(IJESIR) International Journal of Science and Innovative Research
e-ISSN: 2724-3338
2021, 02(08)
https://novuspublishers.org/ Paper id: 0100071IJESIR

E-banking Information Security Risks Analysis Based on Ontology

Noura Salman Haidar , Muhammad-Mazen Al Mustafa

Faculty of Information Technology, Syrian Virtual University, Damascus, Syria

ARTICLE INFO

Received: 05.09.2021
Accepted: 29.09.2021
Final Version: 8. 11.2021

***Corresponding Author:**

Noura Salman Haidar
nourahaidar88@gmail.com

ABSTRACT

Electronic banking services have spread widely. Attacks by unauthorized attackers have increased. This leads to the need to secure the data exchanged between the bank and the customer. Efforts have been made to analyze attacks, know their causes and determine ways to mitigate them. But the analysis process needs to extract knowledge from different sources, present it in a simple and easy-to-understand way, and process it quickly and effectively. Here the need to rely on semantic techniques appears. Semantic techniques allow collecting information from different sources, integrating and reusing it effectively using ontology. Risks analysis based on ontology can make understanding the risks much easier and faster, so this facilitates escaping them. Many researchers used ontology in information security. But the previous security ontologies were general and complex, and could be applied in some fields, but could not be applied in others. Because of the importance and danger of financial transactions in this research, we studied some previous security ontologies and compared them with a goal to analyze electronic banking service attacks and propose an ontology that analyzes these attacks depending on concepts related to pre-defined security ontologies and electronic banking services.

Keywords: Ontology, Risk Analysis, E-Banking

Introduction

Electronic banking services are an integral part of modern banks due to its low costs, availability and ease of use. But it suffers from a fundamental problem, which is the protection of information exchanged between the bank and the customer. According to Singh, Ruhl and Samuel, although one goal of the EMV protocol is to secure debt and credit transactions at the Point of Sale (POS) terminal, there are still vulnerabilities that can lead to unauthorized disclosure of cardholder data and exploit it in many attacks like MITM, Pre-play Attack, NFC Relay Attack and Eavesdrop Attacks. The attack tree method was used to document vulnerabilities and countermeasures against various potential attacks provided [1]. While Ojeniyi, Edward and Abdulhamid analyzed the security risks of electronic banks through a questionnaire that determines the level of risks that may face the bank customers, and showed the need for more awareness regarding saving transaction details and passwords on the customer's devices. They also indicated that the bank should improve the applications to maintain its safety [2]. Eneeji studied the bank fraud. He showed that fraud occurs through impersonation, deception, hacking, and Trojan horses, and there must be a security system capable of defending against external attacks. He used intelligent neural networks and geographic

Copyright © 2021 by Author/s and Licensed by IJESIR-NOVUS Publications Ltd., Italy. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

information systems to monitor and detect fraud [3]. In 2020, Hammood said that the exchange of trust between the bank and the customer is very important. The most of the protection mechanisms are focused on the authentication processes. The customer authentication relies on techniques such as passwords and biometric authentication. And they suggested an authentication mechanism using the global mobile device identification number [4]. Hence, banks and customers have to implement security technologies and standards across devices, applications and network to ensure that data transmitted in a secure and consistent manner. The presence of a single vulnerability in any of them may be the cause of a dangerous and successful attack. The analysis of the attack requires large amounts of data from different sources. Knowledge management systems based on semantics are considered the best systems that suit these analyses.

Semantic Web and Ontology

Semantic Web

The Semantic Web is an extension of Web technology in which information has a special meaning, and it is possible to understand and satisfy people and machines requests using web content. In addition, the Semantic Web allows for effective discovery, integration, and reuse. In 2001, the Semantic Web was proposed by Tim Berners-Lee, James Handler, and Ora Lassia, with the aim of adding some human intelligence behavior to the Web. It can also be known as a symbiosis of web technologies and a representation of knowledge, forming the so-called smart data network, which makes searching easier and more productive. Semantic techniques represent meaning using ontology [5].

Ontology

Ontology is the mainstay in the field of semantic web to represent concepts and their relationships, and make the knowledge machine understandable [6]. Through ontology, we can understand the structure of knowledge that well reflects the complexity of the real world. It stores and processes knowledge, and contains not only raw data, but also the meaning of this data [7]. By creating a common vocabulary about the concepts of a field and the relationships between them, the ontology enables sharing a common understanding of the information structure between people and software agents, reusing knowledge, and making domain assumptions explicit. Besides automated computer heuristics, the adoption of ontology will enable reliable data entry, easier information sharing, homogeneous training, and software development among different actors [8]. Ontology consists of:

a) Individuals: these are the objects.
b) Classes: classes in programming languages or object types represent groups and concepts.
c) Attributes: they are characteristics or features.
d) Relationships: relationships between individuals.
e) Function terms: complex structures formed from certain relationships that can be used in place of an individual term in an expression.
f) Restrictions: these are formal, stated descriptions of what must be true for certain assertions to be accepted as input.
g) Rules: IF-else statements that describe the logical inference obtained from an assertion in a particular syntax.
h) Axioms: Assertions including rules in a logical form that together constitute the overarching theory that the ontology describes in its field of application.

i) Events: They change properties or relationships.

Ontology is a good way to systematically categorizes different security concepts, such as vulnerabilities, attacks, countermeasures, and the relationships among them. It also plays a significant role in collecting and analyzing large amounts of data, storing and reusing them later. Risks analysis based on the ontology can make understanding these risks easier and faster. This makes them easier to resist and get rid of them [9].

Method

First, we searched and studied information security risks in electronic banking services. Then, we studied and analyzed many researches that used ontology in the field of information security, and compared them to derive the most important concepts and relationships. Next, we added new concepts and relationships. After that, we linked security concepts with electronic banking service concepts through ontology relations to get the basic concepts of the proposed ontology.

Literature Review

Several researches have been published regarding the construction of ontologies in information security. In 2015, Souag, Salinesi, Mazo and Wattiau proposed security ontology for engineering security requirements, and an interactive environment was developed to facilitate the use of this ontology in engineering security requirements. The ontology was used because it is useful for representing and interconnecting many types of knowledge within a specific field, and because there is a need for security ontology to coordinate the ambiguous definition of information security concepts and their relationships. This ontology was general, so its implementation was more complex than expected, and took a long time to implement. It was necessary to work more than one team at the same time. It could also have been improved by increasing the knowledge and security experience of its workers, narrowing its scope or introducing concepts and relationships in another way. Technically, it could have been updated and moved to a newer version of (OWL / Protégé) [10]. Carvalho, Goldsmith and Creese proposed ontology for mapping criminal organizations and identifying developers of malicious programs by revealing the relationships between many unconnected evidences in 2015. This ontology depends on previous ontologies. This research confirms that ontology is very important in collecting and analyzing large amounts of data, and it can play a large role in investigating cybercrime and discovering evidence. This ontology focused only on malware scams. This ontology neglected fraudulent operations and other types of attacks that could affect any part of the banking system because of security vulnerability. This ontology did not provide security solutions that would mitigate the effects of the attacks [8]. In 2015, Stepanova, Pechenkin and Lavrova suggested the automation of the penetration testing process based on semantic web techniques. Semantic techniques are essential to extract process and store knowledge. This security ontology was developed using Protégé, and a software tool was developed to allow the analysis of data retrieved from various sources. This ontology provided a comprehensive view of the penetration test results, but some stages of the security analysis were not automated, including the clear perception rely on the ontology, and the implicit and explicit knowledge of the system under test. It was also a general

and a complex ontology [11].

While Rosa and Bonacin suggested security ontology to assess security to reach secured systems in 2018. The concept of security assessment is inherited from two concepts: systems evaluation and information security. Two software applications have been developed; the first receives a list of evaluation elements, their dimensions and security features, then, calculates the extent of information security coverage. The second supplies a graphical interface to generate evaluation designs. This ontology focused only on security assessment and not on the whole concept of information security. It ignored practical risk management and vulnerability analysis. It can also be improved by integrating it with other concepts, relationships and characteristics. The concepts used must also be validated by security assessment experts [12]. In 2018, Fenz and Neubauer suggested security ontology equipped with a decision support system to provide a way to formalize the information security features, verify its compliance with the official controls of ISO 27002, and identify the missing measures to ensure compliance and reduce risks to an acceptable level. Previous security ontologies were analyzed to find the concepts and relationships. Then, the ISO 27002 standard was analyzed. Next, new concepts and relationships were added to the previous ontology. After that, the rules created based on ISO 27002 specifications. Finally, a decision support system was developed to verify the company's level of compliance with the controls of the aforementioned standard. The advantage of this work was the existence of a semantic knowledge base confirming that all decision options were compatible with the aforementioned standard, considering the local characteristics of the organization in which they would be applied. It is a formal ontology and did not consider the attack's tool and methods. It focused on security standards according to a specific standard and ignored the rest of the security standards [13]. In 2018, Syed and Zhong developed an ontology-based conceptual model for managing vulnerabilities. This model integrates concepts from both formal sources like CVE and NVD, and informal sources like social media. This ontology extends the vulnerability concepts provided by the National Institute of Standards and Technology (NIST) and can be used as a general vocabulary in vulnerability management. It can be useful for thinking about entity relationships to issue security alerts for vulnerability analysis and management. This ontology focused on the vulnerability management and overlooked some concepts related to the attack that a vulnerability can cause, the tool of the attack, its strategy, and its goal and methods of achieving the target [14]. In 2018, Kotenko, Fedorchenko, Doynikova and Chechulin proposed an ontology-based approach for storing security data to link security data from various internal sources such as intrusion detection and prevention systems, network scanners, event logs, etc., and external ones such as CVE, CAPEC, and NVD, etc. The use of ontology allows easily merging data from different sources, and allows the use of more accurate queries and reduces the time required to process the query. The experimental results showed that using ontology enhances the management of systems security. But the disadvantage of this method is that it depends on the quality of the data stored in the ontology [15]. In 2018, Kotenko, and Doynikova proposed an approach to determine cyber-attack goals based on ontology of security metrics and Neuro-fuzzy networks. The information was got from various sources such as CWE, NVD, CVE and CAPEC. This approach has shown reliable results in preventing the spread of attacks on the information systems. But there are some limitations related to choosing the optimal response because it uses a rather approximate indicator. This ontology is general and focuses on finding the target of the attack in the information systems. It must be expanded in terms of the measures used, and introduces a mechanism for applying the fuzzy neural network to identify different classes of the targets of cyber-attacks [16]. In 2019, Wen and Katt proposed a security ontology to manage the security knowledge of the software considering the context of the application, as the software developers should not only have a general knowledge of security

concepts, but also about the context in which the software is developed. The ontological representation supports the integration of knowledge resources in the various levels of abstraction and advanced search for knowledge, thus supporting the process of sharing and learning about program security. Reliance on ontology is very important in many applications. This ontology has contributed to sharing a common understanding of public security concepts, ensuring application security during its development stages, and neglecting the risks that could face the application after launching and using. This ontology focuses only on software security and ignores hardware security [9].

Brazhuk (2019) discussed the problem of extracting and using knowledge from general dictionaries related to software attacks and their weaknesses to build semantic models of the threat. The aim of the model is to use it as a kernel of a knowledge management system in the field of software security. The reason for using the ontology is the multiplicity of knowledge sources in this field and the difficulty of manually analyzing them. The ontology can be used as part of an intelligent system or a distance learning system, and it uses descriptive logic whose main characteristics are to describe concepts and the relationships between them in a formal way with the possibility of thinking and deduction. This ontology can be used with any knowledge-based system. It's based on CAPEC and CWE. This model considered a software security, but neglected hardware security [17].

Results and Discussion

Previous studies were grouped according to their individual contribution. The goal is to understand the method of using the ontology in the field of information security, and to identify the most important concepts that must be present in any security ontology. See **Table (1)** and **Table (2)**. Comparing ontologies showed that:70% of the ontologies used a protégé platform. Query languages varied among SQWRL, SPARQL and DL. 90% of the ontologies used a prior ontology. 60% used international security standards and classifications. The concepts differed according to the different objectives of the ontologies. There are concepts used only once depending on the goal, and concepts were used many times, and the number of times the concept was repeated indicates its importance in information security. **Fig [1]** shows the percentage of repetition of concepts in the studied ontologies after deleting the concepts mentioned only once.

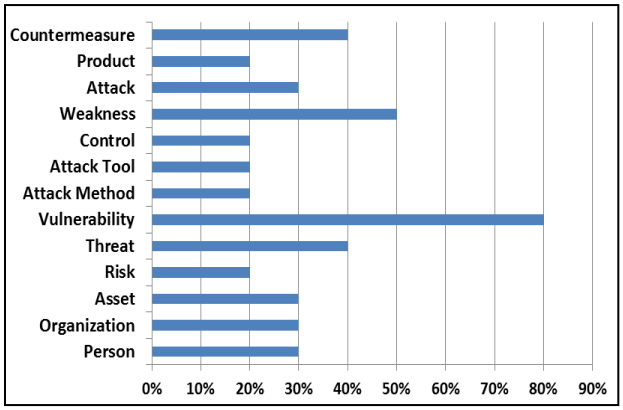

Fig 1: Percentage of concepts in the studied ontology

80% of the studied ontologies focused on the concept of the vulnerability that the attacker exploits carrying out the attack. 50% focused on the concept of a weakness, which represents an error in the design, environment or program, leading to a vulnerability that can be exploited in an attack. 40% focused on countermeasures, which represent the method of protection. 40% focused on the threat in its general sense, which includes the natural threat, security incident or intended threat (attack), the attack was mentioned only in 30% of the ontology and the organization was mentioned only in 30% of which. 90% of the ontologies were general and not specific to a particular organization; this made it complex and could

Ontology	Goal	Relying on an official standard and classifications	Relying on a previous ontology	Query language	Platform
[10]	Engineering and Elicitation Security requirements	No	Yes	SQWRL	protégé
[8]	Make cybercrime investigation more efficient	No	Yes	-	protégé
[11]	Automate the penetration testing process	Yes	Yes	SWRL/SPARQL	protégé
[12]	Formalizing knowledge in the field of systems security assessment	No	Yes	-	Apache JENA
[13]	Formalize information security controls and verify compliance with security standard ISO 27002	Yes	Yes	-	-
[14]	Managing vulnerabilities	Yes	No	-	protégé
[15]	Storage of security data for analysis and evaluation of systems security	Yes	Yes	DL	protégé
[16]	Determining the objectives of cyber-attacks in information systems	Yes	Yes	-	-
[9]	Software security knowledge management with application context in mind	No	Yes	SPARQL	protégé
[17]	Extract knowledge from different sources to build semantic models of the threat	Yes	Yes	Dl, SPARQL	protégé

Table 1: Comparison of the studied ontologies

	Top Layer Concept
[10]	Person, Organization, Asset , Location, Risk, Severity, Threat, Vulnerability, Impact, Threat Agent, Attack, Method, Attack Tool, Security goal, Security criterion, Security requirement, Requirement document and control
[8]	Contact Medium, Entity, Information element, Data object and Data source
[11]	Person, Organization, Data source, Vulnerability and Host
[12]	Asset, Mistake, Risk, Evaluation, Threat, Fault, Failure, weakness, Attack, Assessment , Defect and Vulnerability
[13]	Data Backup Policy, Data Backup Control Compliant Organization, Control, Threat, Vulnerability, Rating, Attribute, Asset ,Person and Organization
[14]	Vulnerability, Threat, Product, Intelligence and Countermeasure
[15]	Attack, Exploits, Configuration, Product, Weakness, Source, Countermeasure and References
[16]	Attack, Objective, Incident, Attacker, Tool, Event, vulnerability, Action, Target, System, Weakness, Countermeasure, Metric and Sources

[9]	Functional Area, Category, Platform Type, Scenario, Application Category, Security Domain and Contextualized Knowledge
[17]	Weakness, Vulnerability, Detection Method, Mitigation Method, Technical Impact, Scope, Phase and Method Of Attack

Table 2: The basic concepts used in the studied ontology

be applied in one place and likely to fail in another. 10% worked in detecting electronic crimes related to bank fraud, and this ontology ignored other risks that could face electronic banking services Information security risks differ from one organization to another, depending on the organization's components, the services it provides, the way it works, and the sensitivity of its information. Bank information is very sensitive and any vulnerability may lead to a serious attack that affects the bank's reputation, customer satisfaction and leads to huge losses. Hence, the importance of having security ontology specializes in analyzing the security risks of electronic banking services. So that this ontology contains the most important security concepts that must be available in any security ontology, which we got from the studied ontology besides linking them with the concepts of electronic banking services through the relationships provided by the ontology. **Fig [2]** shows the basic concepts of the proposed ontology and the relationships between them.

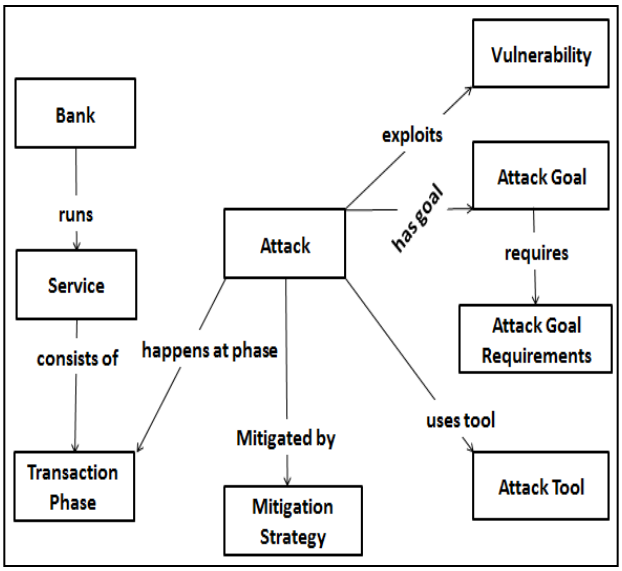

Fig 2: The concepts of the proposed ontology

Conclusion

In this research, we study the risks of information security in electronic banking services. Then, we study many of the previous security ontologies and compare them. The results proved that the studied ontologies are general and not belong to a particular organization. They were complex and have different goals, so the concepts used differed. Because of the need for security ontology to help analyze electronic banking attacks, we extracted the most important concepts used to analyze attacks and add new concepts that help in the analysis process. After that, we linked these concepts with the concepts of electronic banking services using ontology relationships, and developed an initial conception that includes the basic concepts, and relationships of the ontology that will analyze the information security risks in electronic banking services. In the next step, we will develop the integrated ontology using protégé and an interactive interface, and use the SPARQL Query Language to query the information stored in this ontology.

References

1. A. Souag, C. Salinesi, R. Mazo, I. Comyn-Wattiau, A Security Ontology for Security Requirements Elicitation in Engineering Secure Software and Systems, (Springer International Publishing, 2015), pp. 157–177.
2. R. Carvalho, M. Goldsmith, S. Creese, Applying Semantic Technologies to Fight Online Banking Fraud in 2015 European Intelligence and Security Informatics Conference, (2015), pp. 61–68.
3. T. Stepanova, A. Pechenkin, D. Lavrova, Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems in Proceedings of the 8th International Conference on Security of Information and Networks, SIN ’15., (Association for Computing Machinery, 2015), pp. 142–149.
4. F. de Franco Rosa, M. Jino, R. Bonacin, Towards an Ontology of Security Assessment: A Core Model Proposal in Information Technology - New Generations, (Springer International Publishing, 2018), pp. 75–80.
5. S. Fenz, T. Neubauer, Ontology-based information security compliance determination and control selection on the example of ISO 27002. Information & Computer Security 26, 551–567 (2018).
6. R. Syed, H. Zhong, Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model in AMCIS 2018 Proceedings, (2018) (September 5, 2021).
7. I. Kotenko, A. Fedorchenko, E. Doynikova, A. Chechulin, An Ontology-based Storage of Security Information. ITC-J. 47, 655–667 (2018).
8. E. Doynikova, I. Kotenko, Approach for determination of cyber-attack goals based on the ontology of security metrics. IOP Conf. Ser.: Mater. Sci. Eng. 450, 052006 (2018).
9. Wen, Wen, Katt, Managing Software Security Knowledge in Context: An Ontology Based Approach. Information 10, 216 (2019).
10. A. Brazhuk, Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries. International Journal of Open Information Technologies 7 (2019).
11. D. Singh, R. Ruhl, H. Samuel, Attack Tree for Modelling Unauthorized EMV Card Transactions at POS Terminals in ICISSP, (2018), pp. 494–502.
12. J. A. Ojeniyi, et al., Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study. International Journal of Education and Management Engineering 9, 1–14 (2019).
13. W. A. Hammood, et al., A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number. IOP Conf. Ser.: Mater. Sci. Eng. 769, 012061 (2020).

14. B. Bonilla-Morales, X. Medianero-Pasco, Survey: grid computing and Semantic Web. IJCSI (2010).
15. P. Rathee, S. K. Malik, IWD towards Semantic similarity measure in ontology. J. Inf. Optimiz. Sci. 41, 1561–1577 (2020).
16. B. Hnatkowska, A. Kozierkiewicz, M. Pietranik, Semi-Automatic Definition of Attribute Semantics for the Purpose of Ontology Integration. IEEE Access 8, 107272–107284 (2020).
17. S. E. Eneji, M. U. Angib, W. E. Ibe, K. C. Ekwegh, A Study of Electronic Banking Fraud, Fraud Detection and Control. International Journal of Innovative Science and Research Technology 4, 708–711 (2019).