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. Security in Process-Aware Information System (PAIS) is critical for almost every organisation and company, as a lack of security measures leads to vulnerabilities that can, if abused, cause severe fincancial damage. The survey [7] by Leitner and Rinderle-Ma from 2013 analysed in a systematic literature review the researched security controls in PAIS. The authors identified that the usage of Process Mining may be an emerging topic, so this paper provides a systematic literature review to analyze the advances in Process Mining research for security in PAIS and clusters the results by the security goals that are protected as well as the Process Mining applications and concpets that can be used for security in PAIS.

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 [1] and in a report by the Federal Bureau of Investigation from 2023 companies in the United States reported total damages of 37.5 billion US-Dollars due to cybercrime [5]. 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 [7] 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 [1].
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 by Leitner and Rinderle-Ma [7] 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 the following research questions were targeted:

1. How does Process Mining contribute to security in PAIS?
2. Have the research challenges defined in [7] been addressed by recent research?

In Section 2 we will first provide some defintions and explanaitions over the terms used in this paper. Section 3 evaluates 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

Below definitons for the most relevant terms in this paper are provided.

2.1 Process Mining

[9]

2.2 Information Security

TODO: IS definiton

Security Goals Later in this paper the results will be clustered according to the security goals that are protected by the applications proposed by the reviewed papers (Section 4 and 5.1). The clusters are chosen based on the security goals as described by Eckert in [3]. While the CIA-Properties (Confidentiality, Integrity, Availabilty) are commonly agreed on as the primary security goals the other security goals (especially Privacy and Accountability) are acknowledged as valid security goals but their relevance to different use cases is discussed and not commonly agreed on. Nonetheless this six security to goals according to [3] are chosen because clustering only by the CIA-Properties would not reflect the whole bandwith of security research in Process Mining for PAIS while still allowing clear distinctions between them. The following definitions of the different security goals are taken from [3].

Confidentiality Confidentiality to protect information from being disclosed to unauthorized entities. This includes the encryption of data as well as models to restrict the flow of information according to an organisations policies.

Integrity A system is considered to have integrity if it provides protection against unauthorized and unnoticed manipulation of data or processes. To guarantee integrity Access Control mechanisms are used to ensure that only authorized entities with the proper Access Rights can modify data or processes under certain constraints (e.g. limit the amount of money a user can withdraw from an account). In systems where manipulations can not be avoided (e.g. in network communication) cryptographic hashing should be used to detect manipulations and avoid further damages.

Availabilty Availability is the property of a system to be accessible and usable by autorized entities without unauthorized delays or restrictions. Delays that are a result of the normal operation of a system (e.g. concurrency over shared resources) are considered as authorized delays and therefore do not violate the property of availability.

Accountability The property of accountability (sometimes referred to as non-repudiation) is to ensure that an entity can not deny the actions it has taken. Accountability is important for Electronic Commerce to be able to prove in lawsuit that a contract has been signed by a certain entity or that a contract has been fulfilled.

Privacy The ability of individuals to control the collection, use and disclosure of their personal information and obliges organisations to protect the data of identified or identifiable individuals. Privacy is considered a human right [4] and is therfore often regulated by laws like the General Data Protection Regulation (GDPR) in the European Union.

Authenticity Authenticity is the valiation of the identity of an acting entity using unique identifiers or characteristics, such as cryptographic keys or biometric data. The act of verifying the identity of an entity is called authentication, that happens typically using user accounts with a distinct username and a secret password and/or biometric factors. The data that is used to verify the identity (e.g. the password) is called credentials to provide an abstraction of the concrete authentication method used.

2.3 Process-Aware Information Systems

The term Process-Aware Information Systems is definded by Dumas et al. [2] by combining the definitions of Information Systems (as PAIS are a special kind of Information Systems) and business processes. Their understanding of a business process is a "way for an organizational entity to organize work and resources (...) to accomplish its aims". On that foundation PAIS are defined as "a software system that manages and executes operational processes involving people, applications, and/or information sources on the basis of process models". Additionally to the formal defintion they marked that these process models are often represented using visual languages, like Petri-Net notations.

The main difference between a PAIS and a task-driven Information System (e.g. text editor or e-mail client) is described as the fact that task-driven applications are unaware of the process they are used in and therefore can neither support nor restrict the user in the process execution.

3 Related Work

In this section the survey by Leitner and Rinderle-Ma [7], that this paper aims to update, is briefly summarized and other related works are presented and explained how this paper adds further contribution to the research in Process Mining for security in PAIS.

3.1 Survey by Leitner and Rinderle-Ma from 2013

The main objective of this paper is to update the systematic literature review conducted in [7] 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.

3.2 Other Systematic Literature Reviews

The surveys [6] and [8] also 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

References

1. Bundesamt für Sicherheit in der Informationstechnik. Cyber-sicherheits-umfrage – cyber-risiken & schutzmaßnahmen in unternehmen, Apr 2019. Accessed: 2024-07-01.
2. Marlon Dumas, Wil M. P. van der Aalst, and Arthur H. M. ter Hofstede. *Process-Aware Information Systems: Bridging People and Software through Process Technology*. 2005. Cited by: 770.
3. Claudia Eckert. *IT-Sicherheit*. De Gruyter, 10th edition, 2018.
4. European Union. Charter of fundamental rights of the european union. *Official Journal of the European Union*, 55(C 326):391–407, Oct 2012.
5. Federal Bureau of Investigation. Internet crime report 2023, Apr 2024.
6. Robert Kelemen. Systematic review on process mining and security. *Central and Eastern European eDem and eGov Days*, 325:145–164, Mar. 2018.
7. M. Leitner and S. Rinderle-Ma. A systematic review on security in process-aware information systems - constitution, challenges, and future directions. *Information and Software Technology*, 56(3):273–293, 2014. cited By 58.
8. S. Silalahi, U.L. Yuhana, T. Ahmad, and H. Studiawan. A survey on process mining for security. pages 1–6, 2022. cited By 3.
9. Wil van der Aalst. *Process Mining*. Springer, 2nd edition, 2016.