An integrative security modelling environment

Avi Shaked[1,*]

[1] *University of Oxford, Oxford OX1 3QD, UK*

Abstract

We offer a dedicated reflection, based – primarily – on two recent journal articles. Both articles are accessible through open access. The first journal article [1] was published in the top-ranked *Journal of Industrial Information Integration*. It introduces the integrative security modelling methodology and open-source tool TRADES, promoting security by-design and systems security engineering. The second journal article [2] was published in the relatively new *Journal of Cybersecurity and Privacy*. It discusses how the TRADES modelling environment is designed to facilitate the integration of cyber security knowledge from knowledge bases (such as MITRE's CAPEC and NIST SP 800-53 Security Controls) and employ the knowledge to compose security policies and design systems.

Keywords

Security modelling, domain ontology, metamodelling

1. Introduction

Through reflection on two published articles and our ongoing work, we provide a dedicated reflection which is uniquely tailored for the Semantic Shields workshop. We focus on:

(a) the effort to unveil the domain ontology. Specifically, we emphasise the importance of functionality-driven ontology discovery and demonstrate different tactics for ontology elicitation and extraction. By reflecting on the two published papers as well as additional scenarios for TRADES, we demonstrate how a domain ontology can gradually unfold in tandem with our understanding of the domain within specific contexts and for addressing specific challenges.

(b) the use of computer-aided conceptual modelling for rigorous security related design. Specifically, we advocate for capturing the ontology as an executable metamodel, which, in turn, allows to instantiate and reason about concrete cases. By reflecting on the published papers and additional scenarios, we demonstrate how the metamodel that has been integrated into the TRADES modelling environment [3] evolves to provide additional functionality.

Proceedings of the Joint Ontology Workshops (JOWO) - Episode X: The Tukker Zomer of Ontology, and satellite events co-located with the 14th International Conference on Formal Ontology in Information Systems (FOIS 2024), July 15-19, 2024, Enschede, The Netherlands.

* Corresponding author.

avi.shaked@cs.ox.ac.uk (A. Shaked)

0000-0001-7976-1942 (A. Shaked)

(c) the design of the security modelling environment's user experience (UX). Specifically, we emphasise the importance of providing users an interface that is natural to them, for viewing and for constructing the models.

2. Abstracts of published articles

Abstract of [1]: addressing cybersecurity aspects while designing systems is challenging. As our systems increasingly rely on digital technology to perform, security and resilience aspects need to be considered during the system design process. However, the integration of pertinent information into the systems engineering lifecycle is not trivial, as it is characterized by following verbose guidelines and documentation, and has no practical, model-based methodology to support threat-aware design of systems. In this article, we address this gap by presenting an integrative, model-based methodology to support the design and assessment of systems' security aspects. We discuss the methodology's design, specifically with respect to system development scenarios, and detail industrial case studies demonstrating the applicability of the methodology.

Abstract of [2]: security threat and risk assessment of systems requires the integrated use of information from multiple knowledge bases. Such use is typically carried out ad-hoc by security experts in an unstructured manner. Also, this ad-hoc use of information often lacks foundations that allow for rigorous, disciplined applications of policy enforcement and the establishment of a well-integrated body of knowledge. This hinders organisational learning as well as the maturation of the threat modelling discipline. In this article, we uncover a newly developed extension of a state-of-the-art modelling tool that allows users to integrate and curate security-related information from multiple knowledge bases. Specifically, we provide catalogues of threats and security controls based on information from CAPEC, ATT&CK, and NIST SP800-53. We demonstrate the ability to curate security information using the designed solution. We highlight the contribution to improving the communication of security information, including the systematic mapping between user-defined security guidance and information derived from knowledge bases. The solution is open source and relies on model-to-model transformations and extendable threat and security control catalogues. Accordingly, the solution allows prospective users to adapt the modelling environment to their needs as well as keep it current with respect to evolving knowledge bases.

Acknowledgements

This research was funded by Innovate UK, grant number 75243.

References

[1] Shaked, Avi. "A model-based methodology to support systems security design and assessment." Journal of Industrial Information Integration 33 (2023): 100465. https://doi.org/10.1016/j.jii.2023.100465.

[2] Shaked, Avi. "Facilitating the Integrative Use of Security Knowledge Bases within a Modelling Environment." Journal of Cybersecurity and Privacy 4 (2024). https://doi.org/10.3390/jcp4020013.

[3] TRADES Github repository, https://github.com/UKRI-DSbD/TRADES. Accessed: 05/08/2024.