SPIDER

5G CYBER RANGE

SPIDER 5G Cyber Range as a Service

June 2022

The SPIDER project has received funding from the Horizon 2020 EU research & innovation programme under GA No 833685

Authors

Antonio Alvarez, Guillermo Yuste, Jesús Villalobos, Jorge Martínez – ATOS

Michail Chronopoulos – CITY

Matthias Ghering, Irene Karapistoli, George Alexopoulos – EXALENS

Chiara Lombardo, Jane Frances Pajo – CNIT

Carla Marcenaro, Pierluigi Polvanesi – ERICSSON

Cristina Costa – FBK

Manos Athanatos, Nikolaos Petroulakis – FORTH

Alexandros Mokkas, Ioannis Tsampoulatidis – INFALIA

Guerino Lamanna, Maurizio Giribaldi – INFOCOM

George Amponis, Maria Zevgara, Savvas Ouzounidis – K3Y

Martin Bärmann, Martin Skarregaard, Simon Egenfeldt-Nielsen – SGI

Andreas Miaoudakis, Dimitris Ntegiannis, Michalis Smyrlis – STS

Bruno Vidalenc, Filippo Rebecchi, Geoffroy Chollon – THALES

Antonio Pastor, Diego López – TELEFONICA

Panagiotis Gouvas – UBITECH

Platon Velonias, Ilias Aliferis, Ilias Kontakos – UNISYSTEMS

Alberto Mozo, Diego Rivera, José Ignacio Moreno, Luis de Marcos, Stanislav Vakaruk, Amit Karamchandani – UPM

Anna Angelogianni, Ilias Politis, Christos Xenakis – UPRC

Vasileios Fragkos, Konstantina Papachristopoulou – 8BELLS

Editor

Konstantina Papachristopoulou – 8BELLS

Contents

Acknowledgement

The authors of the present document would like to acknowledge and express their thanks to the leading WP3, WP4 and WP5 contributors as well as to the partners that actively contributed and provided their insight and expertise towards the successful completion of the relevant work objectives (within the wider scope of the SPIDER project). Their work that is reflected within the corresponding SPIDER D3.6, D3.7, D3.8, D3.9, D4.3, D4.4, D4.5, D4.6, D4.7, D4.8, D5.6 and D5.7 deliverables, has been extremely useful and constitutes the main input for preparing the current document in the form of a White Paper.

Abstract

The purpose of this White Paper is to provide an insight on the SPIDER 5G Cyber Range components and technological aspects as defined through the implementation of technical oriented Work Packages (WP), during the second half of the project. More specifically, the current paper focuses on presenting the outputs of the work performed in WP3 “Cyber Range Infrastructure and Supporting Technologies”, WP4 “5G Cyber Security Training”, and WP5 “Economics of 5G Security”. In particular, current White Paper provides a summary of the work completed and documented in the related Deliverables.

Disclaimer

Introduction

During the last years, the number of cyber-attacks has gradually increased and various recent security incidents worldwide have demonstrated the fact that there is an increase also in the complexity and severity of cyber security threats. The attackers are becoming more sophisticated and they are using even more advanced methods and techniques. This has led organizations operating on various sectors to look for more advanced techniques in which to protect their infrastructures and assets.

In order to ensure a safer environment for organizations around the world, improved cyber security awareness is vital and cyber security training must become more advanced in order to be in place to respond to the emerging challenges. Conducting such training programs requires dedicated testbeds and infrastructures that help realize and execute the training scenarios and provide a playground for the trainees.

5G does not only improve on radio aspects but also introduces a completely new core network architecture, fully based on the concept of network softwarisation and oriented towards cloud-native concepts. 5G proposes a more secure architecture with improvements in several areas, such as integrity of user plane data, the privacy of the user data, encryption of the International Mobile Subscriber Identity (IMSI), compartmentalization. Even though the design of 5G has already taken under consideration the subject of security, the novel features as well as the complexity of the architecture, combined with the scale of deployment and the wide range of services and applications, yields the need for continuous testing and training.

The modern cyber security landscape is demanding. Modern Communication Service Providers (CSPs) are facing several threats caused by the technology shift. This shift has introduced new attack vectors (cloud/virtualization, mobility, big data, digitization/IP-fiction, collaboration, Internet of Things). On the other hand, the attackers have become more mature and the attacks more complex and persistent. Simultaneously, the lack of proper cyber security training of the operational personnel and the extension of 5G as the backbone for many critical systems such as connected cars, industry 4.0, and healthcare, indicates that the impact of the potential attacks is considerable.

SPIDER offers a multi-modal educational platform targeting the specificities of security training for modern virtualized/5G networks. Its functionality is wrapped in four distinct modalities, namely:

- Modality 1: Theoretical Training
- Modality 2: Emulation Training
- Modality 3: Simulation Training
- Modality 4: Security Awareness Training.

The goal of SPIDER is to define and develop a novel 5G cyber range platform which virtualises and unifies the 5G network while offering security testing and training capabilities. The SPIDER platform is also capable of performing risk analysis on the 5G infrastructure and proposing cyber security investment recommendations. To support this vision, SPIDER encompasses state-of-the-art technologies such as Artificial Intelligence/Machine Learning for attack emulation, game-based learning environment for the cyber security trainings as well as the latest econometric models.

During the second period of the SPIDER project lifecycle and towards the completion of defined milestones and objectives, the consortium partners worked intensively in designing, developing, deploying and validating SPIDER's 5G Cyber Range integral components. The purpose of this White Paper is to provide an overview of the technical aspects of our cyber arena, based on the work performed and completed within the second half of the project.

SPIDER Cyber Range Infrastructure and Supporting Technologies

5G programmable/virtualised infrastructure management

SPIDER Cyber range uses an integrated network orchestrator that combines novel technologies based on Network functions virtualization (NFV) and Software-defined networking (SDN) to set up customised solutions for different 5G training scenarios. The programmable virtualized infrastructure forms the basis to setup dynamic 5G services, automate configurations, and deploy cyber range services for 5G platform management and orchestration for SPIDER cyber range as a service, for modelling and emulation of security mechanisms, and for data collection and visualisation, in order to support different use cases and 5G testbeds. MATILDA orchestration framework is used as base for the range test scenarios and MOUSEWORLD as machine learning lab to generate the required traffic and training the machine learning algorithm used as tools in SPIDER cyber-range exercises. It covers both, the hands-on emulation scenarios represented by the Cyber Range MANO, and the Machine Learning (ML) training scenarios, identified as the Machine Learning Lab. The 5G infrastructure used in SPIDER platform and in the Machine Learning Lab is based on the virtualization of the 5G core network.

5G platform management and orchestration for SPIDER cyber range as a service

5G platform management and orchestration covers the lifecycle and orchestration of 5G-ready applications and 5G network services over a programmable infrastructure, describing the design and integration activities needed to adopt a unified programmability model and a set of control abstractions. This design is fully compliant with the 3GPP and ETSI NFV specifications, and integrates state-of-the-art control building blocks such as the WIM, the OSM NFV Orchestrator, the Open Daylight SDN controller, OpenStack ("Queen" release), and a network (OSS/BSS) and Vertical Application Orchestrator (VAO). Together, these components are able to instantiate 5G network slices as-a-Service that serve as virtual playground for emulation activities on the cyber range. Within this framework, Lifecycle Management activities are fundamental, as the correct and efficient instantiation of the constituent components of an emulated scenario is a necessary

prerequisite for carrying out the hands-on activities. Lifecycle management defines the processes needed for the implementation, delivery, operation, and maintenance of deployed components over the course of their existence. These activities are automatically performed every time a new emulation scenario is recalled. Each emulation scenario involves the creation of network-slice of the 5G programmable infrastructure and a set of properly configured application- and network-level components relevant for the test/training. Moreover, an intelligent management and orchestration (MANO) solution is integrated into the cyber range platform to support the automated end-to-end deployment and provisioning of applications, network services and slices. When an emulation scenario is provisioned, it goes through multiple phases, commonly referred as Day-0, Day-1, and Day-2. Once emulation scenario is deployed, several operations may be necessary as the training progresses. These operations that may be necessary both at the application and network levels as the training progresses such as monitoring, reconfiguration, scaling, load balancing, maintenance and changes to the virtual environment are referred to as Day-2 operations.

Modelling and emulation of security mechanisms

5G deployments leverage on end-to-end programmability, building on the concept of network slices to meet disparate application requirements by multiplexing independent virtualized logical networks on the same physical network infrastructure. Such end-to-end slices are composition of either Virtual or Physical Network Functions (VNF and PNFs) and virtual Applications (defined as executable service graphs in SPIDER). It follows that a 5G infrastructure makes extensive use of the concept of virtualization. From a cyber-security point of view, this dependence is by far a double-edged sword: on the one hand, programmability allows flexible responses to cyber security threats; on the other hand, virtualization of the network and hosted services could open up cyber risks. From the training point of view, SPIDER offers two distinct learning environments. On the one hand, the emulation environment provides the possibility to interact (hands on) with a real 5G infrastructure ranging from bare metal to antennas. On the other hand, the simulation environment runs scripted scenarios (also dealt with as serious games) that are influenced by the

decisions of the trainees. The security assets that are specific to the emulation environment of the SPIDER cyber range are built on top of Open-Source software, and have been selected to maximize the coverage of possible functions to be deployed in training scenarios.

Data collection and visualisation toolkit

The data collection framework handles the huge network traffic produced by the various 5G-related virtualised assets, network functions, devices, applications and by the SPIDER cyber range platform itself, focusing on gathering the log files produced within the SPIDER 5G cyber range environment, in addition to collecting triggered actions from SPIDER components acting as middleware or proxy. On the other hand, the visualisation toolkit aims to provide a customisable interactive graphical user interface (GUI) for displaying the information collected within the SPIDER cyber range, across space and time; information processing includes operations such as: Decision risk quantification, progress quantification and gamification metrics. In particular, the visualisation toolkit supports personalised dashboard views for the different user groups of the SPIDER platform (i.e., non-expert cyber security trainees, red and blue team members, risk auditors and training scenario supervisors), which facilitate their interaction with the system and the comparison and inspection of data produced within the cyber range framework. Also, it outputs the individual SPIDER components to the platform's GUI either via dedicated APIs or via a high-throughput interface, implemented by Apache Kafka stream, which supports the fault tolerant handling of high-velocity and high-volume data. Supplementary, it also provides an administrator view for system monitoring and alerting based on Netdata. Data collection and visualisation toolkit is part of the SPIDER monitoring and reporting layer that tracks trainees' activity, their progress, and outcomes while they are training within the SPIDER Cyber Range as a Service (CRaaS).

5G Cyber Security Training

Self-paced and team-based cyber exercises

A set of exercises covering several aspects of 5G security together with their accompanying manuals and guidelines have been implemented in SPIDER Cyber Range. 14 out of 27 in total SPIDER-developed scenarios, are dedicated to expert end-user upskilling and more specifically SPIDER's Modality 2: hands-on exercises on the emulated part of the platform. The collection of the SPIDER-developed exercises aspires to provide a holistic cybersecurity training, learning from cloud to radio access network security. A new addition in the list of scenarios is the Open Radio Access Network (ORAN) scenario, with the aim to introduce cybersecurity experts to state-of-the-art radio technologies. ORAN is an evolution of the Next Generation RAN (NG-RAN) architecture, based on cloud native principles to achieve a totally disaggregated approach. These 14 scenarios have been selected as such after careful study on the user requirements and range in levels of difficulty and skills to-be-acquired and focus on different parts of the SPIDER platform. The ultimate goal is to provide a holistic training from web to radio access parts of a 5G infrastructure to offer a flavor of the challenging 5G landscape to security experts.

5G serious game solution

While often overloaded, the simulation term in SPIDER refers to the ability to calculate the cyber risk of a realistic 5G topology that includes (artificial) vulnerabilities associated to the assets and against a set of possible attacking and defensive actions. As such, the axis of freedom of such a simulation are practically infinite since the assets, their interconnections, the associated vulnerabilities, and the attacking and defensive controls can be arbitrary. In a nutshell, these models take under consideration several 'logical consecutive' steps that are executed by ethical hackers (Red team) or cyber respondents (Blue team) during an attack/defence scenario. Since in the actual calculation of a simulated scenario these actions are obscured, SPIDER developed a game where these actions can be 'played' in the frame of a Serious Game Security Skills Training. The game is named RxB and intends to bridge the gap between theoretical training (Modality 1)

and hands-on training (Modality 2). RxB is a turn based asymmetrical strategy game about cyber-attack and cybersecurity based on the Red vs. Blue "interactions" used at hackathons, real life security simulations and company security training. Red is a hacker team trying to fulfil an objective while Blue is a cyber security team that tries to prevent this. It allows users to play on top of a predefined asset graph with given vulnerabilities. RxB has been created with the following audiences in mind:

- Technical people new to cyber security (e.g., cyber security students, trainees, juniors as well as operational technologist, engineers and IT professionals outside cyber security) and interested in cyber security or cyber security risk management as a career.
- Cyber security managers, chief information security officer or technical specialist that want/need to understand and train cyber security strategies, cyber security management and threat prevention.
- Non-cybersecurity personnel that need cyber security awareness but doesn't necessarily have to understand all the technicalities.
- Finally, RxB could potentially be used in various contexts such as corporate security training, College and universities or individual self-training.

5G gamification solution

SPIDER's gamified learning environment enables trainees to master how to use domain-specific cyber protection technologies and improve their ability in handling incidents and risks. The gamification awareness training application, is also referred to as Modality 4: Security Awareness Training through Gamification. It 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 scope of the gamification cyber security awareness training solution is increasing security awareness among those employees in organisations who do not have specific cybersecurity skills. This educational activity is implemented by means of micro-learning praxis-near quests for continuous training, which may be carried out when time allows. In fact, social engineering plays a crucial role to provide real and lasting impact, especially

in relation to on-site security, hence, special care must be given to avoiding risky behaviours that can jeopardize cyber security. The acquired fundamental technical skills are extremely essential since it has turned out that the human factor is the most severe vulnerability. The most 'lethal' attacks commence through the successful exploitation of the human factor. Hence, the elementary competences acquired through these micro-learning praxis-near quests contribute in the radical increase of the cyber-immunity.

Human-in-the-Loop performance assessment tool

SPIDER is a multi-modal educational platform delivering a unique educational value proposition targeting the specificities of security training for modern virtualized/5G networks. To tackle these educational challenges, an articulated platform has been developed offering the four complementary learning modalities. Each of these educational modalities have diverse learning goals and diverse means of quantifying the efficacy of the educational value proposition. In other words, the progress of users and the impact of this progress to real-life competencies is a major challenge by its own. Apart from Modality 4 which is not subjected to scoring/quantification since it is targeting non-expert users, the rest three modalities entail their own parameters of quantification. For Modality 1 (theoretical training), the endmost goal of the offered functionality is to quantify the so-called Theoretical Skill Level (TSL) vector. Such vector maps specific CAPEC-MITRE competencies that are ranged from 0 to 10. In order to quantify TSLs the user has to interact with theoretical challenges and certification tests that contain training material that is pre-annotated as far as their difficulty is concerned. The initial 'bias' of the vector is produced by a self-assessment session that tries to identify the TSL level per competency of the trainee using a variety of challenges of mixed level. The commitment of the trainee and therefore the recurrent execution of challenges is crucial for moving upwards or downwards. For Modality 2 (emulation-based training) a different vector space is defined i.e., the Practical Skill Level (PSL). Although PSL is also mapped to CAPEC it is quantified in a completely different way. More specifically, each hands-on session challenges the trainee to 'hack' vulnerable network topologies that are multi-asset. Each asset contains vulnerabilities with variable exploitability. The exploitability of the vulnerabilities,

the time needed for a trainee to make use of this vulnerability along the feedback from the deployed Security information and event management (SIEM) are the key variables that define the trainee's performance. Finally, it should be clarified that modality-3 (simulation-based training) ships with two flavors. The first flavor is the Serious Game - oriented where users are playing a turn-based game with the ultimate goal to penetrate a network or defend a network (depending on weather you take the role of the red or the blue team). The second flavor relates to triggering of Simulation-sessions per se on top of arbitrary network topologies that contain synthetic vulnerabilities and controls. In the first flavor, scoring relates to multiple in-game parameters such as amount of turns played, induced cost per move, time consumed etc. The second flavor produces risk calculations based on user-driven actions (e.g., apply an artificial control). Quantification in this flavor is more difficult since it employs reverse propagation technique i.e., calculate the distance between the effect of a user's action against the near optimal action for a given problem, e.g., minimize the risk on a specific asset with this given cost.

SPIDER Configurable Virtualised Security Operations Center (SOC)

SPIDER delivers a novel cyber-range platform specifically targeting 5G deployments. In doing so, SPIDER offers both emulation and simulation environments: while the latter is configured to execute simulated scenarios (also addressed as serious games), the former provides the ability to interact (hands on) with an experimental facility implementing a real 5G infrastructure, including gNodeBs, 5G Core functions, and the hardware and software resources (both at control- and data-plane levels) to support NFV according to ETSI MANO framework. In the context of SPIDER, the Configurable Virtualised - Security Operations Center (CV-SOC) has a double scope: firstly, it works as a SOC, which trainees can use during exercises to familiarize with SOC technologies and, secondly, practices 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. Thus, CV-SOC in SPIDER is developed in a way to effectively analyse large amount of data, handle all the generated logs in a reliable way, provide meaningful insights, reconstruct context starting from the raw logs and the configurability of the framework, as well as adapt its analysis to the requirements of the specific training scenario.

5G threat knowledge base and incident repository

Vulnerability/Threat Knowledge Base is, on the one hand, used during the training sessions of SPIDER and on the other hand, has general applicability in the 5G ecosystem. SPIDER 5G Cyber Range platform differs significantly from a general-purpose cyber range platform since it takes under consideration the specificities of a modern mobile telecommunication network. The conceptualisation of such a network is not an easy task since modern networks entail several configurable modules, most of which tend to be virtualised. This sophisticated programmable infrastructure spans from the backhaul part of the network to the radio access part and is the cornerstone of the 5G slicing concept. According to this concept, programmable slices can be dynamically created to satisfy application requirements in terms of storage, compute, and traffic utilisation. The introduction of this dynamicity radically increased the number of attack vectors that are exposed by 5G operators. Virtualisation of substrate networks, along with the virtualisation of hosted services, raises many cyber risks that need to be identified and mitigated by security experts. As a result, 5G deployments suffer from many threats. SPIDER formalizes the schemas for these threats to create reusable and meaningful knowledge objects in the 5G domain.

Economics of 5G Security

Continuous risk analysis: models and assessment engine

Following the CORAS modelling methodology, a set of graphical cyber risk models addressing nine different attacks has been developed: 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. The models encompass key ingredients such as threats, attacks, vulnerabilities, mitigations, assets, security properties and a company business profile. Their ultimate goal is the calculation of the economic cyber risk exposure associated to the ICT infrastructure and related digital assets of the company. To perform this computation, the CORAS methodology envisions a set of guidelines to transform the graphical models into machine-readable code, developed in the R programming language. These scripts written in R evaluate the cyber risk exposure and need a set of inputs which are obtained and processed by the component called Continuous Risk Assessment Engine (CRAE). CRAE is the software component that calculates the cyber risk exposure of the emulated infrastructure in emulation scenarios. The CRAE, upon obtaining all this information invokes these scripts passing such information as inputs. Some of the inputs are static and are provided at the beginning of an exercise in the configuration phase, being mainly devoted to the characterization of the client company and its ICT infrastructure, including the relevant digital assets; while the rest of the inputs are dynamic and are provided as different events happen during the exercise. Input obtained using cybersecurity information coming from external repositories is also included. CRAE can be a useful supporting tool in the process of ISO27001 and ISO27005 certifications. Within SPIDER 5G Cyber Range, CRAE is used in both emulation and simulation scenarios.

SPIDER Cybersecurity Investment Component

Cybersecurity Investment Component (CIC) is in charge of providing tailored cybersecurity investment advice to 5G security managers, through SPIDER Cyber Range. CIC component in the

SPIDER architecture is threefold: (1) assigning priorities to detected vulnerabilities; (2) defining remediation solutions to mitigate detected vulnerabilities using an optimisation model to address the short-term problem of optimal allocation of a limited budget; and (3) analysing how the long-term, dynamic evolution of underlying uncertainties impacts the value of optionality in relation to investment in cybersecurity. As the name suggests, the CIC component implements cyber economic econometric models considering as input the outcomes of Continuous Risk Analysis. The output of the CIC component feeds the SPIDER dashboard and Graphical User Interface (GUI) and empowers the 5G system administrators to take optimal cybersecurity investment decisions. CIC also allows the risk auditors and investment decision support managers of the 5G infrastructure to interact with the SPIDER platform in order to provide their preferences, rules, policies, recommendations, and risk priorities; parameters that are used to instantiate the SPIDER cyber economic models. SPIDER's cybersecurity investment component outcomes are not only interpretable and adaptable to risk and monetary changes, but also to user defined constraints. The novelty of the economic framework is to account for both the sequential nature of a cyber-attack and key underlying uncertainties, thereby facilitating a more detailed evaluation the organisation's risk exposure. This more formal treatment of risk is subsequently utilised to facilitate the decision-making process for optimal cybersecurity investment that considers risk preferences in the light of limited availability of financial resources. Another novel aspect of the risk calculation performed by the CIC's economic models is that it can be applied as evaluation mechanism for solutions provided by the users. Finally, the CIC can provide the SPIDER Dashboard with statistics about the detected vulnerabilities. This gives the user a more readable overview of the vulnerabilities and their evolution over time, which is useful especially for the defenders of the Blue Team enabling them to quickly assess the situation and see their progress as new vulnerabilities are discovered and mitigated.

Conclusions

SPIDER Innovation in a nutshell

SPIDER is an Innovation Action that is making a leap forward in several knowledge areas spinning around cybersecurity and in particular the delivery of cyber training. As made evident from the technological advancements presented in this White Paper, a variety of innovation streams can be identified within SPIDER, as summarised below:

- **SPIDER is a cyber range focused on 5G, not a generalist one**: Cyber ranges constitute a flourishing market and most existing platforms are conceived in a generalist way, providing cross knowledge from the basics to advanced levels. Leveraging knowledge and experience acquired in recent years, the SPIDER Consortium intended to focus on the telecom sector, particularly on 5G communications, expected to represent key technological enablers for several vertical industries in the next decade. While there are no works on cyber ranges focused on 5G cybersecurity, SPIDER covers the whole chain of end-to-end services, from the end-device up to the application deployed in the cloud, via the radio access and the core networks. The ability to interact with a real 5G deployment is extremely valuable since it unleashes the potential of experienced users to perform sophisticated attacks that include pivoting and escalation techniques.
- **SPIDER is a cyber range that follows a hybrid approach combining both emulation and simulation techniques**: Regarding emulation, SPIDER offers high flexibility to deal with a wide range of situations with respect to resources availability. In the likeliest situations, it is not possible to count on real 5G equipment in order to materialize a scenario in the frame of a training exercise. This is solved thanks to virtualization and the ability to recreate different networked interconnected assets playing different roles in the emulated infrastructures. On the other hand, it offers the possibility to support scenarios where virtualized services (e.g. a virtual EPC) and physical assets (e.g. a USRP module) are both configured; since an interplay between them is required for sophisticated exercises. This is fully in line with the existing trend of creating, not only virtual-physical arenas associations, but also federations of cyber ranges

that share resources and make each other more powerful to deliver highly sophisticated cyber training.

- **Provision of self-paced learning through gamification**: The application of gamification to cybersecurity training is a very innovative pathway to explore in depth. The amusing component of these games eases the engagement of the trainee, the acquisition of the knowledge and its eventual retention. The game elements are closely tied to what the user already does in the real world. It is a way to focus more clearly on the right behaviour, get feedback when things done right, and get motivated by seeing clear progress in the form of level-ups, achievements or similar. This type of training is an easy opportunity to practice cybersecurity strategies and management, abstracting away the complexity of using very specific technical tools. For non-experts, SPIDER gamification solution gives the chance to offer training in small daily learning pills (microlearning), easy to digest, in which the employees adopt an active role in their learning process, increasing retention and easing the transfer of knowledge. Security threats and attacks are ongoing and typically the "weakest link" the non-experts are exploited.
- **Live library of 5G components to emulate which can be parameterized and spawned on demand**: The project has an innovation stream addressing the need to characterize with greater fidelity different 5G components. These bricks are employed to build realistic fully fledged 5G infrastructures in the most-common case when real-world components cannot be used for experimentation and training. The programmable infrastructure offered by SPIDER plays a key role to make it possible. SPIDER uses VNFs, PNFs or virtual applications for the slices. The flexibility of this library enables the support of multiple use cases.
- **Live library of 5G fully focused scenarios**: Assembling the different bricks available in the component library, and always keeping the possibility to make them interoperable with real elements, SPIDER offers a library of 5G fully focused scenarios ready to be used to run a practical training on top of them. It is important not to forget that SPIDER not only addresses training, but also testing, and can be used to test new security technologies. Finally, SPIDER also offers scenarios targeting risk managers in order to provide proper support to optimally decide

on the best investments to strengthen corporate infrastructures against potential cyber threats and attacks.

- **Usage of Artificial Intelligence / Machine Learning to train models that can be used for sophisticated offensive or defensive activities**: For attacking, Generative Adversarial Networks is a variant that is available to generate synthetic network attacks that are different to each other yet with similar statistical characteristics. This tool can be used in emulation scenarios and the traffic generated is highly realistic. It addresses a recurrent problem for cyber ranges, which used to have to trust 3rd party components to obtain this traffic which is fundamental for emulation exercises and/or bring specialized red-teamers to inject this traffic directly in the emulation. Unlike the prevailing existing data augmentation solutions, we obtain synthetic flow-based traffic that can fully replace real data. Therefore, this solution can be applied in scenarios where data privacy must be guaranteed. The SPIDER platform contains a Machine Learning Lab which is a key asset of its value proposition. This lab is used to create offensive and defensive "primitives" to be used in the emulation scenarios.
- **Possibility for trainees to bring their own tools**: The SPIDER platform offers the chance to incorporate third party tools that are not included in the set SPIDER makes available for the trainees. This way the trainee can benefit from a more customized learning experience, as well as bridge possible gaps existing in the SPIDER platform. This is applicable to both the red and blue team members.
- **Automatic scoring system embedded in the platform, and specific to each scenario**: SPIDER uses as much as possible information logged during the execution of an exercise to automate the evaluation of performance for user/s teams involved in the exercise. The performance evaluation system is very adaptable to the needs of each scenario, considering the type of information that will be available to make such an evaluation. The system is continuously giving the users feedback about the effect of their actions. Additionally, the platform can automatically assess the level of expertise of the user and assign upcoming exercises according to such a level. SPIDER welcomes users from a very wide range of expertise levels, from non-experts to highly experienced people who seek to improve their preparation for major cyber incidents, though.

- **SPIDER security self-monitored and certified**: SPIDER incorporates a Security Assurance Platform, which is a horizontal component responsible to monitor and assess the security of the SPIDER platform. It ensures the security and the privacy of the data held in the SPIDER platform. It provides a real-time view of the security posture of the 5G testbed. This mechanism assures the confidentiality, integrity and availability, which are continuously monitored basing on gathered events and Event Calculus logic.

Future of Cyber ranges: Network Digital Twins for Cyber Range Applications

The Conceptual Ideal for Product Life Management, can be considered as the seminal concept of the Digital Twin (DT) and was first proposed by Dr. Michael Grieves in 2002 as "a digital representation of a physical object or system throughout its life cycle." Based on this initial formulation, a DT has evolved over the years to represent a digital replica of a physical object or system that can be used to monitor and manage a physical asset or system in real-time or use it to recreate its behavior in predefined virtual scenarios. DT technology can be used to improve the design of products, to optimize manufacturing processes, and to provide real-time feedback on the performance of products.

Network Digital Twin (NDT) is a new technology based on the concept of Digital Twins (DT) to create a virtual representation of the physical objects that exist in a telecommunications network and their corresponding interconnections. An NDT captures data from the physical system in real time and uses this information to recreate its behavior in a virtual environment.

In response to the pressing demand to respond to the continuously evolving nature of cyber-attacks, the NDT concept has been proposed as a new methodology for more advanced experimentation in the cybersecurity domain. In this regard, the adoption of NDT technology to cyber-scale applications has the potential to significantly improve the efficiency and effectiveness of cybersecurity operations. More specifically, an NDT can serve as a testbed to simulate the behavior of a network under different types of attacks and to test the resilience of network security systems in a secure, flexible, and realistic environment, while allowing to thoroughly dissect the

system under study to better understand the effects of cyber incidents. In this way, an NDT can support improved cybersecurity design, training, simulation, and analysis in a variety of contexts, such as network defense, incident response, forensics and learning over cyber ranges. Efforts are in progress to create a reference architecture around this NDT idea in standardization bodies such as IETF.

To construct an NDT, it is necessary to build a model of the physical system to be represented. This model can be built using various methods, such as data mining, network traffic emulation and reverse engineering. However, due to the heterogeneous, dynamic, and complex nature of telecommunication networks, Artificial Intelligence (AI) techniques are particularly suited to the task of modeling these complex systems. SPIDER has created an initial AI-based NDT architecture, called B5GEMINI, to support the modeling and emulation of 5G networks that has the potential to serve as a key enabler of intelligence-driven Cyber Range applications by providing a realistic and scalable testbed for the evaluation of network security systems. In this NDT, network behavior can be accurately and quickly reproduced in a virtual environment under a variety of conditions to train security professionals against a wide range of cyber-attacks and cyber-warfare scenarios.

References

[1] SPIDER D3.6 “5G programmable/virtualised infrastructure management - final version”, 2022

[2] SPIDER D3.7 “5G platform management and orchestration for SPIDER cyber range as a service - final version”, 2022

[3] SPIDER D3.8 “Modelling and emulation of security mechanisms - final version”, 2022

[4] SPIDER D3.9 “Data collection and visualisation toolkit - final version”, 2022

[5] SPIDER D4.3 “Self-paced and team-based cyber exercises”, 2021

[6] SPIDER D4.4 “5G serious game solution”, 2021

[7] SPIDER D4.5 “5G gamification solution”, 2021

[8] SPIDER D4.6 “Human-in-the-Loop performance assessment tool”, 2021

[9] SPIDER D4.7 “SPIDER Configurable Virtualised SOC - final version”, 2021

[10] SPIDER D4.8 “5G threat knowledge base and incident repository - final version”, 2021

[11] SPIDER D5.6 “Continuous risk analysis: models and assessment engine - final version”, 2021

[12] SPIDER D5.7 “SPIDER Cybersecurity Investment Component - final version”, 2021

[13] Digital Twin Network: Concepts and Reference Architecture, https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/

[14] Mozo, A., Karamchandani, A., Gómez-Canaval, S., Sanz, M., Moreno, J. I., & Pastor, A. (2022). B5GEMINI: AI-Driven Network Digital Twin. Sensors, 22(11), 4106.

SPIDER Consortium

https://spider-h2020.eu

spider-h2020-funded-project

@spiderh2020_eu

SPIDER.H2020