Paideusis: a remote hybrid cyber range for hardware, network, and iot security training

PAIDEUSIS: A Remote Hybrid Cyber Range for Hardware, Network, and IoT Security Training*

Giulio Berra[1], Gaspare Ferraro[1], Matteo Fornero[1], Nicolò Maunero[1,2], Paolo Prinetto[1,2], and Gianluca Roascio[1,2]

[1] Cybersecurity National Laboratory, Consorzio Interuniversitario Nazionale per l'Informatica
[2] Dipartimento di Automatica e Informatica, Politecnico di Torino, Turin, Italy
giulio@gmx.com
ferraro@gaspa.re
matteo.fornero@consorzio-cini.it
{nicolo.maunero, paolo.prinetto, gianluca.roascio}@polito.it

Abstract

Today, simulation environments known as cyber ranges are attracting considerable attention across the cybersecurity ecosystem, for their ability to emulate realistic situations and offer pragmatic training to security professionals and students. The extraordinary capabilities of virtualization systems provide great impetus to the development of such platforms, which can scale and be easily maintained. However, many security threats related to the hardware domain of devices are difficult to reproduce in such environments, while instead they are assuming a strategic importance, in a world permeated by electronic devices, which control the objects of our daily life and which handle a large flow of people's private data.

This paper presents PAIDEUSIS, a hybrid training environment that seeks to combine the advantages of virtualization and scalability with the realism of hardware devices physically present and connected to the cyber range, including a wide range of devices such as IoT, industrial control, and network hardware devices. Issues faced during the implementation and the management of the platform are presented, as well as the features of some hosted theatres and scenarios based on embedded and IoT devices, some of which already used in relevant Capture-the-Flag (CTF) competitions.

1 Introduction

In recent times, cyber incidents have shown a considerable increase. An ever-growing number of companies, in all sectors, have now transferred the management of their infrastructures and their products to the digital domain. This significantly increased the attack surface, including all the connected IT and OT devices, up to data centers. If data are everywhere, then *the attackers are everywhere* too.

Training is thus becoming more and more crucial, not just for cutting-edge security professional teams, but also for students, with the aim of reducing corporate or critical infrastructures and, on the other hand, by the availability of proper labs and well-equipped training environments for a large number of students. In both cases the problem is the same: how to train an increasing number of people on scenarios as real as possible?

The answer to this question led to the spread of the "cyber ranges" [34], i.e., platforms where it is possible to emulate realistic scenarios, replicating a plethora of cyber-attacks, to

enhance skills of operators and users in identifying cyber-breaches and in finding mitigation strategies to arrest them [31]. The most relevant military organizations, such as NATO [20] or the US Department of Defense [11], have been implementing training platforms to virtualize realistic scenarios and likely dangerous situations, and a wide variety of cyber ranges is now available also from many digital corporates at international level, such as [26] and [2].

But in the bulk of the market, perhaps something is still missing. Today the possibilities of virtualization are almost unlimited, and the spread of SDN (Software-Defined Network) [29] demonstrates the possibility to abstract a large part of the hardware from the physical domain to implement a network for corporate use. Even if attracted by these possibilities, the community should not underestimate that *not everything* can be reduced to software: many corporate networks still have routers, switches and physical firewalls in their IT and OT infrastructures, especially when they need to interface with ICS and SCADA. Plus, IoT networks that permeates our cities, our businesses, our houses, and our bodies are definitely not virtual. Virtualizing these realities for training reasons could be limiting, as it has been proven that attackers themselves use absolutely realistic testbeds to develop complex exploits [15].

This is why it is important to design cyber ranges capable of combining the virtual scenarios with am additional set of scenarios based on *real*, *physical* devices. *Hybrid cyber ranges* aim to solve the problem, combining the dynamism and flexibility of fully virtual cyber ranges, with the realism of Cyber-Physical Systems (CPS), IoT, and IIoT scenarios.

In addition to the introduced "realism", the exploitation of physical devices in training platforms also adds the possibility of enabling training and education on security aspects related to the hardware components of the system, and not only to the software they run. In fact, there is a wide range of threats related to the physicality of devices and enabled by vulnerabilities introduced in the their design and production phases [24], regardless of all the protections that can be adopted in the higher software layers.

In this paper, we present PAIDEUSIS, a cyber training camp implemented in Turin, that merges virtualized components and physical devices, including a wide range of IoT devices, industrial control devices, and network devices. The word $\pi\alpha\iota\delta\epsilon\upsilon\sigma\iota\varsigma$ (read /paideusis/) was used in the Ancient Greece to indicate the education of young people to life and war, and by extension also the place where this education was provided. The transliteration of this word, PAIDEUSIS, was chosen to name our hybrid cyber range project. Through the combination of devices and services, the purpose of PAIDEUSIS is to offer multiple scenarios and testbeds, ranging from guided programming training of devices to actual training sessions in VAPT (Vulnerability Assessment & Penetration Testing), including gaming sessions in the CTF (Capture-the-Flag) domain [10], up to Cyber-Defense Excercises (CDX) for security specialists [19].

PAIDEUSIS is a cyber range:

- fully usable from remote, with the possibility of interacting with real devices from any position;
- with non-fixed but adaptable scenarios, according to needs;
- reconfigurable remotely, thanks to formal methods and languages for defining new scenarios.

Among the others, PAIDEUSIS offers scenarios for:

- training in the programming and exploitation of Hardware Security Modules and Platforms, such as the **SE***cube*™ device[1];

[1] https://www.secube.eu/

- training in the configurations issues and in vulnerabilities artificially introduced in communication devices, such as the Tiesse TGR Wi-Fi Routers[2];
- training on side-channel attacks over real processors, such as the the ChipWhisperer-Nano devices[3];
- training and competitions based on vulnerable hardware devices, both synthesized on FPGAs and emulated through customized EDA (Electronic Design Automation) environments, such as ModelSim[4];
- reproducing IoT networks and ICS's, with real sensors and SCADA devices.

The remainder of the paper is organized as follows. Section 2 provides background information on cyber ranges and analyzes the current state of the art; Section 3 details the PAIDEUSIS features and architecture, providing some examples on the the most significant scenarios; Section 4 finally concludes the paper.

2 Background

2.1 Cyber Range Taxonomy

According to NIST, "*cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment*" [1]. Yamin *et al.* [34] introduced and provided a comprehensive taxonomy for cyber ranges, classifying them by purpose, by composition and construction of the testbed and scenarios, and by used technologies, among the other metrics. Figure 1 gives a schematic view of the proposed classification scheme.

Among dimensions of the taxonomy, there are:

- **Scenario**: it defines the storytelling and the virtual setting for the test, the competition or the exercise that is performed, but also the steps to be performed and how the events described are interlaced, in order to help users in identifying the simulation. It is further charachterized by (a) a *Purpose* (e.g., an experimental session, a test of new components or of a defence mechanism, a competition, a training or a teaching session), (b) an *Environment* (*physical*, *virtual* or *hybrid*, see below), (c) a *Storyline*, i.e., how the activity should be carried out, (d) a *Type* (*static* or *dynamic* depending on the possibility of modifying its composition while played), (e) a *Domain* (e.g., industrial, IoT, etc.) and (f) the *Tools* used for design and development of the given scenario.
- **Teaming**: it defines the categorization of the groups of people, users or maintainers, who interact with the cyber range. User teams are of two types: *Red Teams*, in charge of finding and exploiting the vulnerabilities of a scenario, and *Blue Teams*, in charge instead of correcting the vulnerabilities and stemming the problems found within the scenario. Among maintainer teams, there are *White Teams*, which represents the team of experts in charge of setting up the scenarios and inserting the vulnerabilities, and *Green Teams*, responsible for the design and development of the infrastructure that hosts the scenarios.

[2] http://www.tiesse.com/
[3] https://www.newae.com/products/NAE-CW1101
[4] https://www.intel.it/content/www/it/it/software/programmable/quartus-prime/model-sim.html

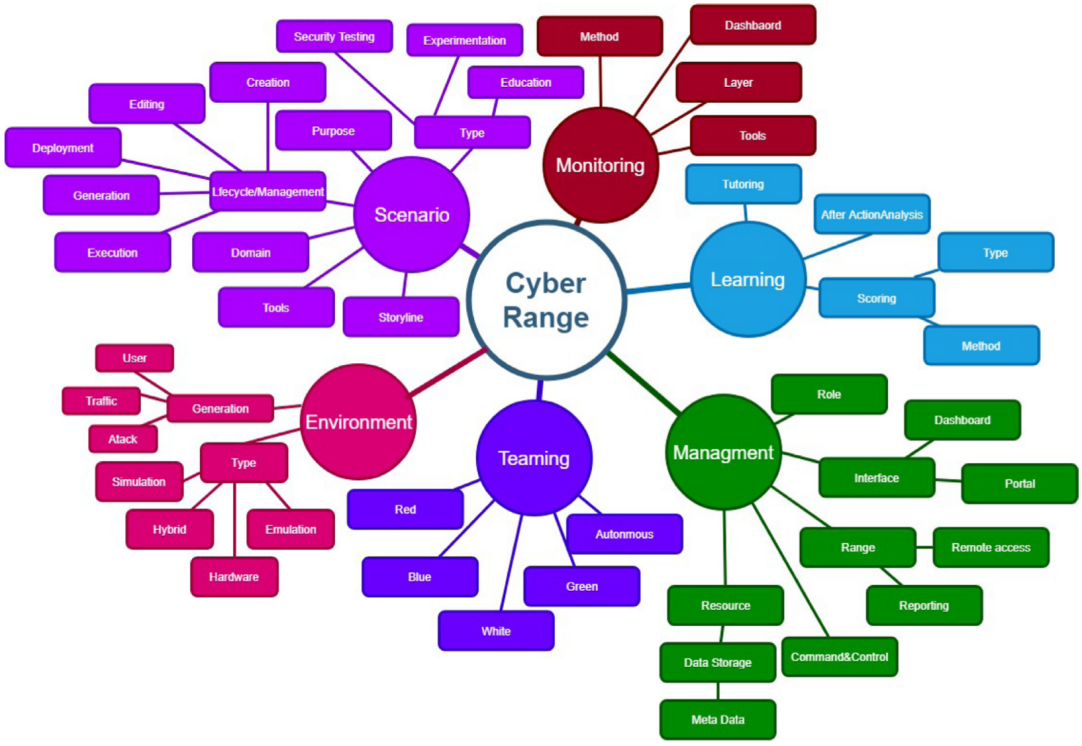

Figure 1: Cyber ranges taxonomy [34].

- **Monitoring**: it defines how user teams' activity is controlled by management teams, to ensure compliance with agreed rules and to assign scoring. It is characterized by employed *Methods* and *Tools*, as well as by the abstraction *Layer* at which the control is carried out.

- **Scoring**: it defines the methods for assigning the score, which can be by objectives (e.g., the discovery of a *flag* [10] within the scenario), or through the analysis of the logs produced by the activity of the participants.

- **Management**: it establishes the management methods of the cyber range, through the definition of *Roles* and *Resources*; it also establishes the methods with which the scenarios are offered through portals or dashboards (*Range Management*).

2.2 State of the Art

2.2.1 Physical cyber ranges

Physical cyber ranges aim to provide an exact replica of the target infrastructure in an isolated and secure environment. All the devices composing the scenario are the real, physical one, and no part of the reference infrastructure is emulated. This approach provides the maximum

loyalty with respect to a target infrastructure or target devices, but loses the ability to easily scale, provides little flexibility, and has a considerable impact in setup costs.

A notable example is the National SCADA Testbed (NSTB) [8], implemented by the US Department of Energy. The aim of the project is to study, on the one hand, how an electricity supply system would respond to cyber attacks and on the other hand, to provide a hyper-realistic testbed for vulnerability identification and mitigation techniques. The testbed is composed of a full-scale electrical power grid and several substations, all implemented using industry standard technologies, such as SCADA, and various network and industrial protocols (e.g., IP and MODBUS).

Another example is provided by Morris *et al.*, who developed a critical infrastructure testbed at the Mississippi State University [22]. 7 scenarios are proposed including, among the others, petrochemical, steel manufacturing and electrical power grid. The range consists of a control system that includes PLCs, sensors, actuators, interface and management software commonly found in the industrial world, and several physical processes modelling components of the target infrastructure, such as containers for water and oil and smart grid transmission. The system is used not only for security assessment and research activities, but also in teaching activities within the courses offered by the university itself.

2.2.2 Virtual cyber ranges

In virtual cyber ranges, all the scenario components are emulated through the adoption of virtualization solutions. This approach provides the maximum degree of flexibility and scalability, but sacrificing in realism. The category of virtual cyber ranges is certainly the richest in examples, due to the much higher ability to maintain a completely virtual component infrastructure compared to physical cyber ranges.

One of the most important work in this area is the advancement and aggregation of competence that the Horizon 2020 European project is promoting through the projects CONCORDIA[5], SPIDER[6] and CYBERWISER.eu[7].

Within the CONCORDIA project, several cyber ranges are being proposed, each of the with different purposes and domains. One of the most important is KYPO [9], developed by the Mosaryk University and recently released as an open-source platform. Provided under the *Platform-as-a-Service* paradigm [16], the KYPO cyber range is designed to be modular, flexible and with an high degree of scalability. It is built to be hosted on cloud infrastructure. Virtualization mechanisms allow to build complex network infrastructure with many interacting devices and different entities to represent the target infrastructure. The cyber range is completely accessible through a web interface with different functionalities base of the user role within the range, from scenario preparation to active execution.

The CODE Cyber Range is a completely virtual platform developed by the CODE research institute of the Munich University[8]. So far, it implements 3 different scenarios with 80 individuale exercises from different subject area used for experimentation but also for training in the master degree program of the university.

The RISE Cyber Range, developed by the RISE Sweden's national research institute, allows the possibility of emulating the customers' network or build complex scenarios thanks to virtualisation and emulation[9]. The focus of the project is to provide a cybersecurity training

[5] https://www.concordia-h2020.eu
[6] https://spider-h2020.eu
[7] https://www.cyberwiser.eu
[8] https://www.unibw.de/code/forschung/zentrallabore/cyber-range
[9] https://www.ri.se/en/cyberrange

platform testbed for the public and private sector, including SME's, which often lack the resources to carry on this type of activities. It is important to highlight the use of this cyber range as a test and validation facility for cybersecurity certification in Sweden.

The CYBERWISER.eu project focuses its work on the development of a platform for the training of cybersecurity professional. All the courses and material provided are composed on lecture material and hands-on practical experience on the remote cyber range platform. Particular attention is being put on defining precise guideline for scenario development, from specification to requirements and deployment, in order to allow a long term maintenance of the platform.

The SPIDER European project is focusing its attention on emerging telecommunication technologies and in particular on 5G networks [5]. They propose a Cyber Range as a Service (CRaaS) platform that offers dedicated training to professional as well as non-expert in the field. The platform leverage on traditional virtualisation technologies to emulate 5G functions. The focus of the proposed cyber range is not only to provide training support but also, by including econometric models, provide decision support for investments and metrics for understanding the economical impact of a possible succesful attack.

Another notable example is FITS, presented by Moraes *et al.* [21]. The testbed is thought as an infrastructure for network experimentations, leveraging on virtualisation softwares to recreate the network environment the users needs for testing their solutions. To support the infrastructure, several nodes are placed around the world, not only in Brazilian institutions, but also in European ones. In a later work, the FITS infrastructure has been enhanced with the RIO platform [4], an orchestration infrastructure to ease the experimental scenario deployment. In RIO, it is possible to define the characteristics of the experiment through a descriptive language gathered in a configuration file. During the creation of VMs and all the virtual components of the scenario, the configuration file is parsed to apply the described characteristics.

Recently, cyber ranges have started to be adopted in cybersecurity academic teaching. The Tele-lab platform [32], developed at the University of Potsdam, is a laboratory built around the use of virtual machines assigned to students for their exercises. Virtual machine content changes based on the learning objective it is dedicated for, and different machines are created from a pool of starting templates. In the abovementioned work, authors posed the attention on the dynamic deployment of exercise scenarios: it is possible to change a set of parameter for the the virtual machines (scripts for executing programs, network connections, and so on) to create easily new scenarios avoiding the reuse of old ones.

2.2.3 Hybrid cyber ranges

As the name suggests, hybrid cyber ranges to take the best of both physical and virtual approaches: adopting virtualisation techniques to improve the scalability and flexibility, while using real hardware devices as targets of the activity carried out, to provide a good degree of realism.

Among the notable works, Mallouhi *et al.* proposed a testbed to evaluate security solutions for SCADA systems [18]. They propose a hybrid testbed, composed of a real SCADA controller and several virtual components to emulate a Smart Grid infrastructure. Several macro blocks can be identified: (i) a control center providing control and the way to interact with the components of the simulated model, (ii) a power distribution grid, (iii) a network of simulated components such as PLU, RTU and various devices, and (iv) a simulation system, using commercial applications, of the electric grid, controlled by the SCADA system.

In [14], another example of a power grid hybrid testbed is proposed by Hong *et al.*. A real SCADA system has been adopted, while the power system and the various electronic devices

are, instead, simulated using software solutions and virtualization.

Furfaro *et al.* [12] propose a hybrid cyber range where real smart devices (such as surveillance cameras and Android smartphones) and emulated ones coexist and cooperate within a virtual environment used for studying security for IoT applications. The most interesting part of this work is the original software used to deploy the scenarios, SmallWorld [13]. In SmallWorld, the scenarios are not seen as monolithic blocks, but composed of several interconnected parts that facilitate reusability and scalability. Therefore, it is possible for developers to deploy virtualized components customised for the specific scenario, from operating system to the devices.

Another important aspect of this work is represented by the emulation of active entities' behaviour, such as malicious users or applications. The evolution of the scenario during its execution can be different each time, even with the same starting conditions, increasing considerably their reusability.

Tsai *et al.* presented Testbed@TWISC [30], a network emulation testbed developed in Taiwan for research purposes. A web-based interface is provided to users, who are able to create scenarios using the available hardware and virtual resources, as well as a series of toolkit for security analysis, such as exploit tools for the offence, or firewalls and access controllers for the defence. To build the scenario, users have a series of the hardware components at their disposal, such as switches, IoT devices and routers. To improve scalability and flexibility of the system, it is possible to simulate other components, network infrastructures and devices using virtualization solutions.

Within the CONCORDIA European project, there are two cyber ranges that fall in the hybrid cyber range category. One is the TELECOM Nancy Cyber Range, having at its core the DIATEAM HNS (Hybrid Network Simulation) cyber range server[10]. The platform is used in the TELECOM Nancy University to support teaching activities and experimentations. While it uses standard virtualisation for running scenarios, it is possible to attach other physical networking platform or devices for testing and experimentations.

The other one is the Airbus Cyber Range, developed by Airbus[11]. Also in this case, the core of the cyber range leverages on virtualisation technologies to build scenarios with the possibility of adding and integrating physical networks and OT components.

2.3 Cyber Range Orchestration: CRACK

A non-marginal role in the success of a cyber range is played by the possibility of reconfiguring its scenarios to continuously create new ones. This aspect becomes fundamental when the cyber range must be used for training or cybersecurity competitions, where the reuse of an old scenario would make the exercise and activity of the participating teams almost vain.

Considering the complexity of the scenarios usually proposed within a cyber range, creating a new scenario can take a considerable amount of time, especially if compared to the time of use of the latter. It is therefore necessary to use orchestration solutions that facilitate the definition and deployment of scenarios. The most promising project in this area is CRACK [28], a framework for the design and deployment of scenarios developed and maintained by the University of Genoa. At the foundation of this framework is CRACK SDL, a Scenario Definition Language, based on TOSCA, an infrastructure specification language developed by OASIS [23]; TOSCA is a notable example from the *Infrastructure-as-Code (IaC)* paradigm [6], that in the last years emerged as the main infrastructure design approach.

[10] https://www.diateam.net/what-is-a-cyber-range/#hybrid_cyber_ranges
[11] https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/

The fundamental element of CRACK SDL is the *node*, representing an element within the scenario that can be a network device, a virtual machine or a firewall, but not only: through a node, it is possible to represent users, software, networks, security policies, vulnerabilities and many other items. Therefore, the approach makes possible to break down a scenario into its fundamental elements, that can be combined with each other in a simple and intuitive way to easily build new scenarios.

In the work of Russo [27], various application examples and utilities of CRACK SDL offer are presented. In fact, it is possible to create a real pipeline starting from the definition of the components, the required features of the scenario and how these elements must be interconnected; the design is then automatically deployed on the cyber range infrastructure after passing through a verification phase, checking that the described features are consistent with the objective of the scenario.

3 Features

As already introduced, the main objective of PAIDEUSIS is to be a training platform for security aspects related to the hardware domain, which very often do not play central roles in the current ecosystem of cyber ranges. The greatest challenge is therefore to be able to adapt the known virtualization capabilities in order to enable scenarios to host physical devices as their main actors. This means that, on the one hand, virtualization techniques are exploited in order to (i) implement the interfaces with the hardware devices, (ii) properly export their services, (iii) provide the needed connections inside the scenario. On the other hand, wired or wireless links are used between these devices (actually present and visible in the scenario) and other supportive devices (e.g., network infrastructure) to allow them to participate in the scenarios.

Internally, PAIDEUSIS is organized as follows. The fundamental entity is the **component**, i.e., any hardware or software element, virtual or real, that makes up the cyber range. A **subnet** is a set of components directly interconnected via LAN (Wi-Fi, Ethernet) or PAN (USB, Bluetooth) interfaces (in case of real hardware devices), or via virtual interfaces when devices are virtualized. The **range** (or **theater**) is a set of one or more subnets aimed to host compatible and coherent scenarios. The subnet/range relation is in principle *many-to-many*: a range may need more subnets to be set up, and several ranges can use a same subnet of components (Figure 2).

The **scenario** is here defined as a particular setting of the range, and represents what already presented in Section 2. Finally, a **session** is the single instance of an interaction, scheduled over time, between a user team and a particular scenario, being user teams (Red or Blue) as defined in Section 2. Sessions are *stateless* over time: once the session is gone, every information about how users interacted with the scenario is lost.

The physical topology of PAIDEUSIS is depicted in Figure 3. From the outside, it is possible to access two main services, represented by two virtual servers: one for user teams (in yellow) and one for maintainer teams (in green). Downstream of these, there are infrastructure servers, to which the target physical devices are connected. Among others, Wi-Fi routers, SCADA controllers, microcontrollers, FPGAs, general-purpose IoT cards connected to sensors or actuator devices and also customized boards for physical attacks are present.

Depending on the scenarios, these servers are responsible for the virtualization of the terminals interfacing with the devices, or for the direct exposure of their services. Alternatively, the machines can be used to virtualize the devices themselves, to enable scenarios where only emulated hardware is present, or emulated hardware together with physical hardware.

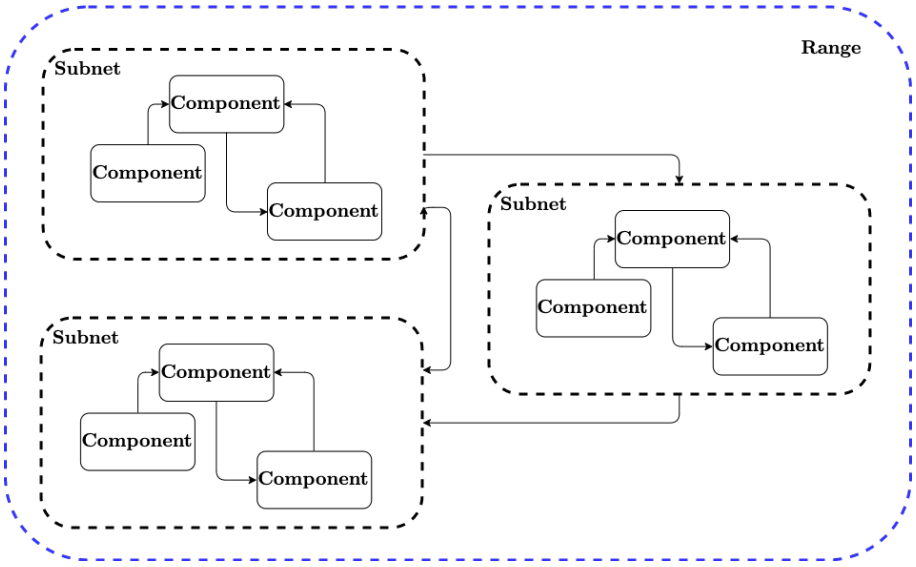

Figure 2: PAIDEUSIS internal organization.

The groupings of identical or similar devices are directly connected to a server customized for them, e.g., sized according to the specificities of the possible scenarios linked to these devices. The union of one of these "thematic" servers with its cluster of devices *may* constitute a range by itself, but may also not. A range can be set up by grouping any set of components within the cyber range, in any place, thanks to network virtualization techniques.

In such a promiscuity between virtual and real devices, the setting up of new theaters may require the Green Team to operate directly on the physical infrastructure. On the contrary, as for the setting up of the scenarios and the operations of the White Team, PAIDEUSIS is overcoming this limitation thanks to the use of TOSCA and CRACK SDL (see 2.3)

The tool used for creating virtual machines within the infrastructure is PROXMOX VE[12], which offers an intuitive graphical interface for management. For setting up the virtual networks, WireGuard[13], an open-source tool, is used. WireGuard uses strong cryptography and has better performance than other similar tools such as OpenVPN. Thanks to WireGuard, users connect to the scenario transparently with respect to the infrastructure, passing through the user services without even seeing them. In other words, WireGuard *configuration files* are distributed to users, that are projected into the scenario once applied the configuration in their terminals. Once connected, users start the session through authentication or other mechanisms provided by the scenario specifications. In addition to the convenience for the users, WireGuard has the advantage of abstracting the service from the infrastructure, also allowing an *isolation-by-design* that acts as a security tool for the platform itself: devices not to be included in the scenario are not included in the VPN configuration, and they are in no way reachable.

As for monitoring and scoring, PAIDEUSIS does not establish any *a-priori* criterion, and delegates the implementation of the methods for user activity monitoring and score assignment to the White Team in charge of setting up the scenario. These features can be conveyed through the maintainer services, which remain active during the sessions, and are obviously

[12] https://www.proxmox.com/en/
[13] https://www.wireguard.com/

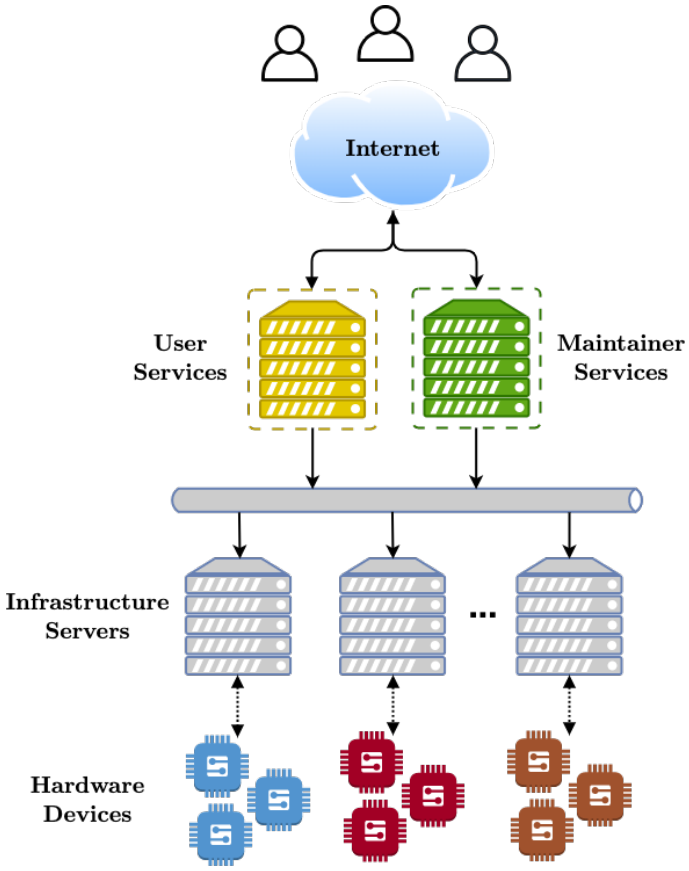

Figure 3: PAIDEUSIS topology.

connected to the infrastructure in which the scenario is being played. PAIDEUSIS has been used in conjunction with external CTF competition platforms, such as *CyberChallenge.IT*[14], which separately offered its flag submission service, with these hidden in the scenarios hosted by the cyber range.

3.1 Ranges

Some of the ranges currently hosted within PAIDEUSIS are presented below.

- **SE***cube*™ **Range**: this range is mainly suitable for hosting training scenarios for programming the **SE***cube*™ device[15], a System-in-Package (SiP) developed by Blu5 Group[16] and designed for high security applications. **SE***cube*™ embeds in one chip 3 components: (i) a STM32F4 microcontroller by STMicroelectronics, (ii) a MachX02 FPGA by Lattice Semiconductor and (iii) an EAL5+ certified Smart Card by Infineon. Users are offered interaction with a Xubuntu[17] virtual desktop, to which the development board is connected.

[14] https://cyberchallenge.it/
[15] https://www.secube.eu/
[16] https://www.blu5group.com/
[17] https://xubuntu.org/

The VM is provided with the necessary tools for programming the 3 components of the SiP. A Cisco UCS C240 M4 High-Density Rack Server, with 2 Intel Xeon processors and 128 GB of RAM, runs concurrently 40 virtual machines. The server has been expanded with PCI-Express additional cards to support all the necessary USB connections. Each USB port has a separate controller, in order to isolate the IOMMU groups. The range can also be used for scenarios other than programming scenarios, such as CTFs based on the exploit of vulnerabilities present in the firmware of the microcontroller or in the design synthesized on the FPGA. At the moment, the range is actively used for the practice part of the course "Cybersecurity for Embedded Systems", held as Master Degree course in Politecnico di Torino.

- **ChipWhisperer Range**: this is the theater dedicated to the ChipWhisperer-Nano devices[18], a board of NewAE Technology Inc. that allows to experiment physical attacks against a victim chip on the board, such as *power side-channel analysis* [17] or *fault attacks* [7]. The dedicated server has a setting similar to that for the **SE***cube*™ Range, even if the interaction machines need much less resources, having no graphical interface and not requiring the use of specific tools for programming or synthesis: interaction with the device is done via Python scripts. Also in this case, in addition to training scenarios for starters, there is the possibility to host more advanced gaming scenarios, thus enabling a category of challenges barely present in the international CTF panorama [25].
- **Digital Hardware Emulation Range**: this range is used to host challenges on security problems stem from digital hardware designs [25]. The adopted EDA Environment is currently centered around ModelSim[19], through which it is possible to simulate any digital circuit descriptions in both Verilog and VHDL (e.g., from small size such as simple OTP authenticators or random number generators, up to real microprocessors, microcontrollers or DSPs). In several scenarios, hardware trojans [33] or other logical vulnerabilities are artificially inserted into the circuits. Participants have offline access to the hardware description, and can interact with the simulated devices via a customized command line interface. This acts as a filter to and from the ModelSim instance that runs on an interface virtual machine and simulates the device. The output of the simulation is strictly limited according to the requirements of the specific scenario. Red Teams typically use an encoded sequence of inputs (ranging from simple ModelSim commands to set and view signals, up to complex Assembly programs) to exploit the introduced vulnerabilities and capture the hidden flags. Blue Teams are instead supposed to submit effective patches to the vulnerabilities.
- **Network Security Range**: this range hosts network hardware devices, such as routers, switches or firewalls, on which one can exercise his/her skills relating security-oriented configuration and programming, but on which it is also possible to develop competition scenarios. The range has in fact hosted a scenario among those included in the 2020 national final event of the *CyberChallenge.IT* CTF competition, which was attended by 28 teams of ethical hackers from Italian academies. The challenge name was `home_r00ter` and it consisted of 28 Wi-Fi routers by Tiesse[20], arranged in a same room and programmed with a custom developed firmware, connected to the same switch but isolated from a networking standpoint due to the use of a separate VLAN for each device. Each team-assigned router was only reachable through a dedicated VPN. First, participants had to

[18] https://www.newae.com/products/NAE-CW1101
[19] https://www.intel.it/content/www/it/it/software/programmable/quartus-prime/model-sim.html
[20] http://www.tiesse.com/

find an entry point and break into their assigned router. Secondly, once inside their device, the goal was to exploit the other teams' routers, but using the physical Wi-Fi connection.

- **Industrial Control System Range**: this theater represents the cyber range adaptation of a real aqueduct emulator, *EVA* [3], which includes industrial control devices such as SCADA controllers. These communicate, using protocols like MODBUS over Wi-Fi, with IoT devices connected to sensors and actuators, opening valves or indicating tank levels. It is an important critical infrastructure of reference for hosting, e.g., training scenarios for Blue Teams such as Incident Response Teams from the industrial world.

4 Conclusions

The preset paper outlined PAIDEUSIS, a hybrid cyber range specifically developed as a training platform for security issues related to real hardware devices. These are physically included in the infrastructure, and made available to the users via a proper combinations of several different virtualization services. Available devices currently include microcontrollers, FPGAs, open security platforms, ICS's and SCADAs, IoT and IIoT devices, communication devices, and specific boards for side-channel analysis exploitation.

The paper also presented some implementation details and some of the exploited management tools, including PROXMOX, WireGuard and CRACK. Significant examples of theaters and scenarios set up within the infrastructure were provided, as well.

A complex environment such as PAIDEUSIS requires continuous maintenance, improvements, and upgrades. In particular, we are currently focusing on the following aspects: (i) a greater adaptability of CRACK in order to manage a scalable number of physical devices within theaters and (ii) new ranges that faithfully reproduce smart buildings and smart cities scenarios, including, among the others, general-purpose IoT devices connected to physical access control devices, air quality monitoring stations, and video surveillance cameras.

5 Acknowledgments

The activities presented in this paper are partially supported by: (i) the Italian CINI Cybersecurity National Laboratory via the program *CyberChallenge.IT*, and (ii) Blu5 Labs. Thanks also go to the technical partners of PAIDEUSIS, including Blu5 Labs[21], Cisco[22] and Tiesse[23], as well as to LINKS Foundation[24] in Turin for the physical hosting of the infrastructure.

References

[1] Cyber Ranges - NIST. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf. [Online; accessed 10-March-2021].

[2] IBM X-Force Command Brochure. https://www.ibm.com/downloads/cas/GO7BG1XV. [Online; accessed 06-March-2021].

[3] S. Ahmad, N. Maunero, and P. Prinetto. Eva: A hybrid cyber range. 2020.

[21] https://www.blu5group.com/
[22] https://www.cisco.com/
[23] http://www.tiesse.com/
[24] https://linksfoundation.com/

[4] I. D. Alvarenga and O. C. Duarte. Rio: A denial of service experimentation platform in a future internet testbed. In *2016 7th International Conference on the Network of the Future (NOF)*, pages 1–5. IEEE, 2016.

[5] A. Angelogianni, A. Brignone, N. Gerosavva, M. Ghering, D. Kavallieros, E. Karapistoli, V. Machamint, P. Polvanesi, E. Veroni, and C. Xenakis. The spider concept: A cyber range as a service platform.

[6] M. Artac, T. Borovssak, E. Di Nitto, M. Guerriero, and D. A. Tamburri. Devops: introducing infrastructure-as-code. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, pages 497–498. IEEE, 2017.

[7] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, Nov 2012.

[8] K. Barnes and B. Johnson. National scada test bed substation automation evaluation report. Technical report, Idaho National Laboratory (INL), 2009.

[9] P. Čeleda, J. Čegan, J. Vykopal, D. Tovarňák, et al. Kypo–a platform for cyber defence exercises. *M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization*, 2015.

[10] C. Eagle. Computer security competitions: Expanding educational outcomes. *IEEE Security Privacy*, 11(4):69–71, 2013.

[11] B. Ferguson, A. Tall, and D. Olsen. National cyber range overview. In *2014 IEEE Military Communications Conference*, pages 123–128, 2014.

[12] A. Furfaro, L. Argento, A. Parise, and A. Piccolo. Using virtual environments for the assessment of cybersecurity issues in iot scenarios. *Simulation Modelling Practice and Theory*, 73:43–54, 2017. Smart Cities and Internet of Things.

[13] A. Furfaro, A. Piccolo, D. Saccà, and Andrea A. Parise. A virtual environment for the enactment of realistic cyber security scenarios. In *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, pages 351–358. IEEE, 2016.

[14] J. Hong, S. Wu, A. Stefanov, A. Fshosha, C. Liu, P. Gladyshev, and M. Govindarasu. An intrusion and defense testbed in a cyber-power system environment. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–5, 2011.

[15] KasperskyLab. Threat landscape for industrial automation systems. https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/. [Online; accessed 06-March-2021].

[16] E. Keller and J. Rexford. The" platform as a service" model for networking. *INM/WREN*, 10:95–108, 2010.

[17] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Annual International Cryptology Conference*, pages 388–397. Springer, 1999.

[18] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri. A testbed for analyzing security of scada control systems (tasscs). In *ISGT 2011*, pages 1–7, 2011.

[19] J. A. Mattson. Cyber defense exercise: A service provider model. In *IFIP World Conference on Information Security Education*, pages 81–86. Springer, 2007.

[20] F. J. R. Melón, T. U. Väisänen, and M. Pihelgas. Eve and adam: Situation awareness tools for nato ccdcoe cyber exercises. In *Systems Concepts and Integration (SCI) Panel SCI-300 Specialists' Meeting on 'Cyber Physical Security of Defense Systems'*, pages STO–MP, 2018.

[21] I. M. Moraes, D. Mattos, L. H. Ferraz, M. E. Campista, M. Rubinstein, L .Costa, de M. Amorim, P. Vellosoand O. C. Duarte, and G. Pujolle. Fits: A flexible virtual network testbed architecture. *Computer Networks*, 63:221–237, 2014.

[22] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi. A control system

testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, 4(2):88–103, 2011.

[23] OASIS. OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca. [Online; accessed 10-March-2021].

[24] P. Prinetto and G. Roascio. Hardware security, vulnerabilities, and attacks: A comprehensive taxonomy. In *ITASEC*, pages 177–189, 2020.

[25] P. Prinetto, G. Roascio, and A. Varriale. Hardware-based capture-the-flag challenges. In *2020 IEEE East-West Design Test Symposium (EWDTS)*, pages 1–8, 2020.

[26] P. Qiu. Cyber Range - Cisco Live. https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2016/pdf/BRKSEC-2653.pdf. [Online; accessed 06-March-2021].

[27] E. Russo. *On the Design and Implementation of Next Generation Cyber Ranges*. PhD thesis, University of Genoa, 2020.

[28] E. Russo, G. Costa, and A. Armando. Building next generation cyber ranges with crack. *Computers & Security*, 95:101837, 2020.

[29] G. P. Tank, A. Dixit, A. Vellanki, and D. Annapurna. Software-defined networking-the new norm for networks. 2012.

[30] P. Tsai and C. Yang. Testbed twisc: A network security experiment platform. *International Journal of Communication Systems*, 31(2):e3446, 2018.

[31] E. Ukwandu, M. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens. A review of cyber-ranges and test-beds: current and future trends. *Sensors*, 20(24):7148, 2020.

[32] C. Willems and C. Meinel. Online assessment for hands-on cyber security training in a virtual lab. In *Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON)*, pages 1–10. IEEE, 2012.

[33] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22(1):6, 2016.

[34] M. M. Yamin, B. Katt, and V. Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636, 2020.