E-Commerce Attacks Analysis Ontology Based on CAPEC and CVE

Noura Salman Haidar
Faculty of Information Technology
Syrian Virtual University
Damascus, Syria

Dr. Muhammad-Mazen Mustafa
Faculty of Information Technology
Syrian Virtual University
Damascus, Syria

***Abstract*: Security is the most important feature of electronic banking services. E-commerce is one of these services and its safety is the one of the uppermost visible security that controls the end user during interacting with their business. Sharing sensitive data in insecure medium raises security and privacy issues. Credentials and personal data can be theft by hackers. 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. Here the need to rely on Ontology appears. Ontology allows collecting information from different formal and informal sources, integrating and reusing it effectively. Attack analysis based on ontology can make understanding the risks much easier and faster, so this facilitates escaping them. Relying on CAPEC and other formal resources enriches the analysis process and gives the information great credibility.**

Keywords: E-Commerce, Attack, Ontology, CAPEC, CVE.

I. INTRODUCTION

E-commerce was introduced to the consumer and business worlds as a unique approach in 1990. E-commerce is characterized as a primary business model by means of the selling process of goods, the purchasing of resources, and the distribution or exchange over the Internet. The popularity of e-commerce is mainly because of its online business perspective. It makes it possible to gain and sell goods online, to provide various services and information through the Internet, and to exchange money immediately between businesses. E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. It is described as selling and buying of services or goods through wireless technology using Electronic payment systems that have continued to grow over recent years because of the increase of online banking and shopping .Through electronic payment systems, any person can transfer money and purchase items any place and time based on internet, and without visiting banks [1]. Since the Internet is the medium of data transmission, there are risks to the confidentiality, integrity, or availability of data exchanged between banks and the customers. The presence of vulnerabilities in devices, applications, or network may lead to exploit it by unknown organizations or persons who are not authorized to access this information, in order to achieve unethical goals [2]. Hence the importance of analyzing E-Commerce attacks. This analysis requires large amounts of data to know the goal of the attack, requirements for achieving goal, attack tools, vulnerabilities that led to its occurrence, attack strategy and the stage in which it may occur. The analysis process needs information from various sources, including some global knowledge sources for vulnerabilities and attacks such as CWE, CVE and CAPEC, which enables us to obtain more information related to the attack and vulnerabilities. Semantic-based knowledge management systems are the best suited for these analyzes by using ontology. Ontology is a description of a set of concepts, their characteristics and the relationships between them, and is used for the integration of knowledge and building a conceptual model, as it is used as part of an intelligent system or a distance learning system. Ontology-based systems use descriptive logic in which concepts and relationships are described in a formal way [3].

II. L ITERATURE REVIEW

In 2018, El orche, Bahjat and Ain al-Hayat proposed an approach able to detect and prevent suspicious transactions on various electronic payment systems using ontology. The approach makes to share and adaptive the preventives rule of fraud on an ontology based on multiple and various payment systems [4]. In 2018, Rosa and Bonacin proposed security ontology to assess security to reach secured systems. 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 [5]. 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 [6]. 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 [7]. 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 [8]. 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 [9]. In 2019, Brazhuk 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 [3].

III. ELECTRONIC PAYMENT SYSTEMS

Electronic banking is a set of devices using electronic and computer technology to develop banking transactions. It refers to all the technologies necessary for the use of bank cards and the switching and processing of transactions made from them. Electronic payment systems have become more popular thanks to the increased use of Internet shopping. These systems do not only concern Internet transactions, as more and more resources are being developed to facilitate electronic money transfers. With the increase in technology, the range of devices and processes used to conduct electronic transactions continues to increase as the use of cash and check transactions decreases. This is mainly because it is much easier to carry cards or use cell phones to pay for purchases over money [4].

A. *Electronic Payment System Components*

Cardholder: A client is a person who is going to purchase items by creating payments in a timely manner.

Merchant: A merchant is an enterprise or a person who offers a service or product.

Card issuer: a kind of bank that holds the client’s account and authorizes him or her during account registration. It generally has the money of numerous customers and is specially designed for the goal of keeping the client’s cash on trust.

Acquirer: A merchant bank is a monetary institute, which involves underwriting and company loans, catering mainly to the requirements of big companies and individuals with substantial net worth. In e-commerce, a merchant bank is a kind of bank that permits companies to accept payments through credit or debit cards and is liable for fraud management.

Payment gateway: Every transaction that takes place online is created via
payment gateways. A payment gateway is attached wholly to consumers, banks, and merchants through the Internet and is responsible for the speed, reliability, and safety of all transactions [4] [1].

B. *E-Commerce Transaction phases*

Card holder registers on the merchant's website.
2. Card holder logs into the merchant's website.
3. Card holder searches for the items, selects them, and adds them to the shopping cart.
4. Card holder chooses the type of electronic payment.
5. Card holder goes to the electronic payment system.
6. Card holder enters his personal information, his bank account information and card information.
7. Merchant sends the information to the Acquirer that sends them to payment gateway.
8. The payment gateway checks with the customer's bank, to ensure that the card is valid and that there is sufficient balance for the transaction.
9. If the customer's bank is approved, the amount will be deducted from the customer's account.
10. The customer's bank sends a confirmation to the payment gateway.
11. The payment gateway sends a confirmation to the acquirer who sends a confirmation to the Merchant.
12. Merchant informs the buyer of the confirmation of receipt of the purchase price.
13. The buyer gets a notification from the issuing bank, and the procedures for sending the product to the buyer's address begin.

The most dangerous phases are the seventh and eighth phases, where sensitive data transmission. In these phases sensitive data can be under attack by an unauthorized attacker, which poses a great threat to banks and customers [1] [4] [10].

IV. FORMAL RESOURCES CAPEC, CVE AND CWE

A. *CAPEC*

CAPEC is abbreviation for Common Attack Pattern Enumeration and Classification. It released in 2007. It provides a publicly available catalog of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, and gives guidance on ways to mitigate the attack's effectiveness. Attack patterns help those developing applications, or administrating cyber-enabled capabilities to better understand the specific elements of an attack and how to stop them from succeeding. The CAPEC List continues to evolve with public participation and contributions to form a standard mechanism for identifying, collecting, refining, and sharing attack patterns among the cybersecurity community. CAPEC helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses. Through CAPEC records, we can obtain the following information:

- Attack ID
- Description of the attack
- Prerequisites
- Mitigation Methods
- Related Weaknesses (CWE)
- Likelihood Of Attack
- Attack Severity
- Required skills
- Scope
- Technical Impact [11]

B. *CVE*

CVE is abbreviation for Common Vulnerabilities and Exposures. CVE program has the mission of identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Each vulnerability represented in one record. The vulnerabilities are discovered, assigned and published by organizations that have partnered with the CVE Program. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. CAPEC not directly connected to CVE. It directly connected to CWE which in turn is connected to CVE. So we will get to know about CWE, and in our research, we will use ontology relations to achieve this link between these different sources [13].

C. *CWE*

CWE is abbreviation for Common Weakness Enumeration. It is a list of common software and hardware weakness types} that have security ramifications. Weaknesses are flaws, faults or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack. CWE has a goal to stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate the most common mistakes before products are delivered. Ultimately, use of CWE helps prevent the kinds of security vulnerabilities that have plagued the software and hardware industries and put enterprises at risk. We can obtain the following information form CWE records:

- Weakness description
- Observed Examples that represent CVE records related to CWE records.
- Detection Methods of the weakness
- CAPEC records related to CWE records [12].

Reliance on official sources gives high value to the analysis process and great information credibility. Thus, linking the analysis of electronic banking attacks with CAPEC, CWE and CVE dictionaries will enrich the analysis process with information that will lead to an understanding of how the attacker exploits the vulnerabilities in order to prevent a successful attack. But these sources are not directly related to each other, for example CAPEC is not linked to CVE directly, but the connection is achieved through CWE. Since CAPEC records are linked to CWE records, and CWE records are linked to CVE records. We will achieve the linking between these formal sources on the one hand, other sources of security knowledge on another hand and the E-commerce concepts on the other hand, by using ontology.

V. ONTOLOGY

Ontology is the mainstay in the field of semantic web to represent concepts and their relationships, and make the knowledge machine understandable. 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. 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. Ontology consists of Classes, Attributes, Relationships, Function terms, Restrictions, Rules, Axioms and events.

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 [14].

VI. THE PROPOSED ONTOLOGY

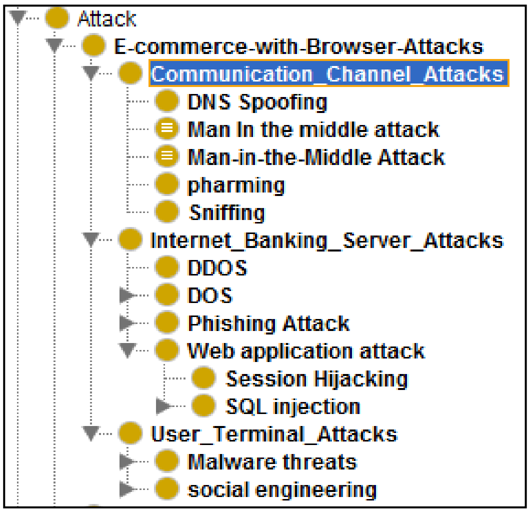
A. *Ontology Concepts*

The top level concepts of the ontology of E-commerce attacks analysis based on CAPEC and CVE shown in Figure 1.

Our ontology contains concepts related to E-commerce System such as E-Banking that represents Electronic payment system with all components. Services that represent electronic services like E-Commerce. Card that represents the customer's card which be used to do e-payment. Account that represent customer account in the card issuer bank. Order that represents all purchases that customer buys. Bill that contains the price of all purchases. Person who is the Card_holder or Merchant. Purchases that refers to items which the customer buys. Transaction_phase that represents the stages of the e-commerce service, and it is the connecting point between the concepts of electronic commerce andsecurityconcepts. Payment_corporation_network that represents the payment network that transmits data among banks and the customer. And the Financial_institution that is either Card_issuer bank or Acquirer bank.

There are concepts related to information security risks analysis like

Attack: that represents the attack can be occurs, and it divided into three groups(Communication_Channel_Attacks, Internet_Banking_Server_Attacks, User_Terminal_Attacks) that shown in Figure 2 and Figure 3.



Attack
E-commerce-with-Browser-Attacks
Communication_Channel_Attacks
DNS Spoofing
Man In the middle attack
Man-in-the-Middle Attack
pharming
Sniffing
Internet_Banking_Server_Attacks
DDOS
DOS
Phishing Attack
Web application attack
Session Hijacking
SQL injection
User_Terminal_Attacks
Malware threats
social engineering

FIGURE 2 ATTACK CONCEPT WITH ITS SUBCLASSES

Vulnerability refers to weakness or vulnerability that can causes an attack. Attack_goal refers to the attacker target of doing attack such as stealing information. Attack_goal_requirements refers to things which attacker should do to achieve its goal. Attack_Tool refers to tools used by attacker to do attack. Mitigation_strategy refers to methods should be done to mitigate attack. Scope refers to information security goals that attack can affect if it occurs such as Confidential, Availability Authorization...etc. Technical_Impact refers to the impact that can attack causes, such as read data, modify data...etc.

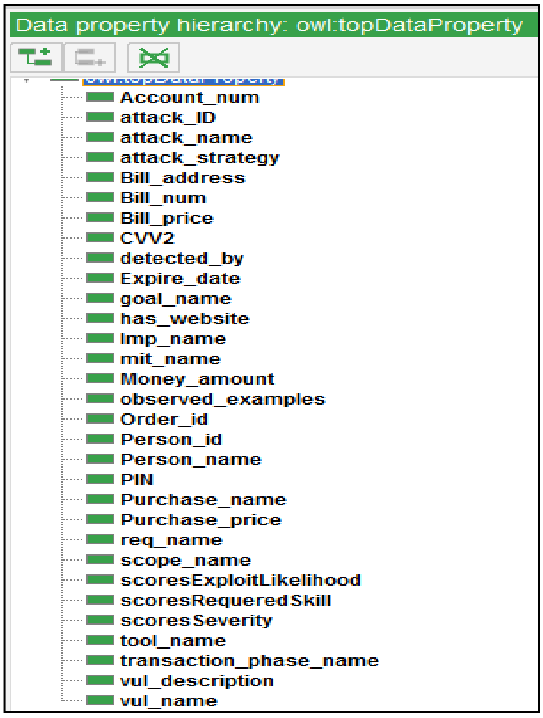
B. *Ontology Relationships*

a. Object properties

Ontology concepts linked each other by relations. Figure 4 Figure 5 shows the basic relations between the concepts. has_card refers to cardholder has a legitimate card. Associate_with refers to a legitimate card associates with an account. Issue_card refers to the card issuer issues a legitimate card. Buy_purchases refers to the cardholder buy purchases. Sell_purchases refers to the merchant sell purchases. Contracting_with refers to the merchant contracting with the acquirer. Form_order refers to purchases form order. Has_bill refers to the order has bill. Processed_by refers to the bill processed by e-banking system. Runs_services refers to e-banking system runs services. Consists_of refers to the service consists of transaction phases. Happens_at_phase refers to an attack can be occurs in a specific transaction phase. Attack_has_goal refers to any attack has a target to achieve. Attack_goal_achievement_requires refers to things that should happen to achieve the attack goal. Exploits_vulnerability refers to an attack exploits a weakness or vulnerability to occur. impactTechnicalImpact refers to an attack can cause technical impacts if occurs. Mitigated_by an attack can mitigate by mitigation strategies. Scopes refers to an attack may affect information security scopes. Uses_tools refers to an attack uses tools to occur.

b. Data Properties

Figure 6 shows data property relations of the ontology.



Data property hierarchy: owl:topDataProperty

Account_num
attack_ID
attack_name
attack_strategy
Bill_address
Bill_num
Bill_price
CVV2
detected_by
Expire_date
goal_name
has_website
Imp_name
mit_name
Money_amount
observed_examples
Order_id
Person_id
Person_name
PIN
Purchase_name
Purchase_price
req_name
scope_name
scoresExploitLikelihood
scoresRequeredSkill
scoresSeverity
tool_name
transaction_phase_name
vul_description
vul_name

FIGURE 6 ONTOLOGY DATA PROPERTY

Attack_strategy refers to the method that can attacker use to do attack. scoresExploitLikelihood refers to Likelihood of a successful attack. scoresRequeredSkill refers to skills that an attacker needs to do the attack are high, low, medium, etc. scoresSeverity represents the severity of the attack if it occurs. detected_by represents the method of detecting the weakness.

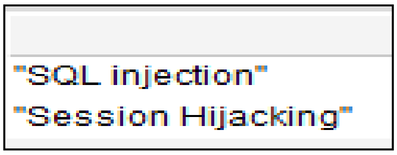
VII. IMPLEMENTATION AND USING

The proposed ontology is represented as an OWL file, using Protege ontology editor. The proposed ontology allows providing multi-aspect analysis of E-commerce attacks and vulnerabilities. To illustrate this below is shown the ability of the ontology to answer queries represented as SPARQL queries. For example, the request "Which attacks with high and very high severity, high likelihood and low required skills can affect E-Commerce service". The corresponding SPARQL query1 is:

```
SELECT ?high_severity_high_likelihood_low_skills_attacks
        WHERE {
?x rdf:type ?y .
?y                                              rdfs:label
?high_severity_high_likelihood_low_skills_attacks .
?y rdfs:subClassOf  ?z .
OPTIONAL {?x n:scoresSeverity ?s .}
OPTIONAL {?x n:scoresExploitLikelihood ?h .}
OPTIONAL {?x n:scoresRequeredSkill ?o .}
FILTER  (  ?z= n:Communication_Channel_Attacks || ?z =
n:Internet_Banking_Server_Attacks          ||          ?z      =
n:Web_application_attack  || ?z = n:User_Terminal_Attacks).
FILTER  ( (?s = 'Very High' || ?s = 'High') &&( ?h ='High'
||?h ='high') ) .
FILTER regex(?o,'Low','i')

}
```

Where n is the prefix of our ontology. And the result is in Figure 7:



"SQL injection"
"Session Hijacking"

FIGURE 7 EXECUTION OF A SPARQL QUERY1 IN PROTEGE

The request " In which transaction phase of E-Commerce service can Sniffing attack occur?". The corresponding SPARQL query2 is:

```
SELECT ?Attack_Happens_at_phase
          WHERE { ?x rdf:type  n:Sniffing.
?x n:happens_at_phase ?k.
?k n:transaction_phase_name ?Attack_Happens_at_phase.

}
ORDER BY( ?Attack_Happens_at_phase )
```

And the result is in Figure 8.
The request " What is pharming attack goal?". The corresponding SPARQL query3 is:

```
SELECT ?ATTACK_GOAL
          WHERE { ?x rdf:type  n:Pharming .
?x n:attack_has_goal ?k.
?k n:goal_name ?ATTACK_GOAL.

}
```

And the result is in Figure 9.
The request " What is Man-in-The-Middle attack ID in CAPEC records? And what are the severity, Likelihood and required skills for this attack ". The corresponding SPARQL query4 is:

```
SELECT ?attack_ID   ?Exploit_Likelihood  ?Requered_Skill
?Severity
          WHERE { ?x rdf:type  n:Man_in_the_middle .
?x n:attack_ID ?attack_ID.

?x n:scoresExploitLikelihood ?Exploit_Likelihood.
?x n:scoresRequeredSkill ?Requered_Skill.
?x n:scoresSeverity ?Severity.
}
```

And the result is in Figure 10.
The request " What are Weakness that cause Man-in-The-Middle attack according to CWE and CAPEC? ". The corresponding SPARQL query5 is:

```
SELECT ?attacker_exploits_vulnerabilities
          WHERE { ?x rdf:type  n:Man_in_the_middle .
?x n:exploits_vulnerability ?k.
?k n:vul_name ?attacker_exploits_vulnerabilities

}
```

And the result is in Figure 11.
The request " What are Vulnerabilities related to CWE-1286 according to CWE and CVE? ". The corresponding SPARQL query6 is:

```
SELECT ?OBSERVED_EXAMPLES
          WHERE {
?a rdf:type n:Vulnerability.
OPTIONAL        {        ?a        n:observed_examples
?OBSERVED_EXAMPLES.}


OPTIONAL { ?a n:vul_name ?x.}
FILTER ( ?x = 'CWE-1286: Improper Validation of Syntactic
Correctness of Input').

}
```

And the result is in Figure 12.
The request " What are scope and technical impact of pharming attack according to CAPEC? ". The corresponding SPARQL query7 is:

```
SELECT  ?scopes ?Technical_Impact
          WHERE { ?x rdf:type  n:Pharming .

?x n:scopes ?k.
?k n:scope_name ?scopes .
?x n:impactsTechnicalImpact ?s.
?s n:Imp_name ?Technical_Impact.

}
```

And the result is in Figure 13.
Our ontology also answers many other inquiries regarding e-commerce attacks and the vulnerabilities that cause these attacks.

VIII. CONCLUSION AND FUTURE WORK

In this research, we proposed ontology to analysis E-Commerce attacks. Analyzing process dependents on formal resources like CVE, CAPEC and CWE. This ontology contains information about E-commerce attacks and vulnerabilities. This ontology can be used by analysts, developers, testers, and educators to understand attacks and enhance defenses. This ontology can be expanded in the future to include studying of other attacks, or by adding other e-banking services and analyzing their attacks, or even by increasing sources of knowledge and relying on other official sources.

REFERENCES

[1] M. Hassan, Z. Shukur and M. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce", Computers, vol. 9, no. 3, p. 66, 2020. Available: 10.3390/computers9030066.

[2] M. Tabiaa, A. madani and N. El kamoun, "E-Banking: Security risks, previsions and recommendations", IJCSNS International Journal of Computer Science and Network Security, vol. 17, no. 11, 2017. [Accessed 14 November 2021].

[3] Brazhuk, "Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries", International Journal of Open Information Technologies, vol. 7, no. 3, 2019. [Accessed 14 November 2021].

[4] EL ORCHE, M. BAHAJ and S. AIN ALHAYAT, "Ontology based on electronic payment fraud prevention", IEEE, pp. 143-148, 2018. [Accessed 14 November 2021].

[5] F. Franco Rosa, M. Jino and R. Bonacin, "Towards an Ontology of Security Assessment: A Core Model Proposal", springer. 2018. Available: 10.1007/978-3-319-77028-4_12 [Accessed 14 November 2021].

[6] S. Fenz and T. Neubauer, "Ontology-based information security compliance determination and control selection on the example of ISO 27002", Information & Computer Security, vol. 26, no. 5, pp. 551-567, 2018. Available: 10.1108/ics-02-2018-0020.

[7] R. Syed, "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system", Information & Management, vol. 57, no. 6, p. 103334, 2020. Available: 10.1016/j.im.2020.103334.

[8] Kotenko, A. Fedorchenko, E. Doynikova and A. Chechulin, "An Ontology-based Storage of Security Information", Information Technology And Control, vol. 47, no. 4, 2018. Available: 10.5755/j01.itc.47.4.20007.

[9] Wen and Katt, "Managing Software Security Knowledge in Context: An Ontology Based Approach", Information, vol. 10, no. 6, p. 216, 2019. Available: 10.3390/info10060216.

[10] T. Xin and B. Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model", International Journal of Security and Its Applications, vol. 8, no. 2, pp. 271-282, 2014. Available: 10.14257/ijsia.2014.8.2.28.

[11] "CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)", Capec.mitre.org, 2021. [Online]. Available: https://capec.mitre.org/. [Accessed: 14- Nov- 2021].

[12] "CWE - Common Weakness Enumeration", Cwe.mitre.org, 2021. [Online]. Available: https://cwe.mitre.org/. [Accessed: 14- Nov- 2021].

[13] "CVE -CVE", Cve.mitre.org, 2021. [Online]. Available: https://cve.mitre.org/. [Accessed: 14- Nov- 2021].

[14] N. Haidar and M. Al Mustafa, "E-banking Information Security Risks Analysis Based on Ontology", (IJESIR) International Journal of Science and Innovative Research, vol. 2, no. 8, pp. 100-108, 2021. [Accessed 14 November 2021].

[15] R. Syed, "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system", Information & Management, vol. 57, no. 6, p. 103334, 2020. Available: 10.1016/j.im.2020.103334.

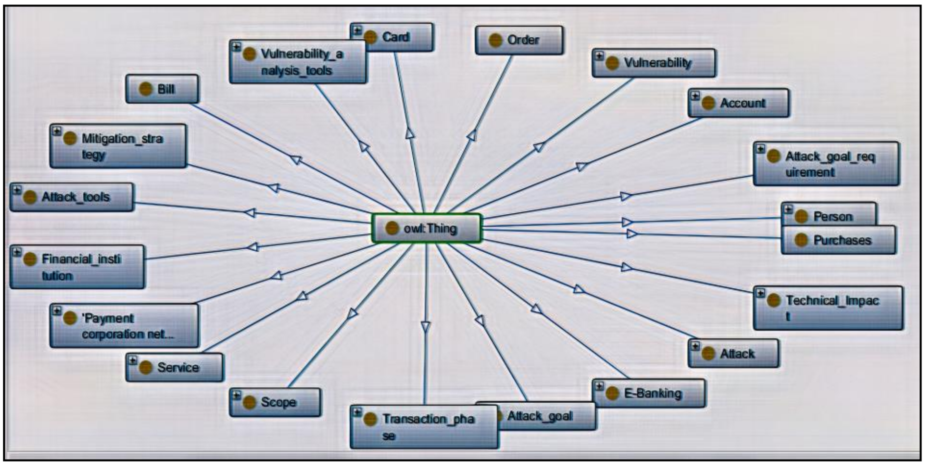


Figure 1 Top level concepts of the proposed ontology

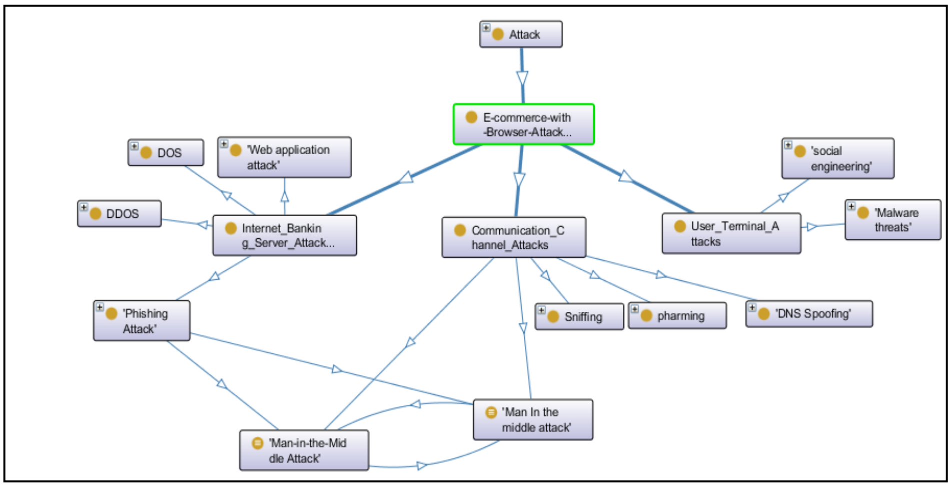

Attack
E-commerce-with -Browser-Attack...
DOS
'Web application attack'
'social engineering'
DDOS
Internet_Bankin g_Server_Attack...
Communication_C hannel_Attacks
User_Terminal_A ttacks
'Malware threats'
'Phishing Attack'
Sniffing
pharming
'DNS Spoofing'
'Man In the middle attack'
'Man-in-the-Mid dle Attack'

Figure 3 Attack Types

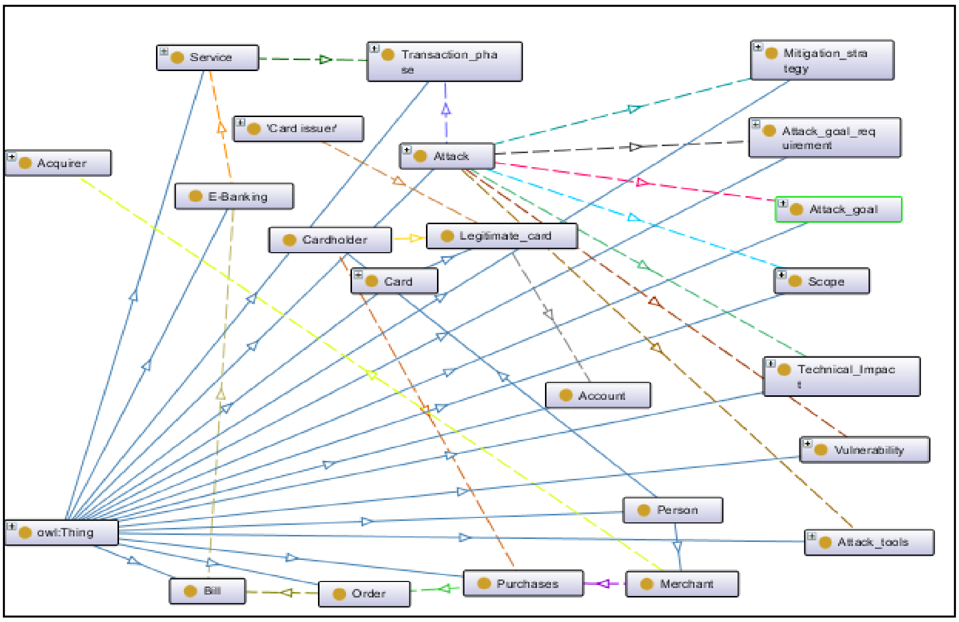
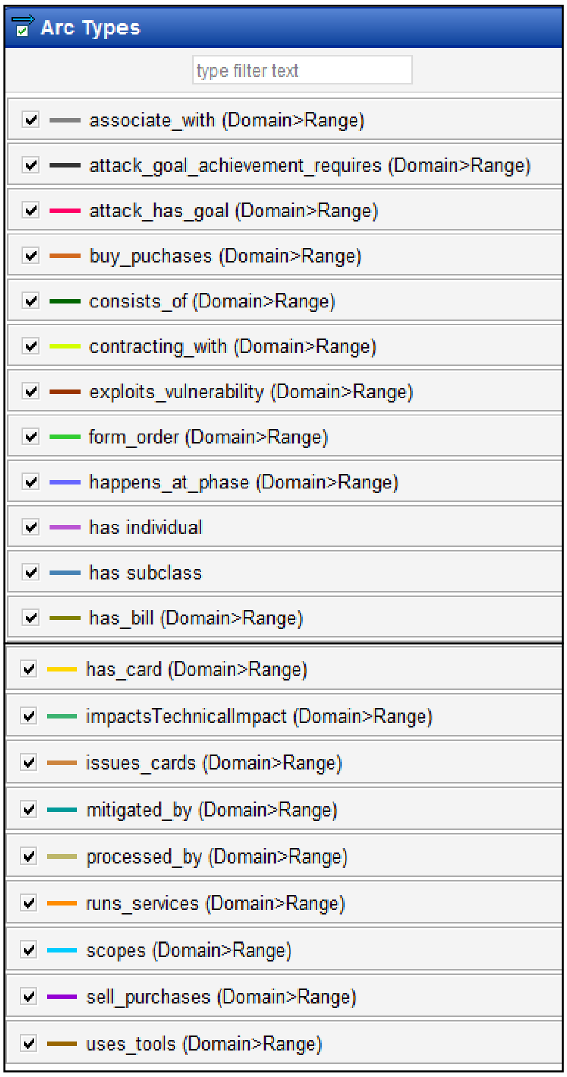


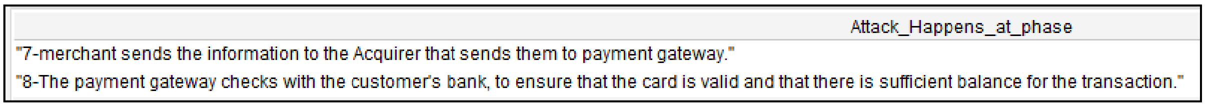
Figure 4 relations between concepts


Arc Types

type filter text

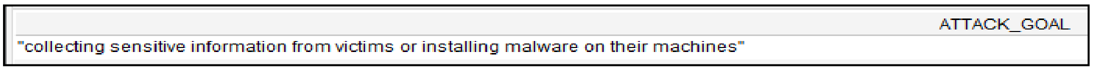
☑ ▬ associate_with (Domain>Range)
☑ ▬ attack_goal_achievement_requires (Domain>Range)
☑ ▬ attack_has_goal (Domain>Range)
☑ ▬ buy_puchases (Domain>Range)
☑ ▬ consists_of (Domain>Range)
☑ ▬ contracting_with (Domain>Range)
☑ ▬ exploits_vulnerability (Domain>Range)
☑ ▬ form_order (Domain>Range)
☑ ▬ happens_at_phase (Domain>Range)
☑ ▬ has individual
☑ ▬ has subclass
☑ ▬ has_bill (Domain>Range)
☑ ▬ has_card (Domain>Range)
☑ ▬ impactsTechnicalImpact (Domain>Range)
☑ ▬ issues_cards (Domain>Range)
☑ ▬ mitigated_by (Domain>Range)
☑ ▬ processed_by (Domain>Range)
☑ ▬ runs_services (Domain>Range)
☑ ▬ scopes (Domain>Range)
☑ ▬ sell_purchases (Domain>Range)
☑ ▬ uses_tools (Domain>Range)

figure 5 Relations Names



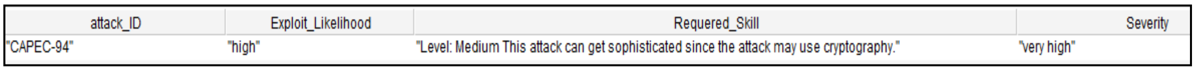
Attack_Happens_at_phase
"7-merchant sends the information to the Acquirer that sends them to payment gateway."
"8-The payment gateway checks with the customer's bank, to ensure that the card is valid and that there is sufficient balance for the transaction."

Figure 8 Execution of a SPARQL query2 in Protégé



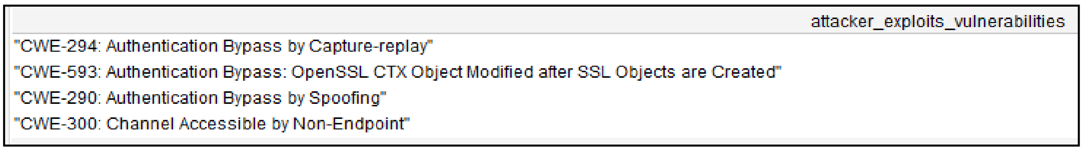
ATTACK_GOAL
"collecting sensitive information from victims or installing malware on their machines"

Figure 9 Execution of a SPARQL query3 in Protégé



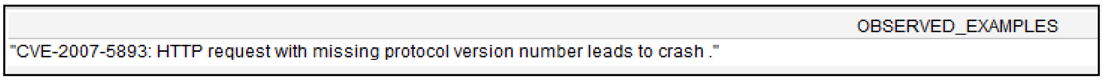
attack_ID	Exploit_Likelihood	Requred_Skill	Severity
"CAPEC-94"	"high"	"Level: Medium This attack can get sophisticated since the attack may use cryptography."	"very high"

Figure 10 Execution of a SPARQL query4 in Protégé



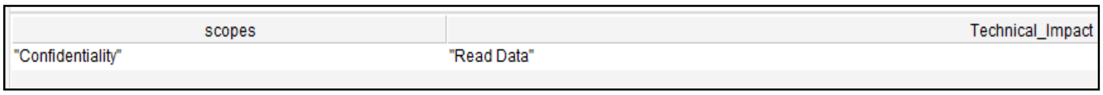
attacker_exploits_vulnerabilities
"CWE-294: Authentication Bypass by Capture-replay"
"CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created"
"CWE-290: Authentication Bypass by Spoofing"
"CWE-300: Channel Accessible by Non-Endpoint"

Figure 11 Execution of a SPARQL query5 in Protégé



OBSERVED_EXAMPLES
"CVE-2007-5893: HTTP request with missing protocol version number leads to crash ."

Figure 12 Execution of a SPARQL query6 in Protégé



scopes	Technical_Impact
"Confidentiality"	"Read Data"

Figure 13 Execution of a SPARQL query7 in Protégé