SPIDER
5G CYBER RANGE

BRIEF SUMMARY

SPIDER NEWSLETTER ISSUE #3

We are pleased to announce the publication of the third issue of our Project newsletter!

SPIDER is a 3-year Innovation Action (IA) from 2019 to 2022, funded under Horizon 2020. The project focuses 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 in near-real world conditions
- supporting organisations and relevant stakeholders in making optimal cybersecurity investment decisions.

SPIDER consortium consists of 19 partners (industries, SMEs, research institutes and universities) coming from nine European countries: Greece, Italy, Spain, France, Cyprus, UK, Denmark, Switzerland, Bulgaria. ERICSSON acts as the project coordinator.

Despite constraints imposed from COVID-19, we can say that Year 2021 was quite positive for our project.

SPIDER project consortium has progressed in terms of technical work and according to plan producing a number of important deliverables.

Furthermore, several consortium members have attended a variety of events which attracted considerable numbers of participants. In this 3rd issue of our Newsletter, we present some of the highlights, which the consortium achieved during the last 12 months.

In the Dissemination Activities section, we present a number of online events, which we either organized ourselves or in which we participated. Also, we present a number of papers related to SPIDER, as well as some collaboration activities with other EU funded projects.

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:

www.spider-h2020.eu | spiderh2020_eu | SPIDER.H2020 | SPIDER H2020 FUNDED PROJECT

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).

This issue covers a period of 12 months from January 2021 to December 2021. During this period of time, significant progress has been reported in several work packages of the project.

Our main focus has been to convert stakeholders' requirements into concrete software implementation, integration and testing. Thus, one of the main achievements during this period was the **release of the second integrated version of the SPIDER prototype** which gathers the various components.

Alongside the roll-out of the SPIDER platform iterative integration plan, demonstration and evaluation methodologies, as well as dissemination and exploitation activities have been the other key pathways, which were proceeding in parallel within the project. Here is a summary of achievements per active Work Package.

◊ WP3 Cyber Range Infrastructure and Supporting Technologies

Activities towards the realization of the core platform that provides support to the execution of emulated exercises in the frame of learning modality-2 took place during this period. To this end, existing **network management and orchestration techniques** are reused and extended in order to facilitate the functional requirements that are relevant to **emulation**. WP3 continues to wrap/procure specific 5G network services (e.g., packet gateway), applications (e.g., web-servers) and security blocks (e.g., firewalls) in order for them to be used during the creation of emulation scenarios. One of the significant outputs of WP3 for the current period is the **delivery of the network configuration and attacker emulation component**, which explains and describes the integration and enhancement of pre-existing building blocks and a set of network attack emulation use cases that are integrated as Cyber Range scenarios and exercises.

◊ WP4 5G Cyber Security Training

Work Package 4 is progressing according to plan. The **serious game**, which is targeted mainly for the junior experts and trainees, **has now been conceptualised**. The game play will simulate a given network that can be played as a Blue- or Red-team member in a single player session. Gaining knowledge of general defense and attack patterns, are the main learning objectives. Significant output of WP4 includes the **delivery of a 5G serious game component**, which incorporates the simulations and systems developed across the project, leveraging the potential of serious games achieving more engaging training. Serious game addresses cybersecurity experts training needs, who will gain specific skills to alleviate, foresee, avoid and counter specific threats. Another important output is the **delivery of the final version of 5G gamification component,** which concerns the gamification awareness training application. This is the type of training targeting non-expert users that aim to acquire some fundamental technical skills that are essential in the security domain (e.g., password strengths, usage of encrypted tunnels). The most 'lethal' attacks commence through the successful exploitation of the human factor. Hence, the elementary competences acquired through these quests contribute to the radical increase of the cyber-immunity. Lastly, another major output concerns the delivery of the **Human-in-the-Loop performance assessment component**, which tackle educational challenges targeting the specificities of security training for modern virtualized/5G networks.

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

◊ WP5 Economics of 5G Security

Work in this WP has continued smoothly, and significant results have been delivered through this period. The main objectives include the **development of a decision-making framework** based on novel risk analysis models supporting continuous assessment of cyber-risks as well as on econometric and capital budgeting techniques that will help risk auditors to assess and forecast the evolution of cyber-attacks and their associated economic impact as well as help them promote investments that ensure a more cyber secure environment. One of the significant outputs concern the **delivery of SPIDER assurance and certification monitoring component**, including the necessary mechanisms (aka security controls) developed to ensure the security and privacy of the SPIDER platform and its data, but also to provide a real-time view of the security posture of the infrastructure where SPIDER is deployed. Another important output is the **delivery of the empirical framework for asset pricing and impact loss analysis component,** realised through the development of a method for classifying vulnerabilities based on the financial risk exposure they may entail if compromised, while loss analysis is carried out by measuring the system's risk exposure under a given configuration using standard risk measures. Finally, another major result concerns the **delivery of the empirical decision support framework for econometric analysis of cyber risk and investment component.** The novelty of this risk-based approach to mitigating cyber risk is the potential to facilitate optimal investment decisions that account for attitudes towards risk.

◊ WP6 SPIDER Cyber Range Integration and Testing

Deployment and validation of the integrated version of the SPIDER platform is progressing well and as planned, following a disciplined plan, in-line with the system design and architecture. **A major milestone has been met through** the delivered result which concerns the release of the second integrated version of the SPIDER platform prototype, delivering the much promising **SPIDER cyber-range framework that offers security testing and training services in the field of cyber security and 5G**. The framework offers multiple learning modalities which span from theoretical knowledge training to simulation and emulation exercises including the ability to evaluate econometric models. As it is inferred from the multi-disciplinary goals of the framework, its development and integration are rather complex tasks. Integration tasks will continue and intensify during the last semester of the project, where more training scenarios will be included and deployed in SPIDER Cyber-Range, followed by validation activities, also performed in alignment with demonstration and evaluation activities.

◊ WP7 Demonstration and Evaluation

Starting with the **release of the initial prototype of the SPIDER Cyber-Range, the activities of demonstration and evaluation have also initiated.** As the key objective is to evaluate the SPIDER platform based on four different pilot use cases, various aspects of the implemented system, both feature-wise including 5G security assessment, training, investment decision support, as well as performance-wise such as flexibility and scalability will be brought to the test. The major output for the current period concerns the **delivery of the Evaluation methodology and measures specifications**, which provides a common evaluation framework across all pilots and define Key Performance Indicators (KPIs) and metrics for evaluation and analysis of the SPIDER pilot use cases and corresponding scenarios and user stories, as have been defined earlier in the project. Targeting a holistic evaluation process, the KPIs will guide the technical performance evaluation of the SPIDER platform, along with appropriate metrics to support evaluation on the front of user acceptance and user upskilling.

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

CLUSTERING ACTIVITIES

The collaboration between H2020 projects FORESIGHT, CYBER-MAR and SPIDER project bore fruits, with the successful organisation of a joint CYBER-RANGE NETWORK webinar. The recording is available at SPIDER's YouTube channel. This collaboration has been extended to other similar projects, like THREAT-ARREST and CONCORDIA. Clustering activities are ongoing and expected to be maximised during the last semester of the project.

The 1st SPIDER 5G Cyber Range workshop for EU CERT/CSIRTs took place virtually on Wednesday 21st of April 2021. The 2nd SPIDER 5G Cyber Range workshop for EU CERT/CSIRTs took place virtually on Thursday 13th of May 2021, and was a continuation of the first workshop, with a basic objective to continue our discussions and establish operational connections with CERTs/CSIRTs. The established link will remain active until the end of the project, providing the SPIDER's technical offerings and training material to the CSIRT/CERTs community, receiving feedback that will assist the exploitation of the platform to more sectors than prior envisioned.

SPIDER and CONCORDIA have been working together to enhance dissemination and communications activities with the use of the services of Horizon Results Booster. In particular, SPIDER is now a member project of the CONCORDIA Group on Horizon Results Booster platform.

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 was introduced in EUCNC 2021 where our partners from University of Madrid (UPM) and TELEFONICA (TID) had been accepted to a workshop session. The session was part of the workshop called: "WS8: From 5G to 6G Automated and Intelligent SecuriTy: FAST" that was held on 8th of June 2021 during the first day of the EuCNC 2021 conference. Our colleague from UPM, Mr. Stanislav Vakaruk represented the SPIDER project delivering a presentation with title "SPIDER: ML Applied to 5G Network Cyber Range".

EUCNC | 6G Summit
Virtual Conference (Porto, Portugal) • 8-11 June 2021

SPIDER project supported CSR 2021 IEEE Workshop on Cyber Ranges and Security Training (CRST) on the 26th of July 2021, where our colleague Mr. Matthias Ghering from CYBERLENS delivered a presentation for the paper "The SPIDER Cyber Security Component ". This paper was a joint effort from the consortium partners CITY, CYBERLENS and EIGHT BELLS. The workshop took place within the context of the 2021 IEEE International conference on Cyber Security and Resilience.

IEEE CSR
Cyber Security and Resilience

SPIDER sponsored the Cybersecurity Hands -On -Training (CyberHOT) Summer School which took place on the 27th and 28th of September 2021 in the city of Chania, Crete, Greece, under the auspices of NMIOTC (NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE). SPIDER project was represented from our partners from FORTH.

Our partners from Sphynx Technology Solutions participated in "Career Day: Meet the companies" virtual event, organized by the Graduate Student's Association of Computer Science Department of the University of Crete on the 18th of Oct 2021. Michalis Smyrlis, who participated on behalf of Sphynx, had the chance to disseminate SPIDER in more than 90 participants of both the academic and industry fields.

SPIDER participated the CONCORDIA OPEN DOOR 2021 as virtual exhibitors; the event took place on the 20th and 21st of October 2021. There, we had the opportunity to display information material, including SPIDER latest updates and provide a link to a demo game as well as links to the SPIDER website and social media.

CONCORDIA
OPEN DOOR 2021

IEEE CAMAD™

Our partners from UPRC participated in "IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks" which took place between 25 and 27 of October 2021, where they had the opportunity to present SPIDER project and the needs it meets, on October 26th 2021.

SPIDER was presented by Ericsson to their internal R&D Italy Innovation Event 2021, that took place on the 1st of December 2021. The aim of this event was to show undergoing innovative projects pursued by the local R&D organizations in front of internal and external stakeholders. It was a dissemination initiative to give an overview of SPIDER as a "cyber-security training centre" that was listed in the next-to-come section to attract interest in view of next year opportunity for concrete engagement when the solution will be fully available and released.

New video available, presenting in a nutshell SPIDER offer regarding a Cybersecurity platform for virtualised 5G cyber range services

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

Journal Papers

- Papadogiannaki, Eva, & Ioannidis, Sotiris. (2021). Acceleration of Intrusion Detection in Encrypted Network Traffic Using Heterogeneous Hardware. Sensors 2021, 21(4), 1140. https://doi.org/10.3390/s21041140. Available for download at Zenodo.org.
- González-Prieto, Ángel, Alberto Mozo, Edgar Talavera, and Sandra Gómez-Canaval. 2021. "Dynamics of Fourier Modes in Torus Generative Adversarial Networks" Mathematics 9, no. 4: 325. https://doi.org/10.3390/math9040325. Available for download at mdpi.com.
- Lyvas, Christos, Ntantogian, Christoforos, & Xenakis, Christos. (2021). [m]allotROPism: a metamorphic engine for malicious software variation development. International Journal of Information Security. https://doi.org/10.1007/s10207-021-00541-y. Available for download at Zenodo.org.
- Christoforos Ntantogian, Panagiotis Bountakas, Dimitris Antonaropoulos, Constantinos Patsakis, & Christos Xenakis. (2021). NodeXP: NOde.js server-side JavaScript injection vulnerability DEtection and eXPloitation. Journal of Information Security and Applications, 58(102752). https://doi.org/10.1016/j.jisa.2021.102752. Available for download at Zenodo.org.

Conference Papers

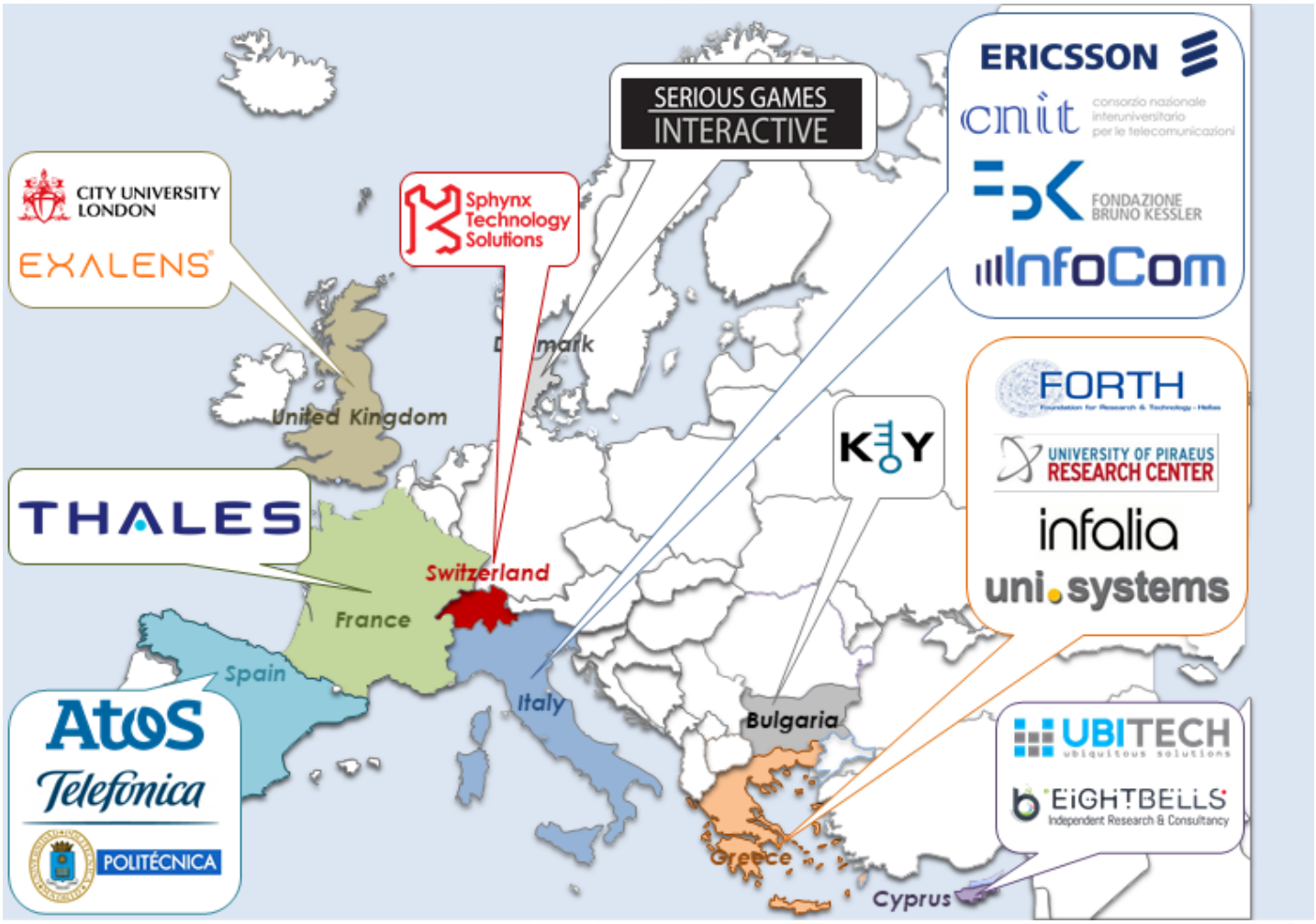
- M. Tsiodra, M. Chronopoulos, M. Ghering, E. Karapistoli, N. Gerosavva and N. Kylilis, "The SPIDER Cyber Security Investment Component (CIC)," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 415-421, https://doi.org/10.1109/CSR51186.2021.9527924. Available for download at Zenodo.org.
- Vakaruk, Stanislav, Mozo, Alberto, & Pastor, Antonio. (2021, June 8). SPIDER: ML Applied to 5G Network Cyber Range. European Conference on Networks and Communications & 6G Summit (EuCNC 2021) (EuCNC 2021), Virtual event. https://doi.org/10.5281/zenodo.5647899. Available for download at Zenodo.org.
- Stanislav Vakaruk, Alberto Mozo, Antonio Pastor, & Diego R. L ópez. (2021, September 22). A Digital Twin Network for Security Training in 5G Industrial Environments. https://doi.org/10.1109/dtpi52967 .2021.9540146. Available for download at Zenodo.org.

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

SPIDER Consortium at a glance



SPIDER Website & Social Media

Please find more information about SPIDER:

- www.spider-h2020.eu
- spiderh2020_eu
- SPIDER.H2020
- SPIDER H2020 FUNDED PROJECT

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