Poster: INSIDE – Enhancing Network Intrusion Detection in Power Grids with Automated Facility Monitoring

Martin Serror
Fraunhofer FKIE
Germany
martin.serror@fkie.fraunhofer.de

Lennart Bader
Fraunhofer FKIE
Germany
lennart.bader@fkie.fraunhofer.de

Martin Henze
RWTH Aachen University
Fraunhofer FKIE
Germany
henze@cs.rwth-aachen.de

Arne Schwarze
Fraunhofer FKIE
Germany
arne.schwarze@fkie.fraunhofer.de

Kai Nürnberger
Fraunhofer FKIE
Germany
kai.nuernberger@fkie.fraunhofer.de

ABSTRACT

Advances in digitalization and networking of power grids have increased the risks of cyberattacks against such critical infrastructures, where the attacks often originate from within the power grid's network. Adequate detection must hence consider both physical access violations and network anomalies to identify the attack's origin. Therefore, we propose *INSIDE*, combining network intrusion detection with automated facility monitoring to swiftly detect cyberattacks on power grids based on unauthorized access. Besides providing an initial design for *INSIDE*, we discuss potential use cases illustrating the benefits of such a comprehensive methodology.

CCS CONCEPTS

• **Security and privacy → Network security**; *Intrusion detection systems*; • **Networks → Cyber-physical networks**.

KEYWORDS

security, intrusion detection, cyber-physical systems, power grid

ACM Reference Format:
Martin Serror, Lennart Bader, Martin Henze, Arne Schwarze, and Kai Nürnberger. 2022. Poster: INSIDE – Enhancing Network Intrusion Detection in Power Grids with Automated Facility Monitoring. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22), November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3548606.3563500

1 MOTIVATION

Power grids are a vital part of a country's critical infrastructure and thus require special protection against sabotage. Besides physical security, e.g., perimeter protection or access control, such protection includes cybersecurity due to the growing digitalization of power grids [7]. Recent events, such as the repeated cyberattacks against the Ukrainian power grid [13], illustrate yet again the insufficient protection of power grids against cyberthreats. Hence, security engineers and researchers must continuously improve security measures. In this context, Intrusion Detection Systems (IDSs) are of paramount importance to complement preventive measures. IDSs enable early detection of malicious activities, which, in turn, facilitates timely reaction to prevent further damage.

However, although IDSs are well-established in office environments and data centers, they are of limited use for the industrial domain since they usually do not consider the underlying industrial process and communication characteristics [4]. Therefore, a new class of *industrial* IDSs has emerged, leveraging context information regarding industrial processes and communication. Nevertheless, improving *accuracy* and, in particular, reducing *false positives* remains one of the major challenges for industrial IDSs [8, 11].

Besides process and communication awareness, further context information is required to improve the accuracy of IDSs substantially. In particular, power grids consist of many remote sites, such as substations and solar parks, which are increasingly interconnected, forming a widespread network. Such a network is particularly susceptible to attacks from within, i.e., attackers bypassing the external network protection mechanisms by gaining physical access to the network [7]. The attackers then use this entry point for targeted attacks over the internal network with devastating consequences. Therefore, IDSs for power grids should react more sensitively to suspicious network activity resulting from unauthorized physical access, e.g., trespassing, to prevent attacks early on.

Hence, automated Facility Monitoring Systems (FMSs) are essential to reliably identify unauthorized accesses on the numerous remote sites of power grids. Such FMSs rely on data from various sensors and access devices, such as cameras, infrared sensors, and keypads, to monitor access violations [10]. Since numerous approaches already exist for smart home surveillance, e.g., [14], their benefits are progressively being discussed in the context of power grids [2, 5]. However, FMSs and network IDSs still operate as decoupled systems whose outputs are not jointly considered.

Therefore, we propose *Intrusion on Site Detection (INSIDE)*, combining an industrial IDS, monitoring suspicious activities in the power grid's network based on process-aware anomaly detection, with an FMS, recognizing unauthorized accesses on the distinct power grid premises. The IDS and FMS results then converge in a *Meta-IDS* for correlation and analysis, targeting to prevent sophisticated cyberattacks on power grids originating from (unauthorized)

CCS '22, November 7–11, 2022, Los Angeles, CA, USA
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3563500

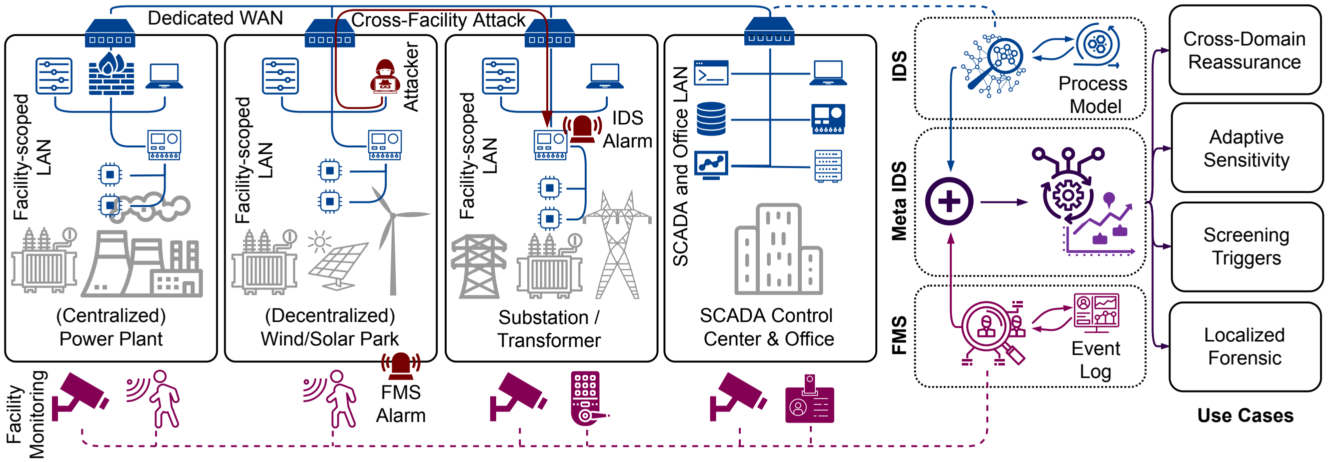

Figure 1: Proposed design of *INSIDE*, combining an industrial IDS with automated facility monitoring to swiftly detect the origins of attacks. Therefore, the Meta-IDS analyses the results of both subsystems to identify the locations of attacking devices.

physical access. The coincidence of unauthorized access and suspicious network traffic thus enables early detection and targeted reaction, e.g., network traffic inspection and blocking connections.

2 THREAT MODEL

In this section, we describe the imminent threat of cyberattacks on power grids resulting from local access to remote sites and the corresponding attack model. We assume that attackers only require limited knowledge about the specific power grid and network structure. However, they opportunistically gain local access to a device connected to the grid's network, e.g., through a Remote Terminal Unit (RTU) in a substation. This is a realistic assumption for insiders (e.g., employees) as well as for outsiders (e.g., external maintenance staff) [7]. Hence, the attackers cannot fully influence their access point within the network and thus rely on network reconnaissance to identify vulnerable protocols and services. With this knowledge, they can gradually extend their access (e.g., to a different subnet), plan the actual attack, and eventually perform it. Therefore, *INSIDE* aims to detect the attack's origin early, i.e., during initial access or network reconnaissance, to prevent more severe damage.

3 DESIGN OF *INSIDE*

As depicted in Fig. 1, *INSIDE* consists of three main components: (i) an industrial IDS monitoring the network traffic for anomalies; (ii) an automated FMS identifying unauthorized access on-site; and (iii) a Meta-IDS analyzing the outputs of (i) and (ii). In the following, we describe the distinct components and their interactions.

3.1 Industrial IDS

Network IDSs offer a cheap and retrofittable solution to detect ongoing cyberattacks, thus complementing preventive security measures. However, their performance depends on their domain-specific implementation and calibration. In industrial settings, such as power grids, IDSs can leverage the predictability of the network traffic due to the regularity of industrial processes [6]. Moreover, *process awareness* leverages knowledge about the underlying physical processes to improve anomaly detection accuracy [16].

Concerning the deployment, we follow a non-invasive monitoring approach [1], where the IDS sensors use the Test Access Ports (TAPs) of the network switches for traffic capturing. The sensors are thus placed at strategically relevant switches, e.g., connecting different network segments, enabling reliable detection of network-based attacks. Nevertheless, a significant limitation of current IDSs lies in their inability to identify the origin of an attack [12], which is particularly challenging in large-scale power grids and may prevent swift reactions. Therefore, *INSIDE* further extends the industrial IDS with an FMS, as presented in the following.

3.2 Facility Monitoring System

Complementing the industrial IDS, our design proposes integrating a Facility Monitoring System (FMS) to enhance the detection of security-related physical incidents, e.g., a maintenance engineer accessing a restricted area. An FMS utilizes information from multiple sensors of various types, e.g., surveillance cameras, motion sensors, and digital keylocks, to monitor facilities for unauthorized access [10]. Essentially, an FMS constitutes an IDS for the physical world. In combination with per-user PIN codes, digital IDs, or automated face recognition, the FMS can detect both legitimate access to certain facilities/areas as well as (attempted) intruders.

Based on the available information, the FMS can issue intrusion alarms, record facility accesses, and log how specific incidents were resolved. These events and annotations are merged with those stemming from the IDS, bridging the gap between digital and physical intrusion and event detection, as explained in the following.

3.3 Meta-IDS

The main task of the Meta-IDS is to aggregate the real-time results from the industrial IDS and the FMS for analysis. The Meta-IDS hence identifies correlations between suspicious network traffic and physical accesses to localize the origin of possible cyberattacks or reduce false positives. For instance, if a maintenance engineer

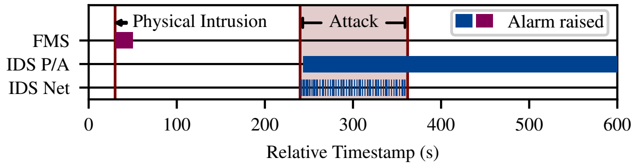

Figure 2: FMS and IDS alarms during the Industroyer2 attack.

would connect a foreign device to the power grid network, the IDS would detect network traffic from an unknown device. However, it could only indicate a rough location, i.e., the corresponding subnet extending over a large area within the power grid. The FMS, in turn, would detect the presence and location of a maintenance engineer in this area. Correlating these two events at the Meta-IDS hence enables the incident response team to localize the origin of the suspicious network traffic. Then, they could determine whether this is a false alarm (e.g., the engineer forgot to schedule the maintenance) or possibly stop an ongoing attack (e.g., by disconnecting the device). In the following, we continue illustrating the benefits of *INSIDE* by presenting use cases and applications.

4 BENEFITS AND FEASIBILITY

We discuss the benefits and feasiblity of applying *INSIDE* in power grids. Specifically, we detail the use cases of *INSIDE* (Sec. 4.1), followed by an example application scenario (Sec. 4.2).

4.1 Use Cases

The combined methodology of IDS and FMS in *INSIDE* facilitates distinct use cases, which we shortly present in the following.

Cross-Domain Reassurance. Combining reports from the IDS and the FMS enables the detection of complex cyber-physical security incidents with increased certainty, which might remain undiscovered if only considered separately, while aiding to reduce false positives by considering both domains.

Adaptive Sensitivity. When the FMS triggers an alarm, the sensitivity of the IDS increases, i.e., assuming a higher level of risk. This improves the reaction to smaller deviations from the normal behavior while also reducing false positives in low-risk times.

Screening Triggers. An FMS alarm may further trigger active system screenings, e.g., active log scans, scans for new hosts, or on-site investigations. Potentially, temporal IDS components (e.g., movable sensors) could be deployed in the area of interest.

Localized Forensic. When the IDS detects suspicious network traffic, previous FMS alarms may help to identify the location of the originating device. This decreases response times, eases the reaction, and might even prevent more severe cyberattacks.

4.2 Example Scenario

We now evaluate a cyberattack against a power grid in a simulated environment, exemplifying the alarms and events from IDS and FMS processed by *INSIDE*. As shown in Fig. 1, the scenario comprises attackers that physically break into a remote facility, e.g., a solar park. The attackers attach a manipulated host to a network switch to perform a cross-facility attack against a nearby substation. Based on the recent Industroyer2 [3] attacks against the Ukrainian power grid, the attack host establishes secondary IEC 60870-5-104 connections to the substation's RTUs and issues control commands for disconnecting multiple circuit breakers to induce a blackout.

We evaluated a process-aware (P/A) IDS [15] and network-based (Net) IDS [9] on a simulated Industroyer2 attack[1]. Fig. 2 shows the time interval of the attack and the raised alarms of the IDSs. Hence, both IDSs promptly detect the attack based on the network traffic. In particular, they uncover the targeted RTUs and the attackers' IP address. However, due to the network configuration, they cannot physically locate the attacking device within the network. Here, the FMS provides valuable information for *INSIDE*: During the (preceding) physical intrusion at the solar park, an FMS sensor detecting the attackers' presence triggers an event, which coincides with the IDS alarm (cf. Fig. 2). Correlating both events, *INSIDE* can detect the attackers' location and allows for an immediate reaction, i.e., disconnecting the host. Thus, this exemplary scenario covers two use cases: *cross-domain reassurance* and *localized forensic*.

5 CONCLUSION

This paper presents *INSIDE*, a comprehensive intrusion detection approach for power grids considering network traffic and facility monitoring to swiftly detect cyberattacks. Our discussion on use cases shows that *INSIDE* is particularly suited to localize the origins of attack at an early stage, facilitating timely and targeted reactions to prevent further damage to the power grid. Future work should, however, primarily focus on the correlation between physical access violations and network traffic anomalies to reliably identify the attack's origin and to fully exploit this idea's potential.

REFERENCES

[1] Amy Babay et al. 2019. Deploying Intrusion-Tolerant SCADA for the Power Grid. In *IEEE/IFIP Int'l Conference on Dependable Systems and Networks (DSN)*.
[2] Tong Chen et al. 2020. Maintenance Personnel Detection and Analysis Using Mask-RCNN Optimization on Power Grid Monitoring Video. *Neural Processing Letters* 51, 2.
[3] ESET Research. 2022. Industroyer2: Industroyer reloaded. *We Live Security*. https://welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
[4] Jairo Giraldo et al. 2018. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput. Surv.* 51, 4. https://doi.org/10.1145/3203245
[5] Antonios Gouglidis et al. 2018. Surveillance and security: protecting electricity utilities and other critical infrastructures. *Energy Informatics* 1, 1.
[6] Jens Hiller et al. 2018. Secure Low Latency Communication for Constrained Industrial IoT Scenarios. In *IEEE Conference on Local Computer Networks (LCN)*.
[7] Tim Krause et al. 2021. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* 21, 18. https://doi.org/10.3390/s21186225
[8] Dominik Kus et al. 2022. A False Sense of Security? Revisiting the State of Machine Learning-Based Industrial Intrusion Detection. In *CPSS*. ACM.
[9] Chih-Yuan Lin et al. 2018. Timing-Based Anomaly Detection in SCADA Networks. In *Critical Information Infrastructures Security*. Springer Int'l Pub., Cham.
[10] Devashish Lohani et al. 2022. Perimeter Intrusion Detection by Video Surveillance: A Survey. *Sensors* 22, 9.
[11] Gauthama Raman M. R. et al. 2021. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation. *Cybersecurity* 4, 1, 27. https://doi.org/10.1186/s42400-021-00095-5
[12] Antonia Nisioti et al. 2018. From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. *IEEE Com. Surv. & Tut.* 20, 4.
[13] Dimitrios Serpanos and Theodoros Komninos. 2022. The Cyberwarfare in Ukraine. *Computer* 55, 7. https://doi.org/10.1109/MC.2022.3170644
[14] Cristina Stolojescu-Crisan et al. 2022. Access control and surveillance in a smart home. *High-Confidence Computing* 2, 1.
[15] Konrad Wolsing et al. 2022. Can Industrial Intrusion Detection Be SIMPLE?. In *European Symposium on Research in Computer Security (ESORICS)*.
[16] Konrad Wolsing et al. 2022. IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems. In *RAID*.

[1] We provide the PCAP files of the conducted attack at https://wattson.it/ccs22