An integrative security modelling environment

Avi Shaked[1,*]

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

Abstract

We offer a dedicated presentation – tailored for the Semantic Shields workshop – covering two recent journal articles. Both articles are accessible through open access, enabling the workshop's attendees to freely obtain them. The first journal article [1] was published last year 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 just 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.

For Semantic Shields, we propose to focus on: (a) the effort to unveil the domain ontology using an evolving metamodel; (b) the use of computer-aided conceptual modelling for rigorous security related design; and (c) the design of the security modelling environment's user experience (UX). *Optional: If possible, we ask for an extended presentation length (40 minutes), to cover pertinent and interrelated aspects of the work reported in the two journal papers in greater depth.*

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.

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.