# Article information:

Towards Automated Attack Simulations of BPMN-based Processes | IEEE Conference Publication | IEEE Xplore
<https://ieeexplore.ieee.org/abstract/document/9626167>

# Article summary:

1. The article proposes a novel approach to use attack graph simulations on processes represented in BPMN, allowing for the identification of vulnerabilities and potential attacks.

2. The approach involves mapping BPMN elements to a Meta Attack Language (MAL)-based Domain-Specific Language (DSL) called coreLang, which enables the automatic enrichment of BPMN instances with cybersecurity analysis.

3. The study demonstrates that non-invasively enriching BPMN instances with cybersecurity analysis through attack graphs is possible without much human expert input, providing valuable insights into potential vulnerabilities for process modelers.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article titled "Towards Automated Attack Simulations of BPMN-based Processes" discusses the use of attack graph simulations on processes represented in the Business Process Model and Notation (BPMN). The authors propose a novel approach to identify vulnerabilities in BPMN processes and demonstrate their approach using a real-world invoice integration process.

Overall, the article provides a comprehensive overview of the research topic and presents the proposed approach in a clear and structured manner. However, there are several points that need to be critically analyzed.

Firstly, the article does not provide a thorough discussion of related work in the field. While it briefly mentions some existing approaches that extend BPMN with security-related concepts, it does not critically evaluate their strengths and weaknesses or compare them to the proposed approach. This lack of comparison limits the reader's understanding of how the proposed approach differs from existing solutions and why it is superior.

Secondly, the article does not provide sufficient evidence or examples to support its claims. For example, it states that non-invasively enriching BPMN instances with cybersecurity analysis through attack graphs is possible without much human expert input. However, no empirical data or case studies are presented to validate this claim. Without such evidence, it is difficult to assess the effectiveness and practicality of the proposed approach.

Additionally, there is a potential bias towards promoting the proposed approach without adequately addressing its limitations or potential risks. The article focuses primarily on the benefits and contributions of the approach but fails to discuss any potential drawbacks or challenges. It would have been valuable to explore possible limitations or counterarguments to provide a more balanced perspective.

Furthermore, while the article acknowledges that process owners may lack security knowledge, it does not address how this issue is mitigated in practice. It would be important to discuss how organizations can ensure that process owners receive adequate training or support to understand and address potential vulnerabilities identified through attack simulations.

In terms of writing style, the article is generally well-structured and easy to follow. However, there are some instances where the language is overly technical and may be difficult for non-experts to understand. It would have been helpful to provide more explanations or examples to clarify complex concepts.

In conclusion, while the article presents an interesting approach for assessing the security state of BPMN processes, it lacks critical analysis of related work, sufficient evidence to support its claims, and a balanced discussion of limitations and potential risks. Addressing these shortcomings would strengthen the article's credibility and provide a more comprehensive understanding of the proposed approach.

# Topics for further research:

* Comparison of existing approaches to secure BPMN processes
* Empirical studies on the effectiveness of attack graph simulations in BPMN processes
* Limitations and challenges of using attack graph simulations in BPMN processes
* Mitigating the lack of security knowledge among process owners in BPMN processes
* Examples of non-invasive enrichment of BPMN instances with cybersecurity analysis
* Explanation of complex concepts in attack graph simulations for BPMN processes

# Report location:

<https://www.fullpicture.app/item/d574287fbc5851c4462f4bf920885dff>