PAIDEUSIS - A Hybrid Cyber Range

Vahid EFTEKHARI MOGHADAM
DAUIN - Politecnico di Torino
CINI Cybersecurity National Lab
Turin, Italy
vahid.eftekharimoghadam@studenti.polito.it

Matteo FORNERO
CINI Cybersecurity National Lab
Turin, Italy
matteo.fornero@consorzio-cini.it

Nicolò MAUNERO
DAUIN - Politecnico di Torino
CINI Cybersecurity National Lab
Turin, Italy
nicolo.maunero@polito.it

Paolo PRINETTO
DAUIN - Politecnico di Torino
CINI Cybersecurity National Lab
Turin, Italy
paolo.prinetto@polito.it

Gianluca ROASCIO
DAUIN - Politecnico di Torino
CINI Cybersecurity National Lab
Turin, Italy
gianluca.roascio@polito.it

Over the recent years, cyber attacks have increased constantly. Attacks targeting sensors networks, or exploiting the growing number of networked devices, are becoming even more frequent. This has led to the need to find a way to train the teams responsible for defending computer systems in order to make them able to respond to any threats quickly. The fact that it is impossible to carry out training operations directly on corporate networks or critical infrastructure has led to the birth of Cyber Ranges, virtual or hybrid systems that allow training in safe and isolated environments.

A *Hybrid Cyber Range* is a range that recreates a critical infrastructure using both real components and components simulated with virtualization technologies. Such an approach aims to combine the positive aspects of pure physical or pure virtual Cyber Ranges, as it has the flexibility of a virtual environment and the realism resulting from the use of real-word hardware components of the reference infrastructure. A hybrid approach is the most suitable for training for scenarios in which an environment is controlled through IoT devices, such as an industrial plant or a smart building, as pure virtualization would obscure or make it very complicated to recreate security issues expressly linked to these scenarios. Furthermore, the presence of real devices makes training sessions related to programming them much more profitable.

These are some of the reasons that led to the creation of PAIDEUSIS, a hybrid Cyber-Range that can host security training sessions in multiple scenarios, including: networks with SCADA controllers for the management of water distribution systems, IoT with sensors for smart cities and smart buildings, microprocessors physically implemented on FPGA or virtualized through HDL simulation tools with architectural vulnerabilities, and much more. All scenarios also offer the possibility of hosting CTF (Capture-the-Flag) competitions, as already happened for the national final event of the 2020 edition of CyberChallenge.IT.