Ontology Modelling of Industrial Control System Ethical Hacking

Thomas Heverin, Ansh Chandnani, Cate Lopex and Nirav Brahmhatt
Drexel University, Philadelphia, USA
th424@drexel.edu
ac3965@drexel.edu
cml476@drexel.edu
nb899@drexel.edu
DOI: 10.34190/IWS.21.091

Abstract: Industrial control systems (ICS) include systems that control industrial processes in critical infrastructure such as electric grids, nuclear power plants, manufacturing plans, water treatment systems, pharmaceutical plants, and building automation systems. ICS represent complex systems that contain an abundance of unique devices all of which may hold different types of software, including applications, firmware and operating systems. Due to their ability to control physical infrastructure, ICS have more and more become targets of cyber-attacks, increasing the risk of serious damage, negative financial impact, disruption to business operations, disruption to communities, and even the loss of life. Ethical hacking represents one way to test the security of ICS. Ethical hacking consists of using a cyber-attacker's perspective and a variety of cybersecurity tools to actively discover vulnerabilities and entry points for potential cyber-attacks. However, ICS ethical hacking represents a difficult task due to the wide variety of devices found on ICS networks. Most ethical hackers do not hold expertise or knowledge about ICS hardware, device computing elements, protocols, vulnerabilities found on these elements, and exploits used to exploit these vulnerabilities. Effective approaches are needed to reduce the complexity of ICS ethical hacking tasks. In this study, we use ontology modeling, a knowledge representation approach in artificial intelligence (AI), to model data that represent ethical hacking tasks of building automation systems. With ontology modeling, information is stored and represented in the form of semantic graphs that express individuals, their properties, and the relations between multiple individuals. Data are drawn from sources such as the National Vulnerability Database, ExploitDB, Common Weakness Enumeration (CWE), the Common Attack Pattern and Enumeration Classification (CAPEC), and others. We show, through semantic queries, how the ontology model can automatically link together entities such as software names and versions of ICS software, vulnerabilities found on those software instances, vulnerabilities found on the protocols used by the software, exploits found on those vulnerabilities, weaknesses that represent those vulnerabilities, and attacks that can exploit those weaknesses. The ontology modeling of ICS ethical hacking and the semantic queries run over the model can reduce the complexity of ICS hacking tasks.

Keywords: ontology, industrial control systems, ethical hacking

1. Introduction

Industrial control systems (ICS) control industrial processes in infrastructure such as nuclear power plants, electric grids, manufacturing plants, ship systems, and more. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) (2020) considers many of these ICS to fall under the category of critical infrastructure that are "...so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Therefore, protecting ICS from cyber-attacks is a critical task.

ICS cyber defenders, who secure and protect ICS from cyber-attacks, face many challenges in their roles. ICS are complex systems which contain unique devices like programmable logic controllers (PLCs), intelligence electronic devices (IEDs), human-machine interfaces (HMIs), remote terminal units (RTUs), distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems. Each of these ICS devices contains unique computing elements including ICS operating systems, software, applications and firmware. ICS devices often use unique protocols like MODBUS, BACnet, CIP, Profinet, DNP3 and more. ICS cyber defenders must learn about the intricacies of ICS devices, computing elements and protocols in order to protect ICS. This ICS learning process can be challenging too.

This "diversity" of ICS devices, computing elements, and protocols also creates new threats which can lead to new exploits. (Shaaban, Gruber and Schmittner, 2019). Additionally, in previous years ICS were not originally designed to be connected to the network or available over the Internet; however, now they are. As a result, ICS have increasingly become targets of cyber-attacks. According to a recent IBM (2020) threat intelligence report, the number of targeted attacks on ICS has increased by over 2,000 percent since 2018. More and more ICS devices, which include Internet of Things (IoT) devices, have become more easily discoverable online.

In terms of cyber defense, ethical hackers play a major role in securing ICS as ethical hackers try to stay ahead of ICS cyber-attacks. Ethical hacking consists of several steps which include conducting reconnaissance, scanning networks, gaining access, maintaining access and hiding steps taken. In the reconnaissance phase, ethical hackers identify software, hardware, protocols and more being used by a target system. Then they identify vulnerabilities, exploits, weakness, potential attack types to use and more as they plain out their attacks. In this whole process for ICS ethical hackers, there is a deluge of data. Not only do ICS ethical hackers have to learn about unique ICS devices, computing elements and protocols but they also have to piece together various cybersecurity data. Ethical hackers need to look at various sources such as the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) Common Attack Pattern Enumeration and Classification (CAPEC), and Exploit Database (ExploitDB) when making their decisions. Assante, Roxey and Bochman stated (2015) that "...consider that these unpredictable elements interact in ways so complex they can never be fully comprehended by us, let alone fully accounted for or protected."

Overall, ethical hacking requires ethical hackers to synthesize data from multiple sources to make judgements and decisions on which paths to follow in order to attack a target. All of this can take a considerable amount of time especially when targeting ICS and planning attacks. Ontologies can be one way to link all these data together to help make judgments and decisions.

2. Background

2.1 Overview of ontologies

As stated in the previous section, the ICS ethical hacking domain is a complex domain due to the unique components of ICS as well as an abundance of cybersecurity data. Ontologies are one of many ways we can use to link all these data together to reduce the complexity of ICS ethical-hacking decision making.

An ontology can be defined as a set of concepts in a domain, attributes that describe the domain concepts, and relationships that link the domain concepts together. Ontologies are often used to make implicit knowledge explicit in order to allow computers to "compute" over them. In other words, ontologies are used to define and link domain data together in a useable format that allows computers to run queries over the data, to sort the results of the queries, to use reasoning to make deeper connections, to use algorithms to produce quantitative results and more. Ontologies fall under the knowledge representation domain, a key part of artificial intelligence (AI).

Ontologies contain three main parts: classes, data properties and object properties.

1. Classes are categories of objects or instances. In the ICS ethical hacking domain, an example class includes "Vulnerabilities." Objects in this class are individual, specific vulnerabilities such as CVE-2017-9644, and CVE-2017-9640 which are drawn from the NVD.
2. Data properties define attributes about objects. For example, we can use data properties to describe attributes about vulnerabilities. An example data property includes the vulnerability severity score. In a more specific example, the vulnerability score for CVE-2017-9664 is 9.8 out of 10. The vulnerability score for CVE-2017-9640 is 6.3
3. Object properties describe relationships between objects. For example, an object property can be named *hasVulnerability*. We can use this to show that a piece of ICS software like WebCTRL 6.5 *hasVulnerability* CVE-2017-9650. We can then use an object property *isExploitedBy* to show that CVE-2017-9650 *isExploitedby* EDB-ID-42544 (an exploit identification number from ExploitDB).

These object properties relationships can be threaded together as shown in this example:

> WebCTRL 6.5 *hasVulnerability* CVE-2017-9650 which in turn *isExploitedBy* EDB-ID-42544.

Object properties allow us to "walk across" an ontology. In other words, due to the specifications of object properties we can reason the following: WebCTRL 6.5 is impacted by the exploit EDB-ID-42544. Within ontologies, this reasoning can be computed automatically which can greatly reduce the amount of time ICS ethical hackers need in finding weaknesses in ICS.

Ontologies can be full of many classes, data properties, object properties to bridge together many concepts in a domain and across domains. Our ontology is defined in Section 3.2.

2.2 Ontologies in ethical hacking and ICS

Ontologies have been used to model various domains within cybersecurity. For example, previous research has examined the use of ontologies for modeling concepts in the ICS which are also called cyber-physical systems (CPSs). Shaaban, Gruber and Schmittner (2019) used ontologies to aid in the requirements development process of ICS. They also link cyber threats to the ICS requirements. A lot of previous work in developing ontologies for cybersecurity has focused on threats. Venkata, Kamongi and Kavi (2018) created on ontology to reason about the impacts of cyber-attacks on ICS along with mitigations to use to minimize the impacts. Van Heerden, Irwin, Burke and Leenen (2012) developed an ontology to create a taxonomy of network attacks from an attacker's view and the defender's view.

Several other projects have created ontologies for other purposes beyond ICS. For example, Avia, Wecel and Abramowicz (2015), developed an ontology to model IT projects, threats and attacks. Ellison, Venter, and Adeyemi (2017), created an ontology to understand the domain of digital forensics. Other forensics research has focused on modeling IT entities and more to aid cyber forensics analysts in searching across thousands of devices for forensics data (Balduccini, Kushner and Speck, 2015).

There has been limited research on developing cyber security ontologies focused on ethical hacking and the reasoning that goes into ethical hacking. Grant (2019) stated that many previous studies on ontologies in the cybersecurity domain had not focused on the planning stages in ethical hacking. A literature review conducted on 20 cybersecurity ontology papers from 1993-2018, found that one of the papers focused on the reconnaissance or planning phases of ethical hacking; rather most papers focus on classifying attack (Grant, 2019). This is a gap in the literature. Our work on using ontologies to model the decision making of the ethical hacking reconnaissance phase aims to fill this gap.

3. ICS ethical hacking ontology

3.1 Ontology development

Various methodologies exist for developing ontologies including a top-down approach and a bottom-up approach (Gosh, 2019). The top-down approach starts from the highest level of abstraction using the most general concepts; then it moves to modeling more specific entities. The bottom-up approach starts from modeling more specific concepts and then builds a structure up to general concepts. It relies on identifying relevant existing data points to extract relevant concepts and the relations between them. Gosh (2019) introduced the possibility of a "middle-out" approach for developing ontologies which is a combination of the top-down and bottom-up approaches. The middle-out approach provides a sense of balance between the specifics included in an ontology and the general domains and concepts represented.

Ontology developers should select an approach based on the domain that is being modeled (Fernández-López and Gómez-Pérez, 2002). ICS ethical hacking is an ever-evolving domain that contains unique ICS concepts, new vulnerabilities, new exploits, new types of attacks and more. As a result, we selected the middle-out approach to combine the advantages of the top-down approach (starting from general cyber security concepts) and the bottom-up approach (starting from unique ICS specifics).

Across ontology development, competency questions are often used to determine the scope of knowledge found in an ontology (Wiśniewski et al., 2019). Competency questions include natural language questions that users of the ontology would ask in a given domain. We developed competency based on questions that ethical hackers ask when conducting reconnaissance on a target, determining which vulnerabilities are found on that target, which exploits to use on those vulnerabilities and more.

Example competency questions in our ontology include:

4. What vulnerabilities are found on this ICS software version?
5. What exploits exist that can exploit those vulnerabilities?
6. What protocols are used by the ICS software version or device?
7. What vulnerabilities are found on those protocols?
8. What type of vulnerability (weakness) does each vulnerability represent?
9. What attacks can be used on those types of vulnerabilities?

These competency questions and others guided the development and structure of our ICS ethical hacking ontology.

3.2 Ontology structure

This subsection describes the architecture of the ICS ontology. The ICS ontology consists of classes, object properties that link classes together, and data properties that describe instances in the classes (such as vulnerability severity metrics from the NVD). The main ICS Classes are listed and shown in Figure 1 (the Credentials class contains a Default Username subclass and a Default Password subclass).

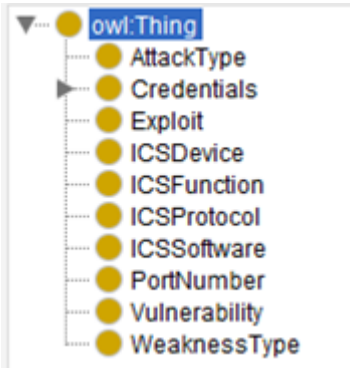

Figure 1: ICS ethical hacking ontology classes

Descriptions of the classes are provided in **Table 1**:

Table 1: ICS ethical hacking ontology class descriptions

Class Name	Class Description	Examples of Individual in the Class
AttackType	Type of attack from CAPEC	CAPEC-540 (overread buffers)
Credentials	Default username and password	Admin; 1234
Exploit	Exploit found in ExploitDB	EDB-ID-42544 (an exploit on WebCTRL)
ICS Device	Type of ICS device or application	Facilities management console
ICS Function	Function of an ICS device or software	Controls security system, controls heating, controls ventilation
ICS Protocol	Protocol used by ICS device or software	BACnet (protocol used for building automation systems)
ICS Software	Name and version of ICS software	WebCTRL 6.5
Port Number	Port number used by ICS device, software or protocol	Port 47808 (associated with BACnet
Vulnerability	Vulnerability found in the NVD	CVE-2017-9640
Weakness Type	The type of vulnerability	CWE-125 (out of bounds read)

Object properties define types of triples that are found in ontologies. A triple is made up of a subject, predicate, and object. An example triple is WebCTRL 6.5 *hasVulnerability* CVE-2017-9650. The object property *hasVulnerability* defines a relationship between WebCTRL 6.5 and CVE-2017-9650. WebCTRL 6.5 is the subject, *hasVulnerability* is the predicate and CVE-2017-9650 is the object.

We can use *hasVulnerability* to define many triples. To do this, we must specify which class makes up the subject (called the “domain”) of the object property and specify which class makes up the object (called the “range”). Multiple classes can fall in the domain and the range. For the above example, the object property

hasVulnerability is used in this context: ICS Software *hasVulnerability* Vulnerability, where the ICS Software class is the domain and the Vulnerability class is the range.

Table 2 defines the object properties of the ICS ethical hacking ontology including the domains and ranges that make up the object properties.

Table 2: ICS ethical hacking ontology object properties

Domain(s)	Object Property Name	Range
ICS Device	*hasSoftware*	ICS Software
ICS Software or ICS Device	*hasFunction*	ICS Function
ICS Device	*usesPort*	Port Number
ICS Device or ICS Software or Port Number	*usesProtocol*	ICS Protocol
ICS Device or ICS Software	*hasDefaultPassword*	Default Password
ICS Device or ICS Software	*hasDefaultUsername*	Default Username
ICS Software or ICS Protocol	*hasVulnerability*	Vulnerability
Vulnerability	*isWeaknessType*	Weakness Type
Weakness Type	*hasRelatedAttackPattern*	Attack Type
Vulnerability or ICS Protocol or ICS Software or ICS Device	*isExploitedBy*	Exploit

Ontologies also provide a way to add data attributes about classes. The data properties selected for this project were based on data directly available for each class. For example, the NVD provides CVE data properties about vulnerabilities. ExploitDB, CAPEC and CWE provide data properties about exploits, attacks and weaknesses respectively. Figure 2 shows the specific data properties in the ICS ontology. Exploit Data Properties are for the Exploit class, Vulnerability data properties are for the Vulnerability class, CAPEC data properties are for the AttackType class and CWE data properties are for the WeaknessType class.

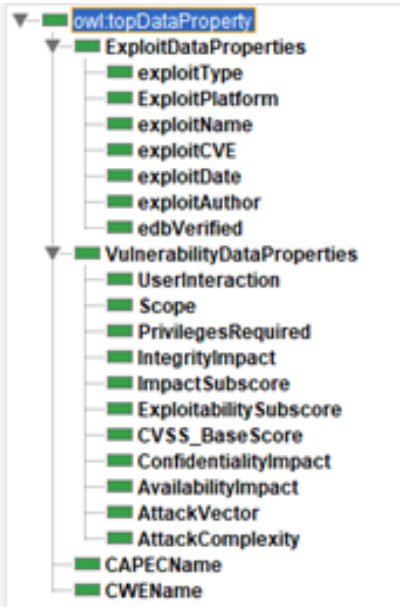

Figure 2: ICS ethical hacking ontology data properties

Object properties and data properties provide a foundation for running queries over the ontology and for sorting results of the queries. For example, ethical hackers will want to know which vulnerabilities exist for a given piece of ICS software (which involves the *hasVulnerability* object property; ICS Software *hasVulnerability* Vulnerability) and then sort the results in descending order of severity score (a data property of the Vulnerability class). More details are provided in the next section about running queries over ontologies.

4. Ontology queries and results

4.1 SPARQL for ontology queries

SPARQL is a recursive acronym that stands for SPARQL Protocol and RDF Query Language. RDF stands for resource description framework which is a standard model for representing triples. SPARQL was built to query patterns of triples used in RDF formats that are found in ontologies.

Formulating and executing SPARQL queries over ontologies allows us to selectively retrieve information to answer competency questions. In a web of information represented through an ontology, SPARQL queries grant a sense of clarity by enabling us to filter results to our needs while still retaining information to answer a multitude of competency questions. In our ontology, we include information about ICS software, protocols, vulnerabilities, exploits, and severity metrics among other things. However, if ICS ethical hackers desire to retrieve information about the available vulnerabilities of existing software without being overloaded with other information, they can use the following SPARQL query:

```
SELECT ?Software ?Vulnerability
WHERE {
?Software ics:hasVulnerability ?Vulnerability .
}
ORDER BY DESC(?Vulnerability)
```

This query searches for all instances of ICS software within an ontology and their related vulnerabilities. In other words, this query searches for instances of the RDF triple: ICS Software *hasVulnerability* Vulnerability and lists the names of all software present along with their vulnerabilities. It also lists them in the descending order of vulnerabilities. Since CVEs are identified by the year they were discovered and followed by a chronological number, listing them in descending order ensures that the most recently found vulnerabilities appear at the top of the results. This provides ICS ethical hackers the most recent vulnerabilities first. The results to the aforementioned query are as such for WebCTRL 6.5 are shown in **Figure 3**.

BACnet	CVE-2019-12480
WebCTRL6.5	CVE-2018-8819
WebCTRL6.5	CVE-2017-9650
WebCTRL6.5	CVE-2017-9644
WebCTRL6.5	CVE-2017-9640
WebCTRL6.5	CVE-2016-5795
WebCTRL6.5	CVE-2014-8384

Figure 3: SPARQL query results for vulnerabilities

4.2 SPARQL query results

Various SPARQL queries can be used to find connections between ICS software versions, vulnerabilities, exploits, weaknesses, attacks, ICS functions and more. SPARQL queries can help automate the reasoning that ethical hackers use when deciding on which targets, which vulnerabilities, and exploits to focus on first. This subsection provides such results of SPARQL queries run over the ICS ethical hacking ontology.

The SPARQL queries and results shown in this paper focus on WebCTRL, an ICS software product commonly used in building automation systems (BAS) to control and manage security systems, heating, cooling, air conditioning, and fire alarm systems. BAS are found across organizations.

The following SPARQL query generates a table that includes a target system (a facilities management web application used to access WebCTRL 6.5), ICS software used by the system, vulnerabilities found on the ICS

software, exploits found on those vulnerabilities, and descriptions/names of the exploits. **Figure 4** shows the results.

```
SELECT ?Target ?Software ?Vulnerability ?Exploit ?Exploit_Name
 WHERE {
?Target ics:hasSoftware ?Software .
?Software ics:hasVulnerability ?Vulnerability .
OPTIONAL {
?Vulnerability ics:isExploitedBy ?Exploit .
?Exploit ics:exploitName ?Exploit_Name .
}
}
ORDER BY DESC(?Vulnerability)
```

Target	Software	Vulnerability	Exploit	Exploit_Name
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2018-8819		
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2017-9650	EDB-ID-42544	"Automated Logic WebCTRL 6.5 - Unrestricted File Upload/ Remote Code Execution"
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2017-9644	EDB-ID-42542	"Automated Logic WebCTRL 6.5 - Local Privelege Escalation"
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2017-9640	EDB-ID-42543	"Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write"
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2016-5795		
FacilitiesMgmtWebApp1	WebCTRL6.5	CVE-2014-8384		

Figure 4: SPARQL query results for ICS software, vulnerabilities, and exploits

By viewing this threaded information above, ethical hackers can see immediately that there are three exploits that they can use to exploit vulnerabilities found on WebCTRL 6.5. Normally, ethical hackers would manually have to search across various sources to find this information and synthesize this information.

Ethical hackers will also want to know which vulnerabilities can be exploited over the Internet (represented by "Network" in the NVD for each CVE) and have a low attack complexity (also found in the NVD). Vulnerabilities that can be exploited over the Internet and are low in complexity, are types of vulnerabilities highly sought after by ethical hackers. The following SPARQL shows the syntax that finds these types of vulnerabilities:

```
SELECT ?CVE ?AttackVector ?AttackComplexity
WHERE {
?CVE ics:AttackComplexity ?AttackComplexity .
?CVE ics:AttackVector ?AttackVector .
FILTER(?AttackVector = "Network" && ?AttackComplexity = "Low")
}
```

The results for this above query are shown below in Figure 5 .

CVE	AttackVector	AttackComplexity
CVE-2017-9640	"Network"	"Low"
CVE-2016-5795	"Network"	"Low"
CVE-2018-8819	"Network"	"Low"
CVE-2019-12480	"Network"	"Low"

Figure 5: SPARQL query results for selected vulnerability properties

Through this query, we were able to filter the information from the ontology that details the attack vector and attack complexity of a vulnerability for WebCTRL 6.5 based on the information from the NVD. By filtering results based on the data properties of a vulnerability, an ethical hacker is able to focus on vulnerabilities that are "easy wins", i.e. vulnerabilities that can be exploited over the internet and that have a low attack complexity. ICS ethical hackers would normally have to look at each CVE manually on the NVD and look at the data attributes separately to generate the list above.

As stated earlier in the paper, many ethical hackers are not familiar with ICS devices and software. Even in general IT or business networks, there can be an abundance of various software names/versions, applications, operating systems, protocols and more. Ethical hackers will often want to pick targets that have high values. We formulated a SPARQL query that links together ICS vulnerabilities, ICS exploits and ICS functions. This SPARQL

query is shown here with the results below with results in **Figure 6:** SPARQL query results for ICS vulnerabilities, exploits, and functions.

```
SELECT ?Vulnerability ?Exploit_Name ?Function
WHERE {
?Software ics:hasVulnerability ?Vulnerability .
?Software ics:hasFunction ?Function .
?Vulnerability ics:isExploitedBy ?Exploit .
?Exploit ics:exploitName ?Exploit_Name .
}
ORDER BY ?Function DESC(?Vulnerability)
```

Vulnerability	Exploit_Name	Function
CVE-2017-9644	"Automated Logic WebCTRL 6.5 - Local Privelege Escalation"	controlsSecurity
CVE-2017-9644	"Automated Logic WebCTRL 6.5 - Local Privelege Escalation"	displaysFloorPlan
CVE-2017-9644	"Automated Logic WebCTRL 6.5 - Local Privelege Escalation"	controlsCooling
CVE-2017-9644	"Automated Logic WebCTRL 6.5 - Local Privelege Escalation"	controlsHeating
CVE-2017-9640	"Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write"	controlsSecurity
CVE-2017-9640	"Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write"	displaysFloorPlan
CVE-2017-9640	"Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write"	controlsCooling
CVE-2017-9640	"Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write"	controlsHeating

Figure 6: SPARQL query results for ICS vulnerabilities, exploits, and functions

This query serves as an example of how an ethical hacker can thread relevant information to understand the impact of exploiting vulnerabilities on a system. This query lists vulnerabilities that have a readily available exploit in Exploit-DB, displays the name of the corresponding exploit, and lists the functions of the ICS software impacted by the vulnerability. In this case, ethical hackers can see that if they can use the stated exploits that exploit the listed vulnerabilities, they can potentially impact WebCTRL 6.5 functions that control things such as security systems, cooling systems, and heating systems while also potentially gaining access to floor plans. Gaining access to floor plans could be severely detrimental to organizations such as military installations.

Formalized testing is needed to evaluate how the results of SPARQL queries reduce decision making time in ICS ethical hacking. As an initial step in that direction, we asked three ethical hackers who have experience in ethical hacking of general networks (but who are new to ICS ethical hacking) to find vulnerabilities on WebCTRL, to analyze which vulnerabilities can be exploited over the Internet as well as which vulnerabilities are easiest to exploit, what kind of weaknesses are represented by the vulnerabilities, what kinds of attacks can be used on those weaknesses, and which vulnerabilities have known exploits. It took the ethical hackers an average of 4 hours to produce results. A formal test is needed to compare the manual processes with our ontology automated processes that require incorporating the time for creating an ontology model.

5. Conclusion and future work

ICS ethical hacking represents a highly complex task given the complexities of ICS. Ethical hackers must search across numerous cybersecurity sources, connect information from the sources, learn about ICS computing components, and then make decisions on which targets to attack and which vulnerabilities to exploit. This can be a time-consuming and challenging process. We developed a framework for an ontology to model ICS devices, software, vulnerabilities, exploits, weaknesses, attacks and more in order to lay the foundation for automating decision making in ICS ethical hacking. We showed that the ICS ethical hacking ontology can automate the process of finding answers to common questions that ICS ethical hackers may have such as when conducting reconnaissance and planning attacks. Limited testing was conducted to compare results from SPARQL queries to manual processes carried out by ethical hackers; however, more testing is still needed to formally evaluate the effectiveness of the ICS ethical hacking ontology.

The next step in our ontology modeling development includes automating information extraction from cybersecurity data sources and ingesting relevant data into our ontology. Various publicly available application programming interfaces (APIs) and web scraping technologies can be used to read structured information of sites such as Exploit-DB, NVD, and CAPEC and insert them into a Protege ontology using appropriate libraries. Furthermore, by using natural language processing it is possible to read information about ICS devices and

determine their core functions. Since building a large, comprehensive ICS ontology manually would be highly time consuming, automating the process would allow for a faster organization of data.

This paper has shown the advantages of using ontology modeling and how ICS ethical hackers could use and benefit from ontology modeling techniques. This may considerably reduce the amount of time ICS ethical hackers need to select targets, vulnerabilities, and exploits to testing the security of ICS which in turn will help cyber defenders better defend ICS that are critical for communities.

Acknowledgements

This research is supported, in part, by National Science Foundation Grant No. 1922202, CyberCorps Scholarship for Service (SFS).

References

Assante, M., Roxey, T. and Bochman, A. (2015). "The Case for Simplicity in Energy Infrastructure." Retrieved from https://www.csis.org/analysis/case-simplicity-energy-infrastructure.

Aviad, A., Wecel, K., & Abramowicz, W. (2015). "The Semantic Approach to Cyber Security Towards Ontology Based Body of Knowledge." The European Conference on Cyber Warfare and Security.

Balduccini, M., Kushner, S., and Speck, J. (2015). "Ontology-driven Data Semantics Discovery for Cyber-security." The International Symposium on Practical Aspects of Declarative Language.

Cybersecurity and Infrastructure Security Agency (2020). "Critical Infrastructure Sectors." Retrieved from https://www.cisa.gov/critical-infrastructure-sectors.

Ellison, D., Venter, H., and Adeyemi, I. (2017). "An Improved Ontology for Knowledge Management in Security and Digital Forensics." The European Conference on Cyber Warfare and Security, pp 725-733.

Fernández-López, M., and Gómez-Pérez, A. (2002). "Overview and Analysis of Methodologies for Building Ontologies." *The Knowledge Engineering Review*, Vol 17, No. 2, pp, 129–156.

Ghosh, M. E., Naja, H., Abdulrab, H., & Khalil, M. (2016). Towards a Middle-Out Approach for Building Legal Domain Reference Ontology." *International Journal of Knowledge Engineering*, Vol. 2, No. 3, pp 109–114.

Grant, T. (2019). "Building an Ontology for Planning Attacks that Minimize Collateral Damage: Literature survey." The 14th International Conference on Cyber Warfare and Security.

IBM (2020). "IBM X-Force Threat Intelligence Index." Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence.

Shaaban, A. M., Gruber, T., & Schmittner, C. (2019). Ontology-Based Security tool for Critical CyberPhysical Systems." The 23rd International Systems and Software Product Line Conference, Vol. B, pp 207-210.

Venkata, R. Y., Kamongi, P., and Kavi, K. (2018). "An Ontology-Driven Framework for Security and Resiliency in Cyber Physical Systems." The 13th International Conference on Software Engineering Advances.

Van Heerden, R., Chan, P., Leenen, L., and Theron, J. (2016). "Using an Ontology for Network Attack Planning." *International Journal of Cyber Warfare and Terrorism*, Vol. 6, No. 3, pp 65-78.

Van Heerden, R., Irwin, B., Burke, I. D., and Leenen, L. (2012). "A Computer Network Attack Taxonomy and Ontology." *International Journal of Cyber Warfare and Terrorism,* Vol. 2, No. 3, pp 12-25.

Wiśniewski, D., Potoniec, J., Ławrynowicz, A., & Keet, C. M. (2019). "Analysis of Ontology Competency Questions and Their Formalizations in SPARQL-OWL". Journal of Web Semantics, Vol. 59.

World Wide Web Consortium (2008). "SPARQL Query Language for RDF." Retrieved August 27, 2020, from https://www.w3.org/TR/rdf-sparql-query/

Chuck Easttom is the author of 30 books and 70 papers, and 22 patents. He holds a D.Sc, Ph.D. , and master's degrees. He is a Distinguished Speaker of the ACM, Distinguished Visitor of the IEEE, as well as a Senior Member of the ACM and the IEEE. He is an adjunct lecturer for Georgetown University

Éric Filiol is professor at ENSIBS, Vannes, France and at National Research University Higher School of Economics, Moscow, Russia in the field of information and systems security. He is also a senior consultant in cyber security and intelligence. He is editor-in-chief of the research journal in Computer Virology and Hacking Techniques published by Springer.

Ryan Gabrys is a scientist with the Naval Information Warfare Center Pacific. His research interests include coding theory with applications to systems, storage and security.

Dr Sheikh Ghafoor is a professor of Computer Science at Tennessee Tech University. His main area of research is High Performance Computing, Cyber Physical, System Security, Computational Earth Science, and Computer Science Education. His research in these areas has been funded by NSF, NASA, DoD, and DoE.

Dr. Scott Graham is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, USA. His research interests center on cyber physical systems, computer architecture, networks, and security for critical infrastructure protection.

Prof. Greiman is an Assistant Professor at Boston University, where she teaches and conducts research in international law and global cyber law and governance. She formerly served in high level appointments at the U.S. Department of Justice and as legal adviser to the U.S. Department of State and USAID in Eastern and Central Europe, Africa and Southeast Asia.

George Grispos is an Assistant Professor of Cybersecurity in the School of Interdisciplinary Informatics at the University of Nebraska at Omaha. He obtained his PhD in Computing Science from the University of Glasgow, Scotland. His research interests include digital forensics, security incident response, information assurance, and applied computing science.

Dr. Thomas Heverin is a cybersecurity teaching professor for Drexel University. He holds a Ph.D. focused on cybersecurity and the CISSP. He has conducted research on cyber threats on industrial control systems and leads the CyberCorps program at Drexel. He also served in the U.S. Navy as a ship officer.

Michael Bennett Hotchkiss is an independent researcher with interests in the psychology of influence, criminology, and nation-state disinformation; especially in the context of Russian active measures. Michael earned a Master of Organization Development from Bowling Green State University; and a Bachelor of Arts in Psychology from the University of Connecticut, graduating Phi Beta Kappa.

Eduardo Arthur Izycki International Relations M.A. Student at the University of Brasília (UnB) and public servant. Eduardo Izycki worked on developing solutions for risk assessments in the cycle of major events in Brazil (2012/2016). He currently works in the Critical Infrastructure Protection Coordination of the Brazilian Institutional Security Office (GSI).

William A. Johnson is a direct-admit PhD and Cyber Corps scholar at Tennessee Tech University. His research areas include Remote Attestation for embedded devices, cryptographic solutions for emerging networks, and ethical hacking. He received his bachelors from Tennessee Tech University in Computer engineering in 2018.

Nida Kazi graduated with a Master of Information Systems from John Hopkins University, in August 2020 and received her Bachelor of Engineering in Computer Science from the University of Pune. Her research has been focused in the fields of Cybersecurity and Cryptography. She is an avid cook and voracious reader, and lives in Virginia with her best friends.

Anne Kohnke, Ph.D. is an Associate Professor and the Principal Investigator for the Center of Academic Excellence in Cyber Defense (CAE-CD) at the University of Detroit Mercy. Dr. Kohnke's research is focused in the area of cybersecurity, risk management, and cybercrime. She has recently coauthored six books and several peer-reviewed journal articles in this discipline.

Daniel Koranek is a research computer scientist with the Air Force Research Laboratory. He holds a B.S. in computer science from Cedarville University and an M.S. in Cyber Operations from the Air Force Institute of Technology (AFIT), and is in doctorate studies at AFIT. Daniel's research interests are in embedded systems security and machine intelligence.

MSc Tiina Kovanen is a PhD student at the university of Jyväskylä. She is interested in various cyber security topics for different cyber-physical systems. Currently she is working towards her degree by studying possibilities and challenges related to ships' remote pilotage environment, ePilotage.