A Digital Twin Network for Security Training in 5G Industrial Environments

Stanislav Vakaruk, Alberto Mozo
Universidad Politécnica de Madrid
Madrid, Spain

Antonio Pastor, Diego R. López
Telefónica I+D
Madrid, Spain

November 15, 2021

Abstract

The evolution of next-generation mobile networks (5G, 6G ...) is highly related to the latest virtualisation technology, which exposes it to new cyber-attack vectors. Therefore, there is an increasing need to train cybersecurity experts in the use of appropriate tools to prevent network attacks, especially those applied in mission-critical industrial environments. To meet this need, there are systems called cyber ranges that can be seen as an exemplification of a digital network twin. SPIDER is a cyber range specially oriented to train experts in next-generation network cybersecurity. In this paper we present how SPIDER is augmenting cyber range environments with ML tools, how it works and the way in which it can be used to train new experts.

Keywords: DTN, mobile network, machine learning, range, security, 5G

1 Introduction

There is a demand for using Machine Learning (ML) in network automation for next-generation network management, aligned with the latest developments in the field of virtualisation and the adoption of cloud-based architectures for implementing the current 5G networks and its successors. One promising solution is the use of ML-based analysis techniques to address the emergence of new points of vulnerability and exposure to new attack vectors. 3GPP introduced in Release 15 (R15), the Network Data Analytics Function (NWDAF) to deliver data analytics, opening the path towards ML automation. Consequently, Security Monitoring Analytics systems [1] emerged using ML techniques to detect network attacks (e.g. [2] and [3]). Moreover, malicious agents are moving forward in the same directions to use ML for their activities or to deceive ML inference engines [4]. As a consequence, there exists an increasing demand for security operation expert personnel.

Digital twin [5] is a well-known concept in the industry sector. It is used as a virtual representation of a physical entity, modelling its components and properties. Also, it serves to model the entity interactions with the environment and define a better industrial process or detect problems before actual implementation. Recently, with the increasing complexity of networks, it has been proposed to apply the same concept of a virtual representation of the network. In recent years, networks operators face architectures with a high level of complexity and interactions due to the emergence of new technologies such as NFV, SDN and zero-touch automation. Therefore, the legacy approach to diagnose and improve network operational status based on static architectures (list of nodes and links) is no more valid. The concept of Digital Twin Network (DTN) proposes a solution to model the complexity of current and future real networks. Despite being a representation, DTN relies on a specific physical infrastructure that can extrapolate correctly real environments. To this end, it requires an orchestration and management component to emulate different scenarios and a solution to collect and manage the data that those representations offer.

Cyber ranges are well defined controlled virtual environments used in cybersecurity training as an efficient way for trainees (e.g. cyber-security personnel) to gain practical knowledge through hands on activities ([6] and [7]). These cyber training arenas can be enhanced with ML-based tools to address more efficiently the emerging threats in 5G networks, especially in those areas related to mission-critical environments. The H2020 SPIDER project ([8]) proposes a cyber range solution that is specifically designed to train cybersecurity experts in telecommunications environments and it covers all the cybersecurity situations in a 5G network environment. The SPIDER platform is not only aimed at training ethical hackers and experts but also at improving their skills. A typical training process in the SPIDER cyber range involves one or two teams, one (the blue team) detecting and defending the infrastructure against attacks, and optionally another (the red team) actively searching for vulnerabilities and performing attacks. The red team may be substituted by predefined scenarios mimicking successions of realistic attack events.

In this paper, we propose to combine the demand for a playground for cybersecurity training and ML applicability under the umbrella of the DTN concept. We are going to introduce how machine learning tools can be integrated into the SPIDER cyber range, how this module works and the way in which it can be used for enhancing training processes by applying DTN principles to build the SPIDER ML-enabled cyber range.

2 System Integration

The SPIDER cyber range platform is a networking environment capable of injecting realistic traffic into a 5G network infrastructure, including attack activity within it. This realistic traffic is generated by Mouseworld environment, a highly-virtualized synthetic traffic generation environment. The Smart Traffic Analyzer (STA) component within the Mouseworld is used to train ML modules that can be utilised later as components of the SPIDER platform for detecting attacks in the injected traffic.

One key novelty included by the SPIDER framework is the intelligent generation of attacks. In this way, the SPIDER platform can generate complex variations of different sets of attacks. This feature circumvents the current limitations of commercial products that using a fixed set of previously stored attacks only generate slight variations of these attacks mainly based on adding noise combinations to mean values. To generate synthetic attacks and normal traffic, SPIDER applies an innovative tech-

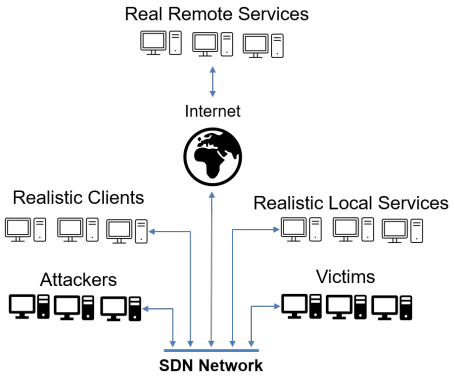

Figure 1: Mouseworld traffic generation environment

nique called Generative Adversarial Networks (GANs). As introduced by Goodfellow in [9], a GAN network is a generative model in which two neural networks compete to improve their performance. In general, standard applications of GANs generate images represented by their pixel map, and the objective of the GAN is to generate new images as similar as possible to the real ones in the dataset. The GAN models of SPIDER are used to obtain synthetic network traffic data (attacks and well-behaved connections) that reproduce the statistical distribution of real traffic. Having trained a GAN model to replicate a given type of attack, the SPIDER platform can generate as many attacks of such type as required. These attacks can be used by red and blue teams for repeating the same type of exercise with different data. Therefore, the analysed attacks and normal traffic are not going to be exactly the same in each run of the exercise. In addition, even if real data are subject to privacy or anonymity restrictions, as the network data used in the exercises by the blue and red teams are the synthetic ones generated by the GANs, no breach of privacy appears during the realization of such exercises.

In the following subsections we detail the Mouseworld traffic generator, the Smart Traffic Analyzer component and the SPIDER architecture (related to the attack detection emulation scenarios).

2.1 Mouseworld Traffic Generator

The SPIDER cyber range platform is able to inject realistic traffic, as generated by the Mouseworld environment, originally developed at the laboratories of Telefonica I+D [10]. This traffic generation system allows deploying complex network scenarios ([11]), running servers and clients that emulate realistic interaction patterns with both internal and external services (e.g. web, video, cloud, cyber-attacks, ...).

Figure 1 depicts the Mouseworld environment with a set of clients and servers in a network topology provided by a SDN-powered network fabric. The components of the Mouseworld environment are as follows:

- **Realistic Local Services**: servers with web, cloud or streaming video services deployed in the SDN based network.

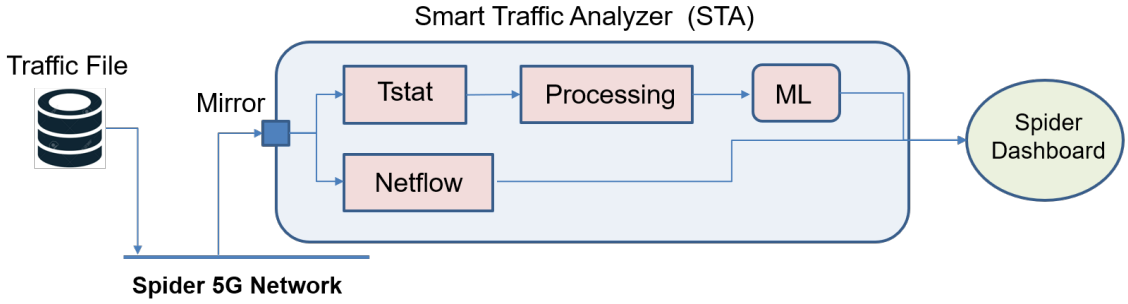

Figure 2: Smart Traffic Analyzer (STA) internal components

- **Real Remote Services**: remote, real and well known services (video streaming, news , cloud , shops, ...).
- **Realistic Clients**: clients which emulate real users accessing to local and remote web based services.
- **Attackers**: clients that can execute a specific attack scenario against the environment or against the victim components.
- **Victims**: servers or clients that are able to emulate victims under a controlled scenario.

The environment is manageable and elastic, providing tools to deploy a set of components on a specific emulation scenario. The network traffic generated is mirrored to a probe and saved as a binary PCAP file. Then, the collected traffic can be labelled, which subsequently allows machine learning models to be trained in the environment and their performance to be verified in realistic scenarios. Various network traffic files and ML trained models obtained in the Mouseworld environment are integrated in the SPIDER platform and can deployed in a SPIDER emulation scenario. It is worth noting that there are more network traffic files than those used for training ML models in order to test them with other ML models running in different scenarios.

2.2 Smart Traffic Analyzer

The Smart traffic analyser (STA) is the component that allows to run ML models (e.g., traffic classifiers) in the SPIDER 5G Network Digital Twin environment. This component is deployed as a VNF (Virtual Network Function) that monitors the network traffic and identifies attack connections. The traffic within the SPIDER 5G network is received by the component as a copy through a mirror interface. Different STA VNFs can be connected in parallel, by mirroring the same traffic to each of the STAs. The STA component is represented in the Figure 2 and is composed of two main modules, the Netflow and the ML modules. The first one uses a standard flow aggregation method based on Netflow v9 protocol and implemented with softflowd. The second module uses the Tstat tool [12] to extract statistical network information from the network packets. Then, this information is processed with a Python script in order to be input to a machine learning model which will output results to the SPIDER dashboard.

The Tstat module extracts network statistics summarising the state of each connection and dump these statistics into an intermediate feature file. Afterwards, the Python script reads the feature file and splits the features that identify the connection (i.e., trasnport protocol, IP source and destination addresses and source and destination ports) from the features that ML models use as input to identify the attack traffic. The features to be used by the ML model are scaled or normalized using their mean and standard deviation. As a paradigmatic example, more details on the features used for detecting a specific cryptomining network attack can be found in [2]. Then, the machine learning model is provided with the input features and it classifies the input traffic in malicious and benign. As the models we have deployed in this module are in general supervised classifiers, the confidence level of predictions can be also obtained. This value is measured as a percentage and usually a classifier identifies a connection as malicious if the confidence is higher than 50%. Note that the minimum confidence level for accepting a connection as an attacker can be modified to provide different levels of sensitivity to the detector. Finally, the classified connections are reported out of the STA component with their identifiers and confidence levels, to a dashboard integrated in the SPIDER cyber range. The dashboard facilitates the inspection and analysis of the results by a human user.

2.3 SPIDER Architecture

The SPIDER high-level reference architecture incorporates the STA component and indirectly the Mouseworld traffic generator. Figure 3 shows an excerpt of the SPIDER architecture which is related to the STA components scenarios.

The components of the SPIDER architecture are:

- **Emulation Scenario Editor**: This component helps to create emulation scenario descriptors. In those descriptors, the virtualized components that will be deployed and the synthetic traffic configurations that will be generated in the course of a scenario are defined.
- **Virtualized Component Repository**: This component stores complex artifacts such as virtual machines and provides two ways of generating synthetic traffic. The first one is based on the injection of Mouseworld generated traffic and the second one uses GANs for generating fresh synthetic traffic (attacks and well-behaved connections).
- **Emulation Scenario Repository**: This component stores different emulation scenario descriptors.
- **Emulation Instantiation Manager**: This component activates trace extractors and deploys the virtualized components that were specified in an emulation scenario descriptor. The trace extractors register the information generated by the virtualized components in the course of the emulation.
- **Machine Learning Orchestrator**: This component spawns specific virtualized STA components and triggers the generation of the synthetic traffic.
- **Defensive Toolbox**: This component contains the specific ML model that receives the generated traffic and classifies it into malicious and benign traffic.

The actors of the SPIDER architecture are as follows:

- **Training Scenario Creator**: Creates a specific emulation scenario descriptor using the Emulation Scenario Editor component.

- **Training Scenario Supervisor**: Starts an emulation using the Emulation Instantiation Manager component by selecting a specific emulation scenario descriptor from the Emulation Scenario Repository component.
- **Blue Team**: The team of trainees that analyses the results of the Defensive Toolbox for a specific emulation scenario.

All the components and actors have to interact over the course of an emulation scenario. Initially, the Training Scenario Creator actor defines a scenario using the Emulation Scenario Editor component with a specific network traffic generation configuration of the Virtualized Component Repository component and a pre-trained ML model of the Defensive Toolbox component. That scenario is saved as an emulation scenario descriptor in the Emulation Scenario Repository component. Then the Training Scenario Supervisor actor selects a emulation scenario from the Emulation Scenario Repository through the Emulation Instantiation Manager component, and triggers the scenario through the Machine Learning Orchestrator component. This last component triggers the Virtualized Component Repository component to generate a network traffic specified by the scenario descriptor and instantiates the STA component with the ML model in the Defensive Toolbox component. Finally, the trainees from the Blue Team analyse the results of the Defensive Toolbox in the SPIDER Dashboard and can repeat the scenario with changes in the Defensive Toolbox component.

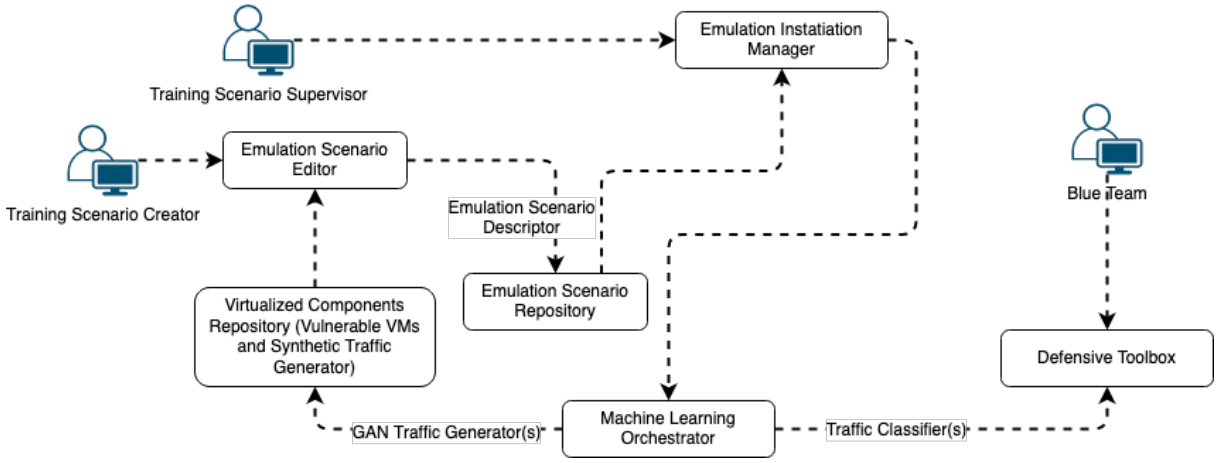

Figure 3: Extract from the SPIDER high-level reference architecture.

As it was previously explained, the STA is directly integrated in the SPIDER architecture as a Defensive Toolbox component and the Mouseworld Traffic Generator is indirectly integrated by measn of a set of pre-generated capture files that can be injected through the Virtualized Component Repository component.

3 Trainee Training Process

The training process in the SPIDER cyber range with ML tools consists of getting the trainee used to working with such tools, tuning the models and interpreting the model results in mobile network environments such as 5G. The trainee can (a) select a generated traffic with different density (more attack traffic or a specific service traffic),

(b) choose the right ML model (e.g. a faster or more accurate one) or (c) modify the ML model settings (e.g. the minimum confidence level for accepting a connection as an attacker). Then, the trainee will always be able to review and compare the results of various ML models on the SPIDER dashboard. Specifically, in a SPIDER scenario the trainee is part of the blue team and has to test various confidence values for each ML model.

4 Conclusions and Future Work

This paper has shown a practical application of a DTN, onto an enhanced cyber range platform, taking advantage of automated newtork orchestration and machine learning techniques. We have shown how the ML-oriented STA module is integrated into the SPIDER cyber range platform, how realistic network traffic is generated, how the modules generated by the STA detects attacker connections and the way in which it communicates the results to the SPIDER dashboard. Finally, it is also explained how trainees can improve their skills with this module on the SPIDER cyber range platform.

Future work in the SPIDER cyber range and the Mouseworld emulation environments will address aspects related with more complex network scenarios, incorporating more realistic representations of access and core networks, the use of multidomain scenarios and the coordination among independent AI-based modules to improve responsiveness and accuracy of the DTN.

Acknowledgments

This work was partially supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 833685 (SPIDER).

References

[1] "Threat landscape for 5g networks report," https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks, accessed: 2021-04-30.

[2] A. Pastor, A. Mozo, S. Vakaruk, D. Canavese, D. R. López, L. Regano, S. Gómez-Canaval, and A. Lioy, "Detection of encrypted cryptomining malware connections with machine and deep learning," *IEEE Access*, vol. 8, pp. 158 036–158 055, 2020.

[3] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del Rincon, and D. Siracusa, "Lucid: A practical, lightweight deep learning solution for ddos attack detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876–889, 2020.

[4] "Malicious uses and abuses of artificial intelligence," https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence, accessed: 2011-04-30.

[5] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2405–2415, 2019.

[6] S. W. Neville and K. F. Li, "The rational for developing larger-scale 1000+ machine emulation-based research test beds," in *2009 International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2009, pp. 1092–1099.

[7] B. Ferguson, A. Tall, and D. Olsen, "National cyber range overview," in *2014 IEEE Military Communications Conference*. IEEE, 2014, pp. 123–128.

[8] C. Xenakis, A. Angelogianni, E. Veroni, E. Karapistoli, M. Ghering, N. Gerosavva, V. Machamint, P. Polvanesi, A. Brignone, J. N. Mendoza, and A. Pastor, "The SPIDER concept: A Cyber Range as a Service platform," Sep. 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4030473

[9] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems 27*.

[10] A. Pastor, A. Mozo, D. R. López, J. Folgueira, and A. Kapodistria, "The Mouseworld: a security traffic analysis lab based on NFV/SDN," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ser. ARES. ACM, 2018, pp. 57:1–57:6.

[11] A. Mozo, J. L. López-Presa, and A. F. Anta, "A distributed and quiescent max-min fair algorithm for network congestion control," *Expert Systems with Applications*, vol. 91, pp. 492–512, 2018.

[12] A. Finamore, M. Mellia, M. Meo, M. Munafo, P. Di Torino, and D. Rossi, "Experiences of Internet traffic monitoring with tstat," *IEEE Network*, vol. 25, no. 3, pp. 8–14, 2011.