Design and Architecture of an Industrial IT Security Lab

Steffen Pfrang(✉), Jörg Kippe, David Meier, and Christian Haas

Fraunhofer IOSB, Fraunhoferstr. 1, 76131 Karlsruhe, Germany
{steffen.pfrang,joerg.kippe,david.meier,
christian.haas}@iosb.fraunhofer.de

Abstract. IT security for Industrial control systems or the Industrial Internet of Things is an emerging topic in research and development as well as for operators of real production facilities. In this paper, we will present the Fraunhofer IOSB IT Security Laboratory for industrial control systems, that enables security research, development and testing of products and training of IT security personnel. Due to its architecture based on both real hardware components and a flexible virtual environment, the IT Security Lab offers a realistic setup of today's production facilities and at the same time a high flexibility with regard to future networking technologies and protocols.

Keywords: IT security · Industrial Internet of Things · Industrie 4.0 · Testbed

1 Introduction and Motivation

Future industrial production facilities will be highly networked. Controllers and embedded systems such as programmable logic controllers (PLC) and sensors or actors communicate with each other, cloud-based systems plan tasks and machine utilization, plant operators monitor and control the system remotely, maintenance staff can access and change the plant's configuration remotely from anywhere on the planet. With more networking and connectivity, IT security mechanisms become an urgent and integral topic well beyond factory or production sites. Attackers could potentially infiltrate critical production networks and therefore harm or destroy production lines or even cause severe injuries.

To protect against damage and production stoppages, suitable measures to prevent security incidents are urgently needed. Yet, the research and development of countermeasures or attack research and vulnerability scanning are often not possible in real production networks due to availability issues or the risk of malfunctions. On the other hand, nearly no test data, e.g. packet capture (PCAP) files of network traffic in industrial sites is available, as this data is often related to intellectual property protection and kept secret. Nevertheless, IT security research and development requires an IT infrastructure that is isolated from productive networks and yet replicates the target environment as

S. Guo et al. (Eds.): TridentCom 2016, LNICST 177, pp. 114–123, 2017.
DOI: 10.1007/978-3-319-49580-4_11

accurately as possible. In this paper we will present the Fraunhofer IOSB IT Security Laboratory for Industrial control systems that enables us to perform security research, development and testing of products and education or training of security personnel in an isolated environment that contains most of today's industrial networks and components in real hardware and software as well.

1.1 Requirements

There are several requirements that the IT Security Laboratory has to fulfill. At first and most important, there is the necessity to perform attack research including Vulnerability scanning and Intrusion detection in a testbed that consists of real automation components connected with real industrial protocols without endangering any real production process.

In order to gain flexibility and reduce costs, there should both real hardware components (e.g. PLCs, industrial switches etc.) and virtualized components. Using a virtualization environment for the production site allows for constructing larger, more realistic production processes and workflows as well as for attacking devices without the danger of destroying components irrecoverably. On the other hand, attacks have to target real components to transfer research results to real production sites.

The laboratory has to be built up to integrate arbitrary automation equipment. Additionally, there has to be the flexibility for reconfiguring the whole laboratory setup by exchanging components through standardized interfaces: Mechanically, electrically as well as the networking infrastructure.

For attack and detection purposes, there has to be a powerful virtualized computing infrastructure which can be used from different locations (e.g. offices) with the ease of virtual machines. And last but not least, the whole laboratory has to be protected from attacks coming from the Internet as well as the Internet, that has to be protected from attacks performed by malicious software that is run within the laboratory.

2 Design

The IT Security Laboratory is a test- and demonstration environment dedicated to the security of industrial IT systems and providing a high degree of flexibility to perform IT security research. From the top-level point of view, the lab consists of two parts:

Virtualization environment (also called the cloud infrastructure)**:** This environment shown on the left side of Fig. 1 is implemented using the Open source software platform Proxmox VE [4] and runs on a three node hardware cluster. In this environment different networks have been set up using virtual switches (Open vSwitch [15]) as well as virtual firewalls (pfsense [10]). Virtual machines connected to these networks provide components of automation systems (e.g. PLC programming stations, SCADA servers), management tools and – to support security research – different attack and detection tools.

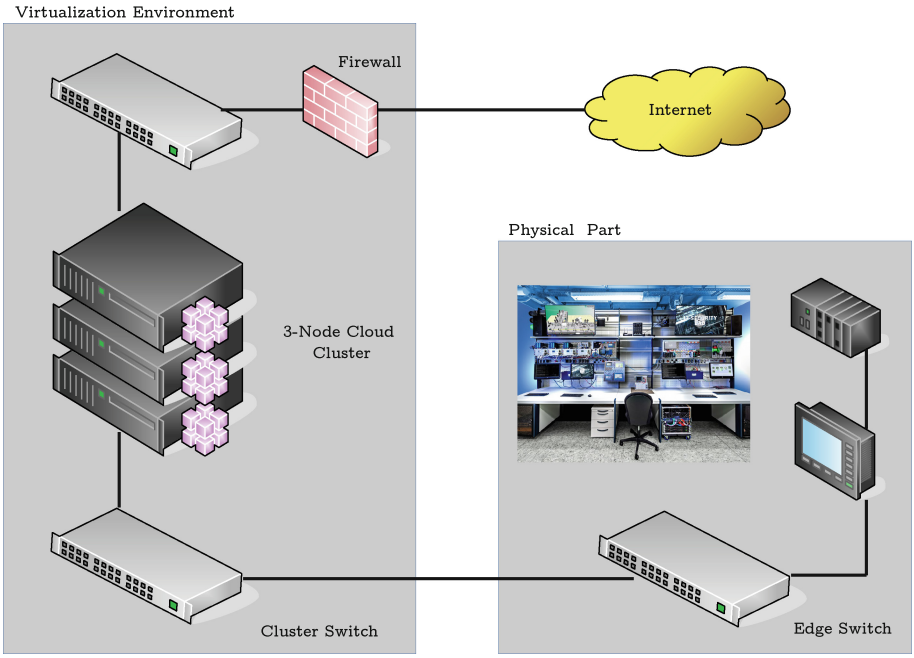

Fig. 1. The virtualization environment and related physical part

The hardware cluster is connected to the Internet and protected by a hardware firewall (Cisco ASA) controlling incoming traffic as in any other Internet connected enterprise network, but additional protection has been implemented to control outgoing traffic and to prevent malicious software from passing from the laboratory networks into the outside world. A cluster switch connects the nodes and provides on a trunk port several virtual LANs set up within the cloud infrastructure building the network infrastructure for the experiments to be run in the laboratory.

Physical part: The physical part shown on the right side of Fig. 1 consists of a mechanical framework construction into which different experiments can be mounted. Experiments consist of slabs, which on turn carry real physical components known from industrial automation systems (like PLCs, industrial switches, HMIs, etc.). The framework construction provides electrical power (different voltages as needed by typical automation equipment) and connection to the networks in the virtualization environment via an edge switch that is connected to the cluster switch.

Both the virtual and the physical part together provide the test- and demonstration environment which allows to run attacks against real automation equipment (which hardly can be simulated using virtual machines) in a flexible way. The slabs carrying the experiments are designed in a modular way and can be changed easily (Fig. 2).

Fig. 2. Picture of the IOSB Industrial IT security laboratory

Figure 3 shows an example network structure with three subnets: The Field network comprising PLCs, sensors and actors, is connected via a firewall with the SCADA network homing a SCADA system. Another firewall connects this network with the Office network. The management, attack and detection tools reside in a separate network which is linked to all of the other networks.

2.1 Monitoring Infrastructure

With respect to network traffic analysis one has to consider the fact that subnetworks/VLANs are spread over different switches in the virtual as well as in the real part of the lab environment. To get a complete view of the network traffic the traffic passing through the different switches has to be monitored and those mirror streams have to be merged. That has been achieved by setting up the mirroring within the Open vSwitch infrastructure and sending the collected mirror streams through Generic Routing Encapsulation (GRE) tunnels to a concentrator which provides a merged mirror stream to the analyzer machine. A visualization of this mirroring infrastructure is shown in Fig. 4.

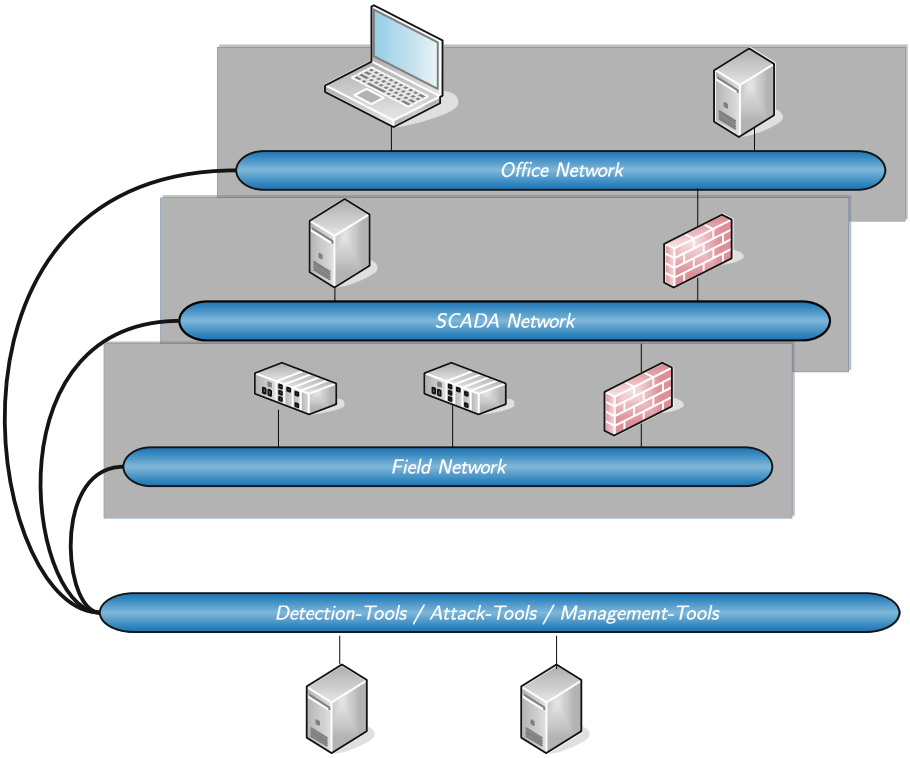

Fig. 3. Example network view with different typically used networks

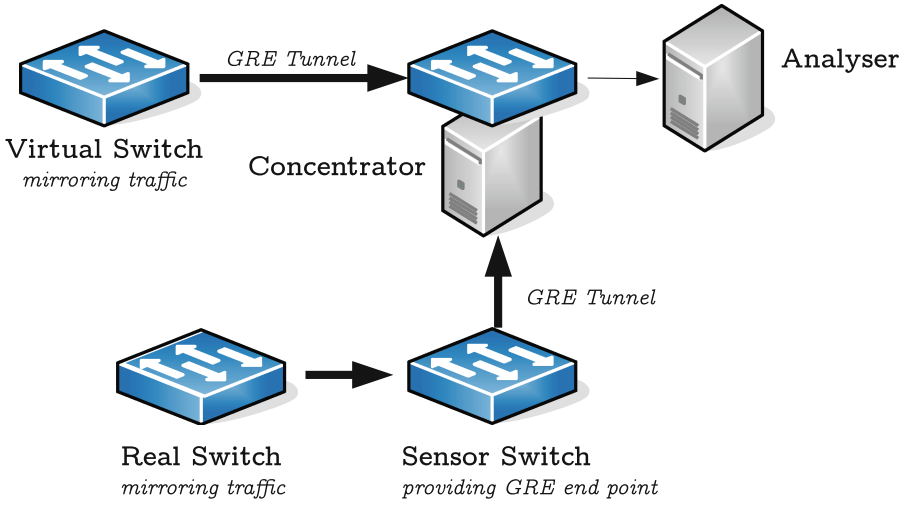

Fig. 4. A mirror infrastructure example comprising one real and one virtual switch

2.2 Detection Tools

The placement and usage of any detection tools depends on the experiments to be conducted. For network based detection tools e.g. a sensor component performing packet capture would be connected to the mirror stream provided by the monitoring infrastructure as described above. For the analysis/testing of host based detections tools, collectors and correlators would be installed in the management network receiving alerts directly from the components under test. In the same way any GUI applications would be located within this network. A dual-homed installation typically would be used for vulnerability assessment scanners, which have one interface in the management network and another where the components to be scanned are residing.

3 Attack Case Study

To demonstrate the capabilities of the Industrial IT Security Lab, an attack case study is presented. This example attack will involve multiple parts of the lab to illustrate security weaknesses and their impact on Industrial IT components.

3.1 Scenario

This scenario is built upon a simulated production process involving multiple simulated machines. The simulated production process is based on a real factory installation from Festo Didactic and simulated using CIROS 6.0 software, also by Festo [3]. The simulated machines are controlled by individual programmable logic controllers (PLC) by wiring their signal in- and outputs to the simulation. This has the advantage that the PLCs can be operated with the same firmware and configuration used in a completely real environment. One part of the production process contains a rotary disk where workpieces are tooled with a molding cutter and a drill. This part of the process is controlled by a single PLC that reacts on sensor input when a new workpiece is ready to get processed. It is then brought into position by the rotary disk and cutter and drill are positioned accordingly. The actual cutting and drilling is also controlled by the signal outputs from the PLC. The real-world installation of this production process part is shown in Fig. 5.

The PLCs are communicating with each other and have industrial Ethernet connections to a OPC-UA server [9], where production data gets aggregated. No security hardening procedures or methods were used on the automation devices. While this would not be common practice in modern IT environments, this is still often found in the industrial IT domain, because of a false perception of security [11]. This also means that access to the PLC is not restricted, for example by using default passwords or no passwords at all.

In this scenario, we assume an attacker has gained access to the plant communication network with typical attack vectors [7] comprising of, for example, infected control stations or manipulated mobile maintenance equipment.

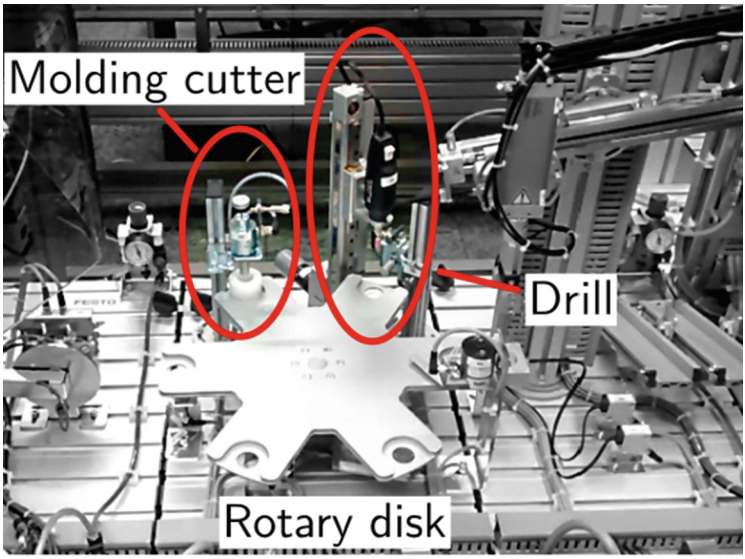

Fig. 5. Picture of process part used for the attack scenario

The attacker has access to the SCADA parts of the network in particular (refer to Fig. 3) and is able to inject arbitrary data into the network. He is therefore also able to intercept data by using ARP spoofing, for example. This also enables the attacker to start communication with devices of his choice.

3.2 Attack Description

The attacker is first starting to scan the network silently to avoid affecting automation devices yet, which often react with errors when confronted with simple network scans. This enables the attacker to learn the devices present in the network. By analyzing MAC addresses, a target PLC can be identified. The attacker can now start communicating with the targeted PLC by using an applicable SCADA protocol. As the PLC in this scenario is a *SIEMENS S7-300*, the *S7 protocol* is the protocol of choice. The protocol enables the attacker not only to read data from the PLC, the attacker can also send commands to the PLC. By issuing a *force order* command, arbitrary values can be set on the in- and outputs. This is a debugging feature to enable quick reaction options, for example in the case of hardware failures. The attacker can now provide the executed PLC program with manipulated inputs or set the outputs of the PLC directly. By setting almost all output signals, the attacker can provoke a constant rotation of the dish while molding cutter and drill are still active and in position. This would, of course, immediately cause damage to the current workpieces and the hardware itself and ultimately lead to the destruction of crucial elements of this process part.

During the attack, the internal computation cycle of the PLC is not altered in any way. As soon as the *force order* is deactivated by the attacker, the current cycle outputs are set and the PLC continues regular operation. This also means that neither the firmware nor the current configuration of the PLC are altered by the attack.

3.3 Detection and Alert Processing

Our simple showcase detection workflow starts with the network-based Intrusion Detection System (IDS) SNORT [12]. Initially, SNORT gets configured with a whitelist containing the information of allowed connections to the PLC.

Once SNORT detects a network packet addressing the PLC whose sender doesn't match the whitelist, it fires an alert. This alert gets forwarded to the correlation engine OSSEC [1] which simply converts the alert into the standardized Intrusion Detection Message Exchange Format (IDMEF) [2]. The alert might be processed by an Incident Management System (IMS). In our case, for demonstration purposes, it triggers a traffic light which is mounted on the mechanical part of the lab and sets it to red.

3.4 Case Study Conclusion

We are able to demonstrate a simple, yet effective attack to a production process. The attack arises because an attacker has got direct access to the SCADA components with the PLCs. This scenario is not only fictitious, it is even ordinary in many production sites based on our experiences with talks to employees and responsable persons: Network separation isn't performed in production sites as it is common in the Office IT.

Additionally, as a second point, Intrusion detection is being performed in the virtualization infrastructure and an alarm gets raised once malicious activities are being discovered. That allows for alerting cyber security personnel that can react properly.

4 Related Work

Testbeds for the Industrial Internet of Things is a hot topic all over the world. For example, there are several testbeds in the Industrial Internet Consortium (IIC) for different emerging topics in the industrial internet, e.g. for condition monitoring an asset efficiency testbed [5]. Another set of testbeds can be found in the German *Plattform Industrie 4.0* consortium, where several testbeds are hosted in the so-called *Labs Network Industrie 4.0*. These testbeds address several hot topics for Industrie 4.0, e.g. Smart Factories, PLUG and WORK or Smart Data Innovation [8]. Neverless, very few testbeds are designed and used for research and development on IT security for the industrial internet. For some educational purposes, some smaller training and test scenarios can be found from

commercial cyber training vendors, e.g. [13,14] or [6]. These smaller test environments usually are used to showcase some specific attacks or detection technique for industrial control systems, yet they often lack the flexibility to use both real hardware and virtual components. Also, often times no real production processes are simulated or run.

5 Discussion and Future Work

With the attack case study presented in Sect. 3, we were able to prove that the testbed fulfills the requirements for an Industrial IT security laboratory enumerated in Subsect. 1.1: A cyber attack disturbing a physical but simulated process gets detected by an IDS component which triggers an alarm.

The architecture is chosen rather flexible allowing for the inclusion of arbitrary physical as well as virtualized components. Using a powerful cloud infrastructure, even heavy-weight attack tools can be run. With the monitoring infrastructure in place, different types of detection tools can be launched and used for both research and educational purposes. Furthermore, it allows for the recording of process automation communication as well as cyber attack traffic resulting in PCAP files which can be used for analysis outside of the laboratory.

Nevertheless, there are some minor limitations of our approach to be mentioned. Even with the flexibility of the lab, it is not possible to reproduce the whole complexity of some real-world automation scenarios because there are nearly no industrial components which can be virtualized with full industrial real-time protocol support.

A limitation might also be the fact that the lab doesn't involve any human operators or workflows which are an essential part of a complete automation scenario. But many infections of production networks arise via the Office network through infected email attachments, malicious code on websites, phishing attacks or infected USB drives because human personnel is vulnerable for social engineering attacks. An inadequate separation of the networks then allows for the spreading of the attack.

5.1 Future Work

Within this paper, we have presented a basic attack and detection scenario. We are planning to elaborate more enhanced attacks on the Field layer as well as on the SCADA layer including attack research on ProfiNet, S7 and OPC UA. In order to detect these security breaches, we are experimenting with more enhanced Intrusion detection and correlation techniques. A goal is also to include the gathered information about security alerts into a security overview of the situation. As a future step, we plan to use our IT security lab in education, using it as an easy way to create awareness for security risks in industrial control systems as well as a good tool to demonstrate how to secure these systems.

Using the flexibility of the laboratory infrastructure, we are also planning to include remote production sites into the lab in order to perform advanced security monitoring.

References

1. Bray, R., Cid, D., Hay, A.: OSSEC Host-Based Intrusion Detection Guide. Syngress (2008)
2. Debar, H., Curry, D., Feinstein, B.: The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765 (Experimental). Internet Engineering Task Force, March 2007. http://www.ietf.org/rfc/rfc4765.txt
3. Festo AG & Co. KG. Festo Didactic (2016). http://www.festo-didactic.com/. Accessed 01 February 2016
4. Proxmox Server Solutions GmbH. Open Source Virtualization (2016). https://www.proxmox.com/en/. Accessed 01 February 2016
5. Industrial Inernet Consortium (IIC). Industrial Inernet Consortium Testbeds (2016). http://www.iiconsortium.org/test-beds.htm. Accessed 01 February 2016
6. International Society of Automation. International Society of Automation Hands-on Training (2016). https://www.isa.org/training-certifications/isa-training/about-isa-training/hands-on-laboratories/. Accessed 01 February 2016
7. Johnson, R.E.: Survey of SCADA security challenges and potential attack vectors. In: 2010 International Conference for Internet Technology and Secured Transactions (ICITST), pp. 1–5 (2010)
8. Labs Network Industrie 4.0. Labs Network Industrie 4.0 Testbeds (2016). http://lni40.de/. Accessed 01 February 2016
9. OPC Foundation. OPC Unified Architecture (2016). https://opcfoundation.org/. Accessed 01 February 2016
10. pfSense. Open Source Security (2016). https://www.pfsense.org/. Accessed 01 February 2016
11. Piètre-Cambacédès, L., Tritschler, M., Ericsson, G.N.: Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs. IEEE Trans. Power Delivery **26**(1), 161–172 (2011). doi:10.1109/TPWRD.2010.2061872. ISSN: 0885-8977
12. Roesch, M., et al.: Snort: lightweight intrusion detection for networks. In: LISA, vol. 99(1), pp. 229–238 (1999)
13. SANS. Assessing and Exploiting Control Systems (2016). http://www.sans.org/course/pentesting-smartgrid-scada. Accessed 01 February 2016
14. SANS. Critical Infrastructure and Control System Cybersecurity (2016). http://www.sans.org/course/critical-infrastructure-csc. Accessed 01 February 2016
15. Proxmox Server Solutions. Open vSwitch (2016). http://openvswitch.org/. Accessed 01 February 2016