Research Challenges in the Security Design and Evaluation of an Engineering Service Bus Platform

Christian Frühwirth
Aalto University School of Science and Technology, Software Business Lab/BIT

Stefan Biffl Alexander Schatten Sebastian Schrittwieser Edgar Weippl
Christian Doppler Laboratory for Software Engineering Integration for Flexible Automation Systems
Vienna University of Technology, Institute of Software Technology and Interactive Systems

Christian.Fruehwirth @ tkk.fi
{Stefan.Biffl, Alexander.Schatten, Edgar.Weippl} @ tuwien.ac.at,
Sschrittwieser @ sba-research.org

1. Introduction

The Open (Software) Engineering Service Bus (EngSB)[6] is based on the Apache ServiceMix ESB and connects software tools across engineering domains and company borders. EngSB allows the integration and automation of engineering processes by connecting multiple tools in seamless information workflows through the use of tool connectors, domain bridges, intelligent service message transformation and routing [3][4][5]. Figure 1 gives an overview of the EngSB application architecture.

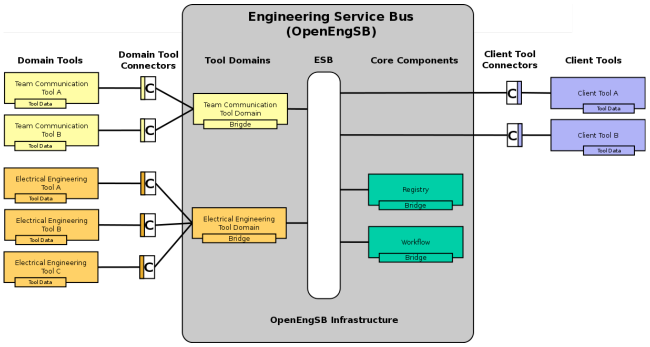

Figure 1 - The Open (Software) Engineering Service Bus Architecture

While the benefits of an engineering service bus application are attractive for companies and researchers, they come with a number of open challenges on the security side. Even though application- and service security has received tremendous attention from the security research community in the past, the engineering service bus approach represents a novel concept that is not yet sufficiently understood on the security level. Thus, before companies can fully adopt and realize the potential of engineering service-bus concepts, more work has to identify and address these open security research issues. This paper aims to guide such future work by proposing a set of research issues in the EngSB context. The presented issues will provide valuable support in the targeted future research work.

2. Security research challenges

We use Schneier's Security Decision Model[5], shown in Figure 2 to determine the areas of open research issues.

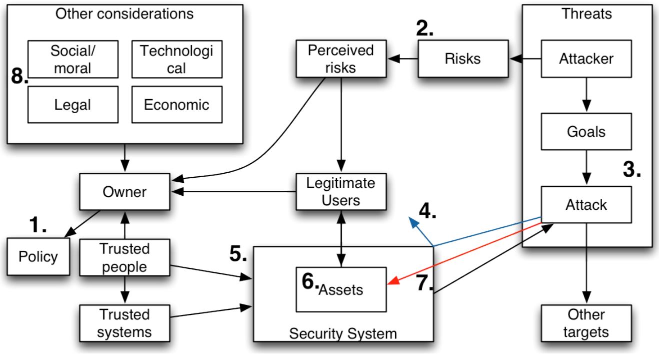

Figure 2 - Identified security research issues, placed in Schneier's Security Decision Model, recreated from [5]. The numbers indicate the interaction area of the identified issue.

Schneier's security decision model is useful because it gives a comprehensive overview of the relations and interactions between information assets, the security system that is set to protect them and the outside world with its various stakeholders. We identified 8 main security research issues by applying the model to the EngSB context:

Issue 1.: Developing a security policy for a Service Bus that integrates economic considerations and competing stakeholder values: An EngSB operates in a complex, distributed environment that spans across engineering domains and companies with conflicting values, thus the inherent risks are less clear than in traditional isolated systems and economic aspects have a strong influence on policy decisions[1][5]. Research work needs to address this issue and find new ways to align competing stakeholder values with quality requirements and economic realities [7].

Issue 2.: Determining risk exposure to enable a value-based management of security: Understanding the relationship between attackers, their motives as well as the differences between perceived and actual risk exposure is essential for value based security management. Little research has yet been done that combines these relationships with the inter-stakeholder dependencies on a service bus under the concept of value based security.

Issue 3.: Improve quality of empirical security data to move from defensive to attacker-focused countermeasures: Traditional security focuses on individual defense (build high walls around everything). Since this is economically unviable in a large, heterogeneous system, a clearer understanding of the attacker and its motives is needed to better target countermeasures (build high walls only around the gold chest) and increase efficiency (build walls only slightly higher than a man can jump). Today's research in this area faces a severe lack of empirical data on attackers and their motives since companies that fall victim to an attack do typically not disclose such information. Future work should address the empirical side of this problem by improving the collection, reliability and communication of both, attack and countermeasure related data.

Issue 4.: Evaluating the effectiveness of a security system with security metrics: The effectiveness of a security system is difficult to measure without a baseline for data comparison. Research in this area would need to determine an empirically valid baseline and set the guidelines for its evaluation. There are numerous security metrics available to evaluate security systems; however, they need to be improved and tailored for the application in a service bus setting. Little research has yet been done on the effectiveness of such metrics, if/how they help developers to improve software quality and how to choose the right metric for a given evaluation task.

Issue 5.: Seamless integrating a security system in the information workflow: Too many developers still consider security an "add-on" feature. This detachment of security from the overall application can lead to interruptions or breaks in the information workflow between the users and the system. System architects thus face the question of how to make better use of "security by design" principles in order to achieve a seamless integration of security in the overall information workflow. There has not yet been extensive research on how much "seamless" security can contribute to the performance of a business process, i.e. how much it would be worth to pay for.

Issue 6.: Asset management and valuation: In order to manage the security of information assets in a system effectively, the nature and value of the assets needs to be know. On a distributed and dynamic platform like the EngSB information assets can change rapidly, thus static asset management is not enough. Even though there are existing solutions to manage inventories of information assets, the problem of putting a value or price tag on a changing asset remains.

Issue 7.: Security Incident management on a service bus: A security incident in an integrated system can jeopardize the operations of several connected companies at the same time, with consequences hard to predict. In order to manage and remediate the risk from security incidents, the EngSB platform needs to find ways of developing survivability capabilities. On the policy level, existing incident management frameworks (like parts of ITIL [8]) need to be adapted to suit the EngSB environment. Adapting existing frameworks, however, raises the question of how these modifications would align with stakeholder requirements, and the overall EngSB (software) architecture. There is yet little research on the integration of the software side of security incidents with the business side (e.g. how can an organization continue to function when the bus that connects its tools is out of order).

Issue 8.: Continuous compliance: The target users of an engineering service-bus are mostly larger companies which typically fall under some form of compliance regulations like the Sarbanes Oxley Act (SOX). Compliance regulations dictate major parts of organizations' IT service management (ITSM) and security policies, thus also the way companies will (or can) use EngSB. In order for service busses like the EngSB to become successful on a wider scale, future work should investigate whether security design in the EngSB architecture can facilitate companies' compliance efforts.

3. Conclusion

We used Schneier's Security Decision Model, to determine areas of open research issues in the security design and evaluation of an engineering service bus. Many of the described issues pointed towards increasingly value-oriented security approaches that will enable application developers and companies to make better decisions on how and where to target their security efforts. We believe that addressing these open research issues will encourage future work in this area and guide improvement efforts in directions that improve the quality and application of engineering service bus concepts.

References

[1] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, 2006, pp. 610-613.

[2] S. Biffl, S.B. Schatten, and A. Zoitl, "Integration of Heterogeneous Engineering Environments for the Automation Systems Lifecycle," *Proc. IEEE Industrial Informatics Conf*, 2009, pp. 576-581.

[3] S. Biffl, W.D. Sunindyo, and T. Moser, "Bridging Semantic Gaps Between Stakeholders in the Production Automation Domain with Ontology Areas," *Proceedings The 21st International Conference on Software Engineering Knowledge Engineering (SEKE 2009)*, 2009, pp. 233–239.

[4] T. Moser, S. Biffl, W.D. Sunindyo, and D. Winkler, "Integrating Production Automation Expert Knowledge Across Engineering Stakeholder Domains," *2010 International Conference on Complex, Intelligent and Software Intensive Systems*, 2010, pp. 352–359.

[5] B. Schneier, "Nonsecurity considerations in security decisions," *IEEE Security & Privacy*, 2007, p. 88.

[6] The Open Engineering Service Bus, available online at http://openengsb.org, 2010.

[7] N. Oza, S. Biffl, C. Frühwirth, Y. Selioukova, and R. Sarapisto, "Reducing the Risk of Misalignment between Software Process Improvement Initiatives and Stakeholder Values," Industrial Proceedings of EuroSPI, 2008, pp.6–9.

[8] ITIL, "The Open Guide. ITIL Incident Management," 2007, p. Available online at: www.itlibrary.org/index.php?page=Incident_Management.