Challenges of Security and Configurability in Enterprise-Resource-Planning Systems

Richard May, Christian Biermann

Harz University of Applied Sciences, Department of Automation and Computer Science

Abstract

In this study, we investigated security of enterprise-resource-planning systems and their modeling based on product-line engineering techniques. Precisely, we systematically analyzed 25 papers to obtain an understanding of the research landscape of the product-line engineering community and to identify which properties are still underexplored. In this context, five important challenges are identified to be considered in future research.

1. Introduction

In recent years, enterprise-resource-planning (ERP) systems have become increasingly important for companies [1]. ERP systems are integrated software solutions that represent, support, and automate a company's business processes in a uniform way [2,3]. These processes include, e.g., planning, controlling, and monitoring resources or personnel [4]. ERP systems are quite complex and need to be adapted to the specific needs of every company and its departments. The configurability is created by relying on modules which provide basic main features but also customized module-specific features [5]. Due to their configurability, ERP systems can be modeled relying on techniques of product-line engineering (PLE) [6]. Precisely, PLE is an established approach to support variability and maintainability aspects during the engineering and evolution of configurable systems with great advantages in terms of time and costs [7]. However, the higher a system's configurability, the higher its complexity. Unfortunately, configurability also leads to a growing surface for cyber attacks due to potentially occurring system vulnerabilities. Such vulnerabilities are often a result of complex configuration options or feature interactions [8–10]. In worst case, exploiting such vulnerabilities can result in data breaches including unauthorized system access [11]. Such risks can lead to fatal consequences, especially regarding process quality, time, and costs (e.g., manipulation of manufacturing processes) [12,13].

Despite the existing research regarding PLE and configurable systems, e.g., requirements elicitation tools for ERP systems [14], we are missing an analysis of current concepts in research regarding secure variability in ERP systems and their characteristics. To address this gap, we conducted a systematic literature review based on the methodology of Kitchenham et al. [15]. Overall, our research objective is to analyze and synthesize the state-of-the-art to provide an overview understanding regarding the intersection of security, PLE, as well as ERP systems and their characteristics (i.e., underlying cloud systems providing similar properties). Moreover, we contribute five highly relevant challenges, particularly for the PLE community, taking into account the secure variability of ERP systems. This way, we aim to help researchers and practitioners in modeling and developing secure PLE-based ERP systems.

2. Methodology

Study design. First, a search string was created consisting of established terms (i.e., including wildcards) in the context of PLE and configurability (e.g., "software family"), ERP systems (e.g., "ERP customization"), characteristics of ERP systems (e.g., "software as a service"), and security (e.g., "secure"). Second, we relied on four selection and quality criteria, including only English language, the time frame 2013–2022, a minimum of three pages per paper, and only peer-reviewed conference papers, journal articles, or book chapters. Third, to extract data, we defined 13 criteria (see Table 1), covering publication-, ERP-, PLE-, and security-related topics.

Study conduct. Based on the search string, the second author performed a search on three established literature databases in the area of software engineering, namely *Scopus*, *IEEE Xplore*, and the *ACM Digital Library*.

The search resulted in 153 papers, which we managed (i.e., duplication removal, title and abstract selection) in the review tool Rayyan. This process led to a number of 15 papers to be considered for full-text review. However, we applied one iteration of backwards snowballing (i.e., analyzing the references of the selected papers) to increase the final number of papers. Finally, both authors independently analyzed 25 full-text papers according to the extraction criteria.

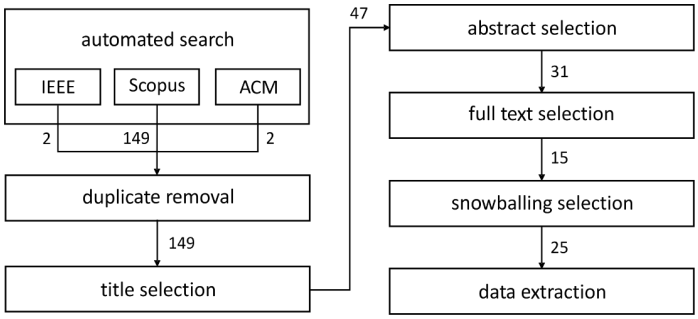

Figure 1: Methodological overview of the systematic literature review.

3. Results

Publication. Most papers are published between 2015–2016 or 2020–2021. The identified domains are quite diverse, ranging from manufacturing over payment to administration processes. However, we extracted also papers solely referring to research without a domain or a more general, unspecified domain. The majority of the publications focuses on configurability. Significantly less papers are concerned with ERP systems or security in an in-depth way. Interestingly, we found that more than half of the papers provide more than one focus.

ERP systems. We found that most papers do not explicitly deal with ERP system architectures or the environment (e.g., cloud systems). Surprisingly, only 20% of the papers primarily focus on ERP systems, while the remaining papers refer more to the characteristics related to ERP systems, e.g., customization or software as a service. Half of these publications described ERP systems or their modules.

Configurability. System evolution is described in 56% of the papers, e.g., evolutionary changes or dynamic configurations of cloud ERP systems. We found about half of the papers dealing with verification or consider it partly. These papers are concerned with the verification of the whole system, i.e., they refer to product-based verifications. Most publications propose methods referring to handle configurability challenges. Except for one paper, these refer to feature modeling, e.g., based on FeatureIDE.

Security. Most papers deal with security in a quite superficial way. Precisely, security measures and standards are only rarely mentioned, e.g., ISO/IEC 27000. In contrast, authors refer more to security goals or threats. More specifically, when threats are specified, security goals are always mentioned as well. Interestingly, all goals of the CIA triad and information security were mentioned at least by 36%. The most common goals are availability, authorization, and confidentiality (see Figure 2).

4. Challenges and Research Opportunities

Based on the results, we derived five highly relevant **challenges (C)** which indicate opportunities for future research.

C_1: Feature-based verification. Although verification of an overall ERP system (i.e., product-based verification) is useful, we emphasize that ERP systems should be verified in a feature-based way due to their high (module) configurability. In this context, the fulfillment of functional requirements and quality objectives as well as their occurring interactions should be addressed. In particular, the quality objectives refer to security, which should be modeled and verified as security as a feature.

Reference	Domain	Focus: configurability	Focus: ERP	Focus: security	ERP architecture	ERP environment	System evolution	System verification	Variability method	Security goals	Security threats	Security measures	Security standard
Schroeter et al. (2012) [16]	U	●	◕	◔	○	○	●	●	●	◔	○	○	○
Olaechea et al. (2012) [17]	U	●	○	◑	○	○	○	●	●	◔	◑	◑	○
Benavides et al. (2014) [18]	A	●	◔	○	◑	○	●	●	●	○	○	○	○
Fernandez et al. (2015) [19]	U	●	○	●	○	○	○	○	○	◕	●	●	●
Galindo et al. (2015) [20]	R	●	●	●	●	○	○	○	●	◕	●	●	○
Preuveneers et al. (2016) [21]	P_2	●	◔	●	○	○	●	●	◑	◕	◑	○	●
Preuveneers et al. (2016) [22]	P_2	●	○	●	○	○	●	○	●	●	◕	●	●
Afzal et al. (2016) [23]	R	●	●	○	◑	○	◑	●	●	○	○	○	○
Jumagaliyev et al. (2016) [24]	U	●	○	◑	○	○	●	○	●	◑	●	○	○
Pereira et al. (2016) [25]	U	●	◑	○	○	○	◔	●	●	○	○	○	○
Ali et al. (2016) [6]	R	●	●	○	○	○	◑	◑	●	○	○	○	○
Khoshnevis and Shams (2017) [26]	R	●	◑	○	○	○	○	●	●	○	○	○	○
Leite et al. (2017) [27]	A	●	○	◔	○	○	●	◑	●	◔	●	●	○
Krieter et al. (2018) [28]	U	●	○	●	○	○	○	○	○	◕	◑	●	○
Varela-Vaca et al. (2019) [29]	A	●	◔	●	○	○	○	○	●	◑	●	○	○
Shaaban et al. (2019) [30]	P_1	●	◔	●	○	◔	○	○	●	◑	●	○	●
Assunção et al. (2020) [31]	R	●	○	◑	○	○	◑	◑	●	◔	●	○	○
Zhou et al. (2020) [32]	R	◕	◑	○	◔	◑	◑	◑	●	○	○	○	○
Thipphonexai et al. (2020) [33]	R	◔	●	●	○	◑	○	○	○	●	●	●	○
Varela-Vaca et al. (2020) [34]	P_1	●	◔	●	○	○	○	○	●	◕	●	●	○
Siegmund et al. (2020) [35]	U	●	○	●	○	○	◕	○	●	◑	○	●	○
Varela-Vaca et al. (2021) [36]	P_1	●	○	●	○	○	○	○	●	●	●	●	●
Orue-Echevarria et al. (2021) [37]	G	◔	◔	●	○	○	○	○	○	◕	○	○	●
Ramos-Gutiérrez et al. (2021) [38]	R	●	●	○	○	○	◑	●	●	○	○	○	○
May et al. (2022) [10]	R	●	◔	●	○	○	●	●	●	●	●	●	●

Criteria fulfillment: ● Fulfilled, ◕ Almost fulfilled, ◑ Half fulfilled, ◔ Partly fulfilled, ○ Not fulfilled

Domain: A: Administration and management; G: Government;

P_1: Production; P_1: Payment; R: Research; U: Unspecified

Table 1: Overview of the extracted data based on the defined criteria.

C_2: System evolution and its influences. The evolution of configurable systems has been mentioned in the papers, but dependencies and influences, especially regarding the ERP architecture and environments, have usually not been considered. Accordingly, we argue that it is essential to address and analyze evolutionary dependencies and influences of features and processes, features on processes, and processes on features. This applies in particular to security features, which, at best, can dynamically adapt to changing system, i.e., module, characteristics – taking into account interactions and interdependencies to avoid vulnerabilities.

C_3: Relationship between configurability as well as security threats and risks. We argue that research is needed regarding the relationship between the configurability of ERP systems and associated security threats and risks. However, without knowing how these influence each other, the mentioning of security goals appears to be quite general and not area- or use case-dependent. So, the transfer of theoretical knowledge into business practice is impaired.

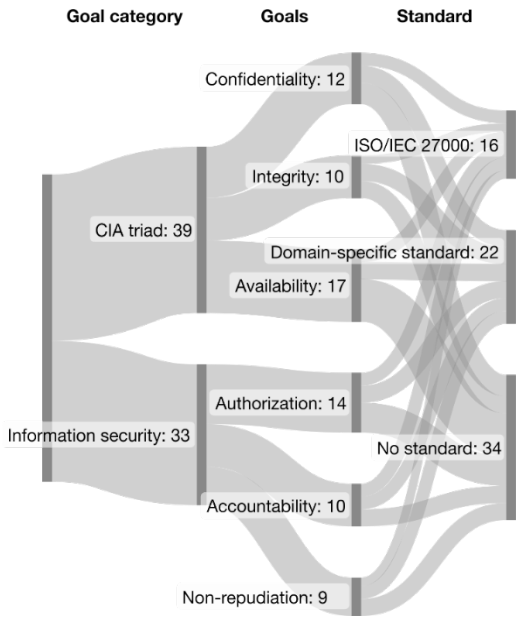

Figure 2: Distribution of security goals mentioned in the papers and their distribution to security standards, in case standards were mentioned along with and associated to security goals in the papers (numbers indicate the amount of goals).

C_4: Security measures and standards. Usually, concrete security measures are not mentioned and standards are not addressed. However, it is not sufficient to know only potential, general threats and risks, but also concrete vulnerabilities related to configurability. So, it is essential to select suitable security measures oriented towards use case-specific threats and risks as well as standards to fulfill certain goals (e.g., CIA triad). This issue is emphasized by Figure 2, which illustrates that although security goals are mentioned, they are often not associated with standards, i.e., standards are usually not referenced in the papers even when goals are named.

C_5: Secure PLE-based ERP systems. Overall, ERP systems based on PLE techniques are often described from a quite general and theoretical perspective, meaning the interdependencies of configurable architectures, infrastructures, and security are rarely addressed. Thus, we argue that there is an under-exploration of ERP systems, their configurability, and security demands from the perspective of PLE. In this context it is already planned to consider research of other fields, such as component-based or aspect-oriented software engineering, and to investigate to what extent their approaches might by transferable.

5. Conclusion

In our literature study, we analyzed 25 papers in the intersection of ERP systems and their characteristics, PLE, and security. This way, we obtained an overview and understanding of the research landscape in this area, taking into account current issues in literature. Precisely, five important challenges are identified to be considered in future research. In addition, with our findings, we aim to help both researchers and practitioners in securely engineering, i.e., modeling and developing, future PLE-based ERP systems.

6. Contact

Friedrichstraße 57 – 59, 38855 Wernigerode
Richard May
rmay@hs-harz.de / 0000-0001-7186-404X
https://richardmay.de/

7. References

[1] Binu, M. S., & Meenakumari, J. (2012): A security framework for an enterprise system on cloud, In: Indian Journal of Computer Science and Engineering, 3, 4, 548–552.

[2] Bakry, A. H., & Bakry, S. H. (2005): Enterprise resource planning: a review and a STOPE view, in: International Journal of Network Management, 15, 5, 363–370.

[3] Tarhini, A., Ammar, H., Tarhini, T., & Masa'deh, R. E. (2015): Analysis of the critical success factors for enterprise resource planning implementation from stakeholders' perspective: A systematic review, in: International Business Research, 8, 4, 25–40.

[4] Shehab, E. M., Sharp, M. W., Supramaniam, L., & Spedding, T. A. (2004): Enterprise resource planning: An integrative review, in: Business Process Management Journal, 359–386.

[5] Mazo, R., Assar, S., Salinesi, C., & Hassen, N. B. (2014): Using Software Product Line to improve ERP Engineering: literature review and analysis, in: Latin-American Journal of Computing, 1, 1, 1–10.

[6] May, R., Biermann, C., Kenner, A., Krüger, J., & Leich, T. (2023): A product-line-engineering framework for secure enterprise-resource-planning systems, in: International Conference on ENTERprise Information Systems, 1–8.

[7] Ouali, S., Kraiem, N., & Ghezala, H. B. (2011): Framework for evolving software product line, in: International Journal of Software Engineering & Applications, 2, 2, 34–51.

[8] May, R., Biermann, C., Zerweck, X. M., Ludwig, K., Krüger, J., & Leich, T. (2024): Vulnerably (mis)configured? Exploring 10 years of developers' Q&As on Stack Overflow, in: International Working Conference on Variability Modelling of Software-Intensive Systems, 112–122.

[9] Abal, I., Melo, J., Stănciulescu, Ş., Brabrand, C., Ribeiro, M., & Wąsowski, A. (2018): Variability bugs in highly configurable systems: a qualitative analysis, in: ACM Transactions on Software Engineering and Methodology, 26, 3, 1–34.

[10] May, R., Biermann, C., Krüger, J., Saake, G., & Leich, T. (2022): A systematic mapping study of security concepts for configurable data storages, in: International Systems and Software Product Line Conference, 108–119.

[11] Gamundani, A. M., & Nekare, L. M. (2018): A review of new trends in cyber attacks: A zoom into distributed database systems, in: IST-Africa Week Conference, 1–9.

[12] May, R., Alex, A. J., Suresh, R., & Leich, T. (2024). Product-line engineering for smart manufacturing: A systematic mapping study on security concepts, in: International Conference on Software Technologies, 1–8.

[13] Wahren, S., Siegert, J., & Bauernhansl, T. (2015): Approach for implementing a control and optimization loop for an energy-efficient factory, in: Procedia CIRP, 29, 45–49.

[14] Elmoniem, M. A. A., Nasr, E. S., & Gheith, M. H. (2017): A Requirements Elicitation Tool for Cloud-Based ERP Software Product Line, in: Africa and Middle East Conference on Software Engineering, 1–6.

[15] Kitchenham, B. A., D. Budgen, & P. Brereton (2015): Evidence-based software engineering and systematic reviews, Boca Raton: CRC Press.

[16] Schroeter, J., Mucha, P., Muth, M., Jugel, K., & Lochau, M. (2012): Dynamic configuration management of cloud-based applications, in: International Software Product Line Conference, 171–178.

[17] Olaechea, R., Stewart, S., Czarnecki, K., & Rayside, D. (2012): Modelling and multi-objective optimization of quality attributes in variability-rich software, in: International Workshop on Nonfunctional System Properties in Domain-specific Modeling Languages, 1–6.

[18] Benavides, D., & Galindo, J. A. (2014): Variability management in an unaware software product line company: an experience report, in: International Workshop on Variability Modelling of Software-Intensive Systems, 1–6.

[19] Fernandez, E. B., Yoshioka, N., & Washizaki, H. (2015): Patterns for security and privacy in cloud ecosystems, in: Workshop on Evolving Security and Privacy Requirements Engineering, 13–18.

[20] Galindo, J. A., Dhungana, D., Rabiser, R., Benavides, D., Botterweck, G., & Grünbacher, P. (2015):

Supporting distributed product configuration by integrating heterogeneous variability modeling approaches, in: Information and Software Technology, 62, 78–100.

[21] Preuveneers, D., Heyman, T., Berbers, Y., & Joosen, W. (2016): Systematic scalability assessment for feature oriented multi-tenant services, in: Journal of Systems and Software, 116, 162–176.

[22] Preuveneers, D., Heyman, T., Berbers, Y., & Joosen, W. (2016): Feature-based variability management for scalable enterprise applications: Experiences with an e-payment case, in: Hawaii International Conference on System Sciences, 5793–5802.

[23] Afzal, U., Mahmood, T., & Shaikh, Z. (2016): Intelligent software product line configurations: A literature review, in: Computer Standards & Interfaces, 48, 30–48.

[24] Jumagaliyev, A., Whittle, J. N. D., & Elkhatib, Y. S. S. A. (2016): Evolving multi-tenant SaaS cloud applications using model-driven engineering, in: Lancaster EPrints, 1–9.

[25] Pereira, J. A., Matuszyk, P., Krieter, S., Spiliopoulou, M., & Saake, G. (2016): A feature-based personalized recommender system for product-line configuration, in: International Conference on Generative Programming: Concepts and Experiences, 120–131.

[26] Khoshnevis, S., & Shams, F. (2017): Automating identification of services and their variability for product lines using NSGA-II, in: Frontiers of Computer Science, 11, 3, 444–464.

[27] Leite, A. F., Alves, V., Rodrigues, G. N., Tadonki, C., Eisenbeis, C., & Melo, A. C. M. A. D. (2017): Dohko: An autonomic system for provision, configuration, and management of inter-cloud environments based on a software product line engineering method, in: Cluster Computing, 20, 3, 1951–1976.

[28] Krieter, S., Krüger, J., Weichbrodt, N., Sartakov, V. A., Kapitza, R., & Leich, T. (2018): Towards secure dynamic product lines in the cloud, in: International Conference on Software Engineering: New Ideas and Emerging Results, 5–8.

[29] Varela-Vaca, Á. J., M. Gasca, R., Ceballos, R., Gómez-López, M. T., & Bernáldez Torres, P. (2019): CyberPLE: a framework for the verification of cybersecurity policy compliance of system configurations using software product lines, in: Applied Sciences, 9, 24, 5364.

[30] Shaaban, A. M., Gruber, T., & Schmittner, C. (2019): Ontology-based security tool for critical cyber-physical systems, in: International Systems and Software Product Line Conference, 207–210.

[31] Assunção, W. K., Krüger, J., & Mendonça, W. D. (2020): Variability management meets microservices: six challenges of re-engineering microservice-based webshops, in: International Conference on Systems and Software Product Line, 1–6.

[32] Zhou, X., Li, C., Zhang, H., Meng, F., & Chu, D. (2020): A Feature Tree and Dynamic QoS based Service Integration and Customization Model for Multi-tenant SaaS Application, in: International Conference on Service Science, 107–114.

[33] Thipphonexai, X., & Guanghui, Y. (2020): Research on analysis and design of cloud ERP based on blockchain technology, in: International Conference on Virtual Reality and Intelligent Systems, 806–810.

[34] Varela-Vaca, Á. J., Rosado, D. G., Sánchez, L. E., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2020): Definition and verification of security configurations of cyber-physical systems, in: Computer Security, 135–155.

[35] Siegmund, N., Ruckel, N., & Siegmund, J. (2020): Dimensions of software configuration: on the configuration context in modern software development, in: Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 338–349.

[36] Varela-Vaca, Á. J., Rosado, D. G., Sánchez, L. E., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2021): CARMEN: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems, in: Computers in Industry, 132, 103524.

[37] Orue-Echevarria, L., Garcia, J. L., Banse, C., & Alonso, J. (2021): MEDINA: Improving Cloud Services trustworthiness through continuous audit-based certification, in: CEUR Workshop Proceedings, 1–8.

[38] Ramos-Gutiérrez, B., Varela-Vaca, Á. J., Galindo, J. A., Gómez-López, M. T., & Benavides, D. (2021): Discovering configuration workflows from existing logs using process mining, in: Empirical Software Engineering, 26, 1, 1–41.