The Danger Within: Insider Threat Modeling Using Business Process Models

Von der Assen, Jan ; Hochuli, Jasmin ; Grübl, Thomas ; Stiller, Burkhard

DOI: https://doi.org/10.1109/csr61664.2024.10679492

The Danger Within: Insider Threat Modeling Using Business Process Models

Jan von der Assen[1], Jasmin Hochuli[1], Thomas Grübl[1], Burkhard Stiller[1]
[1]Communication Systems Group, Department of Informatics, University of Zurich UZH, CH–8050 Zürich, Switzerland
[vonderassen, gruebl, stiller]@ifi.uzh.ch, jasmin.hochuli@uzh.ch

***Abstract*—Threat modeling has been successfully applied to model technical threats within information systems. However, a lack of methods focusing on non-technical assets and their representation can be observed in theory and practice. Following the voices of industry practitioners, this paper explored how to model insider threats based on business process models. Hence, this study developed a novel insider threat knowledge base and a threat modeling application that leverages Business Process Modeling and Notation (BPMN). Finally, to understand how well the theoretic knowledge and its prototype translate into practice, the study conducted a real-world case study of an IT provider's business process and an experimental deployment for a real voting process. The results indicate that even without annotation, BPMN diagrams can be leveraged to automatically identify insider threats in an organization.**

***Index Terms*—Threat Modeling, Insider Threats, Risk Management, Business Process Modeling, BPMN**

I. Introduction

With the technological shift, new cybersecurity threats arise, reaffirming that enterprises face a highly active threat landscape. For example, a recent attack on an AI-based facial recognition system caused losses of over 77 million USD [1]. While empirical evidence justifies the attention to such technology and security trends, the relevance of less technically materialized threats should not be underestimated. To share one example of exploiting processes rather than systems, the frequency of SIM swapping attacks has increased by 400% [2].

Thus, it is critical to consider information systems wholistically, as emphasized by the National Institute of Standards and Technology (NIST), which distinguishes cybersecurity efforts into system-level, process-level, and organization-level [3]. One critical set of threats can be summarized under the term "insider threats". Here, a trusted person or organization intentionally or unintentionally acts as a threat actor. Such attacks are especially difficult to mitigate since technical measures only provide partial defense, and the attackers hold elevated privileges [4]. In one motivating example, the Swiss government gradually rolled out a public COVID-19 certification system. In a wide-scale public security test, over 100 vulnerabilities were discovered and mitigated [5]. Nevertheless, thousands of forged certificates were discovered later. The attackers did not exploit a technical flaw in the system. However, they used authorized personnel from private testing centers to issue forged certificates. In that sense, a weakness in the business process (*e.g.,* absence of a two-person rule, lack of background checks) rather than a technical vulnerability (*e.g.,* breach of authentication or authorization) was exploited [6].

One approach to identify threats and mitigate them at design time is threat modeling. In threat modeling, an abstraction of the target asset is created, enabling experts to reason about the relevant threat events. Threat modeling has emerged as a useful risk-based process due to its ability to work with various abstraction levels (*e.g.,* an architectural diagram or a piece of software) and different representation methods (*e.g.,* data-flow or use case diagrams) [7]. However, the application of threat modeling is often focused on technical aspects of the system. In the literature, there is a lack of methods and studies that apply threat modeling for insider threats. Furthermore, the view on the business processes encompassing different systems is often not considered, opposing the view of industry professionals who argue for capturing diverse viewpoints [8].

Due to these limitations, this paper explores the practicality of leveraging process models for threat modeling and therefore hypothesizes whether existing process models can serve as an input to identify relevant insider threats. More specifically, the hypothesis considers the usefulness of BPMN models that are processed by a security expert but not enriched by additional domain-specific annotations. Based on this automation, insider threat modeling could be included as a lightweight activity identifying specific procedural vulnerabilities around a technical information system. Thus, the work at hand follows the exploration of this question while presenting the following contributions. At the core, several studies describing insider threats are analyzed and ontologically combined into *(i)* a knowledge base. In addition to the threat events, a mapping to the BPMN elements is proposed. This knowledge base enables the development of *(ii)* a prototypical implementation that extracts relevant insider threats from BPMN diagrams. Two experiments are conducted to assess the usefulness of this approach. First, a *(iii)* case study, where the approach is deployed against a real-world business process of an IT service provider. In the second evaluation, *(iv)* the approach is applied to a non-commercial setting by experimentally testing the approach's viability to provide an expert-based analysis of the Swiss voting process.

This paper is structured as follows: after surveying the state-of-the-art in Section II, the architecture and implementation of the approach are described in Section III. The evaluation of the approach is provided in Section IV. Finally, Section V highlights concluding remarks and outlines future work.

II. Related Work and Problem Statement

A semi-systematic literature review targeted Google Scholar, Swisscovery, and IEEE Xplore using variations of the keyword string "insider threat modeling." After analyzing the references of these results (*i.e.,* performing snowballing), the overview, shown in TABLE I was obtained, which excluded papers not relating to security. In the table, these studies are summarized based on publication year, objective (*i.e.,* view), artifactual aspects, and methodology. Furthermore, whether a prototype is provided and insider attacks play a key role was analyzed. Based on 14 papers, two questions were investigated. *(i)* How can process models, especially BPMN, be leveraged in security management, especially within the threat modeling process? *(ii)* How does research on threat modeling consider insider threats?

Related literature on insider threat modeling can be grouped into three bags. First, numerous papers investigate the dynamics of insider threats from a psychological perspective. The focus lies on insider attacks' organizational factors and impacts. For example, [4] leverage game theory as a guiding theoretic model, yielding a simulation approach to explain the organizational factors between attacker and defender. While these studies are relevant for formulating knowledge bases, they do not directly contribute to the research questions.

The second bag of studies presents insights into threat modeling or other risk-based methods for insider threats. For example, [9], [10], [11] use different methods, such as attack graphs or strategic planning methods, to demonstrate how insider threats can be integrated into the risk management of an information system. None of these solutions provide an automated threat modeling approach or focus on business process models as an existing asset to exploit.

Finally, several solutions either cover threat modeling of insider threats or leverage BPMN as a specific abstraction of business processes to manage cyber attacks. For example, [14] presented a methodology and prototype to check the compliance of a process through a BPMN model with previously defined security requirements. In addition, they provided evidence of BPMN as a useful abstraction for security modeling. However, the scope of the work did not focus on insider threats and required a previous requirements specification step.

TABLE I
Overview of the Related Work

Source	*View*	*Aspect*	*Methodology*	*Prototype*	*Insider*
[9] 2018	RA	IS	Several	-	yes
[10] 2014	RA	IS	NIST	ADVISE	yes
[11] 2008	RA	Process	TRIP	-	yes
[12] 2005	TM	IS	Challenge Graph	-	yes
[13] 2014	TM	Process	Fault Tree Analysis	Automated FTA	yes
[14] 2020	TM	Process	SQUARE	-	no
[15] 2017	TM	Process	SecBPMN	Query Engine	no
[16] 2023	TM	Process	ENISA, OWASP	BPMN annotator	no
[17] 2021	TM	Process	NIST-based	coreLang	no
This 2024	TM	Process	Knowledge Map	BPMN modeler	yes

RA=Risk Assessment, TM=Threat Modeling, IS=Information System

Similarly, [16] have relied on additional annotations to model threats based on existing frameworks provided by ENISA and OWASP. In the conducted case study, they present additional evidence on the usefulness of BPMN. However, their approach requires additional annotations and has not focused on insider threats. Regarding approaches focusing on insider attacks, [12] models insider attacks using graphs, thus not considering the process abstraction. [13] is likely the most closely related study since it analyzes processes to find hazardous vulnerabilities. However, only two threats (*e.g.,* data exfiltration and sabotage) are included and for each of them a different method for the analysis is proposed. This complicates it and lacks a holistic view of all possible insider attacks.

Based on these findings, the questions asked in the literature review can be answered. None of the approaches analyze business process artifacts to perform insider threat modeling effectively. Consequently, the research demonstrates that BPMN can be a valuable resource for security discussions. Especially [16] demonstrates that by using annotations, BPMN can be used for threat analysis. Since this approach was deployed in a non-commercial setting and relied on annotations, multiple avenues of research are available. In summary, the following limitations and resulting research questions drive this study.

- ***Q1*** Is it practical to leverage existing BPMN models as an input for automated threat modeling of insider threats?
- ***Q2*** Can such an approach leverage real-world BPMN models without the introduction of security-specific extensions of the visual language?
- ***Q3*** How well does such an automated approach perform in commercial and non-commercial settings?

III. Architecture and Prototype Implementation

To develop a solution that provides the means to conduct practical experiments on BPMN models for automated insider threat modeling, the architecture shown in Fig. 1 is proposed. A five-step process consisting of Objective Identification, Assessment, Decomposition, Threat, and Vulnerability Identification is followed as a guiding meta-model. In the following paragraphs, each step in the meta-model is introduced to outline how the step in the proposed approach fulfills it.

A. Overview

To perform the *objective identification* step, the architecture relies on the formulation of key security objectives. This involves *(i)* the identification of a critical process and formulating security properties through *property filters* (*e.g.,* Confidentiality, Integrity). Identifying a relevant process can be informed by an implicit goal. For example, a threat modeling workshop may be tasked to model a specific system, yielding the surrounding business process. Alternatively, business metrics used in risk management such as revenue or earnings before tax and interest (EBIT) [18] can be used.

To *assess* and *decompose* the asset and its interactions, the proposed methodology *(ii)* involves modeling the process using BPMN. Ideally, BPMN models are already available and can be used for this security analysis. Thus, no additional

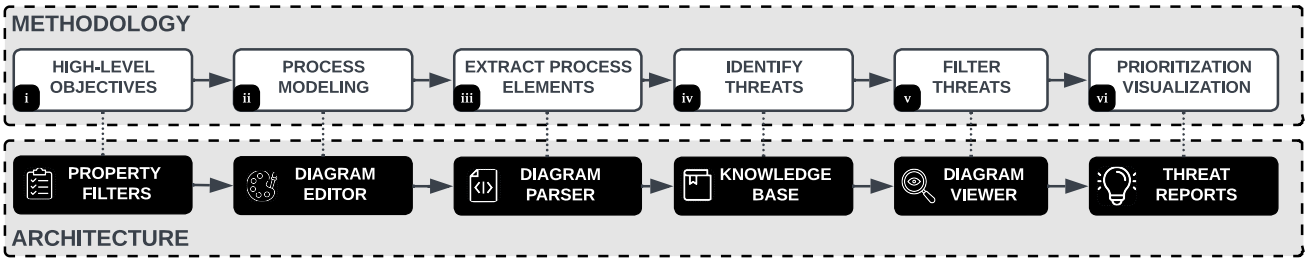

Fig. 1. Methodology (top) and Architecture (bottom) of the Proposed Approach

annotations are mandated besides those defined in the BPMN standard, which can be modeled using a *diagram editor*. This enables *(iii)* the various interactions performed in the business process to be automatically extracted by a *diagram parser*.

Threat Identification is the most novel aspect of the solution. To identify insider threats based on previously extracted process elements, a *knowledge base* was built to synthesize the threats described in the literature. First of all, multiple sources were studied to elicit potential insider threats. After surveying several studies, 99 insider threats were elicited (see Fig. 2) from five sources [19], [11], [20], [10], [21]. The extracted knowledge was then manually structured using a set of security principles. The commonly used principles such as *Confidentiality*, *Integrity*, *Availability* were adopted. Furthermore, *Authenticity* was included based on the reasoning in [11], [22]. Finally, *Authenticity* was included due to its mention in [23], [22].

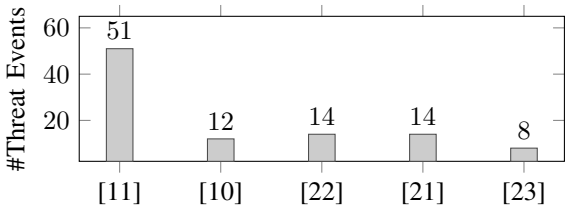

Fig. 2. Knowledge Base Sources: Insider Threats Elicited per Source

After analyzing each threat, removing duplicates, and clustering them according to the principles, it was analyzed whether each threat could be meaningfully mapped to a BPMN element. For example, the *tampering of HTTP-cookies* could be a relevant attack of an (inside) threat actor. However, comparing it against the elements in the BPMN standard, none realistically relate to it. Thus, such threat events were aggregated under the more abstract *data corruption* threat.

Then, to provide a mapping to the BPMN standard, each threat event was mapped to a set containing one or more BPMN elements representing an attack entry point. For example, the threat of maliciously *viewing confidential data* by an insider is relevant at different points. While it could be done at rest (*e.g.,* when an insider can access a *data store*) it can be done before ingestion (*i.e.,* during a *receive task*). Thus, each threat was reviewed against the BPMN elements while focusing on areas that involve human interaction (*e.g.,* activities, data objects, and message flows).

During the actual usage of the knowledge base for *(iv)* threat identification, the knowledge base can be queried against the previously extracted elements (see *(iii)*). The resulting list of threats must then be reviewed and *(v)* filtered with domain knowledge. Again, experts need to consider whether a threat actually applies since BPMN models show a high degree of abstraction. For example, the knowledge base might yield a *credential theft* threat. However, there may be additional technical controls in place (*e.g.,* multi-factor or biometric authentication) that are not visible from a procedural view. Thus, the resulting threat model is the subset of automatically derived threats that experts deem realistic.

The final stage of *vulnerability identification* is achieved through visualization of the threat model. The goal of the threat modeling process is to identify areas of concern (*e.g.,* process steps to include additional technical or procedural controls). Since the input to the approach is already a visual representation (*i.e.,* a BPMN diagram), these areas can be highlighted. Therefore, the procedural steps in the threat model can be extracted. [18] argues to quantify risks – thus, one could leverage the enterprise's data to assess the impacts of the data. Alternatively, the process steps could be color-coded to highlight the number of threat events per element within the *diagram viewer*. However, this requires user awareness since a higher number of threats may not necessarily represent a higher risk.

B. Web-based Implementation

The prototype implementing the previously described methodology was developed as a web-based toolkit. Two reasons supported this design decision: first, the availability of mature BPMN diagram editors, and second, the ability to implement a completely offline data storage component. The tool follows the methodology from Fig. 1. Thus, the main design decisions are elaborated per step.

On the first page of the application, the user defines one or more security principles that are of concern. Although, in reality, every principle is likely relevant, a hint suggests starting with the most impactful one for the business process. Then, a diagram editor provided by the *bpmn.io* JavaScript library [24] is rendered, allowing the user to upload a BPMN diagram. Using the library, all the process elements are extracted. Then, a JavaScript implementation of the previously

compiled knowledge base is queried directly in the browser. This set of identified threats is then visualized, grouping them per process element that represents their attack entry. The user then iterates through them by opening each threat in the main window. There, each threat event is described in detail. The user can then add threats that appear relevant to the threat model, which is stored in the browser's memory. After this filtering step, the report page visualizes the selected threats. The diagram is rendered again, indicating in colors how many threats were selected per element and adding numbering to simplify the identification of each element. Furthermore, the sidebar summarizes the threats per element. Finally, since threat modeling is an iterative and collaborative endeavour [7], the *threat report* can be exported as a PDF, SVG, or XML file that can be loaded into the editor to repeat the process.

Due to space constraints, the solution's user interface is only illustrated in Section IV. The solution's source code and a publicly accessible instance of the running prototype are available through [25].

IV. Evaluations

Evaluating threat modeling approaches is inherently complex. In [18], it is argued that cybersecurity (and broader information security) risks are emerging risks. For such risks, there may not be ground truth information (in this context: an exhaustive list of threats with complete information on attack probability or impact) [26]. Thus, aligned with the initial research questions, the evaluations aim to answer whether the approach can be practically applied to real-world processes. Aside from testing the input (existing BPMN models) and context (processes used by real companies), the output is assessed. Here, the focus is on the relevance of the output, *i.e.,* whether the solution can provide relevant suggestions. It must be acknowledged that the evaluations cannot demonstrate that all threats are identified since some may not even be known. Thus, a case study in a commercial setting and an expert-based field experiment within a governmental and non-commercial context was conducted.

A. Case Study: IT Service Provider

The first evaluation comprises a participatory case study described in [27]. Following this methodology, academic and non-academic stakeholders participate in the study, representing the subject and domain experts. Importantly, the complexities and context of a real-world setting must be preserved. This is important for providing an unbiased view of the usefulness of the BPMN models as an input (*i.e.,* ***RQ1***).

Two requirements were defined for potential enterprises: the existence of formalized processes through BPMN and commercial operation. Several companies did not fit the criteria. For example, a software engineering startup did not hold formally defined processes. Four were sent a proposal to participate after surveying companies that fit the requirements. The company that enabled the case study provides IT solutions for social insurance organizations, helping them digitize their business. The business process provided by said enterprise defines the tasks a clerk in an insurance organization needs to accomplish when an insuree requests an insurance number and card. The process involves ten tasks, two data stores, two artifacts, and an intermediate catch event to receive a message. It comprises three swim lanes, with the clerk being the central actor. Due to its size, the full process is available through [25].

TABLE II
Threat Report of Case Study

Asset	*Type*	*Insider Threats*
Business Case File	Data Object	DA, DV, DT, DD
Case File, Clarification Document	Data Object	DA, DV, DT, DD
Personal Register	Data Store	DA, DV, DC, DD
Citizens Platform	Data Store	DA, DV, DC, DD
Check Further Clarifications	User Task	DC, SC, DD
Check Answer	User Task	DC, SC, DD
Check Employee in System	User Task	DC, SC, DD
Check Responsibility	User Task	DC, SC, DD
Process Return Correspondence	Message Receive	DV, MI
Sign Up Insuree	Message Receive	DV, MI
Order Insurance Number	Message Send	DT, DC
Send Insurance Card	Message Send	DT
Notification Letter	Message Send	DC

DA=Data Acquisition, DV=Data View, DT=Data Transfer, DC=Data Corruption, DD=Data Deletion, SC= System Control Manipulation, MI=Malware Installation

After receiving the process description, it was transformed into the target format (*i.e.,* BPMN 2.0), and sensitive information was removed to preserve the confidentiality of technical details. Then, the process was loaded into the application, and each step (see Section III) was executed. Thus, the enterprise defined the key security requirements based on which the filtering was conducted, where each decision was documented for later review by the domain experts. Finally, the resulting threat model and its creation were presented to the company.

Fig. 3 illustrates the final report page of the case study – highlighting the threat overview, which is grouped by asset. Additional information on each threat is rendered below the process diagram. The threat model (see TABLE II) comprised seven key threats (*e.g.,* Data Acquisition, Data View) and thirteen assets (*i.e.,* process steps or artifacts found in the process). The most critical areas were the *Case File*, the *Personal Register*, and the *Citizen Platform*. Thus, these key assets are highlighted, and the number of applicable threats is displayed.

After the methodology and results were presented, a feedback session was held involving the enterprise's security manager (CISO), its deputy, and the process architect. The results of the semi-structured interview are summarized subsequently.

- **True positives: are the threats relevant and known?** All discovered threats were considered relevant by the experts. Furthermore, the experts agreed on their importance since the confidentiality of the information (digital and physical) is highly sensitive. The company already considered these threats in its threat model and implemented security controls.
- **False negatives: are there threats that were not found?** The security expert indicated that injection, privilege es-

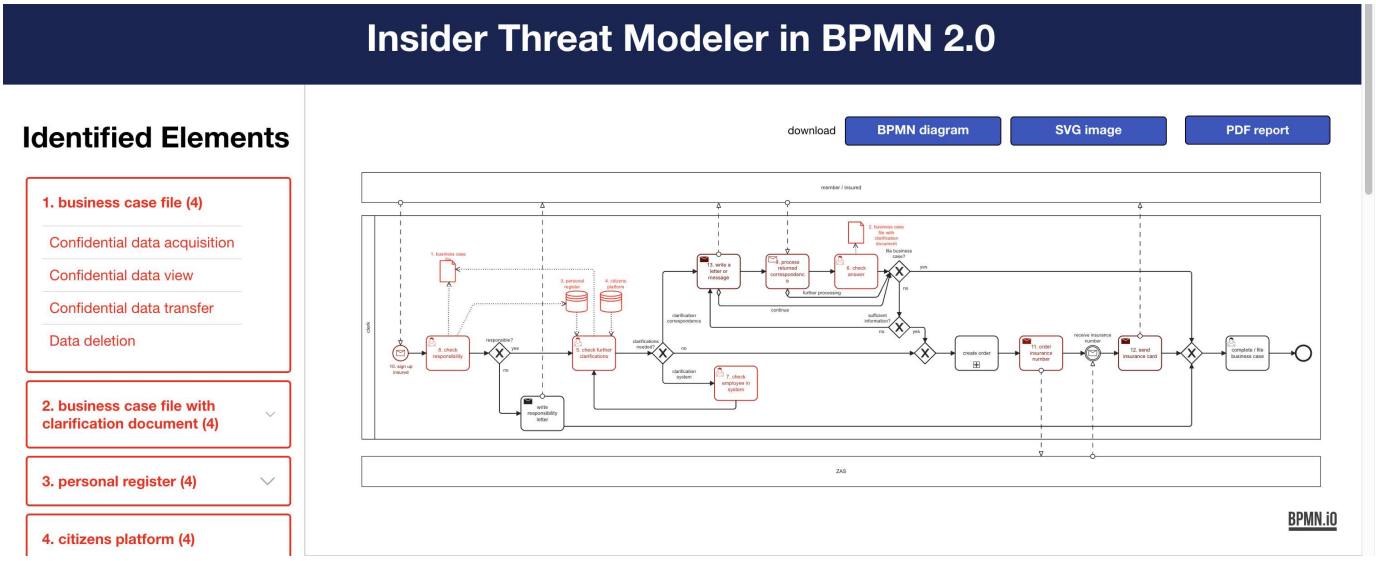

Fig. 3. Report Page of the Threat Model Conducted for the IT Service Provider

calation, and social engineering attacks could be relevant in addition to the elicited threats.

- **Are there countermeasures or controls already implemented where the critical elements were identified?** According to the CISO, the organizational level adopted controls such as employee education, fine-grained access control, and confidentiality agreements. Furthermore, an audit trail ensures that any modifications can be traced. For critical decision-making steps, the four-eyes principle is integrated. From a technical perspective, *Data Deletion* is mitigated through backup and archiving procedures. *Data Corruption* through logging and *Malware Injection* through filtering and sanitization.
- **Are there assets (*i.e.,* process elements), where other threats than the ones identified could be relevant?** The CISO expressed that the database could be attacked through a denial-of-service attack using a complex database query.

Based on this interaction, it could be concluded that the approach can suggest relevant threats by relying on the BPMN model. However, the output will not exhaustively represent all feasible attacks. This is important in relation to several biases commonly found in risk management [18]. Thus, communicating the results requires careful consideration.

The company has already considered all the threats through its security program. While one could conclude that the solution could not stipulate "novel threats," another interpretation is that the enterprise's program is already quite mature. For example, procedural controls such as the four-eyes principle were not found in the motivating example shared at the beginning of the paper [6]. In that sense, the presence of control mechanisms indicates that the provided threats are relevant enough to invest in their mitigation.

B. Field Experiment: Remote Voting

In the second evaluation, a non-commercial setting was considered, which exhibits different characteristics. For example, [28] argue that decision-making, which is needed to secure governmental information systems, is much more difficult due to the decentralized nature of authority.

This experiment considered an established but not formalized business process. More specifically, the process of remote postal voting described in the security analysis [29] was examined. In the paper, the wholistic voting procedure spanning several processes and actors is described. For this experiment, only the process of casting a vote through different channels, storing, and tallying the votes is used. The experiment investigates whether a security professional can leverage the application to formalize the process using BPMN and conduct a meaningful insider threat identification process. The expert in the study has several years of technical work experience in security engineering but no domain knowledge of voting systems and processes. The models created during the experiment are available in [25].

First, the security expert was provided with the description from [29] and the instruction to focus on the *casting*, *storage*, and *tallying* aspects. After opening the tool, the security provider focused on *Integrity* and *Confidentiality* as key objectives. Then, the security expert formalized the process using the built-in BPMN editor. The expert modeled the different voting mechanisms through three swim lanes, representing the different actors (*i.e.,* voters, postal service, municipality). In the third stage, the expert navigated the threats identified by the platform, performing the filtering that resulted in the final threat model. Thus, seven unique threats were analyzed, some affecting several steps. After the filtering step, the threat model comprised 16 threat events affecting 10 assets (*i.e.,* process steps). If no filtering by means of security goal definition or threat applicability analysis had been done, the result

would have comprised 52 threats. The experiment lasted two hours, including familiarization with the application's usage, understanding the voting domain, and actual execution.

Once the threat model was created, the author of [29] was contacted to assess the resulting threat model. Since there are no ground-truth threat models, the author's expertise is used for comparison since the author is considered an expert in this field. The resulting threat report was shared as a PDF, and the process model contained the automatically generated color highlighting. After 15 minutes of studying, the following findings were obtained using a semi-formal interview:

- **True positives: are the threats relevant and known?** According to the author, all threats identified in the report are highly relevant to the scope of the remote postal voting process. Furthermore, the threat model highlighted the highest number of threats for the areas deemed most sensitive by the author. Here, the tool explicitly highlighted two areas: *(i)* the temporary storage between receiving votes and starting the tallying process was highlighted, and *(ii)* the store-and-forward processing in the postal service. A malicious actor could view, corrupt, or destroy the material. Interestingly and unbeknownst to the security expert, this threat has previously occurred. In 2020 [30] a local election worker (*i.e.,* inside actor) destroyed voting material, causing a change in the results.
- **False negatives: are there threats that were not found?** The author highlighted multiple false negatives. Most importantly, artefact corruption (*i.e.,* modifying voting material) would be relevant at almost all steps in the process. However, the threat model indicated it in eight out of ten steps. Furthermore, deletion attacks were missing (*i.e.,* destroying or hiding voting material). This is attributed to the threat's association with *Availability* in the knowledge base. Hence, it was falsely excluded. Finally, the threat of introducing malicious code could be more prevalent, as modeled by the security expert.
- **Are there countermeasures or controls already implemented where the critical elements were identified?** The critical threats modeled by the security expert were mostly focused on the postal service and the municipalities' storage facilities. According to the author's research, the postal service already includes countermeasures and has been audited against several related standards (*e.g.,* ISO 27001, ISO 22301). However, the author stated that the key area indicated by the threat model (*i.e.,* municipal vote storage) is not necessarily covered by physical security controls. This is magnified by the fragmented view since every municipality operates differently and since no central coordinator is overviewing the process.
- **Are there assets (*i.e.* process elements), where other threats than the ones identified could be relevant?** According to the author, the BPMN representation includes all relevant procedural assets. Importantly, this does not prove that it actually reflects the real-world process since the input process diagram is already an abstraction.

Based on these questions and the additional views expressed by the author, several conclusions can be drawn from the experiment. First, the prototype was able to identify relevant threats. In a different setting, for example, if the prototype was applied on the municipal level, discussions on the security of the process could be stipulated. The sensitive area of vote storage could lead to a discussion on additional physical and digital control mechanisms (*e.g.,* four-eyes principle, two-key lockbox, statistical plausibility tests).

However, the application of the prototype also led to the discovery of multiple limitations. *(i)* The time required to adopt the tool and formalize undocumented processes may be too costly and only efficient for critical procedures. *(ii)* Understanding the threat reports requires some interpretation since the descriptions are generic and not domain-specific. For example, in the threat model, a key threat is that the *voting proof* could be stolen from the envelopes. In the PDF, this proof is simply referred to as *credential* and thus requires some time for interpretation. The key limitation expressed by the author is *(iii)* that in a non-commercial setting, the initial prioritization is not as sensible. For example, one could argue that integrity (*e.g.,* forging votes) is more impactful than confidentiality (*e.g.,* losing ballot privacy). However, in practice, different stakeholders may hold different views. Thus, the author argued that in such a setting, everything is relevant.

In addition to these findings related to the overall usage of the tool and its approach, the author suggested usability improvements (*e.g.,* numbering the threats, visualizing them within the diagram).

C. Synthesis and Comparison with Related Work

At this point, the study's initial research questions are reviewed, and findings are highlighted and compared to related work. Regarding ***Q1***, the real-world deployments demonstrated that the underlying approach could successfully identify relevant threats. Furthermore, the experiments indicated that the output can foster actionable discussions. In comparison, [13] argued that process abstraction is suitable to model insider threats. However, this approach was only illustrated and not deployed for a real-world scenario. Similarly, [17] performed process-based insider threat analysis; however, the resulting model was not reviewed by a user. Thus, although one must be cautious about generalizing based on case studies, evaluating this work provides insights into the approach's real-world practicality. Overall, the key limitation of this aspect is the proper communication in the domain's context.

With respect to ***Q2***, the prototype worked well with existing process descriptions and when onboarding a security expert to create a new one. [16] demonstrated that through annotations introducing technical system details (*e.g.,* log level, message size), it is possible to identify threats automatically. In this work, no modifications from the BPMN standard were required. Nevertheless, an overarching concern discovered in such process-based techniques lies in the availability of such data – further research is needed to answer whether it is cost-effective to create new models solely for this purpose.

Overall, the approach appears effective in identifying *relevant* threats (***Q3***). Nevertheless, filtering threats may be less practical in non-commercial settings. In that sense, it questions related studies that have focused only on governmental domains [16]. A key limitation of the work at hand is the potential presence of false negatives since the filtering may exclude certain threats. From a methodological perspective, experiments conducted in this work carry a participatory character and are thus subject to the limitations described by [27]. In addition, while case study research enables collecting rich experience on the methodology, generalization is an issue due to the low number of samples.

V. Summary and Future Work

This paper proposed a threat modeling approach to identify insider threats using BPMN process models. The approach and its implementation cover eliciting security requirements, modeling, and extracting information from existing processes. Then, the threat identification phase leverages a bespoke knowledge base that synthesizes findings from several studies and maps them to BPMN elements. After filtering threats, a simple prioritization is suggested, and threats are visualized in the procedural context. The experiments (*i.e.,* a case study and field experiment) conducted using the platform suggest that existing BPMN models can serve to identify relevant threats using the approach. This includes real-world settings – even when considering commercial and non-commercial settings. Thus, it can be concluded that BPMN is an effective tool for understanding the procedural context surrounding information systems and how to secure it using threat modeling. Based on the deployment against real-world scenarios, it is suggested that procedural threat modeling can serve as a critical abstraction to model the boundaries between systems and operators.

The key limitations include the effort required by analysts, the presence of false negatives, and the prioritizing of threats based on security requirements in non-commercial settings. Thus, future work will include diversifying the experiments and applying other risk-based prioritization methods (*e.g.,* quantitative simulations, and business impact analysis).

Acknowledgment

This work was supported by the University of Zürich UZH. Furthermore, the authors thank Christian Killer for his time.

References

[1] The Mitre Corporation, October 2023. [Online]. Available: https://atlas.mitre.org/pdf-files/MITRE_ATLAS_Fact_Sheet.pdf

[2] Australian Communications and Media Authority, "Reducing the impact of unauthorised high-risk customer transactions ," February 2022.

[3] R. Ross, "NIST SP 800-37, Revision 2," *Guide for Applying the Risk Management Framework to Federal Information Systems*, 2018.

[4] A. P. Moore, K. A. Kennedy, and T. J. Dover, "Introduction to the special issue on insider threat modeling and simulation," *Computational and Mathematical Organization Theory*, vol. 22, pp. 261–272, 2016.

[5] NCSC, "Results of the COVID-19 certificate security tests ," 2021. [Online]. Available: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/covid-zertifikat-pst.html

[6] swissinfo.ch, "Thousands of fake Covid-19 certificates uncovered in Switzerland," December 2023. [Online]. Available: https://www.swissinfo.ch/eng/identities/thousands-of-fake-covid-19-certificates-uncovered-in-switzerland/47214700

[7] J. von der Assen, M. F. Franco, C. Killer, E. J. Scheid, and B. Stiller, "CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling," in *IEEE International Conference on Cyber Security and Resilience (CSR 2022)*, Rhodes, Greece, July 2022, pp. 1–8.

[8] "Threat Modeling Manifesto," November 2020. [Online]. Available: https://www.threatmodelingmanifesto.org

[9] N. A. Hashim, Z. Z. Abidin, A. Puvanasvaran, N. A. Zakaria, and R. Ahmad, "Risk Assessment Method for Insider Threats in Cyber Security: A Review," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018.

[10] N. Nostro, A. Ceccarelli, A. Bondavalli, and F. Brancati, "Insider Threat Assessment: A Model-Based Methodology," *SIGOPS Oper. Syst. Rev.*, vol. 48, no. 2, p. 3–12, 2014.

[11] K. Brancik, *Insider computer fraud: an in-depth framework for detecting and defending against insider IT attacks*. CRC Press, 2007.

[12] R. Chinchani, A. Iyer, H. Ngo, and S. Upadhyaya, "Towards A Theory Of Insider Threat Assessment," in *International Conference on Dependable Systems and Networks*, Yokohama, Japan, 2005, pp. 108–117.

[13] M. Bishop, H. M. Conboy, H. Phan, B. I. Simidchieva, G. S. Avrunin, L. A. Clarke, L. J. Osterweil, and S. Peisert, "Insider Threat Identification by Process Analysis," in *2014 IEEE Security and Privacy Workshops*. San Jose, CA, USA: IEEE, 2014, pp. 251–264.

[14] S. Zareen, A. Akram, and S. Ahmad Khan, "Security Requirements Engineering Framework with BPMN 2.0.2 Extension Model for Development of Information Systems," *Applied Sciences*, vol. 10, no. 14, 2020.

[15] M. Salnitri, F. Dalpiaz, and P. Giorgini, "Designing secure business processes with SecBPMN," *Software and systems modeling*, vol. 16, no. 3, pp. 737–757, 2017.

[16] D. Granata, M. Rak, G. Salzillo, G. Di Guida, and S. Petrillo, "Automated threat modelling and risk analysis in e-Government using BPMN," *Connection Science*, vol. 35, no. 1, p. 2284645, 2023.

[17] S. Hacks, R. Lagerström, and D. Ritter, "Towards automated attack simulations of BPMN-based processes," in *2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)*, Gold Coast, Australia, 2021, pp. 182–191.

[18] S. Hunziker, *Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward*. Springer, 2021.

[19] G. Magklaras and S. Furnell, "Insider Threat Specification as a Threat Mitigation Technique," in *Insider threats in cyber security*. Springer, 2010, pp. 219–244.

[20] P. G. Neumann, *Combatting Insider Threats*. Boston, MA: Springer US, 2010, pp. 17–44.

[21] B. A. L, "Information Security Insider Threats in Organizations and Mitigation Techniques," in *2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC)*. Nagercoil, India: IEEE, 2019, pp. 1–4.

[22] E. Wheeler, *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier, 2011.

[23] W. Stallings, *Network Security Essentials: Applications and Standards*. Pearson, 2016.

[24] Camunda Services GmbH, "Web-based tooling for BPMN, DMN and Forms." [Online]. Available: https://bpmn.io/

[25] J. Hochuli and J. von der Assen, April 2024. [Online]. Available: https://github.com/jvdassen/InsiderThreatModeling

[26] A. Jones, J. Kuehnert, P. Fraccaro, O. Meuriot, T. Ishikawa, B. Edwards, N. Stoyanov, S. L. Remy, K. Weldemariam, and S. Assefa, "AI for climate impacts: applications in flood risk," *npj Climate and Atmospheric Science*, vol. 6, no. 1, p. 63, 2023.

[27] C. Hudon, M.-C. Chouinard, M. Bisson, A. Danish, M. Karam, A. Girard, P.-L. Bosse, and M. Lambert, "Case Study With a Participatory Approach," *The Annals of Family Medicine*, vol. 19, no. 6, 2021.

[28] A. Conklin and G. White, "e-Government and Cyber Security: The Role of Cyber Security Exercises," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Kauai, Hawaii, USA, 2006, pp. 79b–79b.

[29] C. Killer and B. Stiller, "The Swiss postal voting process and its system and security analysis," in *Electronic Voting: 4th International Joint Conference, E-Vote-ID 2019*, Bregenz, Austria, 2019, pp. 134–149.

[30] swissinfo.ch, "Local election official found guilty of fraud." [Online]. Available: https://www.swissinfo.ch/eng/politics/local-election-official-found-guilty-of-fraud/46767148

All links above were last accessed on September 4, 2024.