Syrian Arab Republic
Ministry of High Education
Syrian Virtual University

الجمهورية العربية السورية
وزارة التعليم العالي
الجامعة الافتراضية السورية

تحليل مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية اعتماداً على تقنيات الوب الدلالي

E-banking Information Security Risks Analysis Based on Semantic Web Technologies

بحث مقدم لنيل درجة الماجستير في علوم الويب
إعداد الطالبة: نوره سلمان حيدر
إشراف الدكتور: محمد مازن المصطفى

٢٠٢١

إهداء

إلى روح والدي رحمه الله

الى أمي وأخوتي وأخواتي

شكر و تقدير

الحمد لله أولاً وآخراً على فضله وتوفيقه وبركته..

أتقدم بجزيل الشكر والتقدير الى الدكتور محمد مازن المصطفى، على توجيهاته الكريمة في كل مرحلة من مراحل بحثي، وعلى وقته وحرصه في الإجابة على أسئلتي.

كما أتقدم بجزيل الشكر والامتنان لأعضاء لجنة الحكم، الدكتور باسل الخطيب والدكتور خالد عمر.

دمتم للعلم عطاءً أساتذتي الأفاضل.

الموافقات على النشر

[JATIT] Letter of Acceptance for Submitted Research Paper ID 44895-JATIT Inbox

editor jatit<mailjatit@gmail.com> Tue, Dec 14, 2021 at 3:04 PM

To: noura haidar <nourahaidar88@gmail.com>, noura_94383@svuonline.org, t_mmustafa@svuonline.org

Reply | Reply to all | Forward | Print | Delete | Show original

Dear Corresponding Author **Noura-Salman-Haidar**

We are pleased to inform you that your submission ID: **44895-JATIT** titled **"ONTOLOGY FOR E-COMMERCE ATTACKS ANALYSIS BASED ON CAPEC AND CVE"** having author(s): **NOURA SALMAN HAIDAR, MUHAMMAD-MAZEN AL MUSTAFA** has been accepted for publication in **JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY** (E-ISSN **1817-3195** / ISSN **1992-8645).** The acceptance decision was based on the reviewers' evaluation after double-blind peer review and the chief editor's approval.**[Attached with this acceptance intimation]**

You shall submit the OA processing fee ($450) via Credit Card/PayPal transaction through our online payment system (Use any valid credit card of Yourself / Friend / Family etc) . Please submit the dues via UK Paddle payment system at

IJERT

International Journal of
Engineering Research & Technology
ISSN : 2278 - 0181, www.ijert.org
(Published by : ESRSA Publications)

CERTIFICATE
OF PUBLICATION

This is to certify that

Dr. Muhammad-mazen Mustafa

Has published a research paper entitled

E-Commerce Attacks Analysis Ontology Based on CAPEC and CVE

In IJERT, Volume 10, Issue 11 , November - 2021

Registration No: IJERTV10IS110123 **Date:** 30-11-2021 **Chief Editor,IJERT**

IJERT

International Journal of
Engineering Research & Technology
ISSN : 2278 - 0181, www.ijert.org
(Published by : ESRSA Publications)

CERTIFICATE
OF PUBLICATION

This is to certify that

Noura Salman Haidar

Has published a research paper entitled

E-Commerce Attacks Analysis Ontology Based on CAPEC and CVE

In IJERT, Volume 10, Issue 11 , November - 2021

Registration No: IJERTV10IS110123 **Date:** 30-11-2021 **Chief Editor,IJERT**

الملخص

مع الانتشار الواسع للخدمات المصرفية الالكترونية وازدياد هجمات المهاجمين غير المصرح لهم والحاجة الى تأمين البيانات المتبادلة بين البنك والعميل، تضافرت الجهود لدراسة هذه الهجمات وتحليلها ومعرفة أسبابها وطرق التخفيف منها، ولكن عملية التحليل تحتاج الى استخراج المعرفة من مصادر مختلفة وتقديمها بشكل بسيط وسهل الفهم ومعالجتها بسرعة وفعالية، مما أدى الى الحاجة الى الاعتماد على التقنيات الدلالية التي تسمح بجمع المعلومات من مصادر مختلفة ودمجها وإعادة استخدامها بشكل فعال، وذلك من خلال استخدام الأنطولوجيا. فالأنطولوجيا ذات أهمية كبرى في مجال هندسة المعرفة، حيث إنها تساعد مستعمليها على إثراء النظام المعلوماتي بمعاني ومفاهيم، وتساعد في ربط هذه المفاهيم مع بعضها البعض من خلال العلاقات و تزيد من جودة عملية التحليل، وتسهل عملية تبادل المعرفة وإعادة استخدامها. في هذا البحث سنعرض العديد من الأبحاث التي استخدمت الأنطولوجيا في مجال أمن المعلومات حيث قمنا بدراستها والمقارنة بينها وتبين أن الأنطولوجيا التي تم تطويرها سابقاً كانت عامة ومعقدة وتصلح لبعض المجالات ولا تصلح للبعض الآخر. وبسبب أهمية وخطورة التعاملات المالية، برزت الحاجة الى وجود أنطولوجيا خاصة بتحليل هجمات الخدمات المصرفية الالكترونية، تحتوي المفاهيم الخاصة بهذه الخدمات إضافة الى مفاهيم أمن المعلومات اللازمة لتحليل الهجمات التي من الممكن أن تتعرض لها هذه الخدمات. ففي المقدمة سنذكر بعض الدراسات السابقة في مجال تحليل مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية، وفي مجال استخدام الأنطولوجيا مع أمن المعلومات. في الفصل الأول، سنتحدث عن الخدمات المصرفية الالكترونية. في الفصل الثاني، سنتحدث عن مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية. في الفصل الثالث سنتحدث عن المصادر المعلومات العالمية الرسمية التي سنستعين بها في عملية التحليل. وفي الفصل الرابع، سنتحدث عن الويب الدلالي والأنطولوجيا. وفي الفصل الخامس سنتحدث عن الأنطولوجيا المقترحة. والتطبيق العملي في الفصل السادس.

الكلمات المفتاحية

الخدمات المصرفية الالكترونية e-banking ، الويب الدلالي semantic web ، الأنطولوجيا ontology ، الهجمات Attacks ، نقاط الضعف Vulnerability

مشكلة البحث

أمن المعلومات من أهم و أخطر القضايا التي تواجه العمل المصرفي الالكتروني، ومسألة أمن المعلومات يجب مراعاتها في جميع مراحل تطوير أنظمة المعلومات عامةً والحساسة منها كأنظمة البنوك الالكترونية خاصةً، و يتيح تحليل الأمن إمكانية التنبؤ بالتهديدات وتأثيراتها وتحديد متطلبات الأمان المناسبة، وهذا يتطلب تحليل شامل للتهديد، ولكن بعض البنوك قد لا يكون لديها قدرات كافية بسبب نقص المهارات لدى العاملين و قلة الوعي لدى الزبائن، الكلفة الكبيرة اللازمة للقيام بهذا العمل وبسبب عدم توفر هذه المعلومات في مكان واحد وانتشارها في مصادر مختلفة. تحليل التهديد بطريقة فعالة يتطلب تمثيل مشترك وفهم مشترك للمفاهيم والمصطلحات ذات الصلة وتمثيل رسمي وموحد لها وعلاقات متماسكة ومفهومة فيما بينها، كما يتطلب معلومات من مصادر رسمية وغير رسمية، ربما غير مرتبطة فيما بينها بشكل مباشر. وأفضل طريقة لتحقيق ذلك هي استخدام الانطولوجيا التي تعتبر شكل من أشكال تمثيل المعرفة القادمة من مصادر مختلفة على شكل مفاهيم وعلاقات دلالية فيما بينها.

الهدف من البحث

يهدف هذا البحث الى بناء انطولوجيا أمنية من أجل تحليل المخاطر الأمنية التي قد تواجه الخدمات المصرفية الالكترونية، تحتوي هذه الانطولوجيا نقاط الضعف التي يمكن أن تظهر في بيئة العمل المصرفي الالكتروني، وما يمكن أن ينتج عنها من مخاطر و تهديدات تؤثر على سرية وصحة ووفرة معلومات البنك والزبائن. كما تحتوي هذه الأنطولوجيا أهداف هذه التهديدات ومتطلبات تحقيق هذه الأهداف، والأدوات المستخدمة فيها وآلة حدوثها والإجراءات الوقائية. و تحتوي أيضاً معلومات من مصادر رسمية مثل CAPEC(Common Attack Pattern Enumeration), CWE(Common Weakness Enumeration),CVE(Common Vulnerability and Exposure)، كما سيتم بناء بيئة تفاعلية تمكن المستخدم من معرفة نقاط الضعف التي يمكن أن

تواجه الخدمات المصرفية الالكترونية، والأدوات اللازمة لإيجادها وتقييمها، وتحليل الهجمات التي يمكن أن تحدث نتيجة استغلالها من قبل شخص غير مصرح له.

أسئلة البحث

١. ما هي الخدمات المصرفية الالكترونية؟ وماهي مراحل تنفيذها؟
٢. ما هي نقاط الضعف التي يمكن أن تواجه هذه الخدمات؟
٣. ما هي الهجمات التي يمكن أن تتعرض لها هذه الخدمات؟ وفي أي مرحلة؟ وما هو هدفها و طرق تحقيق الهدف واستراتيجية حدوثها و نقاط الضعف التي أدت لحدوثها و ماهي احتمالية نجاح هذه الهجمات وما هي شدتها وما هي المهارات والأدوات اللازمة للقيام بها وما هو مجال تأثيرها والأثر التقني الناتج عن حدوثها ؟
٤. ما هو الويب الدلالي وماهي الأنطولوجيا؟
٥. كيف سيتم الربط بين هذه المفاهيم باستخدام الأنطولوجيا؟

أدوات البحث

Protégé-5.5.0

لغة استعلام SPARQL

Visual Studio 2012

المحتويات

فهرس الأشكال

فهرس الجداول

المصطلحات

المقابل باللغة العربية	المقابل باللغة الانكليزية	الاختصار
لغة أنطولوجيا الويب	Web Ontology Language	OWL
نقاط الضعف والتعرض الشائعة	*Common Vulnerabilities and Exposures*	CVE
المعهد الوطني للمعايير والتكنولوجيا	National Institute of Standards and Technology	NIST
تعداد وتصنيف نمط الهجوم المشترك	Common Attack Pattern Enumeration and Classification	CAPEC
تعداد نقاط الضعف الشائعة	Common Weakness Enumeration	CWE
هجوم رفض الخدمة	Denial-of-service attack	DOS
هجوم رفض الخدمة الموزع	Distributed Denial-of-service	DDOS
هجوم الرجل في الوسط	Man-in-The-Middle attack	MITM
نظام اسم المجال	Domain Name System	DNS
هجوم ما قبل التشغيل	Pre-play Attack	PPA
الاتصال قريب المدى	Near Field Communication	NFC
أمن البرمجيات	Software Assurance	SwA
الأمن الالكتروني والاتصالات	Cybersecurity and Communications	CS&C
قاعدة بيانات نقاط الضعف الوطنية	National Vulnerability Database	NVD
إطار وصف الموارد	Resource Description Framework	RDF

SPARQL	Simple Protocol and RDF Query Language	بروتوكول ولغة استعلام RDF
RDFs	RDF Schema	مخطط RDF
XSD	XML Schema Definition	تعريف مخطط XML

مقدمة عامة

١- المقدمة

أصبح استخدام تكنولوجيا المعلومات الحديثة عنصراً ملازماً للعمل المصرفي لما توفره من فعالية وسرعة في الإنجاز ووفرة في المعلومات، وبدأت المصارف بالتحول من أسلوب العمل اليدوي الى العمل الالكتروني الذي يعتمد على الوسائط الإلكترونية، وظهر ما يعرف بالبنوك الإلكترونية والخدمات المصرفية الإلكترونية التي مثلت قفزة نوعية في مجال العمل المصرفي، و تم تزويد العملاء ببيئة متناسقة وقوية عبر الانترنت للاستفادة من الخدمات المقدمة. ولكن تصاعد أعمال الغش والاحتيال عبر الشبكة أدى الى ظهور مخاطر أمنية تهدد المعلومات المتبادلة بين البنك والعميل، فأصبح على البنوك والزبائن تطبيق تقنيات ومعايير أمنية على مستوى الأجهزة و التطبيقات والشبكة، وذلك من أجل مصادقة هويات العملاء وضمان انتقال بياناتهم عبر الشبكة بشكل آمن ومتسق، و أصبح تحديد المتطلبات الأمنية ومعرفة نقاط الضعف وكيفية التخلص منها من أهم القضايا التي تواجه العمل المصرفي الالكتروني [1]. والأنطولوجيا وسيلة جيدة لنمذجة وتشارك وتكامل المعرفة، لذلك فإن تحليل الثغرات الأمنية و نمذجة متطلبات الأمان باستخدام الانطولوجيا يسهل استرجاعها والاستفادة منها بالشكل الأمثل . [2]

٢- الدراسات السابقة

٢.١ مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية -e banking services

تعد الخدمات المصرفية الإلكترونية جزءًا لا يتجزأ من البنوك الحديثة وذلك بسبب انخفاض تكاليف المعاملات وتوافرها في جميع الأوقات وسهولة استخدامها، إلا أنها تعاني من مشكلة أساسية وهي حماية المعلومات المتبادلة بين البنك والعميل.

فوفقاً لدراسة قام بها Singh, Ruhl and Samuel عام ٢٠١٨ فإنه على الرغم من أن أحد أهداف بروتوكول EMV هو تأمين معاملات الدين والائتمان في محطة نقاط البيع (POS) ، ولكن لا تزال هناك نقاط ضعف يمكن أن تؤدي إلى الكشف غير المصرح به عن بيانات حامل البطاقة و

يؤدي استغلالها الى العديد من الهجمات مثل MITM و Pre-play Attack و NFC Relay Attack و Eavesdrop Attacks . وقد تم استخدام منهجية شجرة الهجوم لتوثيق نقاط الضعف كما تم توفير الإجراءات المضادة ضد مختلف الهجمات المحتملة. [3]

بينما قام Ojeniyi, Edward and Abdulhamid بتحليل مخاطر أمن البنوك الالكترونية عام ٢٠١٩ من خلال استبيان يحدد مستوى المخاطر التي من الممكن أن تواجه عملاء البنك وأشاروا إلى الحاجة إلى المزيد من الوعي بشأن حفظ تفاصيل المعاملة وكلمات المرور على أجهزة العميل ، كما يجب على البنك تحسين تطبيقات المعاملات المصرفية من أجل الحفاظ على سلامة البنوك . [4]

أما Eneeji و آخرون فقد درسوا الاحتيال المصرفي في عام ٢٠١٩ ، وبينوا أن الاحتيال يحدث من خلال انتحال الشخصية والخداع والقرصنة وأحصنة طروادة. ويجب أن يتوفر نظاماً أمنياً قادراً على الدفاع ضد الهجمات الخارجية. وقد تم استخدام الشبكات العصبية الذكية وأنظمة المعلومات الجغرافية لرصد واكتشاف الاحتيال. [5]

وفي عام ٢٠٢٠ بين Hammood وآخرون أن تبادل الثقة بين البنك والعميل أمر في غاية الأهمية وأن معظم آليات الحماية تتركز على عملية المصادقة وأن مصادقة العميل تعتمد على تقنيات مثل كلمات السر و المصادقة الحيوية واقترحوا آلية مصادقة باستخدام رقم التعريف العالمي للجهاز المحمول. [6]

٢.٢ الأنطولوجيا وأمن المعلومات

نشرت العديد من الأبحاث حول استخدام الأنطولوجيا في مجال أمن المعلومات ، ففي عام ٢٠١٥ اقترح Souag وآخرون أنطولوجيا أمنية لهندسة متطلبات الأمن وتم تطوير بيئة تفاعلية لتسهيل استخدام هذه الأنطولوجيا في عملية هندسة متطلبات الأمان ، استخدمت الأنطولوجيا لأنها مفيدة في تمثيل وربط أنواع كثيرة من المعلومات ضمن مجال محدد ، ولضرورة وجود أنطولوجيا أمنية لتنسيق التعريف الغامض لمفاهيم أمن المعلومات والعلاقات فيما بينها. أثبتت التجربة أن الأنطولوجيا مفيدة جدا عندما يتم استغلال المعرفة المهيكلة فيها بوساطة بيئة تفاعلية واستعلامات مناسبة . كانت هذه الأنطولوجيا عامة ولذلك كان تنفيذها أكثر تعقيداً من المتوقع واستغرق تنفيذها وقت طويل، كما كان من الممكن تحسينها بزيادة المعرفة والخبرة الأمنية للعاملين فيها أو بتضييق مجالها أو بطرح المفاهيم

والعلاقات بطريقة أخرى ، ومن الناحية الفنية كان من الممكن تحديثها ونقلها الى إصدار أحدث من (OWL/Protégé). [2]

أما Carvalho وآخرون فقد استخدموا الأنطولوجيا عام ٢٠١٥ في رسم خريطة المنظمات الإجرامية وتحديد مطوري البرامج الضارة وذلك من خلال كشف العلاقات بين عدد كبير من الأدلة غير المترابطة . وقد ظهرت في هذا البحث أهمية الأنطولوجيا في جمع وتحليل كميات كبيرة من البيانات ، و الدور الكبير الذي يمكن أن تلعبه في التحقيق في جرائم الانترنت واكتشاف الأدلة، ركزت هذه الأنطولوجيا فقط على عمليات الاحتيال باستخدام البرمجيات الضارة أهملت الأنواع الأخرى من الهجمات التي يمكن أن تصيب أي جزء من أجزاء النظام المصرفي نتيجة وجود ثغرة أمنية ما، كما أنها لم تعطي حلول أمنية تسهم بالتخفيف من الهجمات. [7]

وفي عام ٢٠١٥ ايضا استخدم Stepanova وآخرون الأنطولوجيا في أتمتة عملية اختبار الاختراق، واعتبروا التقنيات الدلالية ضرورية لاستخراج المعرفة ومعالجتها وتخزينها. لذلك فقد طورت أنطولوجيا أمنية باستخدام Protégé مع أداة برمجية تسمح بتحليل البيانات التي يتم استردادها من مصادر مختلفة . قدمت هذه الأنطولوجيا نظرة شاملة عن نتائج اختبار الاختراق، ولكن لم تتم أتمتة بعض مراحل تحليل الأمن ومنها التصور الواضح بالاعتماد على الأنطولوجيا، والمعرفة الضمنية والصريحة المتعلقة بالنظام قيد الاختبار، كما أنها كانت أنطولوجيا عامة ومعقدة. [8]

بينما اقترح Rosa و Bonacin عام ٢٠١٨ انطولوجيا أمنية من أجل تقييم الأمن بهدف الوصول الى أنظمة آمنة وبهدف إضفاء الطابع الرسمي على مفاهيم أمن المعلومات، حيث تم اعتبار مفهوم" تقييم الأمن "موروث من مفهومين هما "تقييم الأنظمة " و "أمن المعلومات " . تم بناء تطبيقين برمجيين الأول يستقبل قائمة بعناصر التقييم وأبعادها وخصائص الأمان ويحسب مدى تغطية خصائص أمن المعلومات ، الثاني يزود بواجهة رسومية لتوليد تصاميم التقييم . ركزت هذه الانطولوجيا فقط على تقييم الأمان وليس على مفهوم أمن المعلومات بأكمله كما أنها أهملت إدارة المخاطر العملية وتحليل الهجوم ، ويمكن تحسينها بإضافة مفاهيم وعلاقات وخصائص أخرى ، كما أنه لا بد من التحقق من صحة المفاهيم من قبل خبراء تقييم الأمن. [9]

واقترح Fenz و Neubauer عام ٢٠١٨ طريقة لإضفاء الطابع الرسمي على خصائص أمن المعلومات والتحقق من امتثالها للضوابط الرسمية للمعيار ISO 27002 وذلك بالاعتماد على الأنطولوجيا .حيث قاموا بتحليل المعيار المذكور وتحليل عدة أنطولوجيا سابقة للحصول على المفاهيم والعلاقات الأساسية ، ثم أضافوا مفاهيم وعلاقات جديدة وبنوا قواعد الامتثال ، وبعد ذلك طوروا نظام دعم القرار للتحقق من مستوى امتثال الشركة لضوابط المعيار المذكر سابقاً. وكانت ميزة هذا العمل وجود قاعدة المعرفة الدلالية التي أكدت أن كل خيارات القرارات كانت متوافقة مع المعيار المذكور آخذة بعين الاعتبار الخصائص المحلية للمنظمة التي ستطبق فيها. هذه الانطولوجيا رسمية وعامة ولم تأخذ بعين الاعتبار بعض مفاهيم الهجوم كما أنها ركزت على معيار محدد وأهملت باقي معايير الأمان. [10]

كما أن Syed و Zhong طوروا عام ٢٠١٨ نموذج مفاهيمي قائم على الأنطولوجيا لإدارة نقاط الضعف. يدمج هذا النموذج المفاهيم من مصادر رسمية مثل CVE وغيرها والمصادر غير الرسمية مثل وسائل التواصل الاجتماعي. تعمل هذه الأنطولوجيا على توسيع مفاهيم الضعف التي يوفرها المعهد الوطني للمعايير والتكنولوجيا (NIST) ويمكن استخدامها كمفردات عامة في مجال إدارة الثغرات الأمنية. يمكن أن تكون هذه الأنطولوجيا مفيدة للتفكير في علاقات الكيانات لإصدار تنبيهات الأمان لمحللي الأمان لتحليل الثغرات الأمنية وإدارتها. ركزت هذه الأنطولوجيا على إدارة الثغرات الأمنية وتجاهلت بعض المفاهيم المتعلقة بالهجوم الذي قد يحدث نتيجة لوجود نقطة ضعف. [11]

أما Kotenko و آخرون فقد اقترحوا عام ٢٠١٨ نهجًا قائمًا على الأنطولوجيا لتخزين البيانات الأمنية بهدف ربط البيانات الأمنية من مصادر داخلية مختلفة مثل أنظمة كشف التسلل والوقاية منها ، والماسحات الضوئية للشبكة ، وسجلات الأحداث ... إلخ ، والخارجية مثل CVE، CAPEC، ... إلخ. وقد بينوا أن الأنطولوجيا تسمح بدمج البيانات بسهولة من مصادر مختلفة ، وتسمح باستخدام استعلامات أكثر دقة وتقلل من الوقت المطلوب لمعالجة الاستعلام. أظهرت النتائج التجريبية أن استخدام الأنطولوجيا يعزز إدارة أمن الأنظمة. لكن سلبية هذه الطريقة هي أنها تعتمد على جودة البيانات المخزنة في الأنطولوجيا. [12]

كما أن Kotenko و Doynikova اقترحوا عام ٢٠١٨ نهجًا لتحديد أهداف الهجمات الإلكترونية على أساس أنطولوجيا مقاييس الأمان والشبكات العصبية الضبابية. استخدمت الأنطولوجيا لتحديد

أهداف الهجوم الأمني. تم الحصول على المعلومات من مصادر مختلفة مثل CWE و CVE و CAPEC. أظهر هذا النهج نتائج جيدة في منع انتشار الهجمات في أنظمة المعلومات ، ولكن هناك بعض القيود المتعلقة باختيار الاستجابة المثلى لأنها تستخدم مؤشرًا تقريبيًا إلى حد ما. هذه الأنطولوجيا عامة وتركز على إيجاد هدف الهجوم في أنظمة المعلومات. وتتجاهل طرق الوصول الى هذا الهدف كما تجاهلت التدابير المضادة. [13]

و في عام ٢٠١٩ طور Wen و Katt أنطولوجيا أمنية بهدف إدارة المعرفة الأمنية للبرنامج مع مراعاة سياق التطبيق ، حيث لا ينبغي لمطوري البرامج أن يكون لديهم معرفة عامة بمفاهيم الأمان فحسب ، بل يجب أن يكون لديهم أيضًا السياق الذي يتم فيه تطوير البرنامج. وقد بينوا أن التمثيل الأنطولوجي يدعم تكامل موارد المعرفة في مستويات مختلفة من التجريد والبحث المتقدم عن المعرفة ، وبالتالي يدعم عملية المشاركة والتعلم حول أمن البرنامج. كما بينوا أن الاعتماد على الأنطولوجيا مهم جدًا في العديد من التطبيقات. ساهمت هذه الأنطولوجيا في مشاركة فهم مشترك لمفاهيم الأمن العام وهي مصممة لضمان أمان التطبيق خلال مراحل تطويره وأهملت المخاطر التي يمكن أن تواجه التطبيق بعد إطلاقه ووضعه موضع التنفيذ ، وتركز هذه الأنطولوجيا على أمن البرمجيات ويتجاهل أمن الأجهزة. [14]

أما Brazhuk فقد درس مشكلة استخراج واستخدام المعرفة من قواميس عامة تخص هجمات البرمجيات ونقاط ضعفها وذلك لبناء نماذج دلالية للتهديد بهدف بناء نموذج و استخدامه كنواة لنظام إدارة المعرفة في مجال أمن البرمجيات. وقد استخدم الأنطولوجيا بسبب تعدد مصادر المعرفة في هذا المجال وصعوبة تحليلها يدوياً. فالأنطولوجيا يمكن أن تستخدم كجزء من نظام ذكي أو نظام تعلم عن بعد، وهي تستخدم المنطق الوصفي الذي من اهم خصائصه وصف المفاهيم والعلاقات فيما بينها بطريقة شكلية مع إمكانية التفكير والاستنتاج . فالأنطولوجيا يمكن أن تستخدم مع أي نظام قائم على المعرفة .اعتمد النموذج المقترح على CAPEC و CWE . أخذ هذا النموذج في عين الاعتبار أمن البرمجيات وأهمل أمن الأجهزة. [15]

٣- الخلاصة

قدمنا في هذا الفصل خلاصة لبعض الدراسات السابقة في مجالي مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية، واستخدام الأنطولوجيا في مجال أمن المعلومات.

الفصل الأول: الخدمات المصرفية الالكترونية

١.١ المقدمة

سنتحدث في هذا الفصل عن الخدمات المصرفية الالكترونية، تعريفها، إيجابياتها، وسلبياتها. ثم سنتحدث عن خدمة التجارة الالكترونية باستخدام متصحف الوب وباستخدام طريفة نقاط البيع، لتكون أساس بحثنا.

١.٢ تعريف الخدمات المصرفية الالكترونية

البنوك الالكترونية(Online Bank) تعرف أيضا باسم البنوك الافتراضية(virtual banking) أو الخدمات المصرفية الالكترونية (e-banking services)، وهي عبارة عن نظام دفع الكتروني يمكن زبائن البنك (أشخاص ، منظمات .. الخ) من اجراء مجموعة من المعاملات المالية. ونظام الدفع الالكتروني يتصل عادة مع النظام البنكي الأساسي ويكون جزء منه ، وما يميزه عن أحد فروع البنك هو طريقة وصول الزبائن الى الخدمة المصرفية، حيث يستطيع الزبون الوصول الى الخدمة عن بُعد، باستخدام طرفية ما متصلة بشبكة الانترنت.

١.٣ فوائد وإيجابيات الخدمات المصرفية الالكترونية

الراحة Convenience

عن طريق الخدمات المصرفية الالكترونية، يستطيع الزبون القيام بالأنشطة المصرفية متى يشاء. حيث أنها تقدم الخدمات على مدار ٢٤ ساعة ولا يوجد عدد ساعات عمل محددة من قبل البنك ، لا يتعين على الزبون قضاء الوقت في السفر إلى الفرع و الانتظار وفق نظام الدور ، مما يتيح له مزيدًا من الوقت لفعل ما يريد ولقضاء حوائجه الأخرى .

قابلية التنقل Mobility

حيث يستطيع الزبون القيام بالخدمات المصرفية الالكترونية من أي مكان ، طالما أنه يستطيع الاتصال بالإنترنت .حتى إذا كان بعيداً عن المنزل او العمل أوفي عطلة ، حتى أن بعض البنوك قد أنشأت تطبيقات للهواتف المحمولة تسهل التعامل المصرفي مع أولئك الذين لديهم هاتف ذكي مثل Apple iPhoneأو iTouch أو Blackberry .

لا توجد رسوم No Fees

غالباً لا توجد رسوم مقابل الخدمات المصرفية الالكترونية وإن وجدت تكون رمزية جداً.

التصاريح والتقارير عبر الانترنت Online Statements

حيث يتم تداول المراسلات والبيانات عبر الانترنت، مما يقلل من كمية الورق المستخدم، وهذا سيساعد على تقليل التكاليف و يجعل الخدمات المصرفية الالكترونية خيارًا صديقاً للبيئة .

الإيداع المباشرDirect Deposit

حيث يتم ايداع الأموال بالحساب الخاص بالزبون مباشرة من قبل أي شركة أو منظمة أو شخص آخر داخل أو خارج البنك عن طريق عملية التحويل بين حسابين .

دفع الفواتير Bill Paying

حيث يمكن دفع فواتير لمنظمات أخرى مباشرة بتحويل مبلغ الفاتورة من حساب الزبون الشخصي إلى الحساب الخاص بالمنظمة ولا تستغرق هذه العملية سوى بضعة ثواني.

الحصول على معلومات الحساب في الوقت الحقيقي Real Time Account Information

حيث يستطيع الزبون الوصول إلى حسابه في أي وقت . سواء في الوقت الحقيقي او من خلال الرجوع الى معلومات الحساب في أي تاريخ سابق مما يتيح عملية إدارة أمواله بشكل أفضل وتحقيق أقصى استفادة من الخدمات التي يقدمها البنك.

التحويلات Transfers

حيث يمكن إجراء التحويلات بين الحسابات مع نفس المؤسسة المالية أو مع مؤسسات أخرى عبر الإنترنت بشكل فوري .

عرض الأرصدة View balances

حيث يتمكن الزبون من مراقبة حساباته و التحقق من أرصدته في أي وقت ولا يتطلب منه هذا الأمر الكثير من العمل أو الكثير من الوقت. [16]

عمليات الشراء عبر الانترنت online purchasing

يستطيع الزبون شراء ما يريد دون الحاجة لزيارة المتجر أو البنك و دون الحاجة لحمل النقود ، فكل ما عليه هو عملية تحويل سعر السلعة من حسابه الخاص الى حساب المتجر .

سرعة الإنجاز

يتم تقديم الخدمة للزبون بسرعة كبيرة ، حيث يتم تنفيذ العمليات التي يريدها خلال ثوان. [1]

١.٤ سلبيات البنوك الالكترونية

الأمان Security

بما أن الانترنت هي وسيلة الاتصال بين البنك و الزبون ويتم من خلالها تقديم الخدمات والمنتجات المصرفية ، فإن التأكد من سلامة و أمن تلك الوسيلة هو أساس ومحور ارتكاز العمل المصرفي الالكتروني ، وعنصر السلامة والأمان للإنترنت ليس مهماً على مستوى الحفاظ على أمن البنك وسمعته على المستوى الفردي فحسب، وإنما مهما أيضا لسلامة و أمن الجهاز المصرفي ككل، ولخلق الثقة العامة الجهاز من قبل الجمهور. [17]

ونظراً لكثرة الخدمات المصرفية الالكترونية سنختار منها التجارة الالكترونية بنوعيها عبر متصفح الويب وعبر طرفية نقاط البيع.

١.٥ التجارة الالكترونية

١.٥.١ تعريفها

عرّفت منظمة التجارة العالمية World Trade Organization التجارة الالكترونية بأنها "عبارة عن عملية إنتاج وترويج وبيع وتوزيع المنتجات من خلال شبكة الاتصال." ومن خلال هذا التعريف يتضح أن التجارة الالكترونية تشمل جميع الأنشطة الناشئة عن العلاقات ذات الطابع التجاري على سبيل المثال التوريد والتبادل والبيع والتوزيع وجميعها تتم بوساطة شبكة الانترنت. وهذه العمليات تحتاج الى وهذه العمليات تحتاج الى عملية الدفع الالكتروني e-payment، الذي يعتبر جيل جديد من طرق الدفع التي تقوم على تكنولوجيا الانترنت والاتصالات من ناحية، والأنظمة الذكية التي تربط البنوك وشركات الأموال من ناحية أخرى. [18]

١.٥.٢ نظام الدفع الالكتروني

من خلال الدفع الالكتروني يمكن لأي شخص تحويل أموال أو اجراء عمليات شراء من أي مكان وفي أي وقت دون الحاجة الى زيارة موقع البنك.

ظهرت الحاجة الملحة لوجود أنظمة للدفع الإلكتروني مع ظهور مفهوم التجارة الإلكترونية، واليوم تدخل فكرة الدفع الإلكتروني في الكثير من المجالات بدءاً من دفع المرتبات والفواتير، مروراً بالشراء سواء من المتاجر الإلكترونية أو المتاجر التي على أرض الواقع، انتهاءً بظهور ما يسمى بالمحافظ الإلكترونية الرقمية المستقلة.

يشير نظام الدفع الالكتروني الى كل التقنيات الضرورية لاستخدام البطاقات البنكية ومعالجة الحركات الناتجة عن هذا الاستخدام سواء بإدخال بياناتها عبر متصفح الوب أو بإدخالها في طرفيات نقاط البيع أو تمريرها أمام هذه الطرفيات. يتضمن نظام الدفع الالكتروني الشخص الذي يقوم بعملية الشراء عبر الانترنت والذي أمامه عدة خيارات، فإما يقوم بنقل الأموال من حسابه البنكي مباشرةً أو استخدام بطاقة الائتمان Credit Card أو بطاقة الدين Debit Card.

واستخدام البطاقة هي الطريقة الأكثر شيوعاً. وتُصنع هذه البطاقة عادة من البلاستيك وتحتوي شريط ممغنط، و يرتبط بها معلومات مثل رقم البطاقة واسم حاملها وتاريخ انتهاء الصلاحية وقيمة التحقق وعنوان إرسال الفواتير. [19]

١.٥.٣ مكونات نظام الدفع الالكتروني

١. التاجر Merchant: الكيان المرخص له بقبول الدفع بالبطاقة
٢. المستحوذ Acquirer: المؤسسة المالية وعضو الشبكة التي تتعاقد مع التجار لقبول شبكة الدفع بالبطاقات
٣. حامل البطاقة Cardholder: وهو الشخص حامل البطاقة والمصرح له باستخدام البطاقة
٤. جهة إصدار البطاقة Card issuer: وهي المؤسسة المالية التي تصدر البطاقات لاستخدامها في المعاملات ويدخل اتفاقيات مع حاملي البطاقات لدفع فواتير المعاملات.
٥. شبكة مؤسسة الدفع Payment corporation network : وهي شركة الخدمات المالية مثل فيزا وماستر كارد والتي يعمل معها مصدري البطاقات والمستحوذون. وتضع القواعد و اللوائح التي تنظم معالجة المدفوعات التي تنطوي على البطاقات. كما أنها تشغّل أكبر متجر إلكتروني للبيع بالتجزئة في العالم، وهي التي تسهل تدفق المعاملات بين المشترين ومصدري البطاقات. وتقدم مجموعة من الأنظمة التي تتضمن:

١. خدمة التفويضAuthorization : التي يوافق من خلالها مصدري البطاقات على المعاملات أو يرفضونها.
٢. خدمة المقاصة والتسوية Clearing and Settlement : التي تعالج المعاملات الكترونياً بين المصدري البطاقات والمستحوذين ذلك لضمان:

- ارسال معلومات المعاملات من المستحوذين الى المصدرين للنشر في حسابات حاملي البطاقات.
- تسهيل تفاصيل دفع المعاملات من مصدري البطاقات الى المستحوذين لتضاف الى حسابات التجار.[20]

١.٦ مراحل التجارة الالكترونية عبر متصفح الويب

١. يقوم حامل البطاقة بالتسجيل في موقع التاجر.

٢. يقوم حامل البطاقة بتسجيل الدخول الى حسابه في موقع التاجر.

٣. يبحث المستخدم عن المواد المراد شراءها، ويختارها، ويضيفها الى سلة المشتريات.

٤. يختار المستخدم نوع الدفع الالكتروني.

٥. يتوجه المستخدم الى نظام الدفع الالكتروني.

٦. يدخل المستخدم معلوماته الشخصية ومعلومات حسابه البنكي و بطاقة الائتمان.

٧. يرسل التاجر المعلومات الى بوابة الدفع التي ترسل بدورها المعلومات الى شبكة الدفع.

٨. تقوم شبكة الدفع بالتحقق مع بنك العميل، والتأكد من صلاحية البطاقة ووجود رصيد كافي للعملية.

٩. في حال تمت الموافقة من قبل بنك العميل يتم خصم المبلغ من حساب العميل.

١٠. يقوم بنك العميل بإرسال تأكيد الى شبكة الدفع.

١١. تقوم شبكة الدفع بأرسال تأكيد الى المستحوذ الذي يرسل تأكيد الى بوابة الدفع.

١٢. بوابة الدفع ترسل تأكيد للمتجر الالكتروني، ويخبر المتجر المشتري بتأكيد استلام ثمن المشتريات.

١٣. ويحصل المشتري على اشعار من البنك المصدر وتبدأ اجراءات ارسال المنتج الى عنوان المشتري. [20] [19]

١.٧ مراحل التجارة الالكترونية عبر طرفية نقاط البيع

١. يزود حامل البطاقة التاجر بالبطاقة.

٢. يمرر التاجر البطاقة عبر القارئ أو يدخلها ضمن جهاز قارئ الرقائق أو يلوحها أمام القارئ، ويدخل مبلغ المعاملة وينقل الطلب الى المستحوذ.

٣. يرسل المستحوذ الطلب الى شبكة الدفع.

٤. تمرر شبكة الدفع الطلب الى مصدر البطاقة.

٥. يختبر مصدر البطاقة صلاحية البطاقة ووجود الرصيد الكافي للمعاملة.

٦. يرسل مصدر البطاقة الرد الى المشتري عبر شبكة الدفع.

٧. المستحوذ يرسل الرد الى التاجر.

٨. يتلقى التاجر الاستجابة ويكمل المعاملة وفقاً لها.

٩. التاجر يودع ايصال المعاملة مع المستحوذ.

١٠. المستحوذ يرسل المعاملة الكترونياً الى شبكة الدفع.

١١. شبكة الدفع ترسل المعاملة الى مصدر البطاقة.

١٢. مصدر البطاقة يرسل المعاملة الى حساب حامل البطاقة ويرسل اشعار الى حامل البطاقة. [20]

١.٨ الخلاصة

قدمنا في هذا الفصل لمحة عامة عن الخدمات المصرفية الالكترونية. ثم تحدثنا عن التجارة الالكترونية وعمليات الدفع الالكتروني، والتي ستكون محور بحثنا. ثم انتقلنا الى مكونات نظام الدفع الالكتروني، و مراحل تنفيذ التجارة الالكترونية عبر متصفح الوب وطرفية نقاط البيع ذلك بهدف تحديد المرحلة التي من الممكن أن تتعرض لهجوم في لحظة ما.

الفصل الثاني: مخاطر أمن المعلومات في الخدمات المصرفية الالكترونية

٢.١ المقدمة

سنتحدث في هذا الفصل عن المخاطر الأمنية التي من الممكن أن تتعرض لها الخدمات المصرفية الالكترونية، وخدمة التجارة الالكترونية بشكل خاص. ثم سننتقل الى أهمية تحليل هذه المخاطر وذلك بهدف التغلب عليها قدر الإمكان. فبالرغم من كل الايجابيات التي تتمتع بها البنوك الالكترونية ، يوجد بعض السلبيات و المخاطر التي قد تهدد سرية Confidentiality أو صحة Integrity أو وفرة Availability البيانات التي يتم تبادلها عبر شبكة الانترنت بين البنك والزبون. فوجود نقاط ضعف Vulnerabilities في أحد الأجهزة المستخدمة أو التطبيقات أو في الشبكة قد يؤدي الى استغلالها من قبل منظمات أو أشخاص مجهولين غير مخولين بالوصول الى هذه المعلومات وذلك لتحقيق أهداف غير أخلاقية . نظرًا لأن الأمن أحد الشواغل الرئيسية لكل من المؤسسات الكبيرة والصغيرة، فإن الأنظمة المصرفية الإلكترونية تواجه أيضًا هجمات إلكترونية مثل أي نظام آخر متصل بالإنترنت، ويتمثل التحدي الرئيسي لقطاع البنوك الإلكترونية في الاستخدام المكثف لتطبيقات تكنولوجيا المعلومات المتعلقة بالخدمات المصرفية الإلكترونية، وهذا يؤدي إلى تهديدات الأمن الإلكتروني ، والهجمات الإلكترونية على ملف تعريف العملاء ، والاختلاس ، والاحتيال فيما يتعلق برسائل البيانات ، وسرية عملاء مكافحة السرقة ، وسرية المعاملات المالية. [21]

تقدم العديد من التقارير الإحصائية أمثلة على أبعاد وآثار الانتهاكات الأمنية في الخدمات المصرفية الإلكترونية. ففي شباط ٢٠٠٥ قاضى رجل أعمال في ميامي مصرفه بسبب خسارة ٩٠٠٠٠ دولار من حسابه الخاص عن طريق الانترنت من قبل شخص غير مصرح له . كما أن الولايات المتحدة خسرت حوالي ٣,٥ ترليون دولار من خلال ثلاث شبكات دفع في بنك نيويورك. [22]

ووفقًا لاستطلاع SANS لعام ٢٠١٦ ، والذي يقيس حالة المخاطر والأمان في القطاع المالي ، فإن صناعة الخدمات المالية تقع تحت وطأة هجمات الفدية والقرصنة ، والتي تتزايد بشكل كبير. [21]

٢.٢ أنواع الهجمات:Types of attacks

هجوم رفض الخدمة:Denial-of-service attack (DOS)

هو هجوم عبر الإنترنت حيث يسعى مرتكب الجريمة إلى جعل جهازًا أو مورد شبكة غير متاح للمستخدمين المقصودين عن طريق تعطيل خدمات مضيف متصل بالإنترنت مؤقتًا أو إلى أجل غير مسمى. عادةً ما يتم رفض الخدمة عن طريق إغراق الجهاز أو المورد المستهدف بطلبات زائدة في محاولة لزيادة التحميل على الأنظمة ومنع تلبية بعض أو جميع الطلبات المشروعة.

هجوم الرجل في الوسط Man-In-The-Middle attack

يستهدف سرية وسلامة البينات المنتقلة بين نقطتي النهاية (الضحايا)،حيث يتمكن الطرف الثالث (المهاجم) من الوصول الى القناة الواصلة بين نقطتي النهاية اللتان تظنان أنهما تستخدمان قناة آمنة ، ولكن في الواقع يمكنه الوصول إلى جميع الرسائل المشفرة .

الخداع Phishing

هو سرقة الهوية عبر الإنترنت، حيث يحاول المهاجمون خداع وسرقة الأموال من مستخدمي الإنترنت الشرعيين وذلك بإرسال رسائل البريد الإلكتروني بدلاً من استغلال الأخطاء في برامج الكمبيوتر. يقوم المهاجم بإنشاء موقع ويب احتيالي له شكل ومظهر الموقع الشرعي. تستخدم رسائل البريد الإلكتروني المخادعة مجموعة متنوعة من التكتيكات لخداع الأشخاص للكشف عن معلوماتهم السرية مثل أسماء المستخدمين وكلمات المرور وأرقام التأمين وأرقام بطاقات الائتمان .

تزوير العناوين Pharming

نسخة متطورة من هجمات الخداع. يقوم المهاجم بإدخال أحصنة طروادة و / أو الفيروسات المتنقلة في أجهزة الكمبيوتر الخاصة بالمستخدمين أو خادم DNS الذي يتسبب في أنواع مختلفة من الهجمات (تعديل ملف مضيف المستخدمين وتخريب ذاكرة التخزين المؤقت لنظام أسماء النطاقات ، واختطاف المجال ، وانتحال المجال الثابت ، وما إلى ذلك). سيعيد توجيه هذا النوع من الهجوم مستخدمو الويب إلى الصفحة المزيفة من أجل الحصول على معلومات الخصوصية أو كلمات مرور الحساب أو غيرها من المعلومات الهامة. يتمثل الخطر الرهيب المتمثل في هجوم pharming في أنه حتى لو تحقق المستخدمون بعناية من عنوان URL قبل زيارة موقع الويب ، فلن يتمكنوا من العثور على أي استثناء.

الانتحال Spoofing

عندما يتظاهر الخصم بأنه المرسل الشرعي لنشر رسائل كاذبة، أو يكون المتلقي الشرعي لسرقة معلومات سرية.

هجوم الهندسة الاجتماعية Social engineering attack

يعرّف المؤلفون الهندسة الاجتماعية بأنها "علم استخدام التفاعل الاجتماعي كوسيلة لإقناع فرد أو مؤسسة بالامتثال لطلب محدد من مهاجم حيث يتضمن التفاعل الاجتماعي أو الإقناع أو الطلب كيانًا متصلًا بالكمبيوتر". حيث يتم الاعتماد على الأساليب الاجتماعية مثل تكوين صداقات أو اللعب بالعواطف، أو الإكراه والابتزاز في بعض الأحيان من أجل خداع المستخدمين للوصول الى معلوماتهم الهامة والشخصية . [21]

حصان طروادة Trojans

تهدف الى التأثير على العمليات بطريقة غير مباشرة ،مما يؤدي الى عواقب وخيمة في التطبيقات الهامة ، يمكن أن تهدف أيضًا إلى تسريب معلومات سرية من داخل شريحة عبر قنوات سرية. [21]

وهو عبارة عن شيفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته. [23]

برامج التجسس والبرامج الدعائية Spyware and Adware

هي عبارة عن برمجيات مزودة بإعلانات تستخدم عند تنزيل البرنامج أو استخدامه ، حيث يتم عرض إعلانات غير مرغوبة ، وذلك بهدف جمع بيانات من المواقع التي يزورها المستخدم ، ومن ثم ارسالها الى المهاجم ، فهي بمثابة برامج تجسس تؤدي الى سرقة معلومات المستخدم السرية وإتلاف ملفات النظام .

التنصت على الرزم Packet Sniffers

يقوم المهاجمون بتثبيت المراقبة على الاتصال بين كمبيوتر المستخدم وخادم الويب

للتنصت على معلومات العملاء بما في ذلك معلومات بطاقة الائتمان وكلمة المرور. لذلك يصبح من الممكن الاحتيال على هؤلاء الضحايا. [22]

ونظراً لكثرة الهجمات التي من الممكن أن تتعرض لها، سنقوم بدراسة وتحليل الهجمات التالية باستخدام الأنطولوجيا:

٢.٣ هجمات التجارة الالكترونية باستخدام متصفح الويب

١. هجمات قناة الاتصال
- انتحال DNS DNS Spoofing
- الرجل في الوسط Man-in-The-Middle
- تزوير العناوين Pharming
- الاستنشاق Sniffing

٢. هجمات مخدم البنك
- هجوم رفض الخدمة Denial of Service(DOS)
- هجوم رفض الخدمة الموزع Distributed Denial of Service(DDOS)
- التصيدPhishing

- هجمات تطبيق الوب Web Application attacks
  - اختطاف الجلسة Session Hijacking
  - حقن SQL SQL Injection

٣. هجمات طرفية المستخدم
- البرمجيات الضارة Malware Threats

- الهندسة الاجتماعية Social Engineering . [22] [24]

٢.٤ هجمات التجارة الالكترونية باستخدام طرفية نقاط البيع

١. هجمات التنصت Eavesdrop Attacks

- الطرفية المزيفة Counterfeit Terminal
- الكاميرا والتمرير المزدوج Camera and Double swipe Method
- هجوم التنصت على الإشارة Signal Eavesdropping Attack

٢. هجمات أخرى

- الرجوع الى الشريط المغناطيسي Fall-back to Magnetic Stripe
- الاحتيال بوساطة الحواف Cross-border Fraud
- هجوم ما قبل التشغيل Pre-play Attack(PPA)
- هجوم التعاقب في بروتوكول NFC NFC Relay Attack
- هجوم الشريط في المنتصف Shim-in-the-middle Attack
- هجوم الرجل في المنتصف Man-in-the-middle Attack
- هجوم التعاقب النشط Active Relay Attack [3]

٢.٥ تحليل الهجمات

الخدمات المصرفية الالكترونية معقدة لأنها تحوي برمجيات وأجهزة وشبكة اتصال، وأمن معلوماتها يتطلب النظر في جميع هذه المكونات. ولضمان درجة عالية من الأمان يجب أن تكون التطبيقات والاجهزة والشبكات محمية من أي ثغرة أمنية، فوجود نقطة ضعف واحدة في أيا منها قد يكون سبب هجوم ناجح وخطير. وهذا يتطلب تحليل للهجمات والثغرات، وهذا التحليل يتطلب كميات كبيرة من البيانات لمعرفة هدف الهجوم ومتطلبات تحقيقه و أدوات الهجوم والثغرات التي أدت الى حدوثه واستراتيجية حدوثه والمرحلة التي قد يحدث فيها. ويحتاج التحليل أيضاً معلومات من مصادر مختلفة ومنها بعض مصادر المعرفة العالمية الخاصة بنقاط الضعف والهجمات مثل CWE و CVE و CAPEC والتي تمكننا من الحصول على المزيد من المعلومات المتعلقة بالهجوم ونقاط الضعف. وتعتبر أنظمة إدارة المعرفة المعتمدة على الدلالة أفضل الأنظمة التي تناسب هذه التحليلات، فهي

تستخدم طرائق وتقنيات موجهة للدلالة مثل الانطولوجيا. والانطولوجيا وصف لمجموعة من المفاهيم وخصائصها والعلاقات فيما بينها، وتستخدم من أجل تكامل المعرفة وبناء نموذج مفاهيمي كما انها تستخدم كجزء من نظام ذكي أو نظام تعلم عن بعد. فالأنظمة المعتمدة على الانطولوجيا تستخدم المنطق الوصفي حيث يتم وصف المفاهيم والعلاقات فيما بينها بطريقة رسمية كما يمكن إضافة الاستنتاج لها في بعض الأحيان. [15]

٢.٦ الخلاصة

قدمنا في هذا الفصل لمحة عن أهمية أمن المعلومات في الخدمات المصرفية الالكترونية، ثم انتقلنا الى أهم الهجمات التي قد تواجه الخدمات المصرفية الالكترونية بشكل عام، والهجمات التي تواجه التجارة الالكترونية عبر متصفح الويب وطرفية نقاط البيع بشكل خاص. ثم انتقلنا الى أهمية تحليل هذه الهجمات باستخدام الأنطولوجيا وذلك لفهمها و معرفة طرق التخلص منها.

الفصل الثالث: المصادر الرسمية العالمية للمعلومات

٣.١ المقدمة

سنتحدث في هذا الفصل عن أهم مصادر المعلومات العالمية الرسمية التي تخص الهجمات ونقاط الضعف، وعن دورها الكبير في إثراء عملية التحليل بالمزيد من المعلومات التي تساعد على فهم الهجوم ومعرفة كيفية التخلص منه.

٣.٢ CAPEC

٣.٢.١ التعريف

هو اختصار ل Common Attack Pattern Enumeration and Classification

يوفر قائمة عامة لأنماط الهجوم الشائعة، التي تساعد المستخدمين على فهم كيفية استغلال الخصوم لنقاط الضعف في التطبيقات و الأوساط الإلكترونية الأخرى. وأنماط الهجوم هي الأوصاف والأساليب الشائعة التي يستخدمها المهاجمون لاستغلال نقاط الضعف المعروفة في الأوساط الإلكترونية. تحدد أنماط الهجوم التحديات التي قد تواجه المهاجم وكيفية حلها. يحمل كل نمط هجوم معلومات حول كيفية تصميم أجزاء معينة من الهجوم وتنفيذها، ويقدم إرشادات حول طرق التخفيف من فعالية الهجوم. تساعد أنماط الهجوم مطوري التطبيقات و مديري الأوساط الالكترونية لفهم العناصر المحددة للهجوم بشكل أفضل وكيفية منعها من النجاح.

تم اطلاق CAPEC عام ٢٠٠٧ من قِبل من قبل وزارة الأمن الداخلي الأمريكية كجزء من المبادرة الاستراتيجية لضمان أمن البرامج Software Assurance (SwA) لمكتب الأمن الالكتروني والاتصالات Cybersecurity and Communications (CS&C). و لا تزال هذه القائمة تتطور بشكل مستمر لتشكيل آلية قياسية لتحديد أنماط الهجوم وجمعها وصقلها ومشاركتها بين مجتمع الأمن الالكتروني.

٣.٢.٢ فوائد CAPEC

يمكن لأنماط الهجوم الموجودة بهذه الطريقة الرسمية أن تحقق قيمة كبيرة في مجال أمن المعلومات وذلك على مستوى:

- التدريب: تثقيف مطوري البرامج والمختبرين والمشترين والمديرين .
- المتطلبات: تحديد التهديدات المحتملة .
- التصميم: توفير سياق لتحليل المخاطر.
- التنفيذ: تحديد أولويات أنشطة المراجعة.
- التحقق: توجيه اختبار الاختراق المناسب .
- الإصدار: فهم الاتجاهات والهجمات التي يجب مراقبتها .
- الاستجابة :الاستفادة من الدروس المستفادة في التوجيه الوقائي.

ليست أنماط الهجوم هي الأداة المفيدة الوحيدة لبناء أنظمة آمنة عبر الإنترنت. يمكن أن تساعد العديد من الأدوات الأخرى، مثل نماذج التهديد، ومعرفة نقاط الضعف والضعف الشائعة، وأشجار الهجوم . تلعب أنماط الهجوم دورًا فريدًا وسط هذه البنية الكبيرة للمعرفة والتقنيات الأمنية.

٣.٢.٣ المعلومات التي يوفرها CAPEC

يعد فهم كيفية عمل الخصم أمرًا ضروريًا للأمن الالكتروني الفعال. يساعد CAPEC من خلال توفير قاموس شامل لأنماط الهجوم المعروفة التي يستخدمها المهاجمين لاستغلال نقاط الضعف المعروفة في الأوساط الإلكترونية الممكنة. يمكن استخدامه من قبل المحللين والمطورين والمختبرين والمعلمين لتعزيز فهم المجتمع وتعزيز الدفاعات.

يتم تصنيف أنماط الهجوم في **CAPEC** إما وفق آلية الهجوم أو وفق مجال الهجوم. وكل سجل من سجلات **CAPEC** يحوي معلومات هجوم معين وهي:

- معرف الهجوم ID
- وصف الهجوم Description
- متطلبات مسبقة Prerequisites
- طريقة تخفيف الهجوم Mitigations
- نقاط الضعف المرتبطة بالهجوم Related Weaknesses(CWE)
- احتمال نجاح الهجوم Likelihood Of Attack
- شدة الهجوم Typical Severity

- المهارات اللازمة للمهاجم للقيام بالهجوم Skills Required
- مجال أمن المعلومات الذي يتأثر بالهجوم Scope
- الأثر التقني الذي يتركه الهجوم Impact. [25]

CWE ٣.٣

٣.٣.١ التعريف

اختصار ل Common Weakness enumeration

هي قائمة رسمية مطورة للحصول على معلومات لأنواع نقاط ضعف البرامج والأجهزة .وهي بمثابة لغة مشتركة، ومقياس لأدوات الأمان، وكخط أساس لتحديد نقاط الضعف، والتخفيف من حدتها، وجهود الوقاية.

فنقاط الضعف هي عيوب أو أخطاء في تنفيذ البرامج أو الأجهزة أو التعليمات البرمجية أو التصميم أو الهندسة التي إذا تُركت دون معالجة يمكن أن تؤدي إلى تعرض الأنظمة أو الشبكات أو الأجهزة للهجوم. تُعد CWE والتصنيفات المرتبطة بها بمثابة لغة يمكن استخدامها لتحديد ووصف نقاط الضعف هذه. الهدف الرئيسي من CWE هو إيقاف الثغرات الأمنية في المصدر من خلال تثقيف مهندسي البرمجيات والأجهزة والمصممين والمبرمجين حول كيفية التخلص من الأخطاء الأكثر شيوعًا. ويساعد استخدام CWE في منع أنواع الثغرات الأمنية التي واجهت صناعات البرمجيات والأجهزة وعرَضت المؤسسات للخطر.

كان أول إطلاق ل CWE عام ٢٠٠٦، ويتم تحديثها بشكل مستمر.

٣.٣.٢ فوائد CWE

- وصف ومناقشة نقاط الضعف في البرامج والأجهزة بلغة مشتركة .
- التحقق من نقاط الضعف في منتجات البرامج والأجهزة الحالية .
- تقييم تغطية الأدوات التي تستهدف نقاط الضعف .
- الاستفادة من معيار أساسي مشترك لتحديد نقاط الضعف والتخفيف من حدتها والوقاية منها .
- منع انتشار ثغرات البرامج والأجهزة.

٣.٣.٣ المعلومات التي توفرها CWE

- وصف الضعف Description
- أمثلة مشاهَدة لهذا الضعف في الأنظمة وأدت الى هجوم Observed Examples وهي سجلات في CVE
- طرق الكشف عن هذا الضعف Detection Methods
- سجلات CAPEC التي يرتبط بها هذا الضعف Related Attack Patterns

بالإضافة الى بعض المعلومات التي تخص شدة هذا الضعف ومجاله و احتمالية استغلاله في هجوم ما. [26]

٣.٤ CVE

٣.٤.١ التعريف

هي اختصار ل Common Vulnerabilities and Exposures

تتمثل مهمة CVE في تحديد الثغرات الأمنية الالكترونية التي تم الكشف عنها وتحديدها وفهرستها .يوجد سجل واحد لكل ثغرة في الكتالوج . يتم اكتشاف الثغرات الأمنية ثم تخصيصها ونشرها من قبل المنظمات من جميع أنحاء العالم التي دخلت في شراكة مع برنامج CVE . ينشر الشركاء سجلات CVE لإعطاء أوصاف متسقة لمواطن الضعف يستخدم محترفو تكنولوجيا المعلومات والأمن الالكتروني سجلات CVE للتأكد من أنهم يناقشون نفس المشكلة ، ولتنسيق جهودهم لتحديد أولويات الثغرات ومعالجتها.

تم إطلاق قائمة CVE رسميًا في أيلول ١٩٩٩، ويتم تحديثها بشكل مستمر بإضافة سجلات جديدة.

أوصى المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST)باستخدام CVE من قبل الوكالات الأمريكية. كما أن CVE تعتبر أساساً لقاعدة الضعف الوطنية الأمريكية U.S. National Vulnerability Database (NVD) .

إن الاعتماد على المصادر الرسمية يعطي قيمة عالية لعملية التحليل ومصداقية كبيرة في المعلومات. وبالتالي ربط عملية تحليل هجمات الخدمات المصرفية الالكترونية بقواميس CAPEC و CWE وCVE سيثري عملية التحليل بمعلومات ستؤدي الى فهم كيفية استغلال المهاجم لنقاط الضعف وذلك بهدف منعه من النجاح. ولكن هذه المصادر غير مرتبطة ببعضها بشكل مباشر، على سبيل المثال CAPEC غير مرتبط ب وCVE بشكل مباشر وإنما الربط يتحقق من خلال CWE . حيث أن سجلات CAPEC مرتبطة بسجلات CWE، وسجلات CWE مرتبطة بسجلات CVE، والسؤال هنا، كيف سنقوم بربط هذه المصدر المختلفة مع بعضها من جهة ومع مفاهيم الأمان كهدف الهجوم و استراتيجية الهجوم وأداة الهجوم ..الخ من جهة أخرى، ومع مفاهيم الخدمات المصرفية الالكترونية أيضاً؟

والجواب هو ، سيتحقق الربط من خلال استخدام الأنطولوجيا التي تعتبر إحدى تقنيات الويب الدلالي.[27]

٣.٥ الخلاصة

قدمنا في هذا الفصل معلومات عن المصادر الرسمية التي سنستخدمها في بحثنا، ودورها في إثراء عملية التحليل بالمعلومات، و أهمية الربط بينها باستخدام الأنطولوجيا.

الفصل الرابع: الويب الدلالي Semantic Web

٤.١ المقدمة

سنتحدث في هذا الفصل عن الويب الدلالي وتقنياته. ثم سنتحدث عن الأنطولوجيا ومكوناتها وفوائدها ودورها في جمع المعلومات من مصادر مختلفة وربطها مع بعضها.

٤.٢ تعريفه

يمكن تعريف الوب الحالي المعروف من قبل مستخدمي الإنترنت عموماً بأنه مجموعة من الصفحات المرتبطة فيما بينها، والقابلة للقراءة فقط، تُستخدم لغة HTML في هذه الصفحات مما يجعلها سهلة القراءة من قبل المستخدمين، ولكنها تبقى غير مفهومة بالنسبة إلى الحواسيب أو الآلات عموماً، فعلى الرغم من قيام الحواسيب بتحليل صفحات الوب، ومعالجتها من حيث التصميم والروابط الموجودة ضمنها إلا أنها تبقى غير قادرة على استخراج أي دلالة منها، فلا يمكن للحواسيب أن تعرف بأن أحد الروابط قد يؤدي إلى السيرة الذاتية لشخص ما أو يؤشر إلى كتاب تاريخي . ابتكر مصطلح الوب الدلالي " Semantic Web " من قبل " Tim Berners-Lee " وهو مبتكر الوب ذاته " World Wide Web "حيث عرف الوب الدلالي على أنه شبكة من البيانات القابلة للمعالجة مباشر من قبل الآلات .بالإضافة إلى ذلك يعد الوب في هذه الأيام المصدر الأوسع للمعلومات في جميع المجالات ، وهو في توسع دائم سواء في حجم المعلومات أو في حجم المستخدمين. إن هذا الحجم الكبير من المعلومات والتوسع السريع في الوب يجعلان إدارة المعلومات والوصول إليها أمراً في غاية التعقيد؛ وقد عانى معظمنا من العدد الكبير من الوثائق والروابط التي يعيدها أي محرك بحث رداً على أية عملية استعلام، هذا عدا عن عدم توافق نتائج البحث مع طلب المستخدم. يعود هذا التعقيد إلى سببين أساسيين: الأول، البنية المستخدمة لتخزين الوثائق، فمعظم الوثائق في الوب تُخزن بشكل معطيات نصية يقوم الإنسان بتصنيفها تصنيفاً يدوياً دون أي إمكان للتعبير عن محتوى هذه الوثائق تعبيراً يسمح للآلة أن تتعامل معه، والثاني، طرائق التصنيف والبحث الآلي المستخدمة حاليا، فجميعها طرائق إحصائية لا تتعدى مستوى التحليل الصرفي للنصوص المكتوبة (البحث من خلال الكلمات المفتاحية). وقد طرح ما يعرف اليوم بالوب الدلالي كتوسعة للبنية الحالية للوب، وتعرف الموارد فيه باستخدام لغة توصيفيه تسمح بالتعبير عن المحتوى الدلالي للمورد بطريقة يمكن للآلة تفسيرها، وقد جرى اقتراح عدد من اللغات والآليات للتعبير عن المحتوى الدلالي للمورد واستخدامه لاحقاً في عمليات التصنيف والبحث، غير أن كل آلية من هذه الآليات تهتم بعدد من الجوانب التطبيقية وتغفل

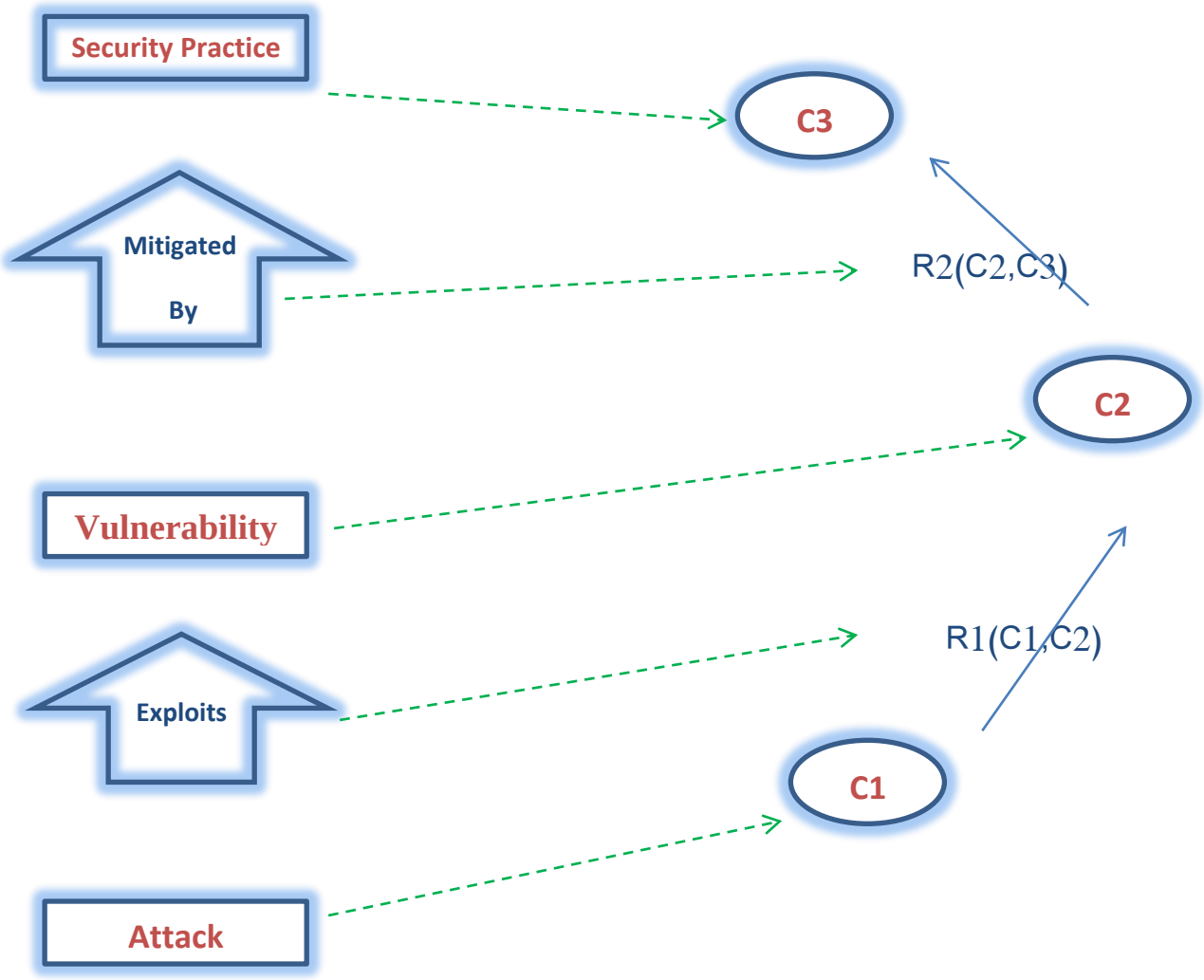
جوانب أخرى ، لذا جرى توحيد جميع هذه اللغات والآليات في بنية موحدة أكثر شمولية وديناميكية هي الأنطولوجيا ، تتيح التعبير عن المحتوى الدلالي للموارد تعبيراً فعالاً يفهمه الإنسان (باستخدام اللغات الطبيعية) والآلة على حد سواء، إضافة إلى الإمكانات الواسعة التي تقدمها هذه البنية للاستعلام عن الموارد. [17] [28]

٤.٣ الأنطولوجيا Ontology

٤.٣.١ التعريف

تحمل كلمة الأنطولوجيا (Ontology) العديد من المعاني، ففي الفلسفة تعني علم الموجودات، أما في المعلوماتية فإنه يمكن القول: إ ن الوجود مرتبط بإمكانية التمثيل فما يمكن تمثيله فقط هو ما يعد موجوداً، حيث تم استخدام هذه الكلمة التي تعبر عن الوجود في تمثيل المعارف ،فيمكن أن تعرف الأنطولوجيا بأنها توصيف للمفاهيم والأغراض والكيانات في مجال محدد إضافة إلى العلاقات فيما بينها، إذ انتشر استخدام الأنطولوجيا في مجال تمثيل المعرفة وإدارتها، إضافة إلى تطبيقات معالجة النصوص وصولاً إلى أنظمة استرجاع المعلومات، حيث تسمح بتمثيل مفاهيم المجال المدروس بالإضافة إلى العلاقات فيما بينها، ويجري ذلك عن طريق مجموعة من اللغات المعيارية من قبل محررات دلالية مختصة، حيث تعد لغة OWL (Ontology Web Language)من أشهر هذه اللغات وتعد لغة معيارية معتمدة من قبل W3C حيث ترتكز على لغة XML و URI. يحتاج استرجاع معارف الانطولوجيا إلى لغة استعلام كما هو الحال عند استرجاع البيانات المخزنة في قواعد البيانات ،وتعد لغة (SPARQL Simple Protocol and RDF Query Language) لغة معيارية للاستعلام ضمن الأنطولوجيا .تعرف الأنطولوجيا الخاصة بمجال معين، بأنها فهم لهذا المجال، يجري الاتفاق عليه بين مجموعة من المختصين والخبراء في المجال، ويعبر عن هذا الفهم بعدد من المفاهيم التي تخص المجال، ومجموعة من العلاقات التي تربط هذه المفاهيم، ويجري تغليف هذه البنية بمجموعة من التعابير اللغوية بلغة خاصة، تشمل هذه التعابير المفاهيم وبعض العلاقات. [17] [28]

سنوضح بنية مبسطة للأنطولوجيا، وآلية استخدامها في الوب الدلالي بالمثال التالي :



الشكل (١) يوضح بنية مبسطة للأنطولوجيا

ففي المجال الأمني يوجد العديد من المفاهيم الأمنية C1,C2,C3 ، ويمكن التعبير عنها بتعبير لغوي واحد أو أكثر مثل الهجوم (Attack) ونقطة الضعف (Vulnerability) والممارسة الأمنية (Security Practice) . ترتبط هذه المفاهيم مع بعضها بعلاقات R1,R2 مثل يستغل (Exploits) ويخفف بوساطة (Mitigated By) .يمكن اغناء هذه الانطولوجيا بالعديد من الخصائص فيمكننا أن نقول مثلاً الهجوم له اسم وتاريخ ووصف ..الخ

يمكن تعريف صفوف فرعية لكل صف رئيسي كأن نقول هناك صفان فرعيان للصف Attack هما internalAttack و externalAttack ،يمكن أخذ أغراض من الصف Attack تمثل انواع الهجوم مثلاً Salami attack

يمكن تعريف قيود كأن نقول عن صف ما أنه ناتج عن اجتماع صفين ،أو لا يمكن أن تتقاطع أعراض من صفين فمثلاً لا يمكن أن يكون هناك غرض مشترك بين ال internalAttack و externalAttack

كما يمكن تعريف قيود على العلاقات كأن نقول عن واصفة ما انها تأخذ كل قيمها من مصدر واحد فقط أو تأخذ قيمها ضمن مجال معين أو لها قيمة صغرى أو قيمة كبرى ، ويمكن تعريف خصائص للعلاقات كأن نقول عن علاقة ما انها انعكاسية أو تناظرية أو وظيفية أو متعدية كما يمكن استنتاج قواعد جديدة من قواعد موجودة سابقا بتطبيق قواعد استدلال مناسبة. [28]

الأنطولوجيا هي الركيزة الأساسية في مجال الويب الدلالي لتمثيل المفاهيم وعلاقاتها لجعل آلة المعرفة مفهومة[29] . فمن خلال الأنطولوجيا نستطيع فهم بنية المعرفة التي تعكس بشكل جيد تعقيد العالم الحقيقي، فهي تخزن وتعالج المعرفة ولا تحتوي فقط البيانات الأولية إنما تحتوي أيضاً معنى هذه البيانات.[30]

من خلال انشاء مفردات مشتركة حول مفاهيم مجال ما والعلاقات فيما بينها فإن الأنطولوجيا تمكن من :

١:مشاركة فهم مشترك للمعلومات.

٢:تمكن من إعادة الاستخدام المعرفة.

بالإضافة الى الاستدلال الآلي للكمبيوتر، فإن اعتماد الأنطولوجيا سيمكن من إدخال موثوق للبيانات ومشاركة أسهل للمعلومات والتدريب المتجانس وتطوير البرامج بين مختلف الجهات الفاعلة. [7]

٤.٣.٢ مكونات الأنطولوجيا

الأغراض Individuals

هي الوحدة الأساسية للأنطولوجيا ؛ إنها الأشياء التي تصفها الأنطولوجيا.

الصفوف Classes

وهي الصفوف في لغات البرمجة أو أنواع الاغراض وتمثل المجموعات والمفاهيم.

الخصائص Attributes

وهي الميزات التي تصف الصفوف والأغراض.

العلاقات Relations

وهي صلة الوصل بين الأغراض أوبين الصفوف

Function terms

البنى المعقدة التي تتشكل من علاقات معينة و يمكن استخدامها بدلاً من مصطلح فردي في تعبير ما.

القيود Restrictions

وهي أوصاف رسمية معلنة لما يجب أن يكون صحيح لبعض التأكيدات لتكون مقبولة كمدخلات.

القواعد Rules

عبارات بصيغة IF–else تصف الاستدلال المنطقي الذي يمكن الحصول عليه من تأكيد ما في صيغة معينة.

البديهيات Axioms

وهي تأكيدات تتضمن قواعد بصيغة منطقية وتشكل معاً النظرية الشاملة التي تصفها الأنطولوجيا في مجال التطبيق الخاص بها.

الأحداث Events

وهي التي تغير الخصائص أو العلاقات.

الأنطولوجيا أسلوبًا جيدًا لتصنيف مفاهيم الأمان المختلفة بشكل منهجي مثل نقاط الضعف والهجمات والتدابير المضادة ، والعلاقات فيما بينها ، كما أنها تلعب دور كبير في جمع وتحليل كميات كبيرة من البيانات من عدة مصادر، وتخزينها، وإعادة استخدامها لاحقاً. يمكن لتحليل المخاطر المعتمد إلى الأنطولوجيا أن يجعل فهم هذه المخاطر أسهل وأسرع وهذا يسهل مهمة مقاومتها والتخلص منها. [14]

٤.٤ الخلاصة

قدمنا في هذا الفصل لمحة عامة عن الويب الدلالي، وتقنياته التي تعتبر الأنطولوجيا أشهرها. ثم تحدثنا عن الأنطولوجيا ومكوناتها وأهميتها في تمثيل المعرفة، وفي جمع وتحليل كميات كبيرة من المعلومات من مصادر مختلفة، وعن الدور الكبير الذي ستقوم به في بحثنا لجعل عملية تحليل الهجمات أسهل وأسرع ما يمكن.

الفصل الخامس: بناء الأنطولوجيا

٥.١ المقدمة

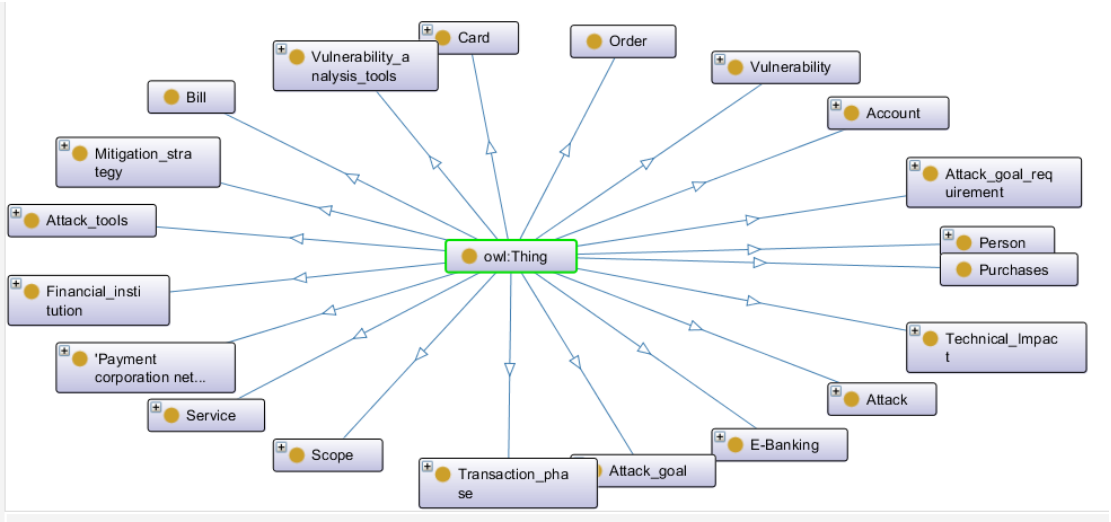
سنقوم في هذا الفصل باستعراض وتفصيل كيفية توظيف الأنطولوجيا في تحليل الهجمات التي من الممكن أن تتعرض لها خدمة التجارة الالكترونية باستخدام متصفح الويب وباستخدام طرفية نقاط البيع. وسنستخدم أداة Protege لبناء الأنطولوجيا ولغة استعلام SPARQL.

٥.٢ منهجية العمل

في البداية قمنا بالبحث عن الخدمات المصرفية الالكترونية واخترنا منها خدمة التجارة الالكترونية باستخدام متصفح الوب وباستخدام طرفية نقاط البيع لنقوم بتحليل مخاطرها، ووضعنا المفاهيم التي تتعلق بها. ثم قمنا بدراسة وتحليل العديد من الأبحاث التي تستخدم الأنطولوجيا في مجال أمن المعلومات وقارنا بينها لاستنتاج أهم المفاهيم والعلاقات التي يجب أن توجد في أي أنطولوجيا أمنية، ثم وضعنا المفاهيم الأمنية الأساسية. بعد ذلك بحثنا عن الهجمات التي من الممكن أن تتعرض لها هذه الخدمة بنوعيها، وقمنا بدراستها وأضفنا مفاهيم أمنية جديدة بغرض تحليلها. وبعد ذلك بحثنا عن هذه الهجمات في المصادر الرسمية CAPEC وCWE وCVE وأضفنا مفاهيم أمنية أخرى للأنطولوجيا ثم ربطنا المفاهيم الأمنية مع بعضها البعض من جهة، ومع مفاهيم الخدمات المصرفية الالكترونية من جهة أخرى من خلال علاقات الأنطولوجيا. لنحصل على المفاهيم الأساسية للأنطولوجيا المقترحة.

٥.٣ المفاهيم الأساسية المستخدمة في بناء الأنطولوجيا

يبين الشكل (٥-١) المفاهيم الأساسية المستخدمة في بناء الأنطولوجيا، حيث تظهر مفاهيم المستوى الأول من الأنطولوجيا المقترحة.



الشكل(٥-١): للمفاهيم الأساسية للأنطولوجيا المقترحة

٥.٣.١ مفاهيم تتعلق بالتجارة الالكترونية

البنك الالكتروني e-banking : ويمثل نظام الدفع الالكتروني بكامل مكوناته وهي الزبون والتاجر و البنك مصدر البطاقة و المستحوذ و شبكة الدفع و الحساب البنكي والبطاقة البنكية.

الخدمة Service : تمثل خدمة التجارة الالكترونية باستخدام متصفح الويب أو باستخدام طرفية نقاط البيع.

الحساب البنكي Account: يمثل حساب الزبون في البنك الذي يصدر البطاقة.

البطاقة Card: وتمثل البطاقة البنكية الخاصة بالزبون والمستخدمة في عملية الدفع الالكتروني.

الشخص Person: يمثل الزبون أو التاجر.

المشتريات Purchases: وتمثل المواد التي يطلبها الزبون من المتجر الالكتروني.

مراحل تنفيذ الخدمة Transaction Phase: ويمثل المراحل التي يتم من خلالها تنفيذ الخدمة بشكل تسلسلي.

شبكة الدفع Payment Corporation Network: تمثل شبكة الدفع التي تعمل وتنقل البيانات ما بين البنك مصدر. البطاقة والبنك المستحوذ.

المؤسسة المالية Financial Institution: وتمثل البنك مصدر البطاقة أو البنك المستحوذ.

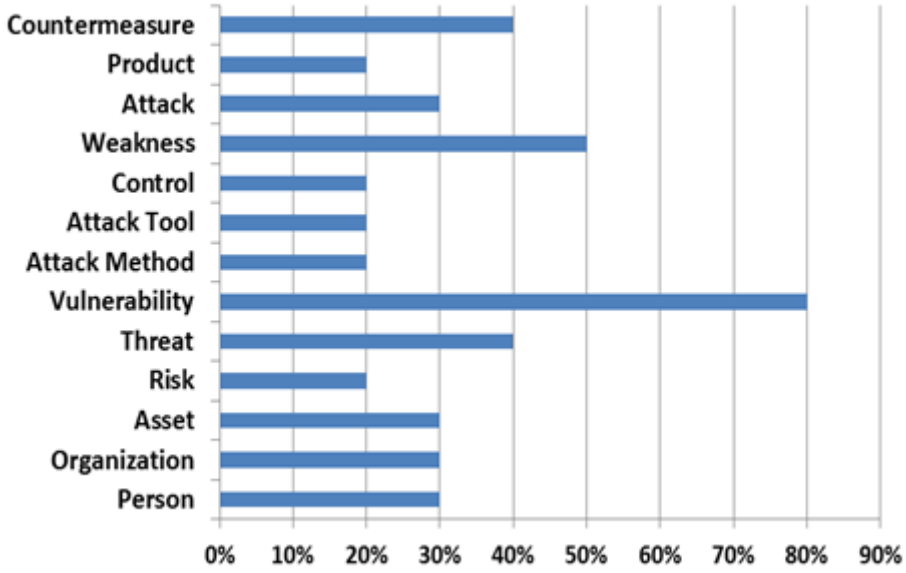
الطلب Order: يمثل مجموعة المشتريات.

الفاتورة Bill: تمثل ثمن المشتريات.

٥.٣.٢ المفاهيم الأمنية

تم الحصول على المفاهيم الأمنية بعد إجراء عملية مقارنة بين الدراسات السابقة التي تخص استخدام الأنطولوجيا في مجال أمن المعلومات حيث تم تجميع الدراسات السابقة وفقًا لمساهمتهم الفردية . الهدف هو فهم طريقة بناء واستخدام الأنطولوجيا في مجال أمن المعلومات وتحديد أهم المفاهيم التي يجب أن توجد في أي أنطولوجيا أمنية كما هو موضح في الجدول(٥-١).

نتيجة اختلاف أهداف الأنطولوجيا المدروسة فقد اختلفت المفاهيم المستخدمة لبنائها، هناك مفاهيم استخدمت لمرة واحدة فقط تبعاً للهدف ، ومفاهيم متعددة الاستخدام ، نسبة تكرار المفهوم يدل على أهميته في مجال أمن المعلومات ، الشكل (٥-٢) توضح النسبة المئوية لتكرار المفاهيم في الأنطولوجيا المدروسة بعد حذف المفاهيم التي ذكرت لمرة واحدة فقط.



الشكل (٥-٢): النسبة المئوية للمفاهيم في الأنطولوجيا المدروسة

الجدول (٥-١): المفاهيم الأساسية المستخدمة في الأنطولوجيا المدروسة

[2]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
الشخص	وسط النقل	الشخص	الأصل	المنظمة	نقطة الضعف	نقطة الضعف	الهجوم	المجال الوظيفي	الضعف الأمني
المنظمة	الكيان	المنظمة	الخطأ	الأصل	التهديد	الهجوم	الهدف	فئة التطبيق	نقطة الضعف
الأصل	عنصر المعلومات	مصدر البيانات	الخطر	التحكم	المنتج	الاستغلال	الحادث	نوع منصة العمل	طريقة الكشف
المكان	غرض البيانات	نقطة الضعف	التقييم	نقطة الضعف	الاستخبارات	الاعدادات	المهاجم	السيناريو	طريقة التخفيف
الخطر	مصدر البيانات	المضيف	التهديد	التهديد	الإجراء المضاد	المنتج	الأداة	الفئة	التأثير التقني
درجة الخطورة			الاخفاق	الصفة		الضعف	الفعل	المجال	الخاصية الأمنية
التهديد			الضعف	التقييم		المصدر	نقطة الضعف	المعرفة السياقية	الهجوم
نقطة الضعف			الهجوم	المكان		الاجراء المضاد	الحدث	المجال الوظيفي	نموذج الهجوم
الأثر			التقييم	الشخص		المراجع	المستهدف		المهاجم
وكيل التهديد			نقطة الضعف	المنظمة					
طريقة الهجوم			الدفاع						
أداة الهجوم									
هدف أمني									
معيار أمني									
متطلب أمني									
وثيقة المتطلبات									
متحكم									

يبين الشكل(٢) أن٨٠ % من الانطولوجيا المدروسة ركزت على مفهوم نقطة الضعف التي يستغلها المهاجم للقيام بالهجوم. ٥٠% ركزت على مفهوم الضعف بمعناه العام الذي يمثل الخطأ في التصميم أو البيئة أو البرنامج والذي بدوره من الممكن أن يؤدي الى نقطة ضعف يمكن أن تستغل في هجوم ما. ٤٠% ركزت على التدابير المضادة والتي تمثل طريقة الحماية.٤٠% ركزت على مفهوم التهديد بمعناه العام والذي يشمل التهديد الطبيعي او الحادث الامني أو التهديد المقصود (الهجوم). مفهوم الهجوم ذكر فقط في ٣٠% من الانطولوجيا السابقة كما ان المنظمة ذكرت فقط في ٣٠ % منها كما أن الأشخاص والأصول ذكروا في ٣٠% من الأنطولوجيا السابقة. وبالتالي فإن المفاهيم الأمنية الواجب توافرها في أي أنطولوجيا أمنية هي:

نقطة الضعف و الضعف بمعناه العام و التدابير المضادة و الهجوم والمنظمة و التهديد بمعناه العام والأشخاص والأصول.

المنظمة في بحثنا تمثل النظام البنكي الالكتروني

ولسنا في صدد دراسة التهديد الطبيعي كالحريق أو الحادث الأمني كالسرقة وسنكتفي فقط بمفهوم التهديد المقصود أي الهجوم.

ولتحليل الهجوم لا بد من إضافة مفاهيم تتعلق بهدف الهجوم، متطلبات تحقيق الهدف، وأداة الهجوم .

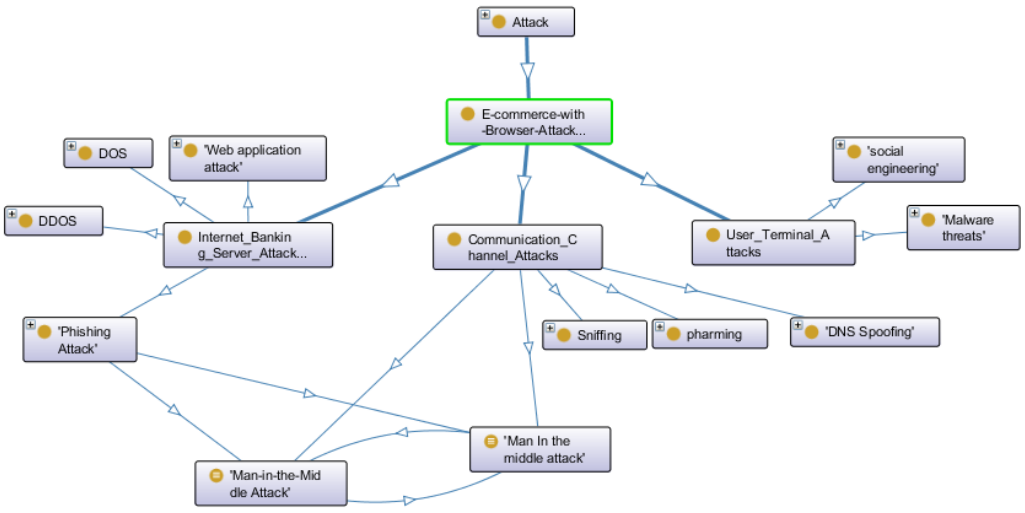
ومن CAPEC أضفنا مفاهيم المجال والأثر التقني.

وبالتالي فإن المفاهيم الأمنية لدينا هي:

الهجوم Attack

ويمثل التهديد المقصود الذي يقوم به المهاجم. وتم تقسيم الهجوم الى فئتين:

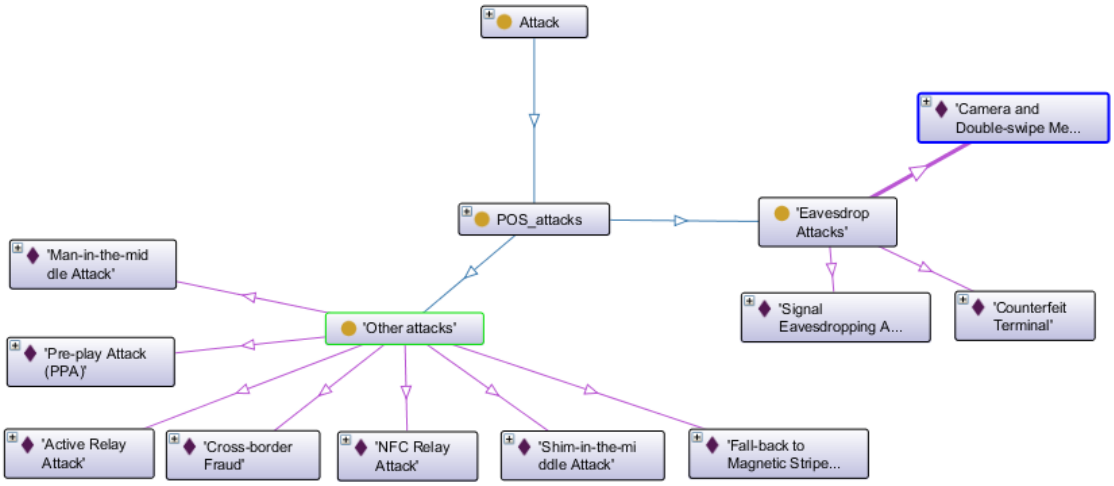
١. هجمات التجارة الالكترونية باستخدام متصفح الوب الموضحة في الشكل (٥-٣)



الشكل (٥-٣):هجمات التجارة الالكترونية باستخدام متصفح الويب

حيث يوضح الشكل هجمات قناة الاتصال و طرفية المستخدم و مخدم البنك بأنواعها المختلفة.

٢. هجمات التجارة الالكترونية باستخدام طرفية نقاط البيع الموضحة بالشكل (٥-٤)



الشكل(٥-٤): هجمات التجارة الالكترونية باستخدام طرفية نقاط البيع

حيث يوضح الشكل(٥-٤) أهم هجمات طرفية نقاط البيع كهجمات التنصت بأنواعها المختلفة وهجمات أخرى.

نقطة الضعف Vulnerability

والذي يمثل الضعف بمفهومه العام، بالإضافة الى نقطة الضعف التي قد تؤدي الى هجوم.

هدف الهجوم Attack goal

ويمثل الهدف الذي يريد المهاجم تحقيقه كسرقة المعلومات أو اغراق المخدم أو غير ذلك

متطلبات تحقيق الهدفAttack goal requirements

ويُقصَد بها الخطوات التي يجب أن يقوم بها المهاجم للوصول الى هدفه من الهجوم.

أداة الهجوم Attack Tool

وهي الأداة التي يستخدمها المهاجم للهجوم.

استراتيجية التخفيف Mitigation Strategy

ويقصد بها اجراءات الوقاية من الهجوم.

المجال Scope

ويُقصد به مجال أمن المعلومات الذي يؤثر عليه الهجوم في حال حدوثه، كالسرية والاكتمال و المصدقة والتخويل وغيرها

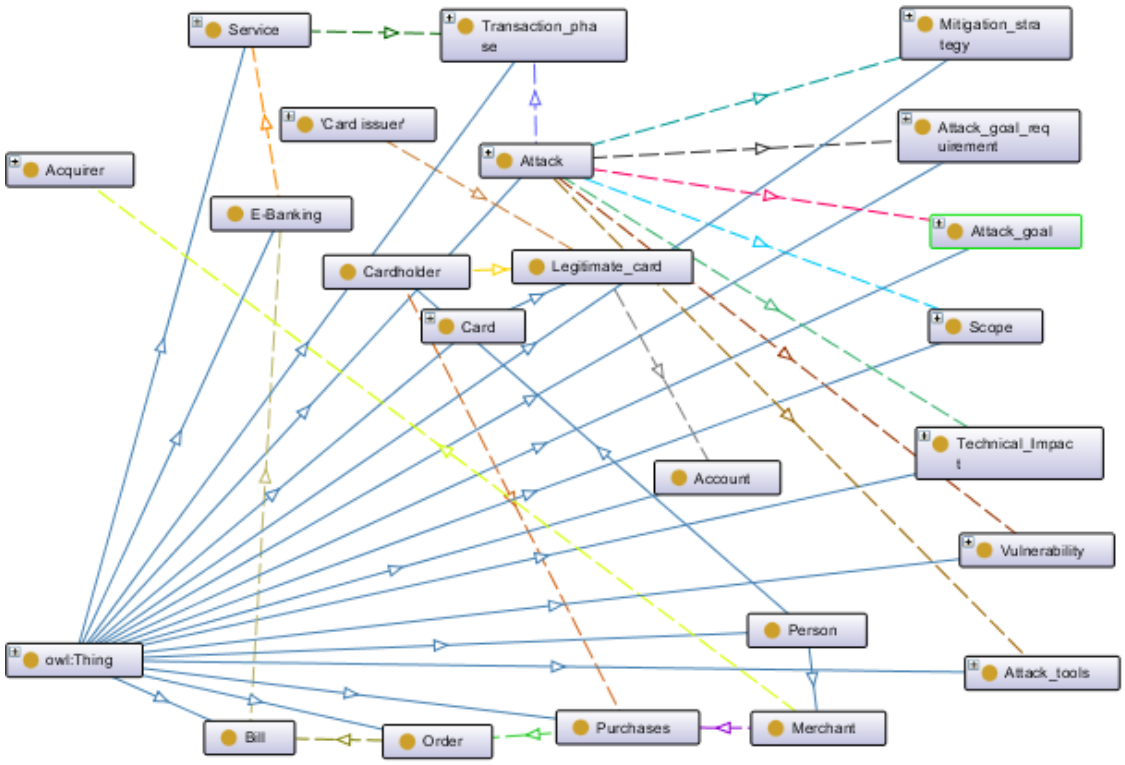
الأثر التقني Technical impact

وهو الأثر التقني الذي يتركه الهجوم في حال حدوثه كقراءة البيانات أو التعديل عليها أو تغيير الصلاحيات وغير ذلك.

٥.٤ العلاقات التي تربط المفاهيم المختلفة

٥.٤.١ Object Property

يوضح الشكل (٥-٥)العلاقات التي تربط مفاهيم الأنطولوجيا مع بعضها البعض



الشكل(٥-٥-١):العلاقات الأساسية بين مفاهيم الأنطولوجيا

الشكل(٥-٥-٢):العلاقات الأساسية بين مفاهيم الأنطولوجيا

يوضح الشكل(٥-٥) عملية الربط بين المفاهيم المختلفة للأنطولوجيا باستخدام العلاقات من نوع Object property . وفي ما يلي الثلاثيات المكونة لهذه العلاقات، وهي من الشكل

: Domain Object property Range

Cardholder has_card Legitimate_card: حامل البطاقة (الزبون) لديه بطاقة دفع.

Legitimate_card associate_with Account: بطاقة الدفع مقترنة بحساب بنكي.

Card issuer issues_card Legitimate_card: البنك مصدر البطاقة يصدر بطاقة الدفع.

Cardholder buy_purchases Purchases: حامل البطاقة يشتري المشتريات.

Merchant sell_purchases Purchases: التاجر يبيع المشتريات.

Merchant Contracting_with Acquirer: التاجر يتعاقد مع المستحوذ.

Purchases form_order Order: المشتريات تشكل طلب.

Order has_bill Bill: الطلب له فاتورة.

Bill Processed_by e-Banking: الفاتورة تتم معالجتها من قبل نظام الدفع الالكتروني.

e-Banking Runs_services Service : نظام البنك الالكتروني يقدِم خدمات.

Service Consists_of Transaction_phase: الخدمة مكونة من عدة مراحل.

Attack Happens_at_phase Transaction_phase: الهجوم يحدث في مرحلة ما من مراحل تنفيذ الخدمة.

Attack Attack_has_goal Attack_goal : الهجوم له هدف.

Attack Attack_goal_achievement_requires Attack_goal_requirement : الهجوم له متطلبات لتحقيق هدفه.

Attack Exploits_vulnerability Vulnerability: الهجوم يستغل نقطة الضعف.

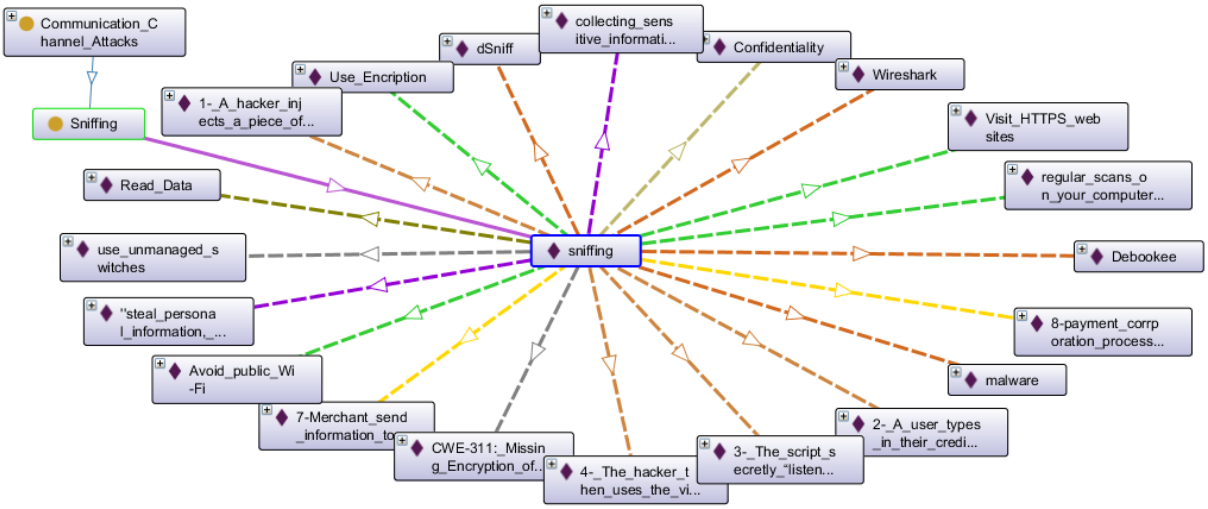
Attack impactTechnicalImpact Technical_Impact: الهجوم يترك أثر تقني.

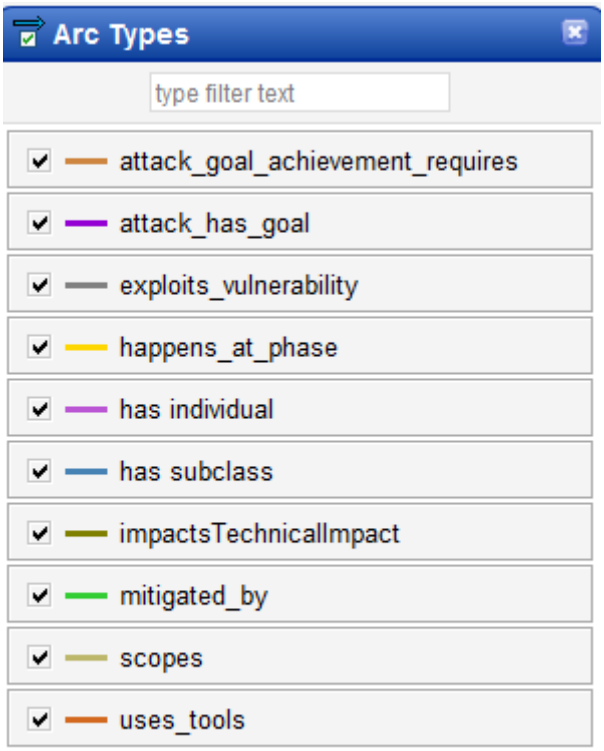
Attack Mitigated_by Mititation_strategy : يتم تخفيف الهجوم باستخدام استراتيجية التخفيف الهجوم.

Attack Scopes Scope : الهجوم يؤثر على مجال أمن أمني معين.

Attack Uses_tools Attack_tools : يستخدم المهاجم أداة الهجوم للقيام بالهجوم.

يوضح الشكل (٥-٦) جزء من عملية تحليل هجوم sniffing وفق المفاهيم والعلاقات السابقة:





الشكل (٥-٦): جزء من عملية تحليل هجوم sniffing

يبين الشكل (٥-٦) أن الهجوم sniffing والذي هو أحد الهجمات التي من الممكن أن تصيب قناة الاتصال، يمكن أن يحدث في إحدى المرحلتين:

٧: عندما يقوم التاجر بإرسال المعلومات الى بوابة الدفع التي بدورها ترسلها الى شبكة الدفع.

٨: عندما تعالج شبكة الدفع الفاتورة وتتصل مع البنك مصدر البطاقة للتحقق من معلومات البطاقة ومن توفر المبلغ في حساب الزبون.

وهذا ما نحصل عليه من خلال الاستعلام عن العلاقة happens_at_phase باستخدام الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
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.
}
```

ونتيجة الاستعلام موضحة في الشكل (٥-٧):

Attack_Happens_at_phase
"7-Merchent send information to payment gateway that send them to payment corporation network"
"8-payment corrporation process bill and communicate with the issuer to ensure that the card is valid and the balance is sufficient."

الشكل(٥-٧):نتيجة الاستعلام عن العلاقة Attack_Happens_at_phase للهجوم Sniffing

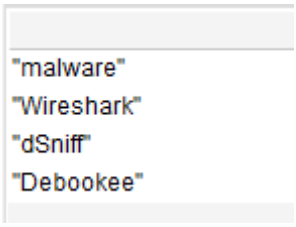
يستخدم المهاجم الأدوات التالية للقيام بهذا الهجوم:

Debookee ،Wireshark ، Malware ، Dsiff

وهذا يتم عن طريق العلاقة الاستعلام عن العلاقة uses_tools، باستخدام الاستعلام :

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns<#
PREFIX owl: <http://www.w3.org/2002/07/owl<#
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema<#
PREFIX xsd: <http://www.w3.org/2001/XMLSchema<#
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#<
SELECT ?attacker_uses_tools
        WHERE { ?x rdf:type  n:Sniffing.
؟x n:uses_tools ?k.
؟k n:tool_name ?attacker_uses_tools.
}
```

ونتيجة الاستعلام موضحة في الشكل (٥-٨)



الشكل(٥-٨): نتيجة الاستعلام عن العلاقة uses_tools للهجوم Sniffing

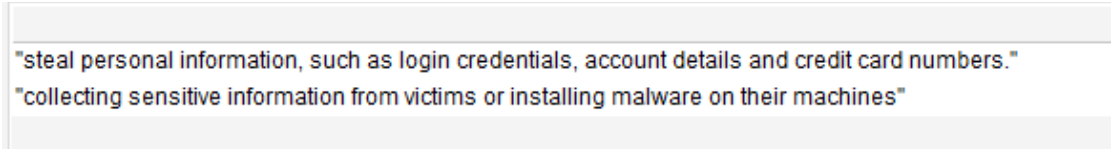
ويهدف هذا الهجوم الى جمع معلومات حساسة من الضحايا أو تثبيت برامج ضارة على أجهزتهم، و سرقة المعلومات الشخصية، مثل بيانات اعتماد تسجيل الدخول وتفاصيل الحساب وأرقام بطاقات الائتمان.

وهذا من خلال العلاقة الاستعلام عن العلاقة attack_has_goal استخدام الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
```

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

ونتيجة الاستعلام في الشكل (٥-٩)



الشكل(٥-٩): نتيجة الاستعلام عن العلاقة attack_has_goal للهجوم Sniffing

ومتطلبات تحقيق هذه الهدف هي:

1-يقوم المخترق بحقن جزء من برمجية خبيثة.

٢-يكتب المستخدم تفاصيل بطاقته الائتمانية .

٣-البرنامج الخبيث يتنصت سراً ويرسل هذه المعلومات مباشرة إلى المخترق.

٤- ربما يستخدم المخترق بعد ذلك بيانات بطاقة الضحية لسرقة أمواله.

وهذا نحصل عليه من خلال الاستعلام عن العلاقة attack_goal_achievement_requires من خلال الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
SELECT ?attack_goal_achievement_requires
        WHERE { ?x rdf:type  n:Sniffing .
```

```
?x n:attack_goal_achievement_requires ?k.
?k n:req_name ?attack_goal_achievement_requires.
}
ORDER BY(?attack_goal_achievement_requires )
```

ونتيجة الاستعلام في الشكل(٥-١٠)

```
"1- A hacker injects a piece of malicious code on a checkout page"
"2-A user types in their credit card details on the checkout page"
"3-The script secretly "listens_in" and sends this information straight to the hacker"
"4-The hacker then uses the victim's card details to steal their money"
```

الشكل(٥-١٠): نتيجة الاستعلام عن العلاقة attack_goal_achievement_requires للهجوم Sniffing

يستغل هذا الهجوم نقاط الضعف التالية:

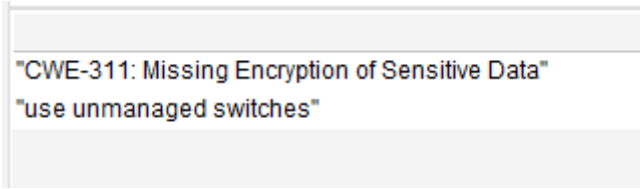
استخدام مبدلات غير قابلة للبرمجة

CWE-311 التي تتحدث عن عدم تشفير البيانات الحساسة.

وهذا نحصل عليه من خلال العلاقة الاستعلام عن العلاقة exploits_ vulnerability باستخدام الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
SELECT ?attacker_exploits_vulnerabilities
        WHERE { ?x rdf:type  n:Sniffing .
?x n:exploits_vulnerability ?k.
?k n:vul_name ?attacker_exploits_vulnerabilities}
```

ونتيجة الاستعلام في الشكل(٥-١١)



الشكل(٥-١١): نتيجة الاستعلام عن العلاقة exploits_ vulnerability للهجوم Sniffing

والأثر التقني لهذا الهجوم هو قراءة البيانات الحساسة، ويؤثر هذا الهجوم على مجال أمن المعلومات المتمثل بسرية البيانات المتبادلة Confidentiality. ونحصل على هذا من خلال الاستعلام عن العلاقة scopes و العلاقة impactsTechnicalImpact باستخدام الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
SELECT     ?scopes ?Technical_Impact
        WHERE { ?x rdf:type  n:Sniffing .
?x n:attack_ID ?attack_ID.
?x n:scopes ?k.
?k n:scope_name ?scopes .
?x n:impactsTechnicalImpact ?s.
?s n:Imp_name ?Technical_Impact.
}
```

ونتيجة الاستعلام في الشكل(٥-١٢):

scopes	Technical_Impact
"Confidentiality"	"Read Data"

الشكل(٥-١٢): نتيجة الاستعلام عن العلاقتين impactsTechnicalImpact و scopes للهجوم Sniffing

وطرق الحماية من هذا الهجوم هي:

زيارة المواقع التي تستخدم برتوكولات آمنة كالتي تبدأ ب https، واستخدام التشفير، وتجنب الشبكات اللاسلكية العامة، والفحص الدوري للشبكات باستخدام أدوات مثل NordVPN.

ونحصل على ذلك من الاستعلام عن العلاقة mitigated_by باستخدام الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
SELECT ?Attack_Mitigated_by
        WHERE { ?x rdf:type  n:Sniffing .
?x n:mitigated_by ?k.
?k n:mit_name ?Attack_Mitigated_by .

}
```

ونتيجة الاستعلام في الشكل(٥-١٣)

"Use Encription"
"regular scans on your computer networks using tools like NordVPN"
"Visit HTTPS websites"
"Avoid public Wi-Fi"

الشكل(٥-١٣):نتيجة الاستعلام عن العلاقة mitigated_by للهجوم Sniffing

وكما ذكرنا سابقاً هذا فقط جزء من عملية التحليل، والجزء الآخر نحصل عليه من خلال العلاقات من نوع Data properties.

٥.٤.٢ Data Properties

Account Account_num xsd:integer : ويمثل رقم الحساب البنكي، وهو عدد صحيح.

Account Money_amount xsd:long : ويمثل المبلغ الموجود في حساب الزبون.

E-commerce-with-Browser-Attack attack_ID xsd:string : ويمثل معرِف الهجوم في سجلات CAPEC.

Merchant has_website xsd:anyURI : وهو رابط موقع التجارة الالكتروني.

Attack attack_strategy rdf: Literal : ويمثل طريقة تنفيذ الهجوم.

Bill Bill_address xsd:string: ويمثل عنوان ارسال الفواتير.

Bill Bill_num xsd:long: ويمثل الرقم التسلسلي للفواتير.

Bill Bill_price xsd:integer : ويمثل ثمن المشتريات أي المبلغ الذي سيتم خصمه من حساب الزبون.

Card CVV2 xsd:integer : ويمثل قيمة التحقق للبطاقة.

Card Expire_date xsd:dateTime : ويمثل تاريخ انتهاء صلاحية بطاقة الدفع.

Attack_goal goal_name xsd:string : يمثل وصف هدف الهجوم.

Technical_Impact Impact_name xsd:string : ويمثل اسم الأثر التقني الذي يتركه الهجوم.

Mitigation_strategy mit_name xsd:string : ويمثل وصف لطريقة تخفيف الهجوم.

Vulnerability observed_examples xsd:string : ويمثل الأمثلة المشَاهدة(نقاط الضعف التي أدت الى هجوم CVE) للضعف العام CWE .

Vulnerability detected_by xsd:string: وتمثل طريقة الكشف عن نقطة الضعف.

Vulnerability vul_name xsd:string: ويمثل اسم نقطة الضعف.

Vulnerability vul_description xsd:string: ويمثل وصف لنقطة الضعف.

Person Person_name xsd:string : يمثل اسم الشخص، سواء حامل البطاقة أو التاجر.

Person person_id xsd:integer : ويمثل معرف الشخص.

Order Order_id xsd:integer : ويمثل الرقم التسلسلي للطلب.

Card PIN xsd:long : ويمثل رقم البطاقة.

Purchases purchase_name xsd:string : ويمثل اسم السلعة التي تم شراءها.

Purchases purchase_price xsd:integer : ويمثل سعر السلعة التي تم شراءها.

Attack_goal_requirement req_name xsd:string : ويمثل اسم متطلَلب تحقيق الهدف.

Scope Scope_name xsd:string: ويمثل اسم مجال أمن المعلومات الذي يؤثر عليه الهجوم.

E-commerce-with-Browser-attacks scoresExploitLikelihood rdfs:Literal : ويمثل احتمالية نجاح الهجوم ، هل هو احتمال مرتفع أو منخفض أو متوسط أو غير ذلك.

E-commerce-with-Browser-attacks scoresRequeredSkill rdfs:Literal : ويمثل تقييم للمهارات التي يحتاجها المهاجم للقيام بالهجوم هل هي مرتفعة أو منخفضة أو متوسطة أو غير ذلك.

E-commerce-with-Browser-attacks scoresSeverity rdfs:Literal : ويمثل شدة الهجوم في حال وقوعه.

Attack_tools tool_name xsd:string : ويمثل اسم اداة الهجوم.

Transaction_phase transaction_phase_name xsd:string : ويمثل اسم المرحلة من مراحل تنفيذ الحركة.

الشكل(٥-١٤) يبين بعض المعلومات التي حصلنا عليها من تطبيق استعلام باستخدام SPARQL على بعض العلاقات من نوع data properties، بما يخص الهجوم sniffing.

حيث يبين الشكل(٥-١٤) أن معرف الهجوم في سجلات CAPEC هو capec-158 ، وأن هذا الهجوم لا يتطلب سوى مهارات منخفضة من المهاجم، حيث أن المهاجم يمكن أن يكون لديه أداة مفتوحة المصدر يستطيع أن يستخدمها للقيام بهذه العملية. كما أن شدة هذا الهجوم متوسطة في حال حدوثه.

attack_ID	Requered_Skill	Severity
"CAPEC-158"	"Level: Low Adversaries can obtain and set up open-source network sniffing tools easily."	"Medium"

الشكل(٥-١٤): نتيجة استعلام العلاقتين scoresRequeredSkill وscoresSeverity للهجوم Sniffing

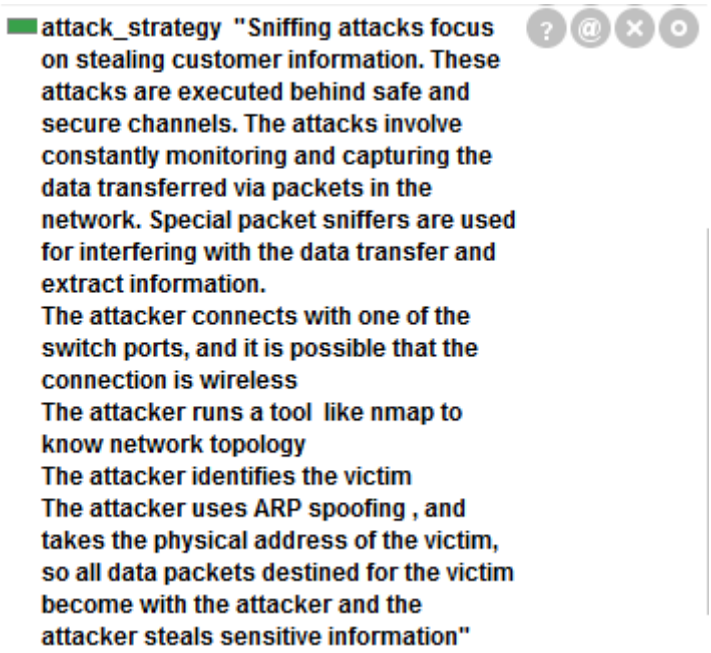
وهذا ما نحصل عليه من خلال الاستعلام التالي:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#>
SELECT ?attack_ID    ?Requered_Skill ?Severity
WHERE { ?x rdf:type  n:Sniffing .
?x n:attack_ID ?attack_ID.
?x n:scoresRequeredSkill ?Requered_Skill.
?x n:scoresSeverity ?Severity.}
```

أما استراتيجية الهجوم يمكن الحصول عليها من خلال الاستعلام عن attack_strategy ، باستخدام الاستعلام التالي:

```
<#PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns
<#PREFIX owl: <http://www.w3.org/2002/07/owl
<#PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema
<#PREFIX xsd: <http://www.w3.org/2001/XMLSchema
<PREFIX n:<http://www.semanticweb.org/noura/ontologies/2020/7/untitled-ontology-7#
SELECT ?attack_Strategy
. WHERE { ?x rdf:type  n:Sniffing
.x n:attack_strategy ?attack_Strategy؟
}
```

والنتيجة موضحة في الشكل (٥-١٥):



الشكل(٥-١٥): استراتيجية الهجوم Sniffing

٥.٥ مقارنة الأنطولوجيا المقترحة مع الأنطولوجيا الأمنية السابقة

يوضح الجدول (٥-٢)مقارنة بين الأنطولوجيا السابقة من عدة جوانب

الجدول(٥-٢): مقارنة بين الأنطولوجيا السابقة

	هدف الأنطولوجيا	الاعتماد على معايير وتصنيفات عالمية	الاعتماد على أنطولوجيا سابقة	لغة الاستعلام	بيئة العمل
[2]	هندسة و استنباط متطلبات الأمان	لا	نعم	SQWRL	protégé
[7]	جعل التحقيق بالجرائم الالكترونية أكثر كفاءة	لا	نعم	-	protégé
[8]	أتمتة عملية اختبار الاختراق	نعم	نعم	SWRL/SPARQL	protégé
[9]	إضفاء الطابع الرسمي على المعرفة في مجال تقييم أمن الأنظمة	لا	نعم	-	Apache JENA
[10]	اضفاء الطابع الرسمي على ضوابط أمن المعلومات والتحقق من الامتثال لمعايير الأمان وفق ISO 27002	نعم	نعم	-	-
[11]	إدارة نقاط الضعف	نعم	لا	-	protégé
[12]	تخزين بيانات الأمان من أجل تحليل وتقييم أمن الأنظمة	نعم	نعم	DL	protégé
[13]	تحديد أهداف الهجمات الالكترونية في نظم المعلومات	نعم	نعم	-	-
[14]	إدارة المعرفة الأمنية للبرمجيات مع أخذ سياق التطبيق بعين الاعتبار	لا	نعم	SPARQL	protégé
[15]	استخراج المعرفة من مصادر مختلفة لبناء نماذج دلالية للتهديد	نعم	نعم	Dl, SPARQL	protégé

يبين الجدول (٥-٢) أن:

٧٠% من الأنطولوجيا المدروسة استخدمت بيئة عمل protégé وفي بحثنا استخدمناprotégé.

تنوعت لغات الاستعلام المستخدمة، بعض الأنطولوجيا استخدم SPARQL والبعض استخدم SQWRL والبعض الاخر استخدم DL وبعض الابحاث استخدمت لغتين من هذه اللغات. وفي بحثنا استخدمنا SPARQL.

٦٠% من الأنطولوجيا المدروسة استخدمت معايير وتصنيفات أمنية عالمية. في بحثنا استخدمنا مصادر رسمية وتصنيفات عالمية.

٩٠% من الانطولوجيا المدروسة كانت عامة ولا تخص منظمة معينة وهذا ما جعلها معقدة ومن الممكن تطبيقها في مكان ما، ومن المحتمل أن تفشل في مكان آخر. أما بحثنا فقد اهتم في مجال تحليل هجمات الخدمات المصرفية الالكترونية، فكانت الأنطولوجيا سهلة الفهم وبسيطة.

١٠% عملت في مجال كشف الجرائم الالكترونية ذات الصلة بالاحتيال المصرفي ، وهذه الانطولوجيا تجاهلت المخاطر الأخرى التي يمكن ان تواجه الخدمات المصرفية الالكترونية. أما بحثنا فقد قام بتحليل العديد من الهجمات وأعطى معلومات مفصلة عنها.

وبالنسبة للمفاهيم المستخدمة، فقد استخدمت الأنطولوجيا المقترحة في بحثنا المفاهيم الأساسية الواجب توافرها في أي أنطولوجيا أمنية إضافة الى مفاهيم جديدة منها متطلبات تحقيق الهدف، واستراتيجية الهجوم. إضافة الى الربط مع مفاهيم الخدمات المصرفية الالكترونية وهذا لم يحدث في أي أنطولوجيا سابقة. إضافة الى الربط بين هذه المفاهيم و CAPEC من جهة، وربط CAPECمع CVEمن خلال CWE من جهة أخرى.

الهجوم كان مفهوماً ثانوياً في كل الأنطولوجيا السابقة، ولم تركز أياً منها على تحليل الهجوم كما فعلت الأنطولوجيا المقترحة في بحثنا، فقد اعتبرت الهجوم مفهوماً رئيسياً، ودرست الهجوم من وجهة نظر المهاجم ومن حيث الأثر الذي يتركه الهجوم في النظام. أي أنها أحاطت بمفهوم الهجوم من كل جوانبه وذلك بهدف فهمه بشكل جيد والحماية منه قدر الامكان.

٥.٦ الخلاصة

تحدثنا في هذا الفصل عن آلية بناء الأنطولوجيا المقترحة باستخدام برنامج Protege . وعن مكونات هذه الأنطولوجيا من مفاهيم مختلفة وعلاقات فيما بينها. واستخدمنا بعض استعلامات SPARQL للتحقق من صحة المعلومات المخزنة فيها، وللتأكد من أنها تقوم بعملية التحليل المطلوبة. ثم قارنا بين الأنطولوجيا المقترحة والأنطولوجيا السابقة بهدف بيان نقاط القوة للأنطولوجيا المقترحة.

الفصل السادس: التطبيق العملي

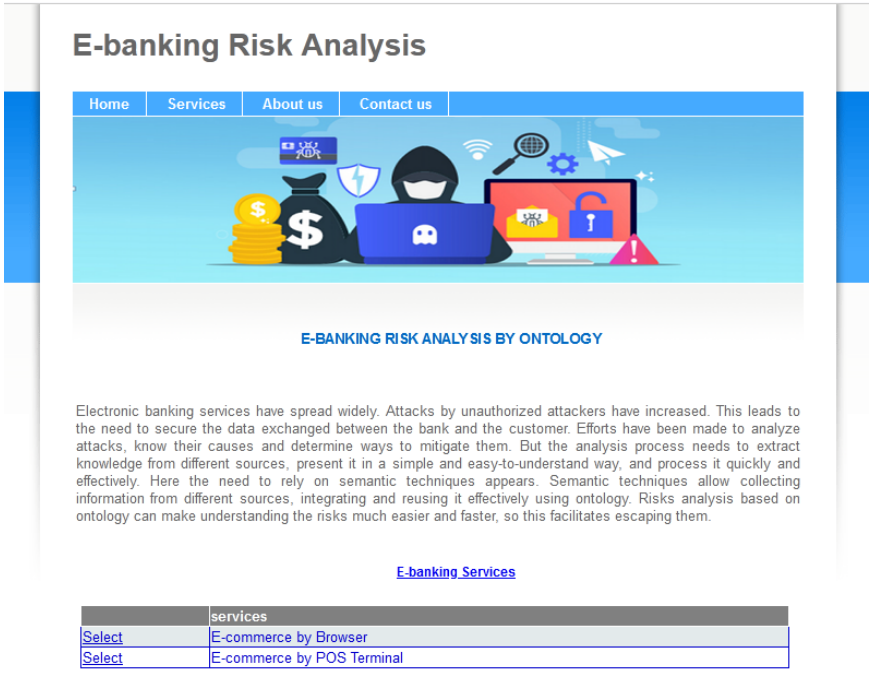
٦.١ المقدمة

سنتحدث في هذا الفصل عن موقع الويب الذي تم تصميمه ليتم تحليل هجمات البنوك الالكترونية من خلاله، بالاعتماد على الأنطولوجيا التي تم تصميمها في هذا البحث. حيث تم استخدام فيجوال استديو ٢٠١٢ Visual studio 2012 ولغة البرمجة C#، بالاستعانة بالمكتبة DotNetRDF التي تمككنا من الاستعلام عن المعلومات المخزنة في الأنطولوجيا باستخدام لغة الاستعلام SPARQL .

٦.٢ المكتبة DotNetRDF

هي عبارة عن مكتبة كاملة صُمِّمت لأجل إعراب وإدارة وكتابة ملفات RDF ، وللاستعلام عنها. وهي واجهة برمجة تطبيقات مشهورة، تُستخدم للتعامل مع مخازن ثلاثيات RDF . ويمكن استخدام هذه المكتبة سواء في سطر أوامر أو واجهات المستخدم الرسومية في نظام ويندوز Windows . تُعتَبر مكتبة مجانية ومفتوحة المصدر. [31]

يبين الشكل(٦-١) الصفحة الرئيسية للموقع:



الشكل(٦-١): الصفحة الرئيسية لموقع تحليل المخاطر

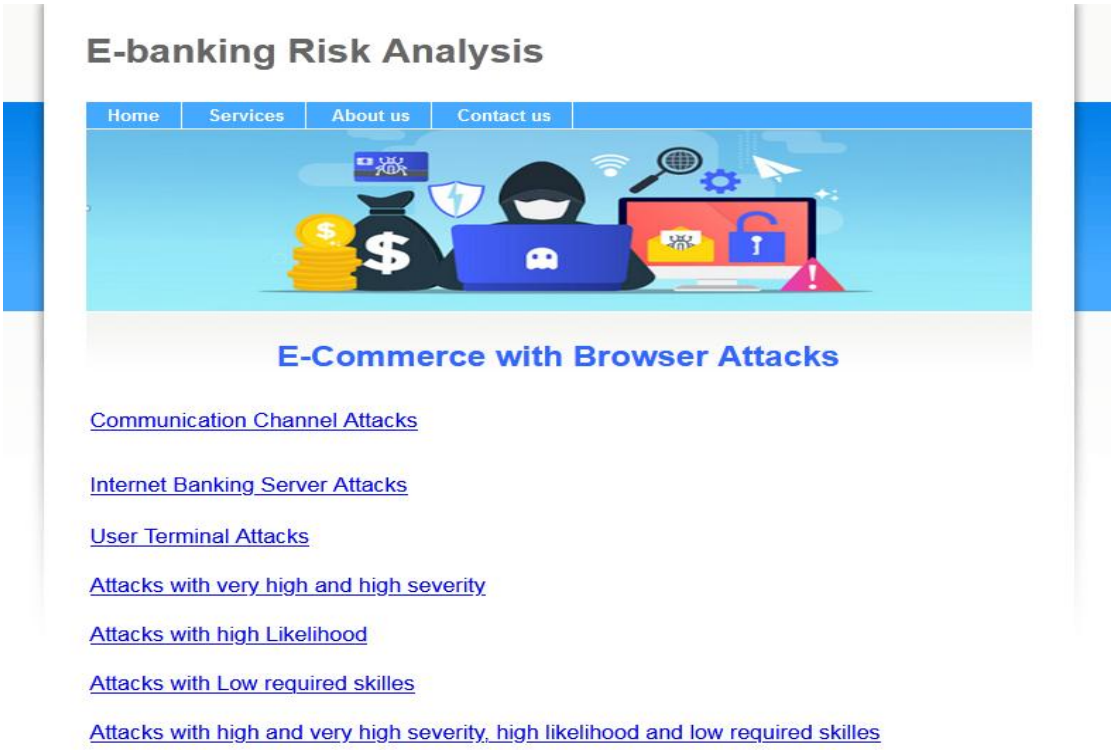
٦.٣ الخدمات Services التي يقدمها الموقع

- تحليل هجمات التجارة الالكترونية باستخدام متصفح الويب.
- تحليل هجمات التجارة الالكترونية باستخدام طرفية نقاط البيع.
- معرفة أدوات ايجاد وتقييم نقاط الضعف، ومعرفة الهجوم الذي من الممكن أن يحدث نتيجة وجود نقطة صعف ما ثم تحليله.

على سبيل المثال عند اختيار

Services ⟶ E-Commerce with browser attacks

تظهر تصنيفات الهجمات التي تتعرض لها التجارة الالكترونية باستخدام المتصفح كما في الشكل(٦-٢)



الشكل(٦-٢):تصنيفات الهجمات التي تتعرض لها التجارة الالكترونية باستخدام متصفح الوب

وعند اختيار صنف ما تظهر أنواع الهجمات ضمن الصنف المحدد كما في الشكل(٦-٣)

Communication_Chanel_Attacks	
Select	DNS Spoofing
Select	Man In the middle attack
Select	pharming
Select	Sniffing

Internet_Banking_Server_Attacks	
Select	DDOS
Select	DOS
Select	Phishing Attack
Select	Web application attack

User_Terminal_Attacks	
Select	Malware threats
Select	social engineering

high_severity_attacks	
Select	Malware threats
Select	pharming
Select	Phishing Attack
Select	SQL injection
Select	Session Hijacking

high_Likelihood_attacks	
Select	pharming
Select	Phishing Attack
Select	SQL injection
Select	Session Hijacking

Low_required_skills_attacks	
Select	DNS Spoofing
Select	SQL injection
Select	Session Hijacking
Select	Sniffing

high_severity_high_likelihood_low_skills_attacks	
Select	SQL injection
Select	Session Hijacking

الشكل(٦-٣): نتائج استعلامات أنواع هجمات التجارة الالكترونية بوساطة متصفح الوب وفق عدة معايير

٦.٤ مثال تحليل هجوم الرجل في الوسط في موقع الوب

إذا تم اختيار خيار الرجل في الوسط Man-in-The Middle Attack، يتم الانتقال الى صفحة تحليل هذا الهجوم كما في الشكل(٦-٤)

الشكل(٦-٤): صفحة تحليل هجوم الرجل في الوسط MITM

و تظهر نتائج عملية التحليل كما في الشكل (٦-٥):

Attack_Happens_at_phase
7-Merchent send information to payment gateway that send them to payment corporation network
8-payment corrporation process bill and communicate with the issuer to ensure that the card is valid and the balance is sufficient.

ATTACK_GOAL
steal personal information, such as login credentials, account details and credit card numbers.

attack_goal_achievement_requires
1-Packet detection
2-Packet injection
3-Session hijacking
4-SSL removal

attacker_uses_tools
Bettercap
BurpSuite
Ettercap
Hetty
MITMPROXY
PROXY.PY
malware

attack_Strategy
MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself, the common scenario involves: Two endpoints (victims) and a third party (attacker). The attacker has access on communication channel between two endpoints, and can manipulate their messages. As a result, the attacker has convinced both victims that they use secure channel, but in reality it has access to all encrypted messages

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

scopes
Access Control
Authorization
Confidentiality
Integrity

Technical_Impact
Gain Privileges
Modify Data
Read Data

Attack_Mitigated_by
Employ encryption
Manage enterprise-wide certificates
Never click links or open attachments in unexpected or suspicious emails
Never utilize public WiFi for website use that is intended to be secure
Utilize a secure VPN to eliminate MITM exposure to ensure that all information is encrypted and cannot be viewed
implement multi-factor authentication to make MITM attacks extremely difficult and success unlikely
Verify TLS/SSL setups

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

الشكل(٦-٥): نتائج تحليل هجوم الرجل في الوسط في موقع الوب

يبين الشكل (٦-٥) أن هذا الهجوم من الممكن أن يحدث عند ارسال التاجر المعلومات الى بوابة الدفع التي بدورها ترسلها الى شبكة الدفع لتعالجها وتتواصل مع البنك مصدر البطاقة للتأكد من صلاحية البطاقة ومن وجود رصيد كافي في حساب المشتري.

وأن هدف هذا الهجوم هو سرقة المعلومات الشخصية، مثل بيانات اعتماد تسجيل الدخول وتفاصيل الحساب وأرقام بطاقات الائتمان. وأن متطلبات تحقيق هذا الهدف هي التحري عن الحزم وحقن الحزم واختطاف الجلسة وإزالة SSL.

وأن المهاجم يستخدم أدوات للقيام بالهجوم مثل Bettercap, BurpSuite, Ettercap, Hetty, MITMPROXY, PROXY.PY, malware

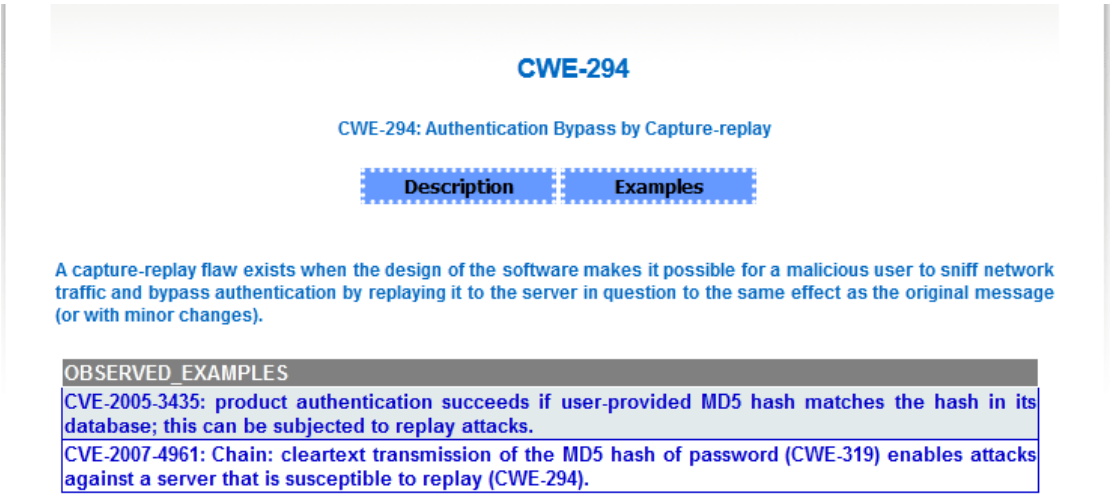
وهذا الهجوم يتم وفق استراتيجية محددة، حيث يستهدف MITM البيانات الفعلية التي تتدفق بين نقاط النهاية ، وسرية وسلامة البيانات نفسها ، ويتضمن السيناريو الشائع: نقطتا نهاية (ضحايا) وطرف ثالث (مهاجم). المهاجم لديه وصول على قناة اتصال بين نقطتي نهاية ، ويمكنه التلاعب برسائلهم. نتيجة لذلك، أقنع المهاجم كلا الضحيتين بأنهما يستخدمان قناة آمنة ، ولكن في الواقع يمكنه الوصول إلى جميع الرسائل المشفرة.

وأن هذا الهجوم يحمل المعرف CAPEC-94، وأن احتمال نجاحه مرتفع، ويتطلب مهارات متوسطة من المهاجم، وفي حال وقوعه تكون شدته عالية جداً. كما أنه يؤثر في حال وقوعه على المصادقة وسرية وتكامل البيانات وعلى التحكم بالوصول. ومن الممكن أن يؤدي الى تغيير الصلاحيات وقراءة وتعديل البيانات.

وأنه من الممكن تقليل فرص التعرض لهذا الهجوم والحماية منه باتباع عدة أساليب كاستخدام التشفير وإدارة الشهادات على مستوى المؤسسة و عدم فتح الروابط والمرفقات من مصادر غير معروفة، وعد استخدام الشبكات اللاسلكية العامة، واستخدام شبكة افتراضية خاصة آمنة ضمان تشفير البيانات ، واستخدام المصادقة متعددة العوامل، والتحقق من اعدادات بروتوكولات TLS/SSL.

و أن سجلات CWE المرتبطة بسجل هذا الهجوم في CAPEC هي CWE-290, CWE-294,CWE-300, CWE-593. [24] [25] [27] [26]

ويبين الشكل(٦-٦) وصف لأحد سجلات CWE المرتبطة بهذا الهجوم، و نقاط الضعف المرتبطة و التي تم رصدها وأدت لحدوث هذا الهجوم سابقاً، ممثلة بسجلات CVE المرتبطة بهذا السجل. [25] [26] [27]



الشكل(٦-٦): نتيجة الاستعلام عن CWE-294

وعند الانتقال الى :

Services ⟶ Vulnerability Analysis

يمكننا الحصول على قائمة لأهم مواقع الويب العالمية المستخدمة للبحث عن الثغرات الأمنية في الأنظمة، مع إمكانية الانتقال الى موقع الوب الخاص بكل منها كما هو موضح في الشكل(٦-٧). [24]

	TOOL_NAME	Website
Select	CNET Blogs	http://news.cnet.com
Select	CodeRed Center	http://www.eccouncil.org
Select	Computerworld	http://www.computerworld.com
Select	HackerJournals	http://www.hackerjournals.com
Select	HackerWatch	http://www.hackerwatch.org
Select	Hackerstorm Vulnerability Database Tool	http://www.hackerstorm.com
Select	Help Net Security	http://www.net-security.org
Select	NVD	http://nvd.nist.gov
Select	SC Magazine	http://scmagazine.com
Select	Secunia	http://www.secunia.com
Select	SecuriTeam	http://www.securiteam.com
Select	SecurityFocus	http://www.securityfocus.com
Select	SecurityMagazine	http://www.securitymagazine.com
Select	SecurityTracker	http://www.securitytracker.com
Select	Security watch	http://securitywatch.com
Select	Symantec	http://www.symantic.com
Select	TechNet	http://blogs.technet.com
Select	Techworld	http://www.techworld.com
Select	US-CERT	http://www.kb.cert.org
Select	WindowsSecurity Blogs	http://blogs.windowsecurity.com

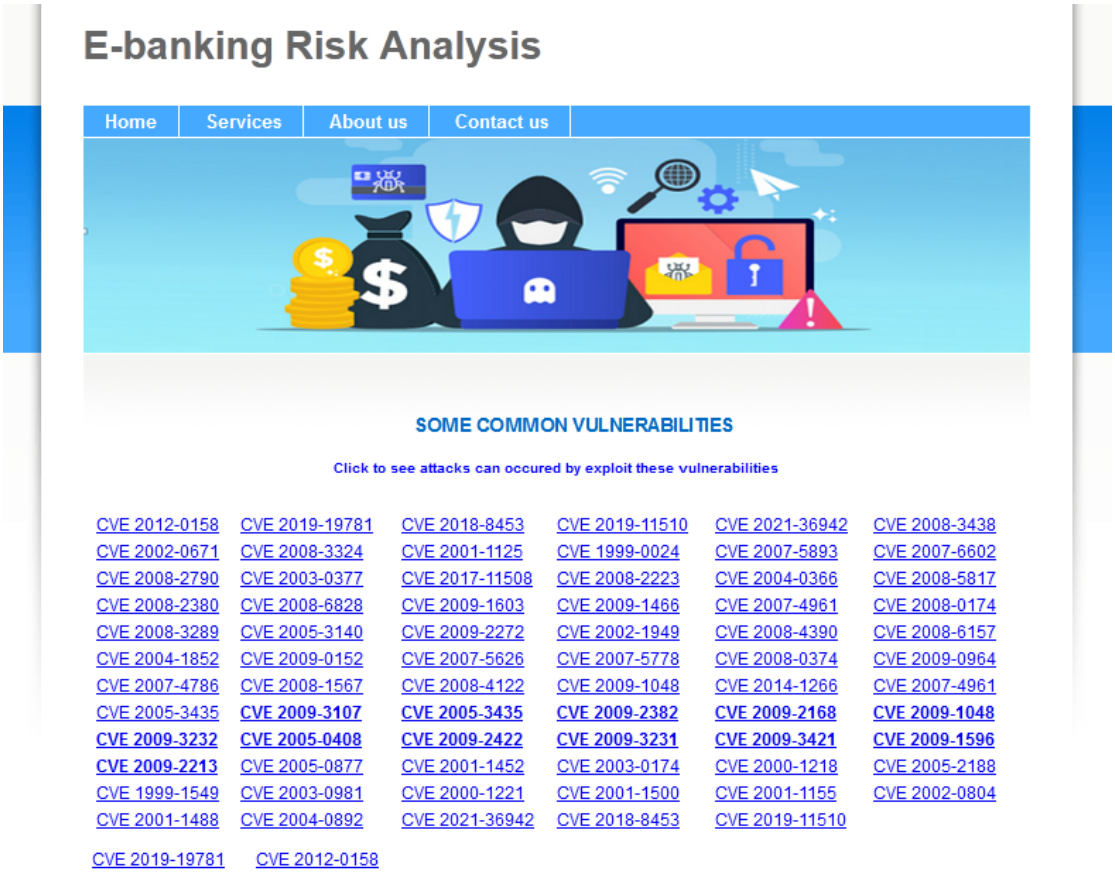
الشكل(٦-٧):نتيجة الاستعلام عن مواقع تحليل نقاط الضعف

أيضاً نجد قائمة بأدوات تقييم نقاط الضعف مع وصف لكل منها [24] كما في الشكل(٦-٨):

TOOL_DESCRIPTION	TOOL_NAME
called Zaproxy is an intercept proxy designed for the security testing of web applications	Owasp-Zap
web application proxy built to identify vulnerabilities while browsing an application	ProxyStrike
web application security reconnaissance tool	Skipfish
is asecurity testing tool used to crawl a website and analyze page content to find links as well as form parameters	Vega
a multi-threaded, multi-platform tool used to audit web servers	Webshag
open source project used to scan and analyze remote systems to find vulnerabilities	Websploit

الشكل(٦-٨): نتيجة الاستعلام عن أدوات تقييم نقاط الضعف

كما نجد قائمة بنقاط الضعف المرتبطة بالهجمات التي تم تحليلها وفق CVE [26] [27]، وعند الضغط على أياً منها يتم الانتقال الى صفحة الهجوم الذي قد يحدث نتيجة استغلال نقطة الضعف هذه كما هو موضح في الشكل(٦-٩).



الشكل(٦-٩): نقاط الضعف التي أدت الى الهجمات التي تمت دراستها

٦.٥ الخلاصة والأعمال المستقبلية

في هذا البحث، درسنا الخدمات المصرفية الالكترونية و مخاطرها الأمنية، واخترنا منها التجارة الالكترونية باستخدام متصفح الويب وباستخدام طرفية نقاط البيع، ودرسنا مخاطر أمن المعلومات التي قد تواجه هذه الخدمة بنوعيها. ثم درسنا الويب الدلالي والأنطولوجيا، واستخدمنا الأنطولوجيا في عملية تحليل هذه المخاطر، حيث قمنا ببناء أنطولوجيا تجمع مفاهيم الخدمات المصرفية الالكترونية ومفاهيم أمن المعلومات، وتم استخدام مصادر بيانات رسمية مثل CAPEC و CWE و CVE ، وتم الربط بينها وبين المفاهيم السابقة من خلال علاقات الأنطولوجيا. ثم قمنا ببناء موقع ويب لتحليل هجمات خدمة التجارة الالكترونية بنوعيها، بالاعتماد على المعلومات المخزنة في الأنطولوجيا المقترحة.

وفي المستقبل، يمكن تطوير هذا البحث إما بتحليل المزيد من المخاطر التي قد تواجه خدمة التجارة الالكترونية كدراسة مخاطر التجارة الالكترونية باستخدام تطبيقات الموبايل. أو بإضافة خدمات

مصرفية الكترونية أخرى الى الأنطولوجيا المقترحة وتحليل مخاطرها. أو بالربط مع مصادر بيانات رسمية بهدف إغناء عملية التحليل بالمزيد من المعلومات.

المراجع

[1] سحنون خالد, *تأثير تكنولوجيا المعلومات على مردودية البنوك*, تلمسان، ٢٠١٦.

[2] Amina Souag, Camille Salinesi, Raúl Mazo, and Isabelle Wattiau, "A Security Ontology for Security Requirements Elicitation," , 2015.

[3] Dilpreet Singh, Ron Ruhl, and Hamman Samuel, "Attack Tree for Modelling Unauthorized EMV Card Transactions at POS Terminals," , 2018.

[4] Joseph A. Ojeniyi, Elizabeth O. Edward, and Shafii M. Abdulhamid, "Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study," *International Journal of Education and Management Engineering*, p. 14, March 2019.

[5] Samuel Eneeji, Maurice Udie, Walter Eyong, and Kelechukwu Chimdike, "A Study of Electronic Banking Fraud ,Fraud Detection and Control," *International Journal of Innovative Science and Research Technology* , March 2019.

[6] Waleed A. Hammood et al., "A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number," , 2020.

[7] Rodrigo Carvalho, Michael Goldsmith, and Sadie Creese, "Applying Semantic Technologies to Fight Online Banking Fraud," in *2015 European Intelligence and Security Informatics Conference*, Manchester, UK , 2015, p. 8.

[8] Taiana Stepanova, Alexander Pechenkin, and Daria 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* , 2015, p. 8.

[9] Ferrucio De Franco Rosa and Rodrigo Bonacin, "Towards an Ontology of Security Assessment: A Core Model Proposal," in *Information Technology - New Generations. Advances in Intelligent Systems and Computing*, Latifi S, Ed.: Springer, Cham, 2018.

[10] Stefan Fenz and Thomas Neubauer, "Ontology-based information security compliance determination and control selection on the example of ISO 27002," 2018.

[11] Romilla Syed and Haonan Zhong, "Cybersecurity Vulnerability Management :ِ An ontology_based conceptual model," in *Twenty-fourth Americas Conference on Information Systems*, New Orleans, 2018, p. 5.

[12] Igor Kotenko, Andrey Fedorchenko, Elena Doynikova, and Andrey Chechulin, "An Ontology-Based Storage of Security Information," *Journal of Information Technology and Control*, p. 13, Oct. 2018.

[13] Elena Doynikova and Igor Kotenko, "Approach for determination of cyber-attack goals based on the ontology of security metrics," in *IOP Conference Series: Materials Science and*

Engineering, 2018, p. 7.

[14] Shao-Fang Wen and Basel Katt, "Managing Software Security Knowledge in Context," *www.mdpi.com/journal/information*, June 2019.

[15] Andrei Brazhuk, "Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries," *International Journal of Open Information Technologies*, January 2019.

[16] G.NEDUMARAN Maran and Baladevi Kaleeswaran, "PROS AND CONS OF ONLINE BANKING SERVICES," *International Journal of Research in Humanities, Arts and Science*, april 2018.

[17] جمال خالد النائب، مصنف دلالي لمستخدمي وسائل التواصل الاجتماعية "تويتر" باللغة العربية ، ٢٠١٨.

[18] الدكتور خالد ممدوح ابراهيم. (٢٠٢١, May) elmaarifa. [Online]. https://elmaarifa.info/

[19] (2020, Dec.) alrab7on.

[20] Ahmed EL ORCHE, Mohamed BAHAJ, and Soumya AIN ALHAYAT, "Ontology based on electronic payment fraud prevention," *IEEE*, p. 6, 2018.

[21] Meriem Tabiaa, Najib EL KAMOUN, and Abdellah madani, "E-Banking: Security risks, previsions and recommendations," *International Journal of Computer Science and Network Security*, November 2017.

[22] Samuel Eneji, Fergus Uchenna, and Walter Eyong, "A Detailed Study of Electronic Banking Security Techniques and Safety Measures," *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT*, November 2017.

[23] (2019, june) wikipedia.

[24] *CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs*, 10th ed. London, 2018.

[25] (2007) CAPEC. [Online]. https://capec.mitre.org/

[26] CWE. [Online]. https://cwe.mitre.org/

[27] CVE. [Online]. https://cve.mitre.org/

[28] Belén Bonilla- Morales and Miguel Vargas- Lombardo, "Survey: Grid Computing and Semantic Web," *International Journal of Computer Science Issues*, 2010.

[29] Preeti Rathee and Sanjay Kumar Malik, "IWD towards Semantic similarity measure in ontology," *Journal of Information & Optimization Sciences*, 2020.

[30] BOGUMIŠ A HNATKOWSKA, ADRIANNA KOZIERKIEWICZ, and MARCIN PIETRANIK, "Semi-Automatic Definition of Attribute Semantics for the Purpose of Ontology Integration," 2020.

[31] dotNetRDF. [Online]. https://dotnetrdf.org/