Pilot use case scenarios and architecture of the SPIDER project

White Paper release v1.0

Published 11/01/2021

Main Contributors (names)

UBITECH	Panos Gouvas
UPRC	Anna Angelogianni,Ilias Politis, Christos Xenakis
8BELLS	Neofytos Gerosavva
ATOS	Antonio Alvarez
FORTH	Manos Athanatos
CNIT	Jane Pajo
TID	Antonio Pastor, Jeronimo Nunez Mendoza
UPM	Alberto Mozo, Stanislav Vakaruk
INFOCOM	Maurizio Giribaldi
CLS	Irene Karapistoli, Matthias Ghering, George Alexopoulos
SPHYNX	George Spanoudakis
ERICSSON	Pierluigi Polvanesi, Angela Brignone

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

Glossary

Acronym	Explanation
5G	Fifth generation technology
AI	Artificial Intelligence
API	Application Programming Interface
CIC	Cyber Security Investment Component
CRaaS	Cyber Range as a Service
CRAE	Continuous Risk Assessment Engine
CVE	Common Vulnerability Enumeration
DoH	DNS over HTTPS
DoS	Denial of Service
DNS	Domain Name Service
GAN	Generative Adversarial Network
LAN	Local Area Network
ML	Machine Learning
NFV	Network Function Virtualisation
NFVO	NFV Orchestrator
NGC-CP	Next Generation Core - Control Plane
OSS	Operations Support System
PPTP	Point-to-Point Tunneling Protocol.
PUC	Pilot Use Case
SBA	Service Based Architecture
SBI	Service Based Interface
SDN	Software Defined Networking
SOC	Security Operations Centre
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VAO	Vertical Application Orchestrator
VIMs	Virtual Infrastructure Managers
VNF	Virtual Network Function
VPN	Virtual Private Network
vSOC	Virtual Security Operations Centre
WSCs	Wide-area SDN Controllers
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

Acknowledgement

The authors of the present document would like to acknowledge and express their thanks to the leading WP2 contributors as well as to the partners that actively contributed and provided their insight & 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 D2.3, D2.4, D2.5 and D2.8 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 WP2 activities during the first half of the project. More specifically, the current paper focuses on presenting the activities on WP2 "Requirements Analysis, Architecture Definition and Pilot Use Cases", and especially the outcomes of the deliverables D2.3 "Spider Platform Reference Architecture - Initial Version", D2.4 "SPIDER use cases and pilots definition – initial version", D2.5 "SPIDER user requirements and the 5G cybersecurity threat landscape – final version" and D2.8 "SPIDER use cases and pilots definition – final version".

The purpose of D2.3 is to elaborate on the reference architecture of SPIDER while D2.4 is the result of the studies conducted during the first twelve months of the SPIDER project as part of the Task 2.4: "Design of the SPIDER Pilot Use Cases". The scope of the deliverable D2.4 is the definition of the SPIDER use cases and the pilots. The D2.5 is the extraction of the SPIDER user requirements and the definition of the 5G cybersecurity threat landscape. Finally, the D2.8 provides the final version of SPIDER Pilot Use Cases.

The current paper will provide a summary of the work completed by the aforementioned deliverables.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

CONTENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

1 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 [1]. 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 [2].

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.

During the first year of the SPIDER project lifecycle and towards the completion of defined milestones and objectives, the consortium partners conducted studies within the context of the analysis, collection and extraction of SPIDER user requirements as well as the definition of the 5G cybersecurity threat landscape and the related stakeholders in order to outline the possible attack scenarios for the SPIDER's training platform.

In order to help identify and understand the business needs, and to derive the requirements that the architecture development must address, SPIDER actors, business and user scenarios were initially identified, including the relationships among the SPIDER related stakeholders and the defined scenarios. The purpose of this White Paper is to provide a description of the WP2 activities completed within the first 18 months of the project and more specifically to present D2.3, D2.5 and D2.8 output results.

The remainder of this White Paper is organized as follows:

Section 2 describes the SPIDER approach and objectives and provides also some background information.

Section 3 refers to the SPIDER architecture as this was described in D2.3.

Section 4 presents the SPIDER uses case scenarios as those were defined in D2.4, D2.5 and D2.8.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

2 THE SPIDER APPROACH AND OBJECTIVES

2.1 BACKGROUND

The 5G technologies through their potential to enable and support a spectrum of functions and applications would play a major role towards the successful digital socioeconomic transformation in the EU affecting a wide range of sectors such as IoT, energy utilities, healthcare, public safety, manufacturing, media and entertainment, transportation (e.g. autonomous cars), financial sectors etc.

For instance, estimations strengthen the importance of 5G by placing worldwide revenues from 5G approximately to 225 billion in 2025 [3], thus 5G cyber security is crucial for enabling the full potential of the opportunities that come along. The 5G technologies bring together a variety of benefits, such as enhanced speed and performance, lower latency, and better efficiency, scalability and flexibility but also pave the way for new security threats. These potential threats may affect software, hardware or arise from potential deficiencies in the security processes of any of the various involved actors [3][4]. Based on national cyber-risk assessments provided to EC and ENISA from individual member states on July 2019, the European Commission consolidated and released on October of the same year a document named "EU Coordinated Risk Assessment of the cybersecurity of 5G networks" [5], describing the risk scenarios and threat actors, and providing a situational overview on technical and non-technical vulnerabilities to be taken into account towards 5G deployment within EU. The report underlines the fact that there are many issues and challenges to be taken into consideration towards 5G secure network architecture development and the complexity of 5G technologies bring together additional vulnerabilities on the 5G network infrastructures.

Moreover, the complexity of threats and malicious activities in cyberspace have continued growing and cybercrime attackers are getting more organized and are continuously fine-tuning their tactics as well as the respective attack vectors while at the same time they incorporate even more advanced and automated techniques and tools. This can cause severe security breaches on critical infrastructures (for instance according to the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures, sponsored by Herjavec Group, cyberattacks will cost the world $6 trillion annually by 2021, (in comparison with the $3 trillion in 2015) [6]. According to the same report, cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. Another study of 2017 [7] refers to the fact that cyber security professionals have to deal with an increasing velocity of malware hitting their networks at a relentless pace.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

Moreover, the COVID -19 situation brought new challenges relating to cybersecurity as it is easily understood that not all organizations were prepared for switching to a full remote working mode. IT workers had to extend remote working capacity in order to provide to the employees the potential to perform their duties and conduct operations remotely and as a consequence this can increase the level of cyber threats potentials. For instance, hackers, are initiating COVID-19 themed attacks in the form of phishing emails that can help them penetrate companies' systems, disrupt normal operations and steal data and user credentials. Also, attackers can use temporary websites or even take over vulnerable ones for hosting malicious code. Then they can redirect potential victims to these sites in order to intrude their devices through malicious code. Additionally, this kind of fake websites request donations for daily wage earners through email links. A recent example is the hacking of videoconferencing systems (e.g. ZOOM) [8].

This complex landscape surrounding today's cyber security strengthens the need for better trained and qualified experts securing critical multi-tenant and multi-service environments, such as 5G mobile networks.

Private organizations worldwide understand how important is to safeguard their infrastructures, providing at the same time a secure and protected remote access capacity and towards this direction they need to define and execute reliable cybersecurity strategies either in the form of training or through information provision.

It is easily understood that new approaches, innovative cyber security models and training environments are needed for mitigating both technical and non-technical risks associated with 5G applications and for strengthening 5G network operators' and providers' capacity to prevent and respond accordingly to cyber-attacks.

Thus, there is a need for appropriate tools that can deal with cybersecurity threats and **cyber range training platforms can represent a reliable solution**.

Cyber ranges are well defined controlled virtual environments used in cybersecurity training as an efficient way for trainees to gain practical knowledge through hands on activities [9]. Traditionally, cyber ranges were platforms that enabled commercial companies, government agencies and military organizations to study the effectiveness of their cybersecurity technologies, test their infrastructures and identify and assess potential vulnerabilities. These platforms can provide the chance to their potential users to simulate real-world complexity cyber scenarios with high fidelity and train employees and customers on the latest threats through high quality realistic cyber exercises, without endangering the productive environment, which is just replicated virtually in harmless manner.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

2.2 APPROACH

SPIDER proposed solution will take into account all relevant advancements and latest trends and will capitalize on current state of the art offering a synthetic and sophisticated war-gaming environment that will provide to the training users the ability of playing the part either of the attacker either of the defender (in jargon they are known as red and blue team respectively). SPIDER users will be trained under realistic conditions and this way, they will further enhance their skills and will specialize in a variety of issues. The SPIDER solution features integrated tools for cyber testing including advanced simulation and emulation tools, novel training methods towards active learning as well as econometric models based on real-time emulation of modern cyber-attacks. SPIDER basic objective is not only to provide the users with the capability of predicting the evolution of cyber-threats but also to analyse the associated economic impact and cost that is brought with the respective attack. Involving economics is a very attractive way to engage the managerial positions of the company in the learning process, presenting the risk in the language they understand. In consequence, cybersecurity will be no longer just matter of technicians, but the managers can come into play and team up with them, with a positive effect in the decision-making process on how to use the budget allocated to cybersecurity to give the best protection to the infrastructure and its digital assets. Artificial Intelligence is part of the Cybersecurity ecosystem, not only for detecting new types of attacks, but also as an opportunity to improve attack emulation capabilities. SPIDER ambition includes a machine learning platform to provide the capacity to use this technology in the Cyber range exercises, creating specific AI-based tools. It will open an opportunity to learn how to use and defend for both, BLUE and RED team members.

The main expected output of the project will be a cutting edge CRaaS platform that will offer to its intended users a digital gamified and serious game-based learning environment capable of training experts and non-experts following a Red vs Blue team format. More specifically, through various types of gaming scenarios, the platform players will have two options: they could be either performing the role of the attacker (RED TEAM member) in which the Red team conducts malicious activities against emulated networks and systems or they will have the option to play the role of the defender (BLUE TEAM member). Red team members shall be able to perform all the security penetration steps and initiate several types of attacks. On the other hand, the Blue team members will have all the required privileges to perform defensive actions on the 5G infrastructure, configure security critical mechanisms and apply custom rules and configurations for mitigating attacks and minimizing the attack surface.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

Furthermore, SPIDER's vision is to address the needs of both experts and non-experts' trainees. SPIDER platform will be used for enhancing users' skills, through gamification and generation of various cybersecurity simulation scenarios that will offer to the trainees the chance to participate in various types of cyber tests (both pre-built and customised).

Moreover, SPIDER has the ambition to act as a serious gaming repository for a variety of related stakeholders for sharing training data and improving efficiency through the provision of complex cyber tests. Additionally, to this and as mentioned, SPIDER will deal with the generation of improved risks analysis and econometric models towards a more effective decision-making and faster cyber risk responding security measures. Also, SPIDER will incorporate and integrate well known simulation techniques such as Monte Carlo for designing robust optimisation techniques in order to address the challenges coming by the efficient allocation of limited financial resources under uncertainty and additionally for forecasting the long-term dynamic evolution of various cyber security metrics.

3 SPIDER ARCHITECTURE

The SPIDER reference architecture consists of a proper componentization along with proper interaction and dependency tracking among these components. The functional goals of SPIDER will be materialized by an integrated platform which will be "de-composed" in several architectural modules. The decomposition process by itself aims at the enhancement of conceptualization, the acceleration of development and the proper analysis of the entire platform. The business logic of each component along with their interactions in high-level view are identified and elaborated.

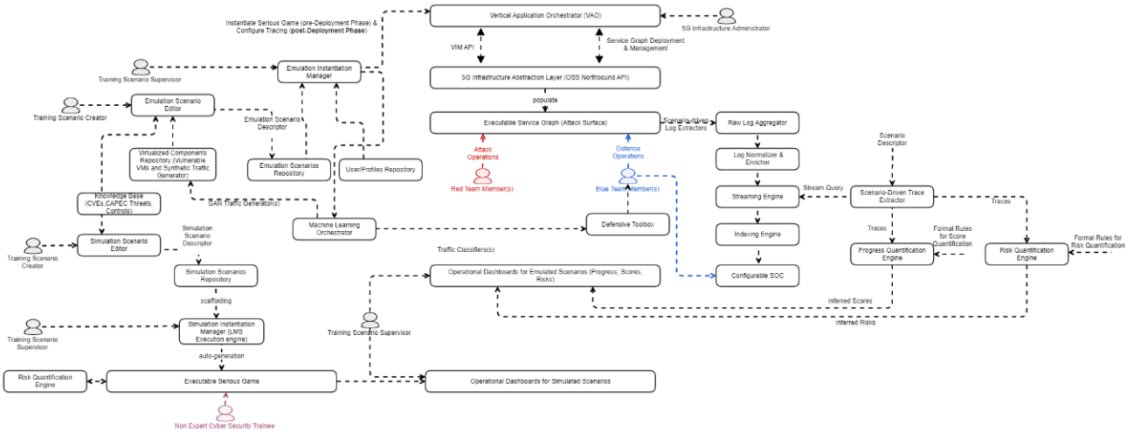

Figure 1: Overview of SPIDER Reference Architecture

The architecture components are listed below along with their short description

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

C1 COMPONENT -knowledge base: The knowledge base is the architecture component that monitors and keeps track of the various 5G asset types, vulnerabilities, potential threats control elements and other.

C2 COMPONENT - Emulation Scenario Editor: The emulation scenario editor is the component that will assist towards training scenarios creations that will be instantiated on top of a 5G infrastructure. It is responsible for the management and the creation of service graphs that represent complex attack scenarios with the associated attack paths and will be deployed in a programmable 5G testbed.

C3 COMPONENT-Emulation Scenarios Repository: This component is the emulation scenarios repository that is responsible for the storage and preservation of the service graphs that are being generated by the C2 Component (Emulation scenario editor).

C4 COMPONENT-Virtualized Components Repository: The virtualized components Repository is responsible for managing the registration of virtual components (Containers). Each one of these components can be used within the context of a service graph.

C5 COMPONENT Emulation Instantiation Manager: This is the component that is responsible for loading an emulation scenario from the repository and coordinating its instantiation in the 5G resources. Each emulation scenario consists of multiple virtualized components that formulate an application graph. Moreover, the Emulation Instantiation Manager is the component that will trigger the application deployment & trace configuration.

C6 COMPONENT: Vertical application orchestrator. This is the component that manages the choreography of service graph life-cycle management from initial deployment to un-deployment. The basic objective of the vertical application orchestrator is to materialize a placement plan of an emulation scenario.

C7 COMPONENT Operational Support System. The Operational Support System component is the component responsible for the configuration and management of programmable 5G infrastructure depending on the needs of an emulation scenario.

C8 RAW Log Aggregator. The component that is configured to accept raw logs of all runtime components (Virtual Machines of applications, switches, VNFs).

C9 COMPONENT Streaming and Rule Engine. This component offers a Complex Event Processing functionality that is used to issue specific events that are valuable for SPIDER analysis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

C10 COMPONENT Indexing Engine. The Indexing Engine performs the functionality of storing all logs and events and furthermore makes the events searchable.

C11 COMPONENT Machine Learning Orchestrator. This is the component that can be activated in an "off-line" mode for training specific models towards the initiation of sophisticated offensive or defensive activities.

COMPONENT C12 Defensive toolbox. This is the component that aggregates the virtualized defensive mechanisms (i.e. ML IDS classifiers) that can be deployed by a Blue Team member.

COMPONENT C13 Simulation scenario editor. This is the component that manages the creation of virtual scenarios that can be deterministically transformed to executable gamification application.

COMPONENT C14 Simulation scenario repository. This is the component that persists the aforementioned virtual scenarios that are created by the Simulation Scenario Editor.

COMPONENT C15 Simulation Instantiation manager. This is the component responsible for triggering the creation of Gamification application based on a virtual scenario that is defined.

COMPONENT C16 Risk calculation engine. This is the component that calculates risks based on given assets, relationships among them, vulnerabilities controls, ongoing threats and attacks and any other type of anomaly detected.

COMPONENT C17 User profiles repository. This is the component that persists the (anonymized) users along with their competency level along with their historical performance data.

COMPONENT C18 Operational Dashboard for Emulated Scenarios. This is the component that visualizes the progress of running emulated scenarios.

COMPONENT C19 Operational Dashboard for Simulated Scenarios. This is the component being responsible for providing visualization of the progress of a running simulated scenario.

COMPONENT C20 Security Assurance Platform. This is the component being responsible for monitoring and evaluating the security level of SPIDER platform. It listens for events created by the SPIDER platform components and evaluates based on those events and predefined rules the security and privacy level of the platform

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

4 USE CASE DESCRIPTION

The use case analysis leads to the definition of three pilot use case scenarios(PUCs):

#	Pilot Use Case	Description
1	PUC1.a	Cybersecurity Testing Of 5G-Ready Applications And Network Services
2	PUC1.b	Cybersecurity Of Next Generation Mobile Core SBA
3	PUC2.a	5G Security Training For Experts
4	PUC2.b	5G Security Training For Non-Experts
5	PUC3	Cybersecurity Investment Decision Support

PUC1: Cybersecurity Testing

4.1.1 PUC1.a: 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 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, with emphasis on the emulation of network-wide attacks, from rudimentary to highly complex ones.

The SPIDER Cyber Range platform will leverage fully emulated 4/5G network environments to support PUC1.a (and PUC2.a) scenarios, guaranteeing highly reliable evaluations (and exercises) without the risks of adverse impacts on actual networks or proprietary data loss. In more detail, an emulation scenario is a 4/5G network environment that consists a combination of assets – such as User Equipment (UE) or UE emulators, vertical application components, physical/virtual network functions (P/VNFs), Virtual Infrastructure Managers (VIMs), VIM tenant spaces, and Wide-area SDN Controllers (WSCs), generating an attack surface that spans from the access to the core part of the infrastructure.

PUC1.a is built on the outcomes of the H2020 5G-PPP MATILDA project (www.matilda-5g.eu), which has designed and developed an integrated orchestration framework for both vertical applications and network services over 5G network sliced infrastructures. The SPIDER emulation scenario components (both at application and network level) are deployed on the MATILDA infrastructure under the control of two interworking orchestration engines: (i) the Vertical Application Orchestrator (VAO), which is in-charge with the network slice negotiation, as well as the deployment and decommissioning of the (geo-distributed) application components; (ii) the Operations Support System (OSS), which is in-charge with the slice network creation, including the coordination of all the other building blocks in the network layer control platform – namely, the multi-site NFV Orchestrator (NFVO), Virtual Infrastructure Managers (VIMs), Wide-area Infrastructure Manager (WIM) – to set up and to properly

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

configure base 4/5G network services (NSs), edge computing resources, and wide-area connectivity. Furthermore, SPIDER embeds tracing capabilities into the MATILDA framework to monitor the status of assets involved in the executed test scenarios.

4.1.2 PUC1.b: Cybersecurity of Next Generation Mobile Core SBA

3GPP is defining the Next Generation Core (NGC) in 5G mobile networks. This 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. This new architecture defines SBI as Web based REST API interfaces both for the internal and external NGC-CP. In addition, HTTP2 has been selected as the transport protocol for SBA, and therefore TLS (Transport Layer Security) encryption will be used by default. Current cybersecurity network tools will be stressed in this environment. An extended threat surface is expected in 5G because of this design, from lack of visibility (encrypted traffic) to new attacks applying existing tools (currently exploiting web service and application environments). PUC1.b aims at testing and evaluating this new paradigm in SBA from the current security procedures based on fixed reference points connecting them in a rigid, predefined schema, to a very dynamic environment of REST API interfaces and different type of encrypted traffic over TLS.

Over the variety of potential scenarios that affects encrypted traffic over TLS, SPIDER PUC1.b has selected some that can be considered as representative ones, to demonstrate how cybersecurity experts need to be prepared for new attack vectors in 5G infrastructure.

Representative scenarios:

Cryptominer discover. 5G Core and specifically microservices and SBA architecture promotes the use of public or hybrid cloud solutions. This new approach deteriorates perimeter control of critical assets. Specifically, a malicious agent, insider or cloud provider employee, could introduce malware, such as cryptomining, in some of the microservices. Both legal and cryptomining traffic will use TLS traffic, which complicates the identification of the malware. SPIDER will deploy a scenario where BLUE TEAM will learn how to operate a ML based detection tools over encrypted traffic.

Attack a DNS infrastructure. In the 5G SBA architecture one of critical components is the DNS server. It can be based on classic protocol (UDP/53), but new deployments will adopt DNS over HTTPS (RFC8484) that increase the resource consumptions cause by cryptographic calculations needed. The motivation of this scenario is to allow that a student learn to detect DNS attacks, such as DNS request floods or DNS tunneling in the new DoH protocol. In this scenario, the Blue Team will learn how to use both security tools and ML based detectors to detect and identify the attacks.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

Vulnerability scans. The use of 3GPP standardized REST API as SBI, will expose interfaces that will be easily scannable looking for new attack vectors. Typically, BLUE team members, such as, Security Operative Center (SOC) employees need to learn to monitor these attempts despite being encrypted.

The ML Toolboxes of each scenario are going to have some pre-trained models. There are different pre-trained models because some of them are going to be faster, more precise or will provide explainable results. Also, it is going to be possible to re-train these models.

It is worth noting that the generation of attacker traffic will be also addressed in this use case researching and applying a complementary and innovative technique based on the recently appeared Generative Adversarial Networks (GANs). GANs emerged in 2014 as a type of deep neural network architecture utilised to solve unsupervised learning problems in the Computer Vision area. Basically, a GAN model is represented by two independent neural networks (the Generative and the Discriminative) that compete among them in a game. The Generative tries to create synthetic data that fools the discriminative network and causes an incorrect identification of synthetic data as real data. Conversely, the discriminative network tries to learn from the real and synthetic data and classify the former as correct and the latter as incorrect or fake. The result of this game in case we achieve to reach a convergence path is a Generative network able to generate synthetic data that mimics real data. Finding a convergence path in this game is not a simple task as in many occasions the training process falls in a divergence point and so, the obtained Generative network is far from replicating the real data. Nowadays, many research efforts are being applied to find solutions to this problem but it is still open.

Although GAN models have been broadly studied and applied into several fields to solve many problems not only over images but also over different types of data, currently not so many research works have studied GANs with their application in the field of network traffic replication and in particular in the generation of synthetic network traffic attacks. In this context, SPIDER will develop GAN models able to generate synthetic network traffic reproducing the distribution of real network traffic data than can be applied to train ML models for early identification and detection of threats and network attacks without using real data for training processes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

4.2 PUC2: 5G SECURITY TRAINING

4.2.1 PUC2.a: 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 field. PUC2.a scenarios will be used to assess the cyber range's training capabilities for equipping cybersecurity professionals (both individuals and teams) with 5G security skills essential for protecting the extremely high-performance, multi-tenant and virtualized telecommunications infrastructure from both old and new threats. PUC2.a training exercises include team-based exercises (i.e., attack, defend and force-on-force scenarios), and self-paced exercises (i.e., attack and defend scenarios). Moreover, Blue (defence) and Red (attack) team exercises will be implemented and tested as there are educational gaps in the existing platforms in this area (i.e., Red vs Blue teams).

As previously anticipated in Section 4.1.1, fully emulated 4/5G network environments will be exploited to implement the training scenarios. Each asset involved can contain some vulnerabilities (either inherent system properties tagged according to the Common Vulnerability Enumeration (CVE**)** system, or "deliberate misconfigurations") that can be exploited for an attack, or for privilege escalation and pivoting in an attack path. Moreover, each emulation scenario can be associated with several learning objectives (i.e., attack/defence actions) for the cybersecurity experts' training, such that relevant infrastructure assets and users' (Red/Blue teams) actions will be monitored for tracking the training progress and performance. Monitored assets include both application- and network-level scenario components (e.g., vertical application components, P/VNFs, UEs), as well as a subset of the control platform, such as the VIM and WIM blocks.

A variety of attack scenarios that cover the training requirements for the experts and non-experts users of SPIDER platform have been defined in the deliverable D2.8 "SPIDER use cases and pilots definition – final version". An example of the experts' scenarios is provided in the following paragraph.

Related example:

Attacking the 5G VIM layer: This scenario enables the trainees to develop a deeper understanding of the security vulnerabilities, existing in an open platform, namely OpenStack, that is prominently used by many Telecom providers for prototype deployment and testing of the 5G network virtualization and implementing their NVF and Cloud applications. Moreover, through this scenario the defence techniques for defending the VIM layer can be further studied. Through this process the trainees

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

develop the required skills and techniques to mitigate the attacks and reduce their impact on the virtualised infrastructure. An average level of knowledge of OpenStack platform is required. As many virtual infrastructures are supported in parallel, from a single open stack instance, it is essential that they remain completely separated and not affecting one the other. In this scenario we are getting acquainted with a newly discovered bug CVE that could lead to a DoS attack to all the infrastructures instances running on the same OpenStack instance, resulting to complete availability loss. DoS attacks are difficult to defend against as well as to detect in their early stages. In SPIDER we envision the education of the end-users of the platform, to these types of availability attacks as well as to some mitigation strategies.

4.2.2 PUC2b: 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 fully protect organisations against cyber threats. The users also play a very important role, not only because they are routinely targeted by social engineering attacks, but also because proper cyber hygiene and responsible behaviour in cyber space can help detect and prevent threats. Here, the focus is not on the experts, but on the regular employees of 5G-oriented companies that need to improve their awareness about security threat and solutions and will be trained on cutting edge technologies and the evolving 5G cybersecurity landscape. The goal is to validate that SPIDER 5G security gamification approach results in real change and provide input to the exploitation of the solution after the project end. Thus, within the scope of this use case the cybersecurity non-experts that will be trained on cutting edge technologies and the evolving 5G cybersecurity landscape. A related example on this use case is being described below :

Exploit VPN from coffee shop:

This example refers on training non expert users towards the evaluation of protocol level weaknesses and put them in place to safeguard their sensitive data.

It is very often for IT personnel to use their corporate laptops outside the corporate premises (e.g. home). Most of the times this connection relies on strong cryptographic protocols that guarantee that possible overhearing adversaries will not be able to decipher the communication.
In this scenario our persona is an IT administrator that every day is visiting a coffee shop prior to checking in to the office. Unfortunately, a server-error that happened in the infrastructure urged a colleague of the IT admin to phone-call him requesting his immediate assistance. Instantly, he connects to the coffee shop WIFI and creates a VPN Tunnel using a PPTP connection.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

A hacker nearby is using an extremely low-cost equipment to overhear all traffic of WIFI connected users. His motivation is to collect valuable information from the TCP streams and blackmail victims later on. The IT admin is connected to the management LAN and from this point he is able to connect to the hypervisor that has the problem. To do so, he is using a plain HTTP interface to login to the hypervisor manager since he considers that he is safeguarded.

The hacker dumps the traffic of all connected users. Through introspection he identifies that a weak PPTP session has been captured. He is able to extract an MS-CHAP key [10] and from this key after two days of brute forcing to recover the encryption key. Having the encryption key, the hacker re-evaluates the saved dump and is able to recreate the HTTP calls to the hypervisor manager including the login process. Having done this, he has in his position the management keys for the virtualization platform. Instead of trying to use them he decides to sell the keys in the black market exposed in dark web.

4.3 PUC3: CYBERSECURITY 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. In achieving this goal, SPIDER develops a decision support process via a software tool (entitled Cybersecurity Investment Component - CIC) that is integrated within the SPIDER Cyber Range as a Service (CRaaS) platform and does exactly that; given a certain 5G deployment, it identifies a best-fit suitable defensive strategy (i.e. a best-fit selection of mitigation controls that should be applied at the asset level so as to mitigate cyber-threats or vulnerabilities) subject to resource (e.g. financial budget) constraints. In doing so, CIC can support the relevant stakeholders to not only determine optimal investments to cybersecurity controls, but also to take the necessary steps to implement these controls towards minimizing the cyber-risks of a 5G infrastructure provider in a cost-effective way. The CIC component uses meaningful inputs to optimise the selection of the various actions related to the underlined cyber security resource allocation problem including the list of relevant assets existing in the 5G infrastructure, their relation and economic value, the identified vulnerabilities of the 5G infrastructure, the cyber risk exposure of the 5G infrastructure measured in economic terms, a set of controls that can be used to mitigate the vulnerabilities as well as budget constraints, rules, and additional preferences of the end user.

That's only a summary on SPIDER's efficacy in supporting cybersecurity investment decisions that will be validated by demonstrating how the SPIDER's optimal investment strategy outperforms traditional investment and capital budgeting techniques. This will be done by gauging the extent to which cyber-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

risk is hedged, when allowing for managerial discretion and combining real-time data on various cyber-risk metrics obtained from Continuous Risk Analysis Engine (CRAE) with economic uncertainty.

5 CONCLUSIONS

This White Paper is part of a dissemination action set forth by the SPIDER project with the objective of providing an insight on the WP2 outputs and more precisely on the SPIDER reference architecture and the pilot use cases that were described in D2.3, D2.4, D2.5 and D2.8. Further dissemination activities will be scheduled in order to promote the projects outputs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability

REFERENCES

[1] Yamin, Muhammad & Katt, Basel & Gkioulos, Vasileios. (2019). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security. 88. 101636. 10.1016/j.cose.2019.101636.

[2] Paananen, Hanna; Lapke, Michael; Siponen, Mikko (2020). State of the Art in Information Security Policy Development. Computers and Security, 88, 101608. DOI: 10.1016/j.cose.2019.101608

[3] EU coordinated risk assessment of the cybersecurity of 5G networks 9 October 2019 NIIS COOPERATION GROUP

[4] 13 Reviews of the practices of one of the major network equipment suppliers as regards 4G equipment and services have been for instance carried out by the UK Huawei Cybersecurity Evaluation Centre (HSCEC).

[5] Cybersecurity in the age of 5G technology: the EU's response https://www.iiea.com/digital/cybersecurity-in-the-age-of-5g-technology-the-eus-response/

[6] Cybercrime Damages $6 Trillion By 2021 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

[7] 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk , A Frost & Sullivan Executive Briefing https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

[8] How Covid-19 is Dramatically Changing Cybersecurity https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity

[9] CyRIS : A Cyber Range Instantiation System for facilitating Security Training ,2016 , Pham Cuong, Tang Dat, Chinen Ken-ichi, Beuran Razvan https://dl.acm.org/doi/pdf/10.1145/3011077.3011087?download=true

[10] Breaking Micros, https://www.schneier.com/blog/archives/2012/08/breaking_micros.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685. The information, documentation and figures available in this information sheet are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability