEDIA

VISIT OUR WEBSITE AND SOCIAL MEDIA



1. ERICSSON TELECOMUNICAZIONI
2. CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI
3. TELEFONICA I+D S.A.U.
4. THALES SIX GTS FRANCE
5. ATOS SPAIN SA
6. UBITECH LIMITED
7. UNIVERSIDAD POLITECNICA DE MADRID
8. FONDAZIONE BRUNO KESSLER
9. SINGULAR LOGIC ROMANIA COMPUTER APPLICATIONS
10. EIGHT BELLS LTD
11. FOUNDATION FOR RESEARCH AND TECHNOLOGY
12. SERIOUS GAMES INTERACTIVE APS
13. UNIVERSITY OF PIRAEUS RESEARCH CENTRE
14. CITY UNIVERSITY OF LONDON
15. CYBERLENS LTD
16. INFALIA PRIVATE COMPANY
17. INFOCOM S.R.L.
18. SPHYNX TECHNOLOGY SOLUTIONS AG
19. K3Y LTD

https://spider-h2020.eu https://twitter.com/spiderh2020_eu https://www.facebook.com/SPIDER.H2020

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains