Journal of *Cybersecurity and Privacy*

MDPI

Article

Facilitating the Integrative Use of Security Knowledge Bases within a Modelling Environment

Avi Shaked

Department of Computer Science, University of Oxford, Oxford OX1 3QD, UK; avi.shaked@cs.ox.ac.uk

Abstract: 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.

Keywords: threat; security risk; assessment; security by design; systems security; attack patterns; attack techniques; security controls; security modelling

Citation: Shaked, A. Facilitating the Integrative Use of Security Knowledge Bases within a Modelling Environment. *J. Cybersecur. Priv.* **2024**, *4*, 264–277. https://doi.org/10.3390/jcp4020013

Academic Editor: Danda B. Rawat

Received: 8 March 2024
Revised: 8 April 2024
Accepted: 16 April 2024
Published: 20 April 2024

1. Introduction

Threat modelling, alternatively security threat and risk assessment, "*works to identify, communicate, and understand threats and mitigations within the context of protecting something of value*" [1]. Threat modelling is crucial to understanding and communicating the security posture of systems, as well as being crucial to designing the security aspects of systems [2–5]. Threat modelling typically involves manual effort, as it is a creative process which requires applying knowledge and information to analyse a system of interest [4,6]. The systematic use of the available security body of knowledge can not only assist threat modelling but also contribute to the quality of the resulting artefacts [4].

TRADES (Threat and Risk Assessment for Design of Engineered Systems) is an established model-based methodology to support systems' security design and assessment, supported by an open-source tool implementation, *TRADES Tool* [7,8]. In this paper, we focus on the integration of pertinent information from existing and evolving public-domain security knowledge bases. Specifically, the information of interest is information relating to two important concepts in threat and risk assessment: (1) *threat*, or alternatively *attack*, which is a potential action that could compromise a system or its constituents [3–5,9–13], and (2) *security control*, or, alternatively, *mitigation*, which is a concept that can prevent the successful materialisation of a threat [4,10–13]. We next discuss the public-domain knowledge bases that can be used while modelling instances of these concepts as part of a security threat and risk assessment.

The MITRE organisation offers two distinct repositories—following two different approaches—in support of security risk assessment. Common Attack Pattern Enumeration

and Classification (CAPEC) focuses on application security and includes sociotechnical/non-technical aspects such as social engineering and supply chains [14]. CAPEC enumerates techniques that can be employed by adversaries to exploit weaknesses in cyber-enabled capabilities. As such, it allows for a high-level analysis of systems security. Adversarial Tactics, Techniques and Common Knowledge (ATT&CK), on the other hand, focuses on network defence. ATT&CK typically offers lower-level techniques (compared with CAPEC) that may be used to detail some CAPEC techniques. CAPEC is the approach recommended by MITRE for application threat modelling and educating system developers, which are the primary concerns of our work reported in this article.

Both CAPEC and ATT&CK offer structured records of each attack pattern/technique, with some enumerations and relations to other records (of the CAPEC and ATT&CK knowledge bases) as well as natural language descriptions. Specifically, information regarding the potential mitigation mechanisms remains somewhat lacking. In ATT&CK, proposed mitigations are semi-structured, featuring metadata as well as natural language descriptions. For example, the "User Account Control" mitigation record has a unique ID—"M1052"—and the natural language description says "*Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access*". Furthermore, the use of the mitigations within the context of ATT&CK techniques records is—in fact—a natural language description that provides additional mitigation guidance. For example, in the ATT&CK "Abuse Elevation Control Mechanism" technique (ID: T1548), the aforementioned "User Account Control" (ID: M1052) mitigation is identified, with the "Description" field offering a description tailored to the T1548 technique: "*Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking*" (abbreviations appear in the original description). In comparison, the content of the "Mitigation" field of CAPEC techniques remains entirely freeform and in natural language. For example, the CAPEC-122 "Privilege Abuse" attack pattern record simply specifies "*Configure account privileges such privileged/administrator functionality is not exposed to non-privileged/lower accounts*" as its mitigation. Interestingly, the advised CAPEC-122 mitigation directly corresponds with the M1052 ATT&CK mitigation concept, and indeed, CAPEC-122 suggests mapping onto the ATT&CK T1548 technique which lists M1052 as one of its seven potential mitigations; yet no explicit connection is offered as a collective CAPEC and ATT&CK body of knowledge, attesting to the still somewhat disjointed nature of these two knowledge bases.

While CAPEC and ATT&CK are lacking with respect to a well-structured specification of mitigations, NIST SP800-53 is a comprehensive source on security controls that offers structured definitions of security control mechanisms, including hierarchies of mitigation concepts [15]. Furthermore, NIST promotes the well-structuredness of security controls via the Open Security Controls Assessment Language (OSCAL) [16], and the NIST SP800-53 security control knowledge base is offered as an OSCAL-compliant implementation [17].

It is imperative to consider available security knowledge bases when performing threat and risk assessment if we wish to (1) rigorously reason about the security posture of system designs and (2) improve and promote a common understanding of security threats and mitigation mechanisms [4,5]. We provide a few examples of previous research efforts that exercise security information from the aforementioned knowledge bases. VERDICT employs a specific subset of attack patterns from CAPEC to analyse system designs [18]. Seehusan used a user-specified set of CAPEC attack patterns to create a generic risk model, which should then be further adapted to a specific target of evaluation [6]. Messe et al. used CAPEC definitions for threat enumeration [2]. Riera et al. constructed a dataset that allows for the training of machine learning models to classify attacks based on the "*internationally accepted classification*" of CAPEC [19]. Xiong et al. propose a textual threat modelling language based on ATT&CK techniques and mitigations [20]. Georgiadou et al. mapped ATT&CK mitigations to cyber security dimensions and domains in an attempt to promote the use of the ATT&CK knowledge base for security assessment and defensive design [21]. Ozdemir et al. used metadata from CAPEC attack patterns as well as ATT&CK mitigations

to generate attack graphs [22]. Casola et al. relied on NIST SP800-53's definitions of security controls to compose security policies and perform security analysis [12]. Sommer et al. integrated information from multiple sources—including CAPEC and ATT&CK—into an attack database for a specific application domain (automative), with the intention of promoting "*a common understanding of attack techniques. . . and possible mitigations*" [11]. Maunero et al. propose an ontology-based approach to automate aspects of cybersecurity risk assessment, using CAPEC attack patterns as a catalogue of threats [5].

Of the surveyed approaches that refer to the public-domain knowledge bases, only VERDICT is supported by an open-source modelling environment. The VERDICT modelling environment embeds a specific subset of CAPEC information as a hard-coded attack patterns taxonomy, which is inaccessible to the user and cannot be adapted from a user perspective [18]. Seehusan reports developing a "*proof of concept tool*"—which remains unavailable—for translating CAPEC attack patterns into a general risk model [6]. Casola et al. report developing a supporting prototype tool [12]. Their tool, however, is no longer available, and it is unclear from the article as to whether the NIST security controls definitions were embedded in the tool and to what extent. Ozdemir et al. report the integration of a subset of CAPEC attack patterns into a tool that remains unavailable [22]. Xiong et al. report that none of the existing tools cover the full range of ATT&CK techniques [20]. Furthermore, their own effort to extract information from ATT&CK was performed manually, and the authors explicitly suggest that future improvement can be in automating the extraction process. Interestingly, Xiong et al. report extracting 266 ATT&CK Enterprise techniques without mentioning the MITRE ATT&CK repository version from which these were derived. We were able to trace this number of ATT&CK techniques to ATT&CK v6.3, which was the version of the ATT&CK repository prior to Xiong et al.'s article submission (https://attack.mitre.org/versions/v6/techniques/enterprise/, accessed: 7 March 2024). At the time of their article submission, however, ATT&CK v7.2 had already been published, with complete reorganisation of the techniques into 156 main techniques and 272 sub-techniques (https://attack.mitre.org/versions/v7/techniques/enterprise/, accessed: 7 March 2024), and as of today (v14.1), there are 201 main techniques and 424 sub-techniques. The significant increase in techniques throughout the evolution of ATT&CK attests to the dynamic nature of the security body of knowledge and the need to accommodate it. Xiong et al. explicitly mention the need to further integrate additional information sources—including CAPEC—as well as the need to continuously update their language based on the expanding body of knowledge. Sommer et al. conclude their recent research article by explicitly acknowledging the need for a tool that "*. . .can gather data from diverse taxonomies and link it. . .*" [11]. To our knowledge, there is no security modelling environment that allows for the use of existing knowledge bases (e.g., CAPEC and NIST SP800-53) in an integrated form, let alone in an open manner that allows for their update (as the knowledge bases continuously evolve).

In this work, we deliver security experts and researchers a security modelling environment that integrates information from existing knowledge bases. This supports the disciplined design and analysis of systems' security postures. Also, we provide for building structured security policies and guidance, integrating the knowledge bases and creating new insights.

2. Materials and Methods

We relied on model-to-model transformations to import information from knowledge bases into the modelling environment. Also, we introduced new *TRADES Tool* extensions to support user/modeller interaction with the imported information.

The model-to-model transformations are underpinned by the previously designed TRADES metamodel and, specifically, the "threat" and "control" concepts embedded within the metamodel. These concepts were previously established as concepts that are essential for security analysis [7]. The existence of such concepts and the relations between them allows for accommodating external information as specific/specialised instances of

these concepts, while still maintaining correct-by-construction security analysis models. For this work, we extended the metamodel—which is a core element of the *TRADES Tool* security modelling tool—with additional concepts that allow for tracking the source of external information to provide users with proper references and access to additional information, as discussed in Section 3.1. Additionally, pertinent user interface mechanisms—such as dedicated representational enhancements and import dialogues—were developed, extending the *TRADES Tool*.

For importing attack patterns from CAPEC, we developed a model-to-model transformation from the official MITRE CAPEC XML (Extensible Markup Language) file—downloadable from the online CAPEC website—to a TRADES catalogue, which is a model that is fully compliant with the extended TRADES metamodel (by-design). Every attack pattern appears in the TRADES catalogue as an external threat element. For ATT&CK information, an XML file was not available; instead, we developed tools to download relevant web pages from the online ATT&CK repository and parse them into a TRADES catalogue which contains both ATT&CK techniques (as external threat elements) and mitigations (as external control elements). The CAPEC and ATT&CK transformations were implemented as Python programs. We allow users to trace each external element to its CAPEC/ATT&CK catalogue by specifying—for each element—a link to the original knowledge base's entry.

For importing NIST SP800-53 security controls, we rely on translation from their OSCAL representation into TRADES model elements. First, OSCAL files can be imported into our workspace, instantiating designated OSCAL security control concept elements and resulting in a complete OSCAL catalogue, including detailed attributes and parameter names for each security control. Security controls from the catalogue can then be used within a specific threat and risk assessment, by creating uniquely identified external control elements for each desired security control. This includes setting parameters' values for the control's description. The resulting elements are traceable to their security control concept as it appears in the imported OSCAL catalogue, providing users with access to pertinent information within the modelling environment itself.

All of the mechanisms described in this paper—including our model-to-model transformations and the extended *TRADES Tool*—are available as open-source solutions in a public, online repository [23].

3. Results

3.1. TRADES Tool Extension

Figure 1 shows the *TRADES Tool* metamodel extension, designed to provide references to external knowledge bases in order to trace the origin of imported threats and security controls. This involves new concepts, designated in magenta, and their interrelations as well as relations to existing concepts, which appear in yellow. An "ExternalElement" abstract class conveys the concept of linking to external references. The class includes three attributes: source, for naming the external source of the element (e.g., CAPEC or ATT&CK); link, to provide a direct link to a pertinent record of the external source; and sourceID, to uniquely identify the source. When importing threats, the identifier of CAPEC or ATT&CK ("Capec" or "Attack", respectively) is also added as a prefix to the threat ID, together with its original identification number in each catalogue. Two additional classes are then specified: "ExternalThreat", which is typed as the TRADES "Threat" class/concept as well as the newly introduced "ExternalElement" and is used for expressing externally sourced threat elements, and "ExternalControl", which is typed as the TRADES "Control" class/concept as well as the newly introduced "ExternalElement" and is used for expressing externally sourced security control elements. An existing relation—"mitigatedThreats"—is allowed from Control elements to Threat elements (with a cardinality of [0..*], i.e., there can be any number of relations between the elements) and—by inheritance—is also allowed from ExternalControl elements to ExternalThreat elements.

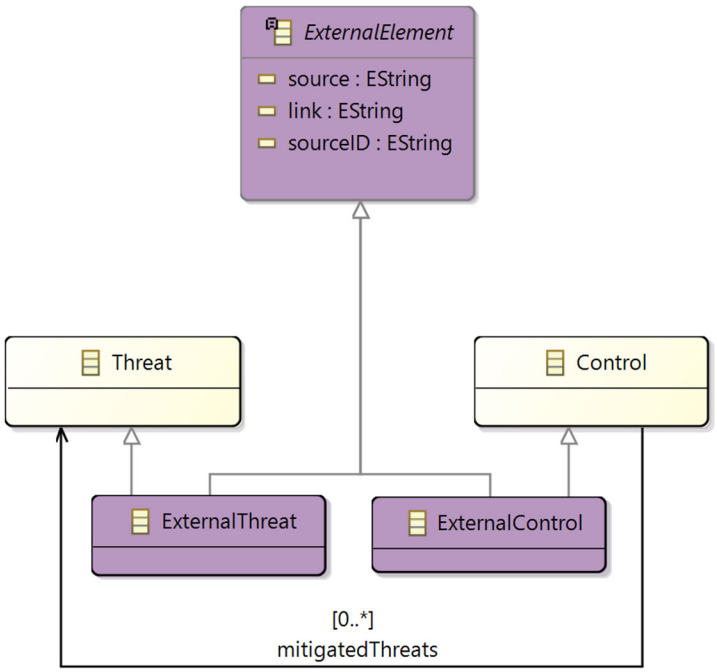

Figure 1. TRADES metamodel extension to support external references.

The extended metamodel definitions are also used for generating model-based representations:

1. Unique symbols are used to differentiate externally sourced threat and control elements from those that are not externally sourced. Figure 2 shows this extended *TRADES Tool* notation.
2. A dedicated "Properties" view shows the additional attribute of an external element to the user, as well as allows accessing the information source (if applicable). Figure 3 shows an example of this view for a specific threat element adopted from CAPEC. The name, CAPEC identification number and description are shown, as well as the designation of CAPEC as the source. Also, the "link" section offers a direct, clickable link to the threat as it appears on the CAPEC online website. This provides the user with pertinent information as well as the means to further research the originating knowledge base.

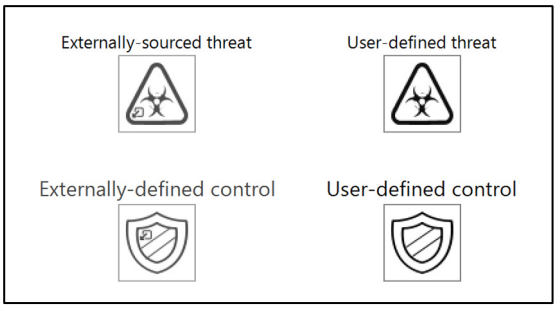

Figure 2. Representation of externally defined vs. user-defined elements.

TRADES Tool is also extended with dialogues for importing catalogues into the security modeller's working environment. Figure 4 showcases the dialogue for importing OSCAL catalogues (used in our work to import NIST SP800-53 security controls). It allows the user to select the catalogue source between a built-in catalogue (currently a specific version of the NIST SP800-53 is embedded) and an external catalogue file.

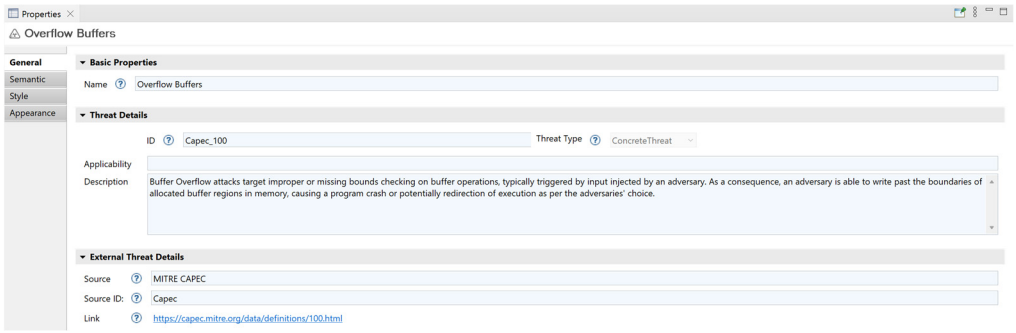

Figure 3. An extended "Properties" view, showing attributes of an external element (the "Overflow Buffers" threat element, imported from CAPEC).

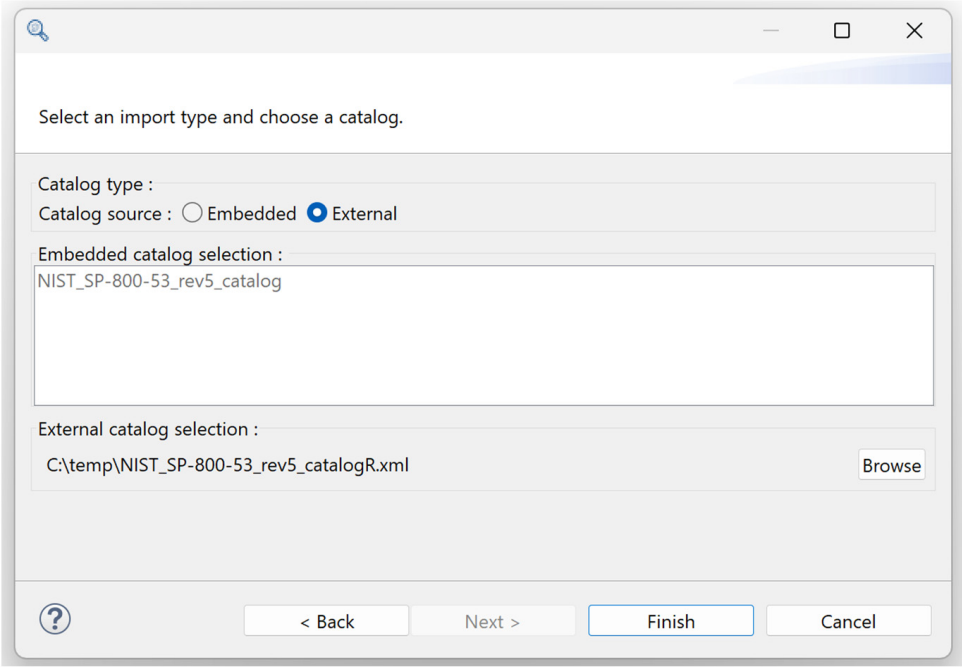

Figure 4. OSCAL catalogue import dialogue.

CAPEC attack patterns, ATT&CK techniques and NIST SP800-53 security controls are all available as catalogues for the *TRADES Tool* modelling environment. A total of 559 CAPEC attack patterns exist in the automatically generated CAPEC TRADES catalogue, containing all CAPEC attack patterns of the current version—version 3.9. A total of 354 ATT&CK attack patterns exist in the automatically generated ATT&CK TRADES catalogue, containing all ATT&CK techniques relating to Enterprise (201), Mobile (72) and Industrial Control Systems (81) of the current version—version 14.1. Also, all 106 ATT&CK mitigation techniques appear in the ATT&CK TRADES catalogue (43 Enterprise mitigations, 12 Mobile mitigations and 52 Industrial Control Systems mitigations, with 1 mitigation—M1013—shared between Enterprise and Mobile). The entire NIST SP800-53 catalogue in its up-to-date revision (5.1.1) is available, directly imported from its OSCAL XML file [17] into the modelling environment. Figure 5 shows these three catalogues imported into a working environment of *TRADES Tool*. The "Catalogs" folder hosts the three catalogues as lower-level elements. The CAPEC and ATT&CK catalogues include threat and control elements representing each of the attack patterns/techniques/mitigations. The elements are not shown explicitly in the figure, yet their presence is denoted by the ">" symbol on the left of each library, which allows the user to expand the view and browse the elements. The NIST SP800-53 catalogue is shown with the various high-level "folders" used to arrange

the lower-level security controls. The ">" symbol on the left of each folder denotes the ability to expand and browse the specific controls. Figure 6 shows a potential use of the catalogues within the modelling tool. The security modeller can use the search option at the top of the "Model Explorer" panel (shown in the figure) to search for elements containing "*access*control" and receive a filtered representation of the catalogues, which shows two threat elements originating in CAPEC definitions and several security controls—in various levels of hierarchy—originating in NIST SP800-53 definitions.

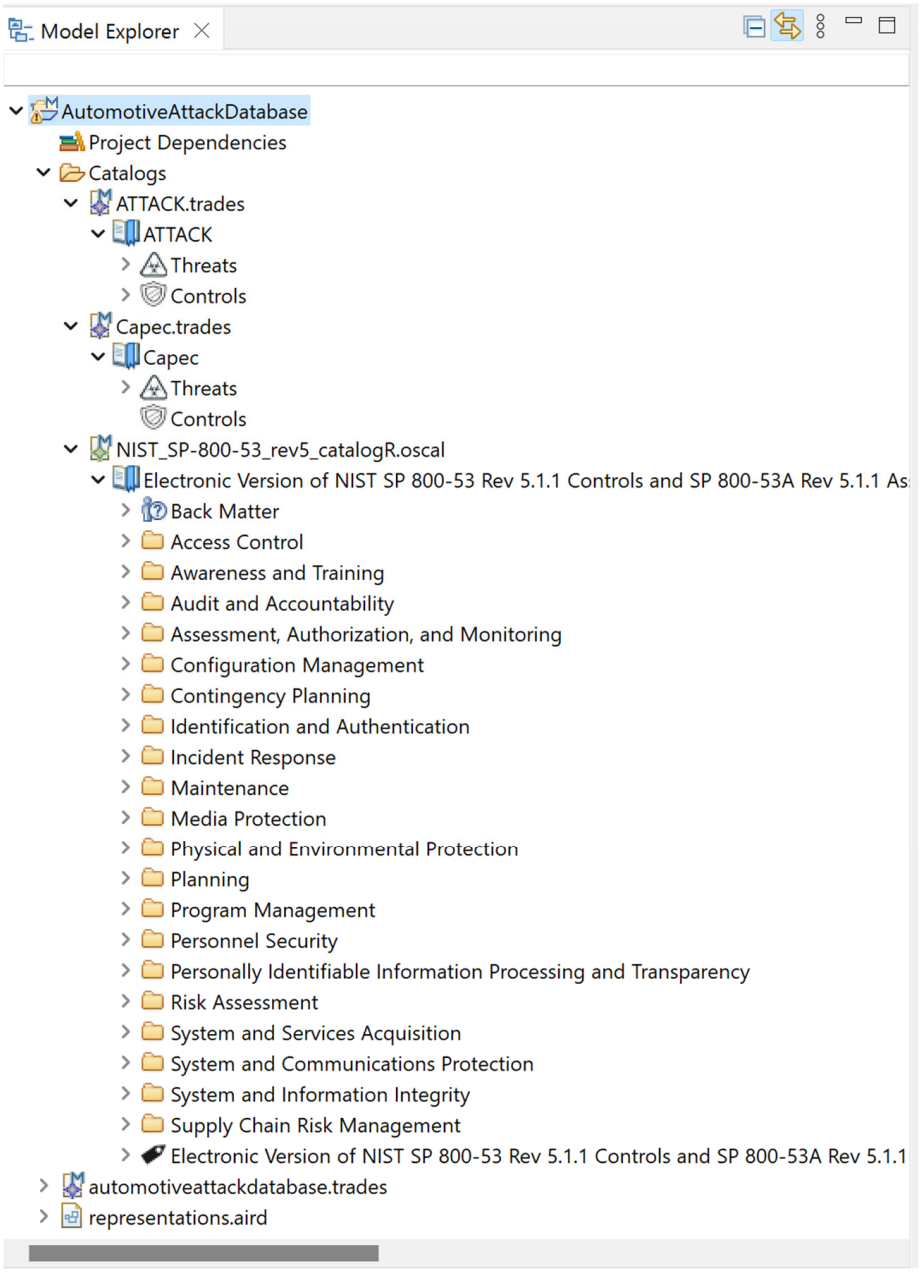

Figure 5. A partial screenshot of a panel from the modelling tool, showing all three catalogues—CAPEC, ATT&CK and NIST SP800-53—successfully installed.

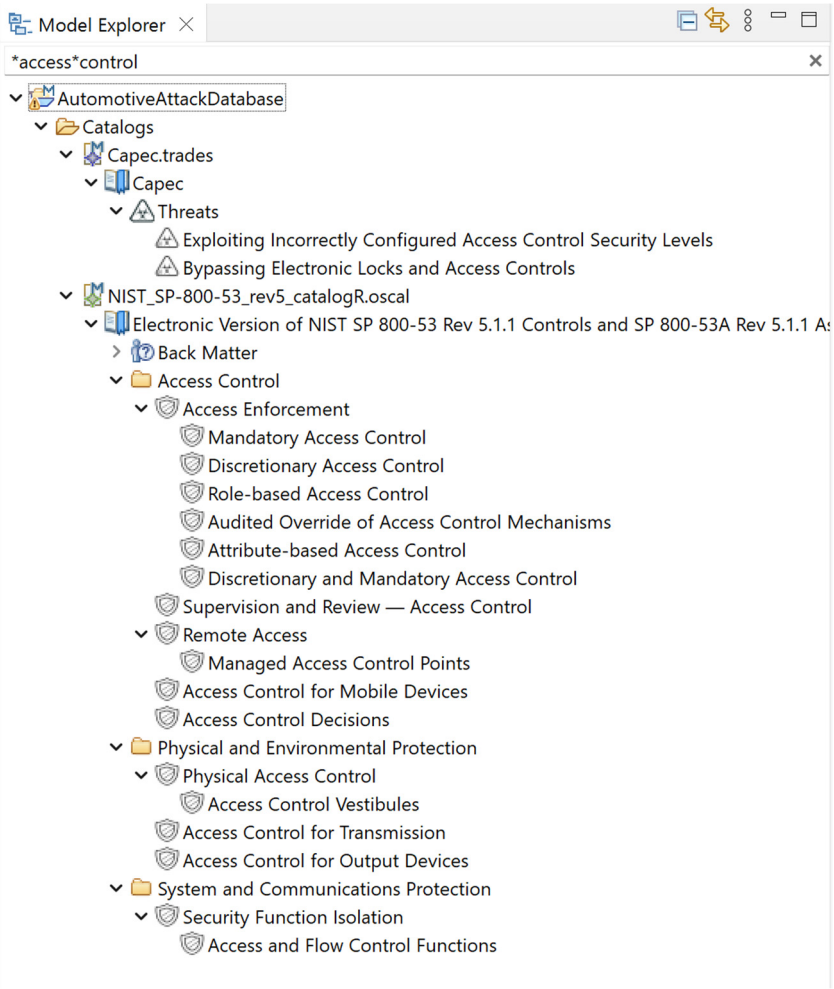

Figure 6. A panel from the modelling tool, showing a filtered view with relevant results from the installed catalogues.

3.2. Curating Security Guidance from Multiple Knowledge Bases

We provide a generalisable example of using the extended *TRADES Tool* to curate security-related information from multiple sources. We discuss the mapping of a specific threat—threat #6 of the United Nations' vehicle cyber security regulation (henceforth: UN-T6) [24]—to CAPEC and ATT&CK information, based on the work by Sommer et al. [11]. We selected this particular threat's mapping due to the relatively low number of mappings to CAPEC and ATT&CK (as identified originally by Sommer et al.), which allows us to concisely demonstrate our contribution to representing and improving the mapping, without overloading the reader.

Figure 7 shows an extended *TRADES Tool* representation of the UN-T6 threat element mapping to CAPEC and ATT&CK, based on the mapping by Sommer et al. This representation suggests a possible authoring technique to curate security information using the extended *TRADES Tool*. The UN threat (UN-T6) is denoted with a red label, and its mappings to other security knowledge bases appear with red edges. Threat elements and relations derived from CAPEC are denoted with black labels and black edges, respectively. Threat and Control elements and relations derived from CAPEC are denoted with blue labels and blue edges, respectively. UN-T6 maps into two CAPEC attack patterns—"Adversary in the Middle (AiTM)" (CAPEC94) and "Content Spoofing" (CAPEC148)—and one ATT&CK technique—"Adversary-in-the-Middle" (T1557). In Sommer et al.'s original mappings of UN threats to ATT&CK, the association of ATT&CK mitigations remains implicit, by their association with the specific ATT&CK techniques that are mapped to each

threat. For UN-T6, the original mapping to ATT&CK T1557 suggests seven mitigations. Using the extended *TRADES Tool*, we explicitly represent these mitigations as security control elements. Figure 7 shows the ATT&CK mitigations as Control elements as well as their mitigation relations to the related ATT&CK-derived threat element.

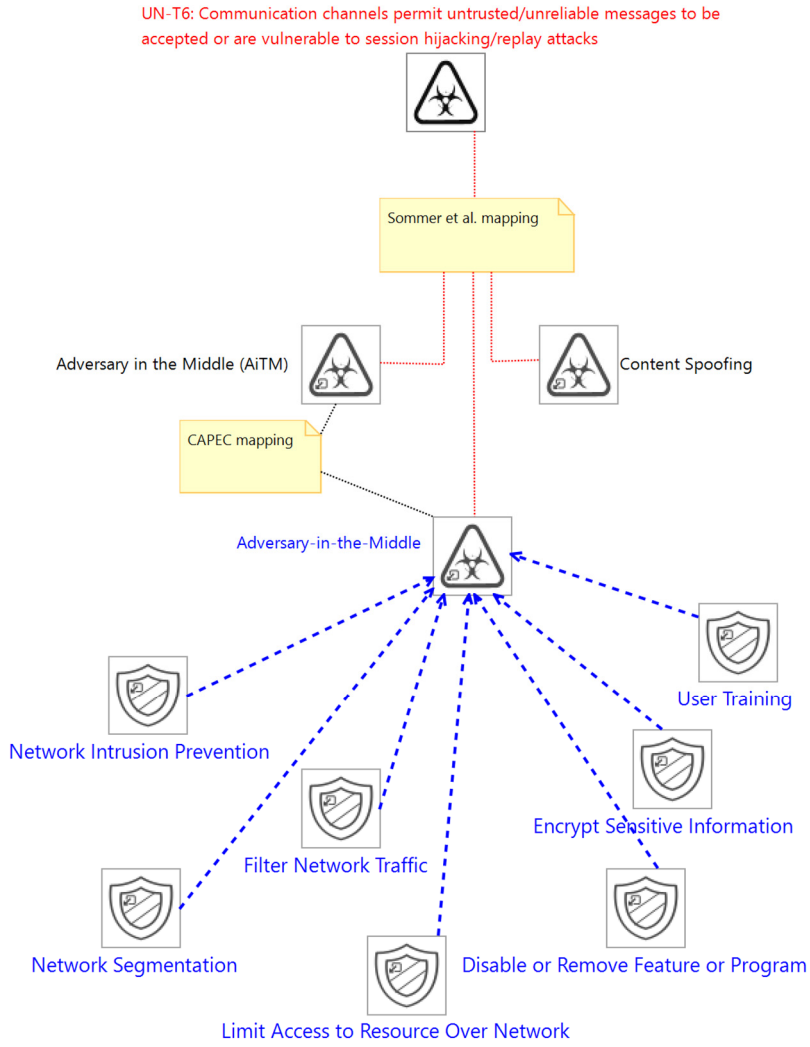

Figure 7. Mapping of UN-T6 to other knowledge bases, based on [11] and visualised using the extended *TRADES Tool*.

The representation in Figure 7 allows for visual, graph-like navigation of the UN threat (UN-T6) mapping, with each element pointing to a respective model element and allowing the security modeller to receive additional information based on the element's properties (e.g., Figure 3) or links to external references. Such representations can be helpful to communicate the mappings and their use as security guidance. The specific representation of UN-T6 mapping can, for example, raise a question with the viewer/reader as to the possible exploitation of ATT&CK to address the CAPEC Content Spoofing pattern. This gap is not communicated by the original textual/table orientation of the mapping [11]. If one methodically looks into the mapping method then—since the specific CAPEC pattern suggests a mapping to an ATT&CK technique—there should be a mapping between the CAPEC pattern into the relevant ATT&CK technique, and this can possibly lead to some ATT&CK-derived mitigation guidance. Specifically, CAPEC maps "Content Spoofing" to ATT&CK's "Defacement" (T1491), and ATT&CK associates this technique with a single mitigation: "Data Backup" (M1053). Figure 8 shows the expanded mapping. Sommer et al. do not explain why "Content Spoofing" and, consequently, UN-T6 remain unmapped to

the relevant ATT&CK technique and mitigation. A possible explanation may be that the specific ATT&CK technique is deemed irrelevant to the domain of interest (automotive). Figure 8 also suggests a possible methodical improvement of the mapping, by omitting the direct link from UN-T6 to the ATT&CK technique. The representation in the figure stresses that this mapping relies on CAPEC mapping rather than original/user mapping. This can be helpful in differentiating and tracing policy/application decisions from knowledge base derived information.

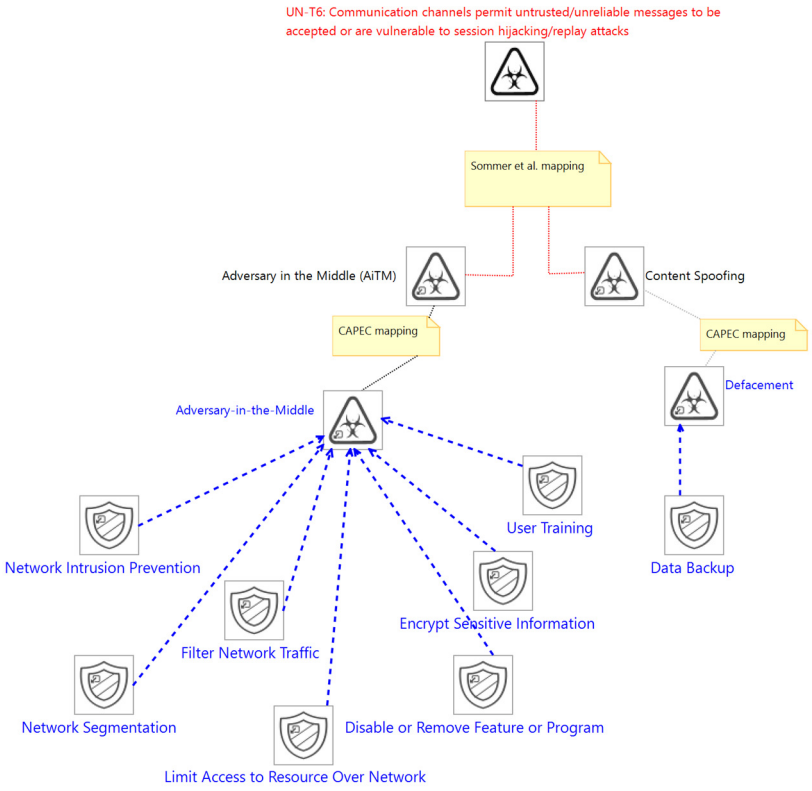

Figure 8. Expanded mapping of UN-T6 to other knowledge bases, visualised using the extended *TRADES Tool*.

NIST SP800-53 provides a more comprehensive and structured catalogue of security controls, compared with ATT&CK. A curation of security policies could include additional mapping between NIST security controls to the CAPEC- and ATT&CK-derived threat elements. In Figure 9, we offer a non-exhaustive extension of the UN-T6 threat mapping to include some pertinent NIST security controls. The NIST security controls and their mitigation relation to ATT&CK threat elements are denoted in black. Each of the associated NIST security controls has significantly more content—including specific parameters and specific control enhancements (de facto, lower-level security controls)—to assist a system designer in implementing the security control. For example, NIST offers two training-related controls—"Literacy Training and Awareness" (AT-2) and "Role-based Training" (AT-3)—that can be used to further design the "User Training" mitigation offered by ATT&CK. The description for ATT&CK's "User Training" mitigation says "*Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction*". Figure 10 shows the extended *TRADES Tool*'s dialogue for importing NIST's "Literacy Training and Awareness" security control. It illustrates the more extensive mitigation guidance offered by NIST (compared with ATT&CK), of which only an excerpt appears in the "Documentation" text area. The figure also demonstrates the ability—built into the extended *TRADES Tool*—to assist users in tailoring the control: the parameter "organization-defined frequency" can

be set by the user (e.g., to "once a year") and reflected in the description of the control (see the highlighted text in the figure).

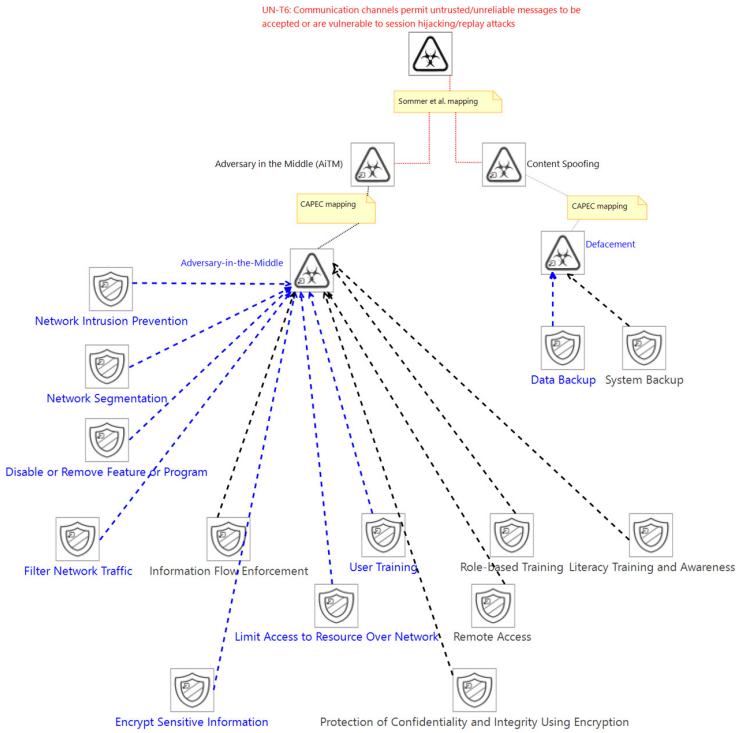

Figure 9. Extended mapping of UN-T6, with additional NIST security controls, visualised using the extended *TRADES Tool*.

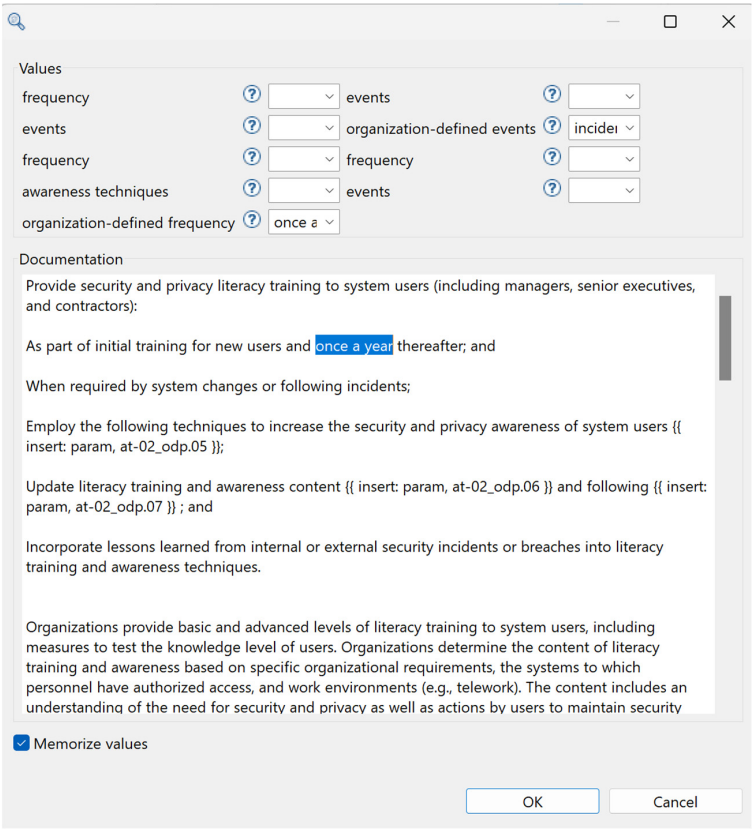

Figure 10. User dialogue in *TRADES Tool*, for importing a NIST security control using OSCAL.

4. Discussion

Threat and risk assessment is a creative effort that should rely on the available security body of knowledge. While threat and risk assessment is likely to remain manual—at least to some extent—due to its creative nature, utilising existing security knowledge bases can contribute to its systemisation and rigour. In this work, we provide an extended security modelling environment. This environment can incorporate and integrate information from multiple security knowledge bases. Specifically, catalogues of threats and security controls are automatically derived from three knowledge bases: CAPEC, ATT&CK and NIST SP800-53. These catalogues are made available within the *TRADES Tool* security modelling environment. Relations between elements imported from these catalogues can be established and their mappings can be visually represented.

The extended *TRADES Tool* modelling environment and the model transformations that generate catalogues are available as open-source solutions, addressing an existing gap [11]. Two complementary aspects of the tools being open are: (1) allowing for extension and updating of information from the available, supported knowledge bases. This can be performed at the user level in a way that accommodates revisions in the knowledge bases; and (2) allowing for adapting and extending the use of knowledge bases within the modelling environment. This can be performed at the organisation/developer level.

We have provided a highly generalisable example of using the modelling environment to integrate and enhance the use of security knowledge bases. By carefully curating and investigating information from knowledge bases, users—typically security specialists, security analysts or security engineers—can compose domain-specific/organisation-specific security guidance and policies. We have demonstrated how the modelling environment can support this as well as how this can be communicated graphically using the tool. Specifically, any derived, tailored or integrated organisational/domain guidance can be differentiated from the more general, public-domain body of knowledge. Still, the relations between the specific guidance and the body of knowledge allow for impact analysis as a result of changes in the integrated knowledge bases. Further adaptations of the tool's representations can be developed by practitioners, accommodating specific needs. Future research can also provide adaptations, exploring how well-structured security models can be effectively composed and communicated.

While our efforts to translate information from existing knowledge bases into *TRADES Tool* were successful, we identified a lack of a standardised form for security knowledge bases as a gap that future work can address. NIST's OSCAL is a step forward in the standardisation of security controls, yet ATT&CK mitigations are not officially available in OSCAL form. Also, while CAPEC patterns are available as a self-contained XML file, ATT&CK information is not. Future efforts may seek to provide a standardised form for attack patterns, techniques and mitigations. The rigorous, ontology and model-based approach that underpins *TRADES Tool*—and allows one to correlate threats with controls—can provide a preliminary direction for such efforts, possibly in tandem with the design of a formal ontology [5,13].

Future work may incorporate additional knowledge bases into *TRADES Tool* in an integrative form. For example, *TRADES Tool*'s underlying methodology is currently being expanded to support vulnerability management, and this can facilitate the integration with MITRE's Common Weakness Enumeration knowledge base. Furthermore, if practiced extensively, TRADES models that integrate and extend various knowledge bases can be used for mining and contributing new security insights—such as a definitive mapping of NIST security controls to CAPEC/ATT&CK or relations between threats in various levels of abstraction. TRADES-based threat modelling can, therefore, contribute to elaborating the codified security body of knowledge.

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

Data Availability Statement: The data presented in this study are openly available in the TRADES Tool GitHub repository.

Acknowledgments: The author wishes to thank Tom Melham for his continuous support.

Conflicts of Interest: The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Victoria Drake Threat Modeling (The OWASP Foundation). Available online: https://owasp.org/www-community/Threat_Modeling (accessed on 7 March 2024).
2. Messe, N.; Chiprianov, V.; Belloir, N.; El-Hachem, J.; Fleurquin, R.; Sadou, S. Asset-Oriented Threat Modeling. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; IEEE: Piscataway, NJ, USA; pp. 491–501.
3. Eckhart, M.; Ekelhart, A.; Weippl, E. Automated Security Risk Identification Using AutomationML-Based Engineering Data. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1655–1672. [CrossRef]
4. Xiong, W.; Lagerström, R. Threat Modeling—A Systematic Literature Review. *Comput. Secur.* **2019**, *84*, 53–69. [CrossRef]
5. Maunero, N.; De Rosa, F.; Prinetto, P. Towards Cybersecurity Risk Assessment Automation: An Ontological Approach. In Proceedings of the 2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Abu Dhabi, United Arab Emirates, 14–17 November 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 628–635.
6. Seehusen, F. Using CAPEC for Risk-Based Security Testing. In Proceedings of the Risk Assessment and Risk-Driven Testing; Seehusen, F., Felderer, M., Großmann, J., Wendland, M.-F., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 77–92.
7. Shaked, A. A Model-Based Methodology to Support Systems Security Design and Assessment. *J. Ind. Inf. Integr.* **2023**, *33*, 100465. [CrossRef]
8. Shaked, A. Digital Modeling of a Domain Ontology for Hospital Information Systems. In Proceedings of the Knowledge Discovery, Knowledge Engineering and Knowledge Management; Fred, A., Aveiro, D., Dietz, J., Salgado, A., Bernardino, J., Filipe, J., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 157–166.
9. Castiglione, L.M.; Lupu, E.C. Which Attacks Lead to Hazards? Combining Safety and Security Analysis for Cyber-Physical Systems. *IEEE Trans. Dependable Secur. Comput.* **2023**, 1–16. [CrossRef]
10. Granata, D.; Rak, M.; Salzillo, G.; Di Guida, G.; Petrillo, S. Automated Threat Modelling and Risk Analysis in E-Government Using BPMN. *Conn. Sci.* **2023**, *35*, 2284645. [CrossRef]
11. Sommer, F.; Gierl, M.; Kriesten, R.; Kargl, F.; Sax, E. Combining Cyber Security Intelligence to Refine Automotive Cyber Threats. *ACM Trans. Priv. Secur.* **2024**, *27*, 16. [CrossRef]
12. Casola, V.; De Benedictis, A.; Rak, M.; Villano, U. A Novel Security-by-Design Methodology: Modeling and Assessing Security by SLAs with a Quantitative Approach. *J. Syst. Softw.* **2020**, *163*, 110537. [CrossRef]
13. Oliveira, Í.; Sales, T.P.; Baratella, R.; Fumagalli, M.; Guizzardi, G. An Ontology of Security from a Risk Treatment Perspective. In *International Conference on Conceptual Modeling*; Springer International Publishing: Cham, Switzerland, 2022; pp. 365–379.
14. MITRE CAPEC. Available online: https://capec.mitre.org/ (accessed on 19 October 2022).
15. NIST Joint Task Force. *NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*; NIST Joint Task Force: Gaithersburg, MD, USA, 2020.
16. NIST OSCAL: The Open Security Controls Assessment Language. Available online: https://pages.nist.gov/OSCAL/ (accessed on 17 May 2023).
17. NIST's OSCAL-Content Repository. Available online: https://github.com/usnistgov/oscal-content/tree/main/nist.gov/SP800-53 (accessed on 7 March 2024).
18. Meng, B.; Larraz, D.; Siu, K.; Moitra, A.; Interrante, J.; Smith, W.; Paul, S.; Prince, D.; Herencia-Zapana, H.; Fareed Arif, M.; et al. VERDICT: A Language and Framework for Engineering Cyber Resilient and Safe System. *Systems* **2021**, *9*, 18. [CrossRef]
19. Riera, T.S.; Higuera, J.-R.B.; Higuera, J.B.; Herraiz, J.-J.M.; Montalvo, J.-A.S. A New Multi-Label Dataset for Web Attacks CAPEC Classification Using Machine Learning Techniques. *Comput. Secur.* **2022**, *120*, 102788. [CrossRef]
20. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model* **2022**, *21*, 157–177. [CrossRef]
21. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors* **2021**, *21*, 3267. [CrossRef] [PubMed]
22. Ozdemir Sonmez, F.; Hankin, C.; Malacaria, P. Attack Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases. *Comput. Secur.* **2022**, *123*, 102938. [CrossRef]

23. TRADES Tool Repository. Available online: https://github.com/UKRI-DSbD/TRADES (accessed on 7 March 2024).
24. UNECE UN Regulation No. 155: Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System E/ECE/TRANS/505/Rev.3/Add.154. 2021. Available online: https://unece.org/sites/default/files/2023-02/R155e%20(2).pdf (accessed on 7 March 2024).