Detection and Defense of Cyber-Physical Attacks

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

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

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

***Abstract*—This paper focuses on the remediation of stealthy adversaries perpetrating cyber-physical attacks. Machine learning is to be applied to cover the verification of data and the discovery of the falsification of events for malicious purposes. Adversarial learning will be addressed as well. The work builds upon the concept of adversarial-learning adaptation and moving target defenses via control and artificial intelligence theory. The required challenge is to distinguish intentional attacks and component faults. Both need different reactions. The comparison of normal system operation with abnormal behaviour is the basis of all detection anomalies. We are currently exploring the possibility of recording the sound of the testbed, a fishertechnick (model of an industrial mini-factory). To differentiate between abnormal and normal sound of each engine of the testbed.**

***Index Terms*—Adeversarial learning, cyber physical systems, Machine learning, cyberattacks, side-channels...etc**

I. Introduction

Cyber-Physical Systems (CPS) is defined as the combination of digital and physical components that interact via a communication network [8]. CPS is the focus of some of the impactful security vulnerabilities in recent history, such as stuxnet or Maroochy Waste Management System, etc [5].

Consequently securing CPS is an important challenge, and it is the focus subject of industrial, university and government. CPS are highly integrated at all layers and scale. This integration with the physical world makes CPS vulnerable against some physical attacks. This research aims establishing detection methods against cyber-physical attacks. A list of possible areas from a synthesis[1] carried out by the NIST and the Universities of Virginia and Berkeley are as follows: IoT and communication, Robotics, Energy, Industrial control systems, health care, Military, Transportation and Physical security. We are focusing on industrial system control in the case of our research.

In the literature, various methods or techniques of anomaly detection are studied in the context of cyber security. However, applying these techniques to counter cyber-physical attacks (Industrial control system) is a new field of research, and researchers are increasingly contributing to it.

In this thesis, we are going to see how to combine several detection techniques to finally have a solid protection method against cyber-physical attacks, e.g. detection anomalies and side-channels. The main objective of our work is to propose a detection method based on side-channels:

1) What are the most relevant attacks against the CPS?
    - Which part of a CPS is being attacked? How is it attacked?
    - How can be identify the relevance of an attack?
    - What is the use-case of these attacks?
2) How to detect attacks using the side-channels based intrusion detection?
    - What it is the side-channels based intrusion detection for CPS?
    - How can propose new detection methods based on side-channels?
    - What makes these methods work? Can these methods be generalized?
3) How mitigate attacks?
    - How to counter for each detected attack?
    - What are we going to base our countermeasures on (what do we want to protect and how do we protect it)?

To answer the first and the second question a literature review is necessary, that's why we are currently working on a survey. Experimentation and manipulation of the data collected from the testbed will lead to the implementation of a new detection method. Then the evaluation and the validation of our detection's method will be taken into account. Finally we investigate to implement countermeasures and improving resilience.

II. Background

A. CPS security

CPS have several challenges, the security is one of them and it is important. The applications of CPS is often critically increased their importance. The widespread use components of the CPS control system and the network are vulnerable to real-time attacks.

1) Security objectives: Define the security objectives to be achieved is essential to improve the security of a system, the most famous are: *Confidentiality* designating the capability to prevent disclosure of information to unauthorized individuals or systems. The *Integrity* refers to the preservation of data without modification unless it is done by an authorized user. For any system to serve its purpose, the service must be accessible when it is needed is the role of *Availability*. And

[1] http://cyberphysicalsystems.org

Authenticity ensure that data, transactions and communications are genuine during the computation and communication process.

2) Attack taxonomy: Attacks on CPS include not only cyber-attacks from conventional IT, but also specific attacks on cyber-physical systems capable of traversing the cyber-physical domain. The literature shows that the likelihood of major attacks having a major effect on CPS is defined as follows: Eavesdropping [4], Stealthy deception attack [7], Denial-of-Services [13], Main-in-the-Middle attack [11], Jamming attack [9], Comprised key attack [2] ..etc.

B. Anomaly Detection

By detecting malicious behaviour and attacks close to real-time, appropriate counter-attack and mitigation measures can be taken to limit or prevent their effects [12]. Anomaly Detection (AD) is s an important technique to detect attacks on a system [12]. This is why it is also closely related to Intrusion Detection Systems (IDS). The authors of [10] give an overview of IDS for CPS. Detection methods are either based on statistics or use specification based models to detect deviations. Most recent statics based ADS are trained by machine learning (ML) methods.

C. Side-channels anomaly detection

Side-channels is often used to attack (retrieve secret data), by definition a side-channel attack is an attack that looks for and exploits weaknesses in security methods and procedures implementation, whether software or hardware, without challenging their theoretical robustness. One of the first side-channels attack was introduced by Kocher (1996) [6], to exploit the implementation of cryptographic algorithm or software.

Recently, the side-channels is applied to detect abnormal behavior in ICS (anomaly detection based side-channels in ICS). In [3], the side-channel information is used to detect attempts to tamper with integrated circuits. Their proposed approach is developed to detect hardware trojans horses in particular. Bolboacă et al. [1], outlined an approach to detect abnormal behaviour in industrial control systems by exploiting information from side-channel information. It consisted in measuring the deviation in the execution of the different parts of the protocol in order to detect abnormal events.

III. Advancement

The survey that we are currently writing consist to define the important notions and give a general overview of the subject based on previous work. In addition, associating each research group (working on the field) by the sub-fields they contribute most will be discussed in our paper.

we have collaborated with a research team from TUM (Technical University of Munich), whom work on anomaly detection for ICS (industrial control systems) based on sound networking. They proposed a theoretical approach, which consists of choosing a sound as the source of the physical level, and then use a passive fingerprinting technique to observe network traffic and sound measurement to detect anomalies. Although, Experiment the appoach to the real-world ICS testbed of the Cyber CNI chair is the planned project.

The comparison of normal system operation with abnormal behaviour is the basis of all detection anomalies. We are currently exploring the possibility of recording the sound of the testbed (fishertechnick) so that we can differentiate between abnormal and normal sound of each engine of the testbed. Here the leakage parameters is the sound and we plan to add (combine) the current consumption as a second leakage parameter.

References

[1] Roland Bolboacă, Béla Genge, and Piroska 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)*, pages 435–441. IEEE, 2019.

[2] Konstantinos Chalkias, Foteini Baldimtsi, Dimitris Hristu-Varsakelis, and George Stephanides. Two types of key-compromise impersonation attacks against one-pass key establishment protocols. In *International Conference on E-Business and Telecommunications*, pages 227–238. Springer, 2007.

[3] Sophie Dupuis, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. On the effectiveness of hardware trojan horse detection via side-channel analysis. *Information Security Journal: A Global Perspective*, 22(5-6):226–236, 2013.

[4] Jung-Chun Kao and Radu Marculescu. Eavesdropping minimization via transmission power control in ad-hoc wireless networks. In *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, volume 2, pages 707–714. IEEE, 2006.

[5] Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494. IEEE, 2011.

[6] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[7] Cheolhyeon Kwon, Weiyi Liu, and Inseok Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *2013 American control conference*, pages 3344–3349. IEEE, 2013.

[8] Edward A Lee. Cyber-physical systems-are computing foundations adequate. In *Position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap*, volume 2, pages 1–9. Citeseer, 2006.

[9] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E Quevedo. Jamming attack on cyber-physical systems: A game-theoretic approach. In *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, pages 252–257. IEEE, 2013.

[10] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4):1–29, 2014.

[11] Roi Saltzman and Adi Sharabani. Active man in the middle attacks: a security advisory. *A whitepaper from IBM Rational Application Security Group*, 2009.

[12] Weizhong Yan, Lalit K Mestha, and Masoud Abbaszadeh. Attack detection for securing cyber physical systems. *IEEE Internet of Things Journal*, 6(5):8471–8481, 2019.

[13] Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen. Optimal dos attack policy against remote state estimation. In *52nd IEEE Conference on Decision and Control*, pages 5444–5449. IEEE, 2013.