Usage of process mining for security in Process-Aware Information Systems

Marlon Müller[1]

Technical University of Munich, Munich, Germany
marlonbenedikt.mueller@tum.de

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.

Keywords: Process Mining · Security · Process-Aware Information Systems · Systematic literature review.

1 Introduction

In 2018 76% of businesses in Germany saw a significant risk for their business processes coming from cyberattacks on their information systems [2] and in 2023 companies in the United States reported total damages of 37.5 billion US-Dollars due to cybercrime [4]. This shows the need for companies to protect their business processes from cyberattacks.
Therefore over the last years the research in security for Process-Aware Information Systems (PAIS) has increased and has produced a vast amount of research papers. The survey [6] conducted a systematic literature review on security in PAIS and identified Process-Mining as an emerging technology that can be used to improve security in PAIS and predicted that the usage of Process Mining for security purposes in PAIS will be a focus of future research.
In 2018, already 65% of German businesses investigated log-files to identify security incidents based on the suspicion of a security incident and 33% use log-files to systematically identify security incidents without concrete suspicions [2].
Therefore Process Mining has the potential to be further enhanced to be used for security in Process-Aware Information Systems and was further researched in the last years. This paper aims to update the survey [6] in the field of Process Mining and to provide an overview over the recent advances in the usage of Process Mining for security purposes in PAIS since 2012. For this goal we will conduct a systematic literature review to outline the possible applications of Process Mining for security in PAIS.

To approach this goal we targeted the following research questions:

1. How does Process Mining contribute to security in PAIS?
2. Have the research challenges defined in [6] been addressed by recent research?

In Section 2 we will first provide some defintions and explanaitions over the terms used in this paper and evaluate the current state of the art. Section 3 evaluates other related works in this field and how this paper adds further contribution to current research. Section 4 outlines the different steps of the literature review consisting of literature search, literature selection, data extraction and the classification of security goals and security concepts. The results of the literature review are described in Section 5 and in Section 6 the results are discussed and the paper is concluded.

2 Fundamentals

In the following definitons for the most relevant terms in this paper are provided and the current state of the art is evaluated.

2.1 Process Mining

[1]

2.2 Information Security

[3]

2.3 Process-Aware Information Systems

2.4 State of the Art

The main objective of this paper is to update the systematic literature review conducted in [6] regarding the Process Mining security control and to provide an overview over the recent advances in the usage of Process Mining for security purposes in PAIS until 2012.

Summary of the survey In that survey the authors identified Process Mining as an emerging technology and gave a brief overview over the security related research regarding Process Mining in PAIS. The authors assigned Process Mining to the action type Detection and placed it in the Change phase of the process lifecycle.
In this survey the authors assigned Process Mining the action type Detection and placed it in the Change phase of the process lifecycle. They identified that the main usage of Process Mining for security purposes in PAIS is to examine the conformance of the process model with the actual process execution that could be derived from the event logs. The derived model from the event logs can be used to detect inconsitencies and anomalious behaviour that could be an indicator for security incidents like fraud or intrusions. Another use case the authors identified is to use event logs to validate the conformity of the process execution with the security policies of the company, like Role-Based Access Control

(RBAC) models or data flow policies. It was concluded, that Process Mining can be used to capture relevant information on data, ressources and task execution to find or address security issues and compliance violations and their root causes.

Research Challenges identified For security in PAIS in general (and not only regarding Process Mining) the authors identified the following research challenges:

1. Agreement on Terminology and Controls
2. Consistency with Related Fields and Concepts
3. Measurement
4. Testing
5. Evaluation
6. Detection Controls
7. Reaction Controls
8. Human Orientation

Agreement on Terminology and Controls The authors identified that the terminology used in the field of security in PAIS is not consistent and in some research no defintion of security or the protected security goals are provided.

Consistency with Related Fields and Concepts Even though research in security in PAIS is an interdisciplinary field, it was identified that except for the NIST standard for RBAC no standards or recoommendations are considered in the research.

Measurement The authors could not identify any methods or metrics are used to evaluate the effectiveness of the security controls in PAIS, while in other security areas well developed standards, e.g. the ISO/IEC 27004 standard, exist.

Testing Most of the security concepts in PAIS research are theoretical models and no method to test these models is provided.

Evaluation In the examined research the evaluation of the security in PAIS centers on post-ex evaluation using Process Mining techniques and the authors stated that It should be considered how to evaluate the security in PAIS at design or run time.

Detection Controls Invastigations of possible security incidents does not happen at run time but the authors identified that it could be benficial to detect anomalies at run time to then be able to react to them.

Reaction Controls So far, reaction controls are focused on failure handling such as exception handling or process recovery. The authors identified that it could be beneficial to react to identified security problems at design time.

Human Orientation Human factors are not considered in the research instead it only focuses on the technological aspects of security in PAIS. The authors stressed that humans are an important factor in business processes and that they also could be a security risk if they are psychologically manipulated during Social Engineering attacks.

3 Related Work

As already stated above, this paper aims to update the systematic literature review conducted in [6] and is therfore based on the results of that survey as described in Section 2.4.
The surveys [5] and [7] already conducted systematic literature reviews on the usage of Process Mining in security applications.

4 Methodology

5 Results

5.1 How does Process Mining contribute to security in PAIS?

Security goals

Security concepts

5.2 Have the research challenges been addressed by recent research?

6 Discussion and Conclusion

Bibliography

[1] van der Aalst, W.: Process Mining. Springer, 2nd edn. (2016), ISBN 978-3-662-49851-4, https://doi.org/10.1007/978-3-662-49851-4
[2] Bundesamt für Sicherheit in der Informationstechnik: Cyber-sicherheits-umfrage – cyber-risiken & schutzmaßnahmen in unternehmen (Apr 2019), URL https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/Cyber-Sicherheits-Umfrage/2018/2018_node.html, accessed: 2024-07-01
[3] Eckert, C.: IT-Sicherheit. De Gruyter, 10th edn. (2018), ISBN 978-3-11-055158-7
[4] Federal Bureau of Investigation: Internet crime report 2023 (Apr 2024)

[5] Kelemen, R.: Systematic review on process mining and security. Central and Eastern European eDem and eGov Days **325**, 145–164 (Mar 2018), https://doi.org/10.24989/ocg.v325.13, URL https://ejournals.facultas.at/index.php/ocgcp/article/view/1542
[6] Leitner, M., Rinderle-Ma, S.: A systematic review on security in process-aware information systems - constitution, challenges, and future directions. Information and Software Technology **56**(3), 273–293 (2014), https://doi.org/10.1016/j.infsof.2013.12.004, URL
[7] Silalahi, S., Yuhana, U., Ahmad, T., Studiawan, H.: A survey on process mining for security. pp. 1–6 (2022), https://doi.org/10.1109/iSemantic55962.2022.9920473, URL