SPIDER
5G CYBER RANGE

BRIEF SUMMARY

SPIDER NEWSLETTER ISSUE #4

We are pleased to announce the publication of the fourth 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.

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 4th issue of our Newsletter, we present some of the highlights, which the consortium achieved during the past 3 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).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

This issue covers a period of 3 months from January to March 2022. During this period of time, significant progress has been reported in several work packages of the project.

Our main focus has been to validate if the stakeholders' requirements have been met though SPIDER's platform, following the final steps and activities for the platform integration. Thus, one of the main achievements during this period was the release of the third integrated version of the SPIDER prototype.

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.

◊ Cyber Range Infrastructure and Supporting Technologies [WP3]

All technical activities pertaining to SPIDER 5G Cyber Range Infrastructure and Supporting Technologies have been concluded successfully, providing a number of significant outputs. Final version of the SPIDER SDN-based and NFV-based network orchestrator has been released, thus finalizing **5G programmable/ virtualised infrastructure management** component. In addition to that, the final output of **5G platform management and orchestration for SPIDER cyber range as a service** has been also realised. Another major output concerned the final version of the specification, design and implementation of basic security functionalities that will be consequently integrated to the SPIDER cyber range. Plus, a set of training topologies embedding these basic building blocks will be used to represent baseline deployment topologies for the SPIDER cyber range. Thus, **modelling and emulation of security mechanisms** is now available as well. Last but not least, another significant output is the **data collection and visualisation toolkit,** which is now available.

◊ 5G Cyber Security Training [WP4]

Activities regarding 5G Cyber Security Training are progressing according to plan, reaching their final stage of implementation. The major output for the previous period concerns the delivery of **SPIDER Configurable Virtualised Security Operation Centre (CV-SOC).** SPIDER Configurable CV-SOC has a double scope. Firstly, it works as a SOC, which trainees can use during exercises to familiarize with SOC technologies and practices; secondly, it works as the main interface for training supervisors to track the progression of trainees interacting with the platform. The CV-SOC is a virtualised software component regrouping security information and event management functionalities for monitoring in real-time and notifying security events of the underlying emulation environment. Via a configurable and scalable **log-process-store data-processing pipeline**, it can be adapted to the varied sources of information of the training scenario and to the expected learning outcomes. The emulated scenarios in SPIDER are expected to generate an enormous amount of raw information (logs), whose analysis forms the basis for providing both the context of the trainees' actions, and the current status of the virtualized 5G infrastructure.

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

◊ Economics of 5G Security [WP5]

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. Additionally, assessment on econometric and capital budgeting techniques 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 concerns the delivery of final version of the **models and assessment engine for continuous risk analysis**. So, the main outcome is a set of graphical cyber risk models addressing nine different attacks: Man-In-The-Middle (MitM), Amplification, Password brute forcing, Privilege Escalation, Cell Data Injection, Local execution of code, Infected software, SQL Injection and Flooding. The models have been selected taking into consideration their relevance in the 5G field and the interests of the SPIDER Consortium. Another output concerns the delivery of the final **SPIDER Cybersecurity Investment Component**. As its name suggests, this component of the SPIDER platform implements the cyber economic models developed earlier in the project, considering as input the outcomes of the Continuous Risk Analysis engine. Visualised output is made available to risk auditors and investment decision support managers of the 5G infrastructure, in order to provide their preferences, rules, policies, recommendations, and risk priorities; parameters that will be used to instantiate the SPIDER cyber economic models.

◊ SPIDER Cyber Range Integration and Testing [WP6]

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, also reaching their pre-final stage of implementation. A major milestone has been met during this period which concerns **the release of the third integrated version of the SPIDER platform prototype**, delivering the most advanced version of the much promising **SPIDER cyber-range framework that offers security testing and training services in the field of cyber security and 5G**. SPIDER 5G cyber range framework now includes a seamless nearly final integration of the progress quantification Application Programming Interface (API), the Machine Learning integration technique, the components of the Continuous Risk Assessment Engine and the Cybersecurity Investment Component. Next steps concern the execution of the deployment in a testing environment.

◊ Demonstration and Evaluation [WP7]

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 and performance-wise, are brought to the test. Feature-wise, the aspects under testing include 5G security assessment, training, and investment decision support. Performance-wise, aspects such as flexibility and scalability are examined. Building on the previously delivered 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, evaluation activities continue to take place as planned. Targeting a holistic evaluation process, these KPIs 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. Demonstration and evaluation activities are expected to intensify during the next period, in essence the final trimester of the project's implementation.

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

We are pleased to announce that SPIDER Project is a member of CONCORDIA Project Group, a cluster of 3 EU Horizon2020 Research Projects that have a specific focus on cyber ranges and aim to provide innovative cyber security training. The Project Group has been formed with the support of Horizon Results Booster, a European Commission service, which is steering research towards strong societal impact, concretising the value of Research and Innovation activity for societal challenges.

HORIZON RESULTS BOOSTER

An initiative of the European Commission

Apart from SPIDER, the other two project members of the cluster are CONCORDIA (Cyber security cOmpeteNCe fOr Research anD InnovAtion) and FORESIGHT (Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments).

In the framework of this collaboration, a joint event is organised in the form of a virtual webinar, entitled "**Training the European workforce of tomorrow: cyber ranges in practice**".

The event will take place virtually on **May 17th, at 10.00 CET**, with the participation of **Mr. Csaba Virág**, Chair of Cyber Range Focus Group of European Cyber Security Organisation (ECSO), who will also assume the role of moderator.

Agenda and further information on event are available here: https://www.cyberwatching.eu/projects/1484/concordia/news-events/training-european-workforce-tomorrow-cyber-ranges-practice. To join us and learn more on Cyber Ranges in Practice, **register here**: https://us02web.zoom.us/webinar/register/WN_2AdCroscSwmo8sQ0J4RDxw

As part of the joint actions currently in progress, the cluster has released of a **joint flyer**, that you may read it online, or download it, by visiting our dedicated section for Media publications at https://spider-h2020.eu/publications/#Others. Additionally, a **short promo video** has been produced to present the common goal of all three projects that have a specific focus on cyber ranges, aiming to provide innovative cyber security training. You may watch it at SPIDER website here https://spider-h2020.eu/2022/04/20/short-promo-video-of-concordia-project-group/.

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 @OSM

Our colleagues Dr. Chiara Lombardo and Prof. Roberto Bruschi from CNIT shared SPIDER's OSM experience, by demonstrating "The SPIDER Platform – deployment and management of virtual topologies in 5G programmable environments" during OSM-MR#12 Ecosystem Day. The event took place virtually on March 9th.

OSM Ecosystem Days allows organizations in the OSM Ecosystem to share about their Open Source MANO experience and how OSM is helping them to achieve their goals. Presentations and demos cover a wide range of aspects from research activities in academia to production deployments and commercial initiatives, many of them focused on 5G and MEC use cases. Slides and videos from the event are available at https://lnkd.in/gHm8kzbM.

UPRC presented SPIDER @ CSDP Research Methodology Course

The members of the Systems Security Laboratory (SSL) of SPIDER partner UPRC, participated in the Doctoral School on CSDP Research Methodology Course, organised by the European Security and Defence College (ESDC).

The course took place in the premises of University of Piraeus from 14 to 16 of March 2022. Professor Christos Xenakis was among the speakers, presenting the research goals and achievements of SPIDER research project, among other research initiatives the team is contributing to, as well as the challenges of the Hellenic Cyber Security Team. The course included insightful and inspiring lectures, from a technical perspective, that allowed the attendants to explore aspects of security that extend beyond cyber.

Events organised for the final three months of the project

- Technology Transfer event – FORTH, May 5th (Virtual)
- 1st Open Annual Workshop on Future ICT (physical meeting), May 25th, 2022, Athens
- CERTS/CSIRTS 3rd Workshop, May 26th (Virtual)
- First European Defence Innovation Day Conference & Exhibition (physical meeting), May 31st, 2022, Brussels
- ICC Event – June '22: The 1st International Cybersecurity Challenge will take place from 14 to 17 June in Athens, Greece
- International Workshop on Massive Digital Twins for the Computer-Networks Evolution (TwinNets), Belfast, UK, June 14 -17, 2022 (Co-located with WoWMoM 2022) www.twinnets22.unipi.it

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

- J. F. Pajo, G. Kousiouris, D. Kyriazis, R. Bruschi and F. Davoli, "ANNs Going Beyond Time Series Forecasting: An Urban Network Perspective," in IEEE Communications Magazine, vol. 59, no. 5, pp. 88-94, May 2021, doi: 10.1109/MCOM.001.2000990
  Available for download at Zenodo.org

- Mozo, A., González-Prieto, Á., Pastor, A. et al. "Synthetic flow-based cryptomining attack generation through Generative Adversarial Networks." Sci Rep 12, 2091 (2022). https://doi.org/10.1038/s41598-022-06057-2
  Available for download at nature.com

Conference Papers

- Filippo Rebecchi, Antonio Pastor, Alberto Mozo, Chiara Lombardo, Roberto Bruschi, lias Aliferis, Roberto Doriguzzi-Corin, Panagiotis Gouvas, Antonio Alvarez Romero, Anna Angelogianni, Ilias Politis, & Christos Xenakis. (2022). "A Digital Twin for the 5G Era: the SPIDER Cyber Range".
  Available for download at Zenodo.org

- A. Angelogianni, I. Politis, P. L. Polvanesi, A. Pastor and C. Xenakis, "Unveiling the user requirements of a cyber range for 5G security testing and training," 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2021, pp. 1-6, doi: 10.1109/CAMAD52502.2021.9617776.
  Available for download at Zenodo.org

- J. F. Pajo, G. Kousiouris, D. Kyriazis, R. Bruschi and F. Davoli, "Evaluating Urban Network Activity Hotspots through Granular Cluster Analysis of Spatio-Temporal Data," 2021 17th International Conference on Network and Service Management (CNSM), 2021, pp. 417-421, doi: 10.23919/CNSM52442.2021.9615584.
  Available for download at Zenodo.org

zenodo

nature

Standardisation

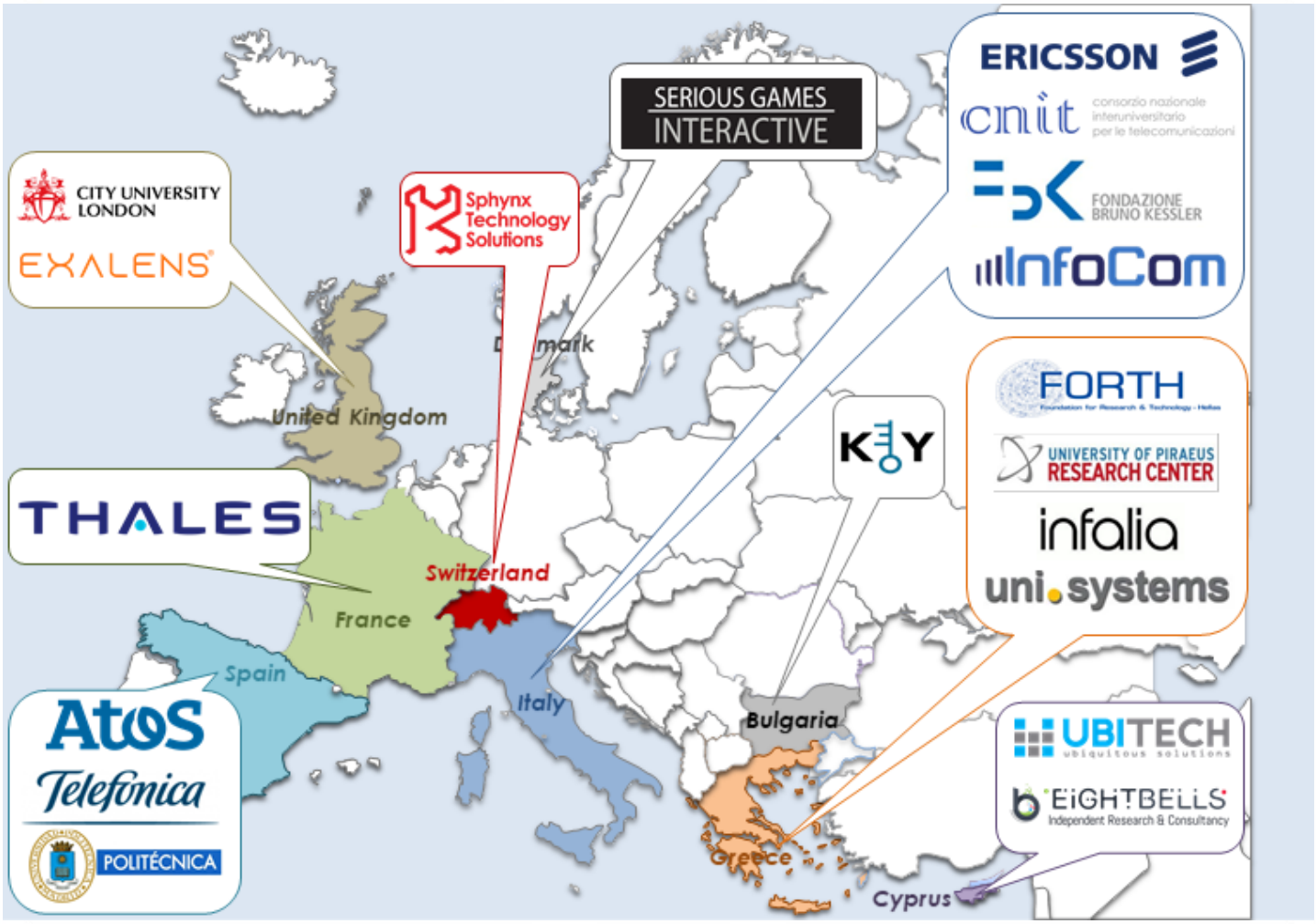
As a result of the discussion on the last Network Management research group (NMRG), at IETF 113 standardization meeting held on Vienna in the last week of March, a first draft on Digital Twin Network: Concepts and Reference Architecture (draft-irtf-nmrg-network-digital-twin-arch-00) was agreed. SPIDER has contributed actively to this achievement with several application scenarios related to security and ML.

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