Detection and Defense of industrial cyber-physical systems through side-channel leakage

Awaleh HOUSSEIN MERANEH
IMT Atlantique, OCIF, Cyber CNI
awaleh.houssein-meraneh@imt-atlantique.fr

Marc-Oliver Pahl
IMT Atlantique, SOTERN, Cyber CNI
marc-oliver.pahl@imt-atlantique.fr

Hélène Le Bouder
IMT Atlantique, OCIF
helene.le-bouder@imt-atlantique.fr

***Abstract*—Industrial Cyber-Physical Systems (ICPS) are intricately networked and highly integrated systems. Due to these connections, these systems are more susceptible to attacks that could result in collateral damage. The goal of this research is to improve the security of Industrial Cyber-Physical Systems (ICPS) by utilizing side-channel leakage. On the one hand, side-channel leakage is used to detect anomalies in real-time while accruing low computation and infrastructure costs. The current state of the art in sound-based anomaly detection methods is reviewed, while limitations and issues are highlighted. To overcome these limitations, a real-time sound-based anomaly detection approach is being developed. On the other hand, the study also focuses on improving the security of lightweight cryptography algorithms, which are commonly used in ICS systems with limited resources. A theoretical attack on the Linear Feedback Shift Registers (LFSR) of the Elephant algorithm is proposed and two countermeasures are suggested to counter this attack.**

***Index Terms*—Side-channels, anomaly detection, lightweight cryptography, countermeasures, real-time, sound-based anomaly detection, etc.**

I. Introduction

Industrial cyber-physical systems (ICPS) connect the cyber and physical worlds through network communication, making them vulnerable to various types of attacks, such as the Stuxnet [1]. Ensuring the security of these systems is a complex problem due to their interaction with the physical world and the wide range of applications.This research work strives to enhance the security of industrial cyber-physical systems by using side-channel leakage to detect anomalies and lightweight cryptographic countermeasures. Our main question is: *how can side-channels be used to improve ICPS security?*

We show the efficacy of side-channel-based anomaly detection in industrial systems in the first part of our research, with high accuracy and low false positives, fast detection time, and low computational and infrastructure cost. The above enables real-time detection and adaptation to real-world industrial environments, actually results in a contribution to the ICPS literature review on Sound-based Anomaly Detection (SAD) and ongoing research for ICPS on real-time SAD.

In the second part, we explore countermeasures for lightweight cryptography algorithms commonly implemented in constrained resources components of industrial systems, such as sensors, actuators, and RFID. We propose a theoretical attack on the Elephant algorithm's Linear Feedback Shift Registers (LFSR) [2], a finalist in the NIST lightweight cryptography competition, and two types of countermeasures.

The paper is organized as follows: In Section II, we provide a brief overview of related work on side-channel-based anomaly detection in ICPS and present an overview of SAD of ICPS. This section also highlights the limitations of existing SAD methods and presents ongoing research on the development of real-time SAD for ICPS. In Section III, we discuss how to counter vulnerabilities in lightweight cryptography through side-channel analysis, including a related work on lightweight cryptography in ICPS and a theoretical attack on a lightweight cryptography algorithm. The section ends with a discussion of countermeasures.

II. Industrial Anomaly Detection Systems using side-channels

Side-channel based anomaly detection is a technique for monitoring the performance of various elements within a system. By using side-channel parameter fingerprinting, this method can detect intrusions even when execution is interrupted, and identify malicious activity even when it appears to be normal in network traffic. This improves the ability to quickly respond to potential threats.

A. Related work on side-channels based intrusion detection

Previous research has explored the use of side-channel fingerprinting to detect abnormal behavior in industrial control systems. Bolboaca et al. [3] presented an approach for detecting deviation in the execution of different parts of a protocol to identify abnormal events. Dupuis et al. [4] proposed a method utilizing power consumption to detect hardware Trojans. van der Meer et al. [5] developed a system that uses electromagnetic measurements to detect behavioral changes in software running on industrial control systems. These related papers all utilize various types of leakage, such as electromagnetic, timing, and power measurements, to detect anomalies. In this thesis, we focus specifically on using sound as a leakage parameter for side-channel based anomaly detection in industrial control systems. One significant benefit is the ease and cost-effectiveness of capturing sound data through the use of low-cost equipment, making it a practical and cost-efficient method for identifying anomalies in these systems.

B. Overview of Sound-based Anomaly detection (SAD)

The field of sound-based anomaly detection (SAD) has grown in recent years, with applications in a variety of

domains including public video surveillance [6], speech analysis and recognition [7], music processing [8], healthcare [9] and predictive maintenance of industrial systems [10]. SAD involves detecting whether a machine's sound is normal or abnormal through a series of steps, as illustrated in Figure 1. These steps include sound preprocessing, feature extraction, and classification or anomaly detection algorithms.

C. Contribution: survey on SAD of ICS

The submitted survey [11] provides a comprehensive overview of the current state-of-the-art in sound-based anomaly detection (SAD) for Industrial Cyber-physical Systems (ICPS). The focus of this research is to detect anomalies in ICS using sound data. The reviewed studies are categorized and presented according to a proposed taxonomy outlined in Fig.2. The key findings of the reviewed SAD methods include: the use of mel-spectrogram as the most commonly used time-frequency domain feature, due to its efficiency and compatibility with computer vision approaches such as CNN [**?**]; the emphasis on unsupervised methods, specifically Autoencoder (AE) based on reconstruction error, for efficient anomaly detection and handling unbalanced sound data; and the use of the ROC-AUC performance metric, which plots the True Positive Rate against the False Positive Rate at different threshold values. One key point highlighted in the survey is that current SAD methods primarily focus on detecting system failures for the purpose of predictive maintenance, but have not yet been applied to detecting ICS attacks. Additionally, the survey identifies several limitations of SAD, such as sensitivity to background noise, high dimensional data, and an inability to fully characterize the behaviors of industrial systems. Additionally, the survey identifies open issues in the field, including unbalanced sound data and real-world application challenges. These challenges include the difficulty of producing abnormal data, and the need to improve SAD methods to make them more representative of industrial systems that operate in the presence of high levels of background noise.

D. Work in progress: real-time SAD for industrial systems

We developed a new platform to address the issue of unbalanced sound data in industrial systems. Our experiments are designed to overcome constraints such as sensitivity to background noise, high dimensionality data, and real-world applications. Our real-time sound-based anomaly detection approach enables industrial systems to accurately and quickly detect any deviation from expected behavior. Our ongoing research focuses on improving system performance by offline training a classification algorithm with only normal data and online prediction of new input data. We intend to optimize key performance metrics such as accuracy, false alarm rate, processing time, compatibility with other systems, and ease of deployment. The system is designed to be easily integrated with other systems, requiring minimal adjustments when used in different environments.

E. Perpectives and future works

In order to overcome the limitations of sound-based anomaly detection (SAD) in industrial control systems, one potential solution is to incorporate other parameters in addition to sound. In the literature, various parameters such as electromagnetic and power consumption have been used independently to detect abnormalities in system behavior. The more sources of data that are used to characterize the system's behavior, the better the anomaly detector algorithm is able to distinguish between normal and abnormal behavior. One perspective for future research is to explore the use of multiple parameters, such as sound and electromagnetic or power consumption, to improve the robustness of side-channel fingerprinting for anomaly detection.

III. Countering Lightweight Cryptography Vulnerabilities through Side-Channel analysis

In industrial systems (Industry 4.0), the secure real-time transmission of data from remote sensors poses challenges for traditional security measures [12].

A. Challenges in Securing Industrial Control Systems

Implementing security measures in industrial control systems (ICS) can be difficult due to the real-time command sending and data acquisition requirements, as well as resource limitations of field devices such as sensors and actuators [13].

B. Related Work on Lightweight Cryptography in ICS

Researchers have turned to cryptographic primitives, specifically lightweight methods, to address the challenges in securing ICS [14]. These methods include symmetric [15] [16] and asymmetric [17] algorithms designed to meet the real-time and resource limitations of ICS.

C. Blind-side Channel Analysis on the Elephant LFSR

We propose a theoretical attack on the Linear Feedback Shift Registers (LFSR) of the Elephant algorithm [2], a finalist in the NIST lightweight cryptography competition. Our attack takes advantage of the usage of intermediate variables dependent on the secret key and demonstrates how this structure could potentially compromise the security of a cryptosystem through side-channel analysis. To counter this attack, we propose two countermeasures.

D. Countermeasures for Lightweight Cryptography Attacks

Countermeasures for lightweight cryptography attacks include the generation of masking functions [18], randomization of LFSR [19], constant-time execution [20], physical tamper-proofing [21], and cryptographic obfuscation [22].

IV. Conclusion

In conclusion, this research improves the security of physical components of industrial systems by detecting anomalies quickly and countering the vulnerabilities of lightweight cryptography by using side-channel information.

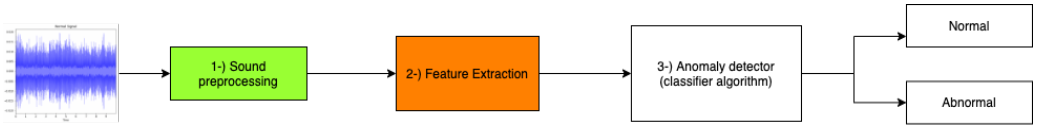

Fig. 1. Overview of SAD domain

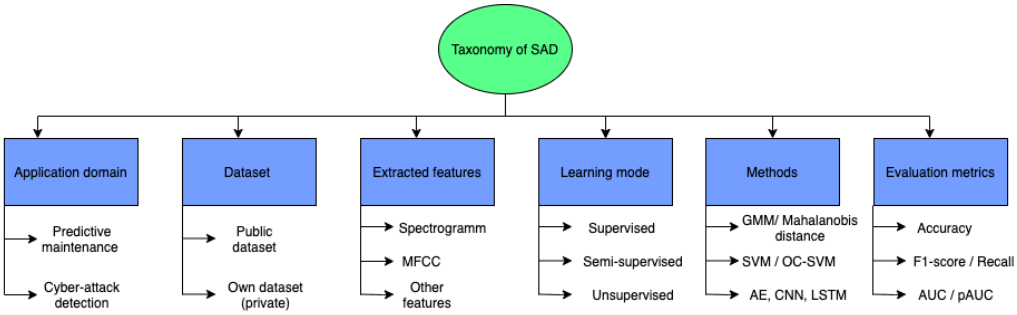

Fig. 2. Proposed taxonomy of SAD

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, symantec corp., security response*, vol. 5, no. 6, p. 29, 2011.

[2] A. Houssein Meraneh, C. Christophe, L. B. Hélène, M. P. Julien, and T. Gael, "Blind side channel on the elephant lfsr." in *Proceedings of the 19th International Conference on Security and Cryptography*, 2022.

[3] R. Bolboacă, B. Genge, and P. Haller, "Using side-channels to detect abnormal behavior in industrial control systems," in *2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2019, pp. 435–441.

[4] S. Dupuis, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "On the effectiveness of hardware trojan horse detection via side-channel analysis," *Information Security Journal: A Global Perspective*, vol. 22, no. 5-6, pp. 226–236, 2013.

[5] P. Van Aubel, K. Papagiannopoulos, Ł. Chmielewski, and C. Doerr, "Side-channel based intrusion detection for industrial control systems," in *International Conference on Critical Information Infrastructures Security*. Springer, 2017, pp. 207–224.

[6] P. Foggia, N. Petkov, A. Saggese, N. Strisciuglio, and M. Vento, "Audio surveillance of roads: A system for detecting anomalous sounds," *IEEE transactions on intelligent transportation systems*, vol. 17, no. 1, pp. 279–288, 2015.

[7] N. Borges and G. G. Meyer, "Unsupervised distributional anomaly detection for a self-diagnostic speech activity detector," in *2008 42nd Annual Conference on Information Sciences and Systems*. IEEE, 2008, pp. 950–955.

[8] Y.-C. Lu, C.-W. Wu, C.-T. Lu, and A. Lerch, "An unsupervised approach to anomaly detection in music datasets," in *Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval*, 2016, pp. 749–752.

[9] J. Ye, T. Kobayashi, and T. Higuchi, "Smart audio sensor on anomaly respiration detection using flac features," in *2012 IEEE Sensors Applications Symposium Proceedings*. IEEE, 2012, pp. 1–5.

[10] D. Henze, K. Gorishti, B. Bruegge, and J.-P. Simen, "Audioforesight: A process model for audio predictive maintenance in industrial environments," in *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*. IEEE, 2019, pp. 352–357.

[11] A. Houssein Meraneh, M.-O. PAhl, H. Le Bouder, and L. Lavaur, "Sound-based anomaly detection for industrial control systems: a survey," *IEEE systems and journal special issue on Artificial Intelligence for Next Generation Industrial Cyber-Physical Systems*, Under review.

[12] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[13] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry *et al.*, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, no. 1. Citeseer, 2009.

[14] Y. Yang, J. Lu, K.-K. R. Choo, and J. K. Liu, "On lightweight security enforcement in cyber-physical systems," in *Lightweight Cryptography for Security and Privacy: 4th International Workshop, LightSec 2015, Bochum, Germany, September 10–11, 2015, Revised Selected Papers 4*. Springer, 2016, pp. 97–112.

[15] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger *et al.*, "Prince–a low-latency block cipher for pervasive computing applications," in *Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18*. Springer, 2012, pp. 208–225.

[16] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy," in *Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21*. Springer, 2015, pp. 411–436.

[17] C.-K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, "Practical id-based encryption for wireless sensor network," in *Proceedings of the 5th ACM symposium on information, computer and communications security*, 2010, pp. 337–340.

[18] H. Maghrebi, J.-L. Danger, F. Flament, S. Guilley, and L. Sauvage, "Evaluation of countermeasure implementations based on boolean masking to thwart side-channel attacks," in *2009 3rd international conference on signals, circuits and systems (SCS)*. IEEE, 2009, pp. 1–6.

[19] W.-H. Yang, L.-C. Chu, S.-H. Yang, Y.-J. Lai, S.-Q. Chen, K.-H. Chen, Y.-H. Lin, S.-R. Lin, and T.-Y. Tsai, "An enhanced-security buck dc-dc converter with true-random-number-based pseudo hysteresis controller for internet-of-everything (ioe) devices," in *2018 IEEE International Solid-State Circuits Conference-(ISSCC)*. IEEE, 2018, pp. 126–128.

[20] G. Barthe, B. Grégoire, and V. Laporte, "Secure compilation of side-channel countermeasures: the case of cryptographic "constant-time"," in *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*. IEEE, 2018, pp. 328–343.

[21] K. Pongaliur, Z. Abraham, A. X. Liu, L. Xiao, and L. Kempel, "Securing sensor nodes against side channel attacks," in *2008 11th IEEE High Assurance Systems Engineering Symposium*. IEEE, 2008, pp. 353–361.

[22] A. Cui, Y. Luo, and C.-H. Chang, "Static and dynamic obfuscations of scan data against scan-based side-channel attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 363–376, 2016.