Threat modeling of cloud systems with ontological security pattern catalog

Andrei Brazhuk

Abstract - **This work considers challenges, related to the lack of methods of automatic threat modeling and well-formed data sources of threats and countermeasures as well as techniques to collect such security knowledge. Cloud computing domain has been in a focus of security scientists and experts for decade, however it is still a problem to make secure the use of cloud systems and their applications, because of distributed nature, variety of deployment models, and different stakeholders.**

Towards automation of the threat modeling process we have proposed an ontological approach both to analysis of a system design (by an ontology-driven threat modeling framework) and creation of security patterns (by an ontological schema of security pattern). This work briefly describes those efforts and concentrated on an ontological catalog of cloud system threats. The work offers an Academic Cloud Computing Threat Patters (ACCTP) catalog as a way of the threat modeling of cloud systems and a set of design primitives as means of learning cloud security challenges.

Keywords — **cloud security, security patterns, threat modeling, knowledge management, OWL**

I. Introduction

Threat modeling of computer systems refers as an approach of identification potential security harm and applying countermeasures. Common approach of the threat modeling consists of an analysis of a system structure and creation of a threat model, aimed to figure out most of security issues. An informal graphical representation of the system structure, called Data Flow Diagram (DFD), is often used there. It is supported by the Open Web Security Project (OWASP) foundation. Common result of this process is a list of relevant threats and countermeasures, used for the risk analysis and making design decisions.

According [1] the threat modeling as an engineering discipline is still on a low maturity layer (defined as initial, ad-hoc); this is caused by lack of research, tools, techniques, practices. A set of actual challenges relates to the modeling, e.g. development of a reference model and reusable threat modeling artifacts, creation of knowledge bases, and design of modeling support. Considering an automation problem of threat modeling [2, 3], existing researches can be classified as traditional systems [4] based on standard data formats (XML, JSON) [5, 6], graph theory based systems [7, 8], and knowledge management based systems [9].

The knowledge management field is considered in this work. Towards automation of threat modeling we have proposed an ontological approach to both an analysis of a system design and creation of security patterns.

The security analysis of a system design has been approached by an ontology-driven threat modeling (OdTM) framework [10]. The OdTM framework uses a conception of ontological domain specific threat models as a way to use security knowledge. An ontological schema (format) of security patterns has been offered [11] to improve the security field. The schema allows creation of security (also threat) pattern catalogs, and mapping patterns with design decisions and security problems. To resolve a challenge of the threat model development, we have proposed a mechanism of creation of domain-specific threat models from security pattern catalogs.

In the focus of this work is the cloud security field. Providing security for cloud-based computer systems and their applications requires the strict division of responsibility where different parts of a system belong to different stakeholders (for example, a cloud provider manages background infrastructure, a network provider supports the Internet access, and customers are in charge of applications). Also, deployment model might change during a cloud system life cycle: at one stage it might be a private cloud application, at another stage it might be a scalable public cloud application.

This work offers an ontological catalog of cloud security threats and a set of learning design primitives. The catalog, called Academic Cloud Computing Threat Patterns (ACCTP), collects knowledge of risk-based cloud security models with the design terminology (like components, flows, boundaries, threats). The ACCTP catalog can be used as a domain specific threat model for the threat modeling of the cloud systems with the DFD approach. To better tackle security design challenges inexpert system architects (developers) can learn the set of design primitives in advance.

All the models, mentioned in this work, have been implemented as Web Ontology Language (OWL) ontologies. OWL has Description Logics (DLs) as a mathematical background. The DLs means are able to describe concepts of a domain and relations between them in very formal way and apply automatic reasoning features with relatively low computational complexity. The use of OWL allows involving strict formalization and object-oriented approach into the design of knowledge management systems, also applying various high-level means, like the Semantic Web Rule Language (SWRL) rules, and the SPARQL queries.

Manuscript received February 9, 2021.

Andrei Brazhuk (e-mail: brazhuk@grsu.by) is with the Yanka Kupala State University of Grodno, Grodno, Republic of Belarus.

To demonstrate our ideas a set of software tools has been developed with Java and the OWL API and Jackson JSON libraries. The tools (and the ontologies) are freely available with the GitHub service (see links below).

II. Related work

The knowledge management approach, based on ontologies [12], is proposed to solve various tasks of industry, medicine, education and science [13, 14]. Some papers are devoted to the information security field [15], in particular, creation of common ontological cybersecurity models [16, 17] based on well-known data formats, like Structured Threat Information eXpression (STIX) and Security Content Automation Protocol (SCAP). There are a lot of works, focused on the use of ontology engineering for different security aspects, like attacks, weaknesses, vulnerabilities [18]. However, this is still a challenge to use taxonomies, ontologies and the knowledge management approach both to the security by design (threat modeling) and operational security, like Cyber Threat Intelligence (CTI). None of existing semantic models covers all the information needed to provide effective CTI; and the problem of creation of multi-layered cyber threat intelligence ontology is quite urgent [19].

A security pattern is a description of security problems, which appears in specific context and presents well proven solution for the problems. Conceptually, security patterns transfer the security knowledge from experts to inexpert developers (system architects). Despite collecting the security (misuse, threat) patterns for decade [20, 21], there are several challenges of security pattern usage for modern computer systems, like lack of methods to identify the necessity of security patterns for a computer system design, and need to their redesign to better tackle modern security problems.

There are several works aimed to formalize security patterns by Unified Modeling Language (UML) [22], Attack Defense Trees (ADT) [23], Model driven approach [24], and OWL ontologies [25, 26]. We have taken some results from [25] and [26] to our schema of security pattern and enrich these results by involving of context and security characteristics in order to enable better mapping between patterns and security context of design decisions.

Cloud security field seems to be researched well, and there are several industry documents and best practices. In 2009 the European Union Agency for Cybersecurity (ENISA) issued a document [27] containing recommendations related to cloud computing security. It has explained cloud computing risks in the technical, policy and legal implications, and based on the ISO/IEC 27005 interpretation of risks as a discrete security risk matrix, the dimensions of which are the probability of threat and impact to business.

The quantitative risk and impact assessment framework (QUIRC) has been presented to assess security risks associated with cloud computing platforms [28]. Work [29] has proposed a cloud security taxonomy based on the architecture, compliance and privacy dimensions.

The EU-hosted project "SEcure Cloud computing for CRitical infrastructure IT" (SECCRIT) has aimed to analyze and research cloud technologies in terms of the security risks and development of methodologies, technologies, and guidelines to create secure, trusted cloud computing environments for critical IT infrastructure [30].

Work [31] has presented a pattern-based approach to the cloud security, including a security reference architecture. And more modern work [32] has described a cloud security pattern catalog with a case study of the Amazon and Azure clouds.

Recent years the security of new cloud based technologies is in research focus [33, 34], like Internet of Things (IoT) [35, 36], Edge computing [37], Cyber physical systems [38], and Machine learning [39].

We have taken in consideration the cloud security challenges as a well-researched topic to learn a knowledge integration problem in the security field [40, 41] using the best findings of the semantic approach [42].

III. Ontology-driven threat modeling ecosystem

We have proposed the ontological approach to the threat modeling as a method of security knowledge management and automatic threat modeling. Fig. 1 shows the ontology-driven threat modeling ecosystem.

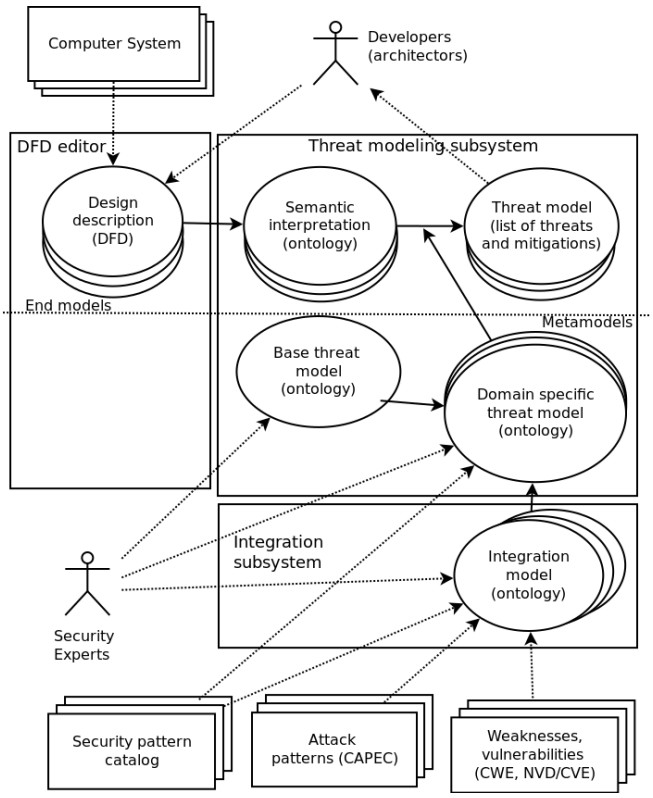

Fig. 1. Structure of ontology-driven threat modeling

A system architect describes a computer system with a data flow diagram (DFD); then automatic reasoning procedures are used to semantically interpret the diagram and figure out relevant threats and countermeasures for the system [10]. A domain specific threat model should be used to perform automatic reasoning. A security expert uses the base threat model to create various domain specific threat models.

Necessary software tools (threat modeling and integration

subsystems) are being developed (you can find the base threat model and our software tools by the link https://github.com/nets4geeks/OdTM). At the moment a simple tool (consoleApplication) exists that is able to load ontologies of the base threat model and domain-specific threat models, read a JSON file of a diagram, compatible with the third-party DFD editor OWASP Threat Dragon (https://threatdragon.org/), create a semantic interpretation of the diagram, and generate a list of threats by the automatic reasoning. Then it is possible to load the modeling results as a JSON file to Threat Dragon for further analysis.

There is a challenge of development of domain-specific threat models. This requires well-formed pieces of expert knowledge and approaches to collect it. Towards a decision we have proposed to use catalogs of security patterns for creation of domain-specific threat models. A security expert uses an existing security pattern catalog and creates mapping between it and a particular threat model. An ontological schema (format) of security pattern has been developed to enable that [11]. The schema is based on a conception of context security pattern, which contains a precise description of security problems and their solutions. Also it has the criteria that allow to “automatically” answer the questions like “Is a pattern suitable for a system design?” and “Does the pattern solve a particular security problem, valuable for its context?”.

Fig. 2 shows a structure of the security pattern schema. The first three sections represent common features, like idea, author, type, hierarchy of patterns, and a set of characteristics used by the scientific community.

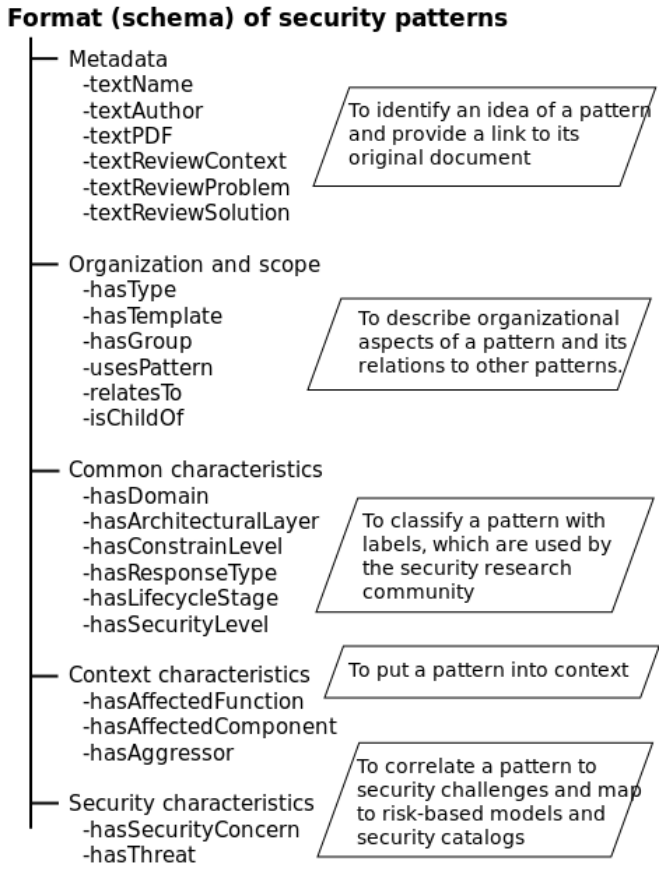

Fig. 2. Structure of security pattern schema

The last two sections are used to put a pattern into a context (via the "hasAffectedFunction", "hasAffectedComponent", and "hasAggressor" properties) and define its applicability as a solution of a security problem (via the "hasSecurityConcern" and "hasThreat" properties). Note, for each domain it requires a model of typical components.

Development of a WEB-based editor of security patterns is further work (you can find the schema and tools there https://github.com/nets4geeks/SPCatalogMaker).

Currently, creation of a catalog includes two stages. Firstly, an ontology, based on the schema, should be created to describe concepts and instances of a specific computing environment. Then a JSON-schema file from the ontology can be generated by a simple tool (Maker). Secondly, pattern descriptions can be created as JSON files with a JSON-schema based editor. Maker allows generating of an ontology of security patterns from the pieces of JSON.

IV. Academic Cloud Computing Threat Patterns Catalog

We have developed the Academic Cloud Computing Threat Patterns (ACCTP) catalog in order to enumerate common threats of cloud-based computer systems and use them for proof the feasibility of the ontological approach to the management of security patterns and threat modeling with DFDs.

The ACCTP catalog is based on the data of the common security knowledge sources like ENISA and OWASP, as well as the academic community findings, mentioned in the "Related work" section. In fact, the catalog “mines” the knowledge of the existing risk-based cloud security models and maps the risk-based terminology (risks, assets) to the design terminology (components, flows, boundaries, threats).

There are several benefits of the ACCTP both for research community and industry. It enables a design point of view with compliance and privacy aspects of the cloud security. Compliance aspects are important, because this requires strict division of responsibility between different actors (customers, cloud providers, network providers). Privacy aspects matter because of a trend towards more stringent personal data legislation like EU General Data Protection Regulation (GDPR) or Russian Federal Law On Personal Data.

The ACCTP catalog uses labels to map the security entities (threats, countermeasures) and classify them. The designed threats are marked by the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) model, proposed by Microsoft as a basics of their STRIDE-per-element threat modeling approach. The STRIDE items can be mapped to security objectives, like Confidentiality, Integrity, and Availability, known as the CIA triad; also Authentication, Non-repudiation, and Authorization. The difference of CIA-like labels from STRIDE is that STRIDE represents adversary point of view rather the viewpoint of resource owner.

Creation of the catalog of cloud threat patterns has required two steps, according our approach. Firstly, an ontological model of cloud computing environment has been

created. Fig. 3 shows a structure of the model. The "Process" and "ExternalInteractor" entities are taken from the base threat model [10], so the "CloudInfrastructure" (as an implementation of a cloud) and "CloudApplication" (a product of the cloud infrastructure) concepts are subclasses of "Process"; "ExternalService" and "RemoteUser" are subclasses of "ExternalInteractor". The "ServerComponent" and "ClientComponent" represent common interpretation of network communication, for example, external service is a server component, and remote user is a client component. Cloud application can be the Infrastructure as a Service (IaaS) application (or virtual machine), Platform as a Service (PaaS) application, or Software as a Service (SaaS) application.

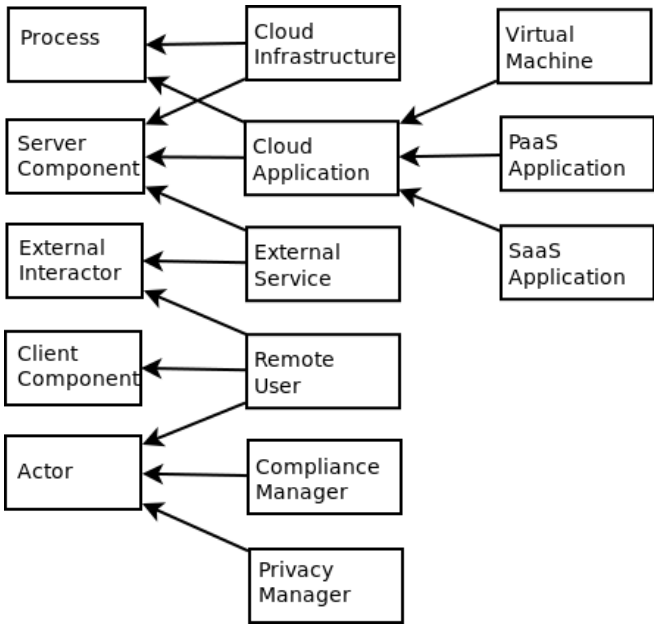

Fig. 3. Model of cloud computing environment

In Fig. 3 the "RemoteUser", "ComplianceManager", and "PrivacyManager" concepts are subclasses of the "Actor" concept, that involves a bit of role-based approach to the model. For example, drawing of privacy manger in a diagram causes extension of a threat model with the privacy-like threats. Note, the developer view is "bult-in", i.e. represents the base threats, mapped with components of a diagram.

Secondly, the threat patterns have been represented as JSON files with the JSON-schema, generated from the ontology, obtained on the first stage. To describe threat patterns the "Context", "Problem", and "Solution" fields of the POSA template format have been used. Also the context and security characteristics have been added.

In order to organize the threats, three base profiles [29] have been created: Architecture profile, Compliance profile, and Privacy profile (see Fig. 4).

The architecture profile contains threats close to a simple cloud system design, like use of a remote service by a cloud application; use of a cloud application (in particular by remote users); and threats to a cloud application, caused by client access of another cloud application, external service, or remote user.

The compliance profile holds threats related to responsibilities of cloud actors, restrictions of cloud environment, and legal issues.

The privacy profile is devoted to the confidentiality of information and personal data.

Also, the ACCTP catalog includes some extended profiles, like IaaS profile, PaaS profile, SaaS profile, and Storage profile; these profiles contain the threats close to specific types of cloud applications.

Example of a threat pattern from a web representation of the catalog (https://nets4geeks.github.io/acctp/) is shown in Fig. 5. The use of JSON allows easily generate various representations of the security knowledge.

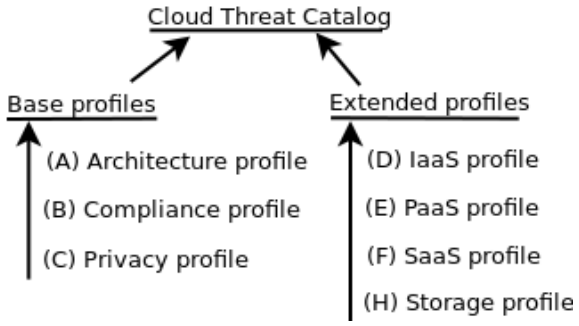

Fig. 4. Structure of the cloud threat catalog

AC01 Malware From Cloud Application

Context	Remote user interacts with a cloud application
Problem	Malicious content (malware) from the cloud application
Solution	Apply antivirus software (remote user); Apply malware scan (cloud application);
References	
Type	ns:type_ThreatPattern
Victim	su:comp_RemoteUser
Aggressor	su:comp_CloudApplication
Aggr. role	ns:role_Server
STRIDE	ns:STRIDE_Information_Disclosure; ns:STRIDE_Tampering

Fig. 5. Example of a threat pattern

V. Design Primitives of Cloud Threat Patterns

The use of the ACCTP catalog for threat modeling requires understanding of security issues and some design experience. We propose a set of design primitives to better tackle these challenges by inexpert users. Learning these primitives in advance enables better understanding security aspects of a diagram that represents a whole design of a computer system.

Fig. 6 shows five design primitives, that depict context of

common threats of cloud computing, used by our ontological catalog. Below short description of each primitive is given (details of threats can be got from the ACCTP catalog, see link above).

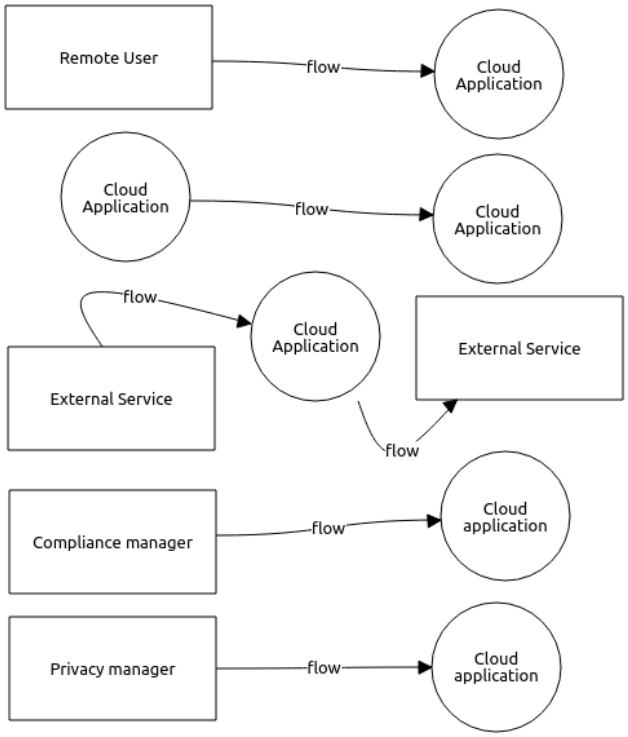

Fig. 6. Design primitives of cloud threat patterns

A) *Simple cloud application*. This scenario considers interaction of remote users with a cloud application. From the network perspective remote users are treated as clients and the cloud application as a server. And an application protocol (e.g. HTTPS) based on TCP/IP can be used for the data transmission.

The cloud application can affect remote users (as well as other entities acting as clients, like another cloud application or external service). For example, unexpected failure of the cloud application (the AB01 threat in ACCTP) or injection of malware (AC01, see fig. 5) can happen.

Clients (remote users, cloud applications, external services) can affect the cloud application. These threats are represented by the 'ADxx' and 'AExx' groups in ACCTP. Examples can be broken authentication (AD01) or DDoS (AE01).

B) *Interaction of cloud applications*. A cloud application often has several components, like frontend (web application) and backend (database or storage). These components influence each other from the security point of view. So, threats to a cloud application as a server and as client should be considered. Those threats are in the ABxx and ADxx groups, mentioned before.

C) *Interactions with external services*. A cloud application can use services, described as external, i.e. "as it is" or with weak agreement between a service and customer (from Cloud Application to External Service). This case is described by the 'AAxx' group of threats in ACCTP. An example can be spoofing of remote service (AA05).

And there is a case of the cloud application usage by an external service (from External Service to Cloud Application). The use of cloud applications is shown by the ABxx and ADxx groups, mentioned above.

D) *Compliance model*. It represents different aspects, depended on division of responsibility between different actors and some non-technical aspects. To enable this scenario, the "Compliance Manager" item should be used as a client.

F) *Privacy model*. It contains the security aspects of the privacy. To enable this scenario, the "Privacy Manager" item should be used as a client.

Fig. 7 shows an example of the ontological threat modeling of the Primitive A and threats assigned with remote users.

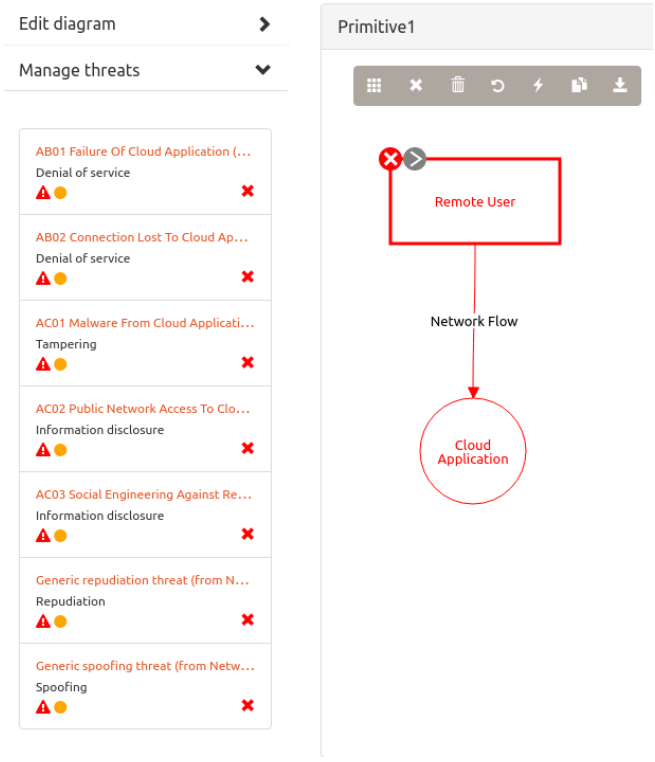

Fig. 7. Example of threat model in Threat Dragon

VI. Conclusions

This work offers the Academic Cloud Computing Threat Patters (ACCTP) catalog as a way of the threat modeling of cloud systems and a set of design primitives as means of learning cloud security challenges for inexpert architects and developers. The catalog contains different profiles (architecture, compliance, privacy, IaaS, PaaS, SaaS, cloud storage); all the entities are mapped to the STRIDE model. To learn security challenges it can be possible to use the primitives, describing interaction of remote users and a cloud application, communications of two cloud applications, interaction with external services and the compliance and privacy aspects.

Actual challenges for further research are development of a set of learning materials (like a guide how to use the model) and performing of a case study of feasibility and effectiveness of the ontological approach over non-formal methods and existing automatic-like approaches.

REFERENCES

[1] Yskout K. et al. Threat modeling: from infancy to maturity //Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: New Ideas and Emerging Results. – 2020. – С. 9-12.

[2] Tuma K. et al. Automating the early detection of security design flaws //Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems. – 2020. – С. 332-342.

[3] Xiong W., Lagerström R. Threat modeling–A systematic literature review //Computers & security. – 2019. – Т. 84. – С. 53-69.

[4] Schaad A., Binder D. Ml-supported identification and prioritization of threats in the OVVL threat modelling tool //IFIP Annual Conference on Data and Applications Security and Privacy. – Springer, Cham, 2020. – С. 274-285.

[5] Cagnazzo M. et al. Threat modeling for mobile health systems //2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). – IEEE, 2018. – С. 314-319.

[6] Schmittner C. et al. Threat modeling in the railway domain //International Conference on Reliability, Safety, and Security of Railway Systems. – Springer, Cham, 2019. – С. 261-271.

[7] Johnson P., Lagerström R., Ekstedt M. A meta language for threat modeling and attack simulations //Proceedings of the 13th International Conference on Availability, Reliability and Security. – 2018. – С. 1-8.

[8] Berger B. J., Sohr K., Koschke R. The Architectural Security Tool Suite—ARCHSEC //2019 19th International Working Conference on Source Code Analysis and Manipulation (SCAM). – IEEE, 2019. – С. 250-255.

[9] Faily S. et al. Contextualisation of data flow diagrams for security analysis //International Workshop on Graphical Models for Security. – Springer, Cham, 2020. – С. 186-197.

[10] Brazhuk A. Security patterns based approach to automatically select mitigations in ontology-driven threat modelling // Open Semantic Technologies for Intelligent Systems (OSTIS). – 2020. – №. 4. – С. 267-272

[11] Brazhuk A., Olizarovich E. Format and Usage Model of Security Patterns in Ontology-Driven Threat Modelling //Russian Conference on Artificial Intelligence. – Springer, Cham, 2020. – С. 382-392.

[12] Kudryavtsev D., Gavrilova T. An Overview of Practical Ontology Implementation in Decision Support Systems //International Conference Cyber-Physical Systems and Control. – Springer, Cham, 2019. – С. 19-26.

[13] Klyshinsky E. et al. Formalization of Medical Records Using an Ontology: Patient Complaints //International Conference on Analysis of Images, Social Networks and Texts. – Springer, Cham, 2019. – С. 143-153.

[14] Golenkov V. V. et al. Semantic technologies of intelligent systems design and semantic associative computers //Doklady BGUIR. – 2019. – №. 3. – С. 42-50.

[15] Sikos L. F. OWL ontologies in cybersecurity: conceptual modeling of cyber-knowledge //AI in Cybersecurity. – Springer, Cham, 2019. – С. 1-17.

[16] Takahashi T. et al. Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information //International Journal of Communication Systems. – 2018. – Т. 31. – №. 3.

[17] Doynikova E., Fedorchenko A., Kotenko I. A semantic model for security evaluation of information systems //Journal of Cyber Security and Mobility. – 2020. – С. 301–330.

[18] Martins B. F. et al. Conceptual Characterization of Cybersecurity Ontologies //IFIP Working Conference on The Practice of Enterprise Modeling. – Springer, Cham, 2020. – С. 323-338.

[19] Mavroeidis V., Bromander S. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence //2017 European Intelligence and Security Informatics Conference (EISIC). – IEEE, 2017. – С. 91-98.

[20] Washizaki H. et al. Taxonomy and literature survey of security pattern research //2018 IEEE Conference on Application, Information and Network Security (AINS). – IEEE, 2018. – С. 87-92.

[21] Jafari A. J., Rasoolzadegan A. Security patterns: A systematic mapping study //Journal of Computer Languages. – 2020. – Т. 56.

[22] Xia T. et al. Cloud security and privacy metamodel //Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development. – 2018. – С. 379-386.

[23] Salva S., Regainia L. A catalogue associating security patterns and attack steps to design secure applications //Journal of Computer Security. – 2019. – Т. 27. – №. 1. – С. 49-74.

[24] Hamid B., Gürgens S., Fuchs A. Security patterns modeling and formalization for pattern-based development of secure software systems //Innovations in Systems and Software Engineering. – 2016. – Т. 12. – №. 2. – С. 109-140.

[25] Guan H., Yang H., Wang J. An ontology-based approach to security pattern selection //International Journal of Automation and Computing. – 2016. – Т. 13. – №. 2. – С. 168-182.

[26] Vale A. P., Fernandez E. B. An ontology for security patterns //2019 38th International Conference of the Chilean Computer Science Society (SCCC). – IEEE, 2019. – С. 1-8.

[27] Catteddu D. et al. Cloud computing risk assessment //European Network and Information Security Agency (ENISA). – 2009. – С. 583-592.

[28] Saripalli P., Walters B. Quirc: A quantitative impact and risk assessment framework for cloud security //2010 IEEE 3rd international conference on cloud computing. – Ieee, 2010. – С. 280-288.

[29] Gonzalez N. et al. A quantitative analysis of current security concerns and solutions for cloud computing //Journal of Cloud Computing: Advances, Systems and Applications. – 2012. – Т. 1. – №. 1.

[30] SEcure Cloud computing for CRitical infrastructure IT. [Online]. Available: https://www.seccrit.eu, Accessed on: Nov 27, 2016.

[31] Fernandez E. B., Monge R., Hashizume K. Building a security reference architecture for cloud systems //Requirements Engineering. – 2016. – Т. 21. – №. 2. – С. 225-249.

[32] Rath A. et al. Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure //Computers. – 2019. – Т. 8. – №. 2. – С. 34.

[33] Soltys M. Cybersecurity in the AWS Cloud //arXiv preprint arXiv:2003.12905. – 2020.

[34] Sen A., Madria S. Application design phase risk assessment framework using cloud security domains //Journal of Information Security and Applications. – 2020. – Т. 55. – С. 102617.

[35] Mozzaquatro B. A. et al. An ontology-based cybersecurity framework for the internet of things //Sensors. – 2018. – Т. 18. – №. 9. – С. 3053.

[36] Choi C., Choi J. Ontology-based security context reasoning for power IoT-cloud security service //IEEE Access. – 2019. – Т. 7.

[37] Xiao Y. et al. Edge computing security: State of the art and challenges //Proceedings of the IEEE. – 2019. – Т. 107. – №. 8.

[38] Venkata R. Y., Kamongi P., Kavi K. An Ontology-Driven Framework for Security and Resiliency in Cyber Physical Systems //ICSEA 2018. – 2018. – С. 23.

[39] Wilhjelm C., Younis A. A. A Threat Analysis Methodology for Security Requirements Elicitation in Machine Learning Based Systems //2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C). – IEEE, 2020. – С. 426-433.

[40] Wen S. F., Katt B. Managing Software Security Knowledge in Context: An Ontology Based Approach //Information. – 2019. – Т. 10. – №. 6. – С. 216.

[41] Välja M. et al. Automating threat modeling using an ontology framework //Cybersecurity. – 2020. – Т. 3. – №. 1. – С. 1-20.

[42] Islam C., Babar M. A., Nepal S. Architecture-centric support for integrating security tools in a security orchestration platform //European Conference on Software Architecture. – Springer, Cham, 2020. – С. 165-181.