Scalable Cybersecurity Training: Integrating Virtual and Physical Security Teaching Environments

Lukas Bechtel, Markus Schramm, Lukas Popperl, Tobias Heer
University of Applied Sciences Esslingen, Germany
{lukas.bechtel,markus.schramm,lukas.popperl,tobias.heer}@hs-esslingen.de

***Abstract*—The number of cybersecurity incidents increases year over year. Cybersecurity education requires hands-on experience to protect infrastructure and services against hackers. However, existing teaching infrastructures face scalability and hardware integration challenges. This paper presents a semi-virtualized security teaching infrastructure combining virtual infrastructure, physical hardware access, and an Attack & Defense framework. The infrastructure is based on a Proxmox cluster, managed through a self-developed platform that allows parallel access to different courses. The teaching concept enables students to solve team-based exercises on personal laptops. Using personal laptops motivates students to create and maintain their own set of tools for cybersecurity analysis. Automated scoring and hardware interaction enhance engagement, providing a flexible platform for practical cybersecurity training.**

***Index Terms*—IT Security, Virtualization, Teaching, Education**

I. Introduction

Cybersecurity education requires practical experience to develop intuition for vulnerabilities to keep pace with evolving technologies and real-world threats. While static teaching infrastructures, where software runs on computers in the lecture room, provide controlled environments, they are often inflexible, resource-intensive, and require extensive maintenance. Virtual teaching infrastructures, i.e., infrastructures that run software in virtual machines (VM) on a server, offer scalability but lack integration of specific hardware, such as wireless networks or commercially available products combining hardware and software. These limitations hinder their effectiveness in providing a comprehensive learning experience.

To bridge this gap, we developed a semi-virtualized security teaching infrastructure that combines virtual and physical components. This setup allows students to interact with both software and hardware, creating a more holistic training environment. The core of the teaching infrastructure is a flexible network virtualization layer that allows to easily set up virtualized networks and specific topologies that match the learning task at hand. For example, courses available in the teaching infrastructure today include web application hacking, analysis and exploitation of wireless networks, and Windows authentication hacking. The teaching concept of the infrastructure is based on the principle by Maria Montessori [1], which encourages students to work in teams and learn or teach the required skills themselves. To strengthen this idea, the teaching infrastructure allows Bring Your Own Device (BYOD) interaction, such that students persist their cybersecurity tool suite on their personal laptops. The infrastructure dynamically and automatically provisions course environments for every team, ensuring consistency, adaptability, and secure access. Every semester, we conduct six lectures offering different independent topologies with 450 VMs for 80 students.

This work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 528745080 - FIP 68. Additionally, this research was supported by the project "FHP: Qualifizierung und Entwicklung des professoralen Personals der Hochschule Esslingen für zukunftsweisende Themen" (FKZ: 03FHP115) as part of the Federal States Program "FH-Personal", funded by the BMBF and MWK Baden-Württemberg. The authors alone are responsible for the content of the paper.

First, we detail the teaching concept in Section II. Second, we explain the technical components of our solution in Section III. Finally, we compare the solution to related work in Section IV and conclude the paper in Section V.

II. Teaching Concept

The field of cybersecurity is very dynamic and comprehensive. This poses a challenge for cybersecurity courses to cover multiple fields of cybersecurity and be up to date. This challenge requires a solution that offers teaching for individual students with different learning speeds and helps them get used to the uncertainty and lack of positive feedback that is part of every hacking task. The concept introduced by Maria Montessori [1] for teaching young children or teenagers aligns well with these requirements. The Montessori concept is designed for young learners to support them in evaluating solutions in new areas where it is unknown whether a solution exists. Similarly, cybersecurity exposes challenges for attackers and defenders never faced before and with uncertain solutions [2].

The teaching infrastructure provides the infrastructure and vulnerable content but leaves the path to the solution open. With the BYOD connectivity to the infrastructure, students can develop their own environment to solve future challenges. That way, students can use tools of their choice, combine tools with scripting, and persist their solution in a useful way.

The teaching infrastructure encourages students to execute their tasks in teams of two or three. The team members have concurrent individual access to a shared network and shared tasks. At this size, the teams are still small enough that everyone contributes to the solution and large enough that students can support each other in challenging exercises. Additionally, the infrastructure offers an *Attack & Defense* mode where teams can attack each other. This mode actively triggers learning in the uncertain, as the required Attack & Defense approaches highly depend on the skill level of the opponents. Similarly, students can learn Attack & Defense strategies by monitoring their opponent's activity.

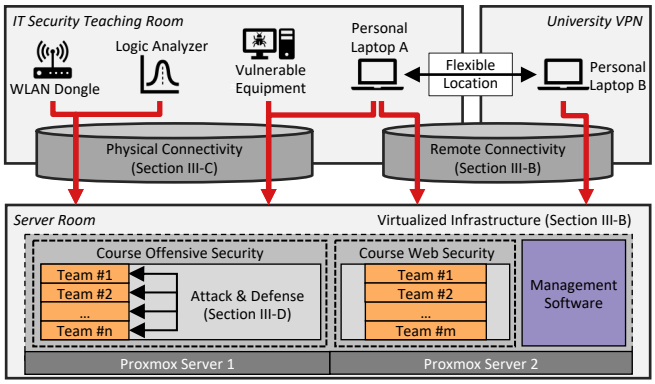

Fig. 1. Security Teaching Infrastructure Architecture

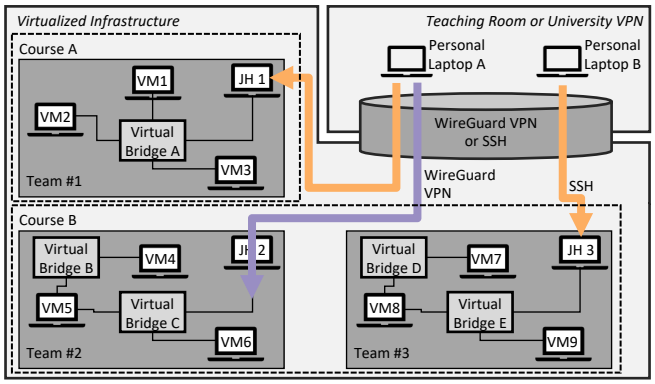

Fig. 2. Virtualized Infrastructure and Remote Access

III. Technical Components

The semi-virtualized security teaching infrastructure consists of three key components that collectively provide a scalable, secure, and effective training environment. We outline the architecture and detail the three components afterward.

A. Overall Architecture

The teaching infrastructure architecture runs on a *Proxmox* cluster (cf. Figure 1). One virtual machine on the servers hosts the self-developed *Management Software*, consisting of a backend and a web-based frontend. The frontend uses the university's *Single Sign-On* for authentication and is accessible in *eduroam* or the University VPN. The frontend allows teachers to automate the deployment of self-designed courses, reducing manual interaction with Proxmox. This frontend is also accessible to students, allowing them to register for courses and work on the exercises. The teachers design a custom network topology for each course that meets the course goals. Figure 1 highlights these team-specific copies of the course topology in orange as *Team #x*. For example, Figure 1 visualizes two courses with independent topologies and teams (cf. Section III-B). The teaching infrastructure offers an *Attack & Defense* mode, where students within a single course can attack each other and defend against attacks (cf. Section III-D).

The teaching infrastructure offers two methods to connect to the virtual environment (cf. Figure 1). We detail the remote connectivity for personal laptops in Section III-B and the physical connectivity of Ethernet and USB devices in Section III-C.

B. Virtualized Infrastructure

The *Management Software* allows teachers to create courses with custom topologies consisting of multiple VMs and networks. The teachers have an interface to create empty VMs, install software on these VMs, and edit configurations. Afterward, VMs are accessible to all teachers for future courses. For each course, teachers can define exercises to guide the students. We offer different types of exercises, some with a coupling to the VMs via the *qemu-guestagent* to verify the success of the exercise live on the system. Other exercise types include PDF submissions or static solutions.

The students can register for the created courses and join a team to work on their exercises. When joining a team, the software clones the course topology for the students and executes further VM configurations via the *qemu-guestagent*. Figure 2 visualizes the topologies for three teams in two courses. The teaching infrastructure handles multiple courses and topologies for multiple teams simultaneously. The tool adds a *Jump Host VM* (JH) to the topology and configures a unique public IP address. These jump hosts isolate the vulnerable systems from the public network. The *Jump Hosts* are a perfect interface for implementing team authentication, which is handled by the *Management Software* and is unique per student. Students can use SSH or WireGuard VPN to connect to their cloned infrastructure. Figure 2 visualizes these cases in orange for SSH and purple for WireGuard. With SSH, students can forward specific services to their private laptops with local port forwarding. With WireGuard VPN, the laptops have a VPN tunnel directly into the virtualized network, which allows them to access all hosts without additional forwarding.

C. Physical Hardware Integration

Physical hardware integration bridges the gap between virtualized security training and real-world cybersecurity challenges. Some cybersecurity exercises require direct interaction with physical devices, e.g., microcontrollers or WLAN access points. Figure 3 visualizes the two methods for connecting physical hardware to the virtual environment: A) Ethernet-capable devices (orange) and B) USB devices (purple). Ethernet-capable devices can be *Personal Laptops* or

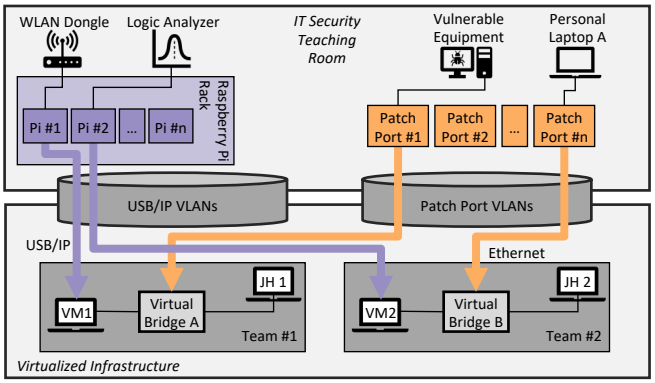

Fig. 3. Integration of Physical Hardware into the Infrastructure

Vulnerable Equipment students are supposed to hack. USB devices include *WLAN Dongles* or *Logic Analyzers*. For both methods, the *Management Software* allows students to dynamically reserve the physical connection for the duration of the lecture. The system can handle the integration of hardware devices for different courses in parallel, requiring automated and continuous reconfiguration of the virtualized network infrastructure in Proxmox. In the following, we detail both of these integrations.

To integrate Ethernet-capable devices, we assign each patch port in the lecture room a unique VLAN ID. For the VLAN-tagged traffic, the virtualized networking within Proxmox is aware of the patch port from which the traffic is coming.

As a direct USB connection between the lecture room on the fifth floor and the virtualized infrastructure in the basement is impossible, we installed a rack of Raspberry Pis in the lecture room. Once students match a Raspberry Pi's USB port with a VM in their team topology, the management software reconfigures the Proxmox network. This reconfiguration includes adjustments of VLANs and the detailed configuration of the tool *usbip* on the Raspberry Pi and VM to forward the USB port via IP traffic, enabling seamless access to the USB device.

D. Attack & Defense Network

Cybersecurity experts must deal with uncertain and non-static environments in the real world. Therefore, we introduce an *Attack & Defense* mode in our teaching infrastructure, connecting networks of the virtual infrastructures of the different teams. In the *Attack & Defense* mode, teams shall analyze and attack the opponents and protect their own infrastructure. Figure 4 visualizes this connection of the team networks. Course topologies for this *Attack & Defense* mode consist of at least one internal network and exactly one Demilitarized Zone (DMZ). A firewall protects the internal network and the DMZ. While creating the infrastructure, the software clones the VMs in the internal networks statically, i.e., the same configuration for every team. For the VMs in the DMZ, each team will have its own subnet to allow routing between the networks. Also, the infrastructure registers a domain name at the Domain Name Server (DNS) for every VM in the DMZ.

To provide feedback on the progress, the developed *Management Software* distributes random flags on all VMs at predefined locations so students can search for them. It regenerates these random flags frequently to motivate students to automate hacking. In parallel, this setting motivates teams to protect their infrastructure. The system analyzes the reachability of key components and serves penalty points if systems are down. Therefore, students cannot block all incoming traffic with a firewall. They must analyze and adopt foreign code and configuration. Students gain the skills to learn new security challenges themselves, as targeted by the Montessori concept.

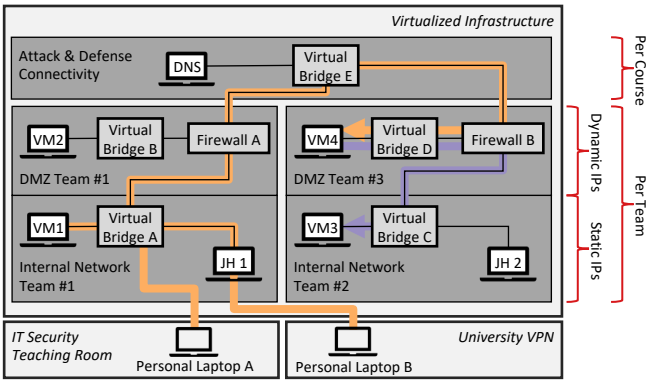

Fig. 4. Attack & Defense Architecture in the Teaching Infrastructure

IV. Related Work

Several academic cybersecurity training platforms share similarities with our security teaching infrastructure, such as the Cybersecurity Virtual Laboratory at Embry-Riddle Aeronautical University [3], the Cyber-SHIP Lab at the University of Plymouth [4], and the Hybrid Cybersecurity Research and Education Environment [5]. These platforms provide remote access to security exercises and simulations of real-world cyber environments but lack the combination of virtual and physical infrastructure and team interaction.

On the commercial side, platforms like TryHackMe [6], Immersive Labs [7], and Cybrary [8] offer interactive cybersecurity training through purely virtual environments. Airbus's CyberRange [9] enables realistic training with virtual and physical elements but lacks the *Attack & Defense* mode. Our approach extends these models by combining virtualized and physical security training with team interaction.

V. Conclusion

The semi-virtualized security teaching infrastructure combines virtual infrastructure, physical hardware integration, and an Attack & Defense framework, creating a scalable and hands-on cybersecurity training environment. The BYOD approach allows students to develop and persist their personal toolsets while automation streamlines course management. Future work includes open-sourcing the teaching infrastructure to encourage wider adoption and collaboration and developing automated attack scenarios to enhance training realism and adaptability.

References

[1] M. Montessori, *The montessori method*. Transaction publishers, 2013.

[2] M. K. Thomas, A. Shyjka, S. Kumm, and R. Gjomemo, "Educational Design Research for the Development of a Collectible Card Game for Cybersecurity Learning," *Journal of Formative Design in Learning*, 2019.

[3] Embry-Riddle Aeronautical University. (2025) Cybersecurity Virtual Laboratory. Accessed: Feb. 9, 2025. [Online]. Available: https://daytonabeach.erau.edu/about/labs/cybersecurity-lab

[4] University of Plymouth. (2025) Cyber-SHIP Lab. Accessed: Feb. 9, 2025. [Online]. Available: https://www.plymouth.ac.uk/research/cyber-ship-lab

[5] G. Visky, A. Šiganov, M. u. Rehman, R. Vaarandi, H. Bahşi, H. Bahsi, and L. Tsiopoulos, "Hybrid Cybersecurity Research and Education Environment for Maritime Sector," in *IEEE International Conference on Cyber Security and Resilience (CSR)*, London, UK, Sep. 2024.

[6] TryHackMe Ltd. (2025) TryHackMe. Accessed: Feb. 9, 2025. [Online]. Available: https://tryhackme.com

[7] Immersive Labs Group. (2025) Immersive Labs. Accessed: Feb. 9, 2025. [Online]. Available: https://www.immersivelabs.com

[8] Cybrary, Inc. (2025) Cybrary. Accessed: Feb. 9, 2025. [Online]. Available: https://www.cybrary.it

[9] Airbus SAS. (2025) CyberRange. Accessed: Feb. 9, 2025. [Online]. Available: https://cyber.airbus.com/en/products/cyberrange