Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model

Emergent Research Forum (ERF)

Romilla Syed  
University of Massachusetts, Boston  
Romilla.Syed@umb.edu

Haonan Zhong  
University of Massachusetts, Boston  
Haonan.Zhong001@umb.edu

Abstract

Prevention of exploits requires timely intelligence about the cybersecurity vulnerabilities and threats. The U.S. Computer Emergency Response Team Coordination Center (CERT/CC) is the official body to disclose vulnerability information. Increasingly, hackers also use social media to share vulnerability and exploit information. In this study, we present a conceptual ontology of cybersecurity vulnerability management that integrates information from official sources with social media intelligence. The ontology models products, threats, vulnerabilities, countermeasures, intelligence and their relations. The ontology extends the vulnerability concepts provided by National Institute of Standards and Technology (NIST) and can be used as a general vocabulary of the domain of cybersecurity vulnerability management. Further, the ontology could be useful for reasoning about the relationships between entities to issue cybersecurity alerts for security analysts to analyze and manage vulnerabilities.

Keywords

Ontology; Cybersecurity vulnerability; Vulnerability management; Social media intelligence

Introduction

Recently, there has been an increase in the number of cybersecurity vulnerabilities discovered and reported. For instance, Common Vulnerabilities and Exposure (CVE), an industry standard for vulnerability and exposure identifiers, published 2230 vulnerabilities between Jan 1, 2018, and Feb 19, 2018. Most of the vulnerabilities are exploited between the time a vulnerability is discovered, and a patch is installed (Joh and Malaiya 2010). Hence, prevention of cybersecurity exploits requires timely intelligence of vulnerabilities and threats for security analysts to develop patches and workarounds. Prior research notes several pathways to vulnerability disclosure (see Kannan and Telang 2005; Ransbotham et al. 2012). While Computer Emergency Response Team Coordination Center (CERT/CC) is the official body to disclose vulnerabilities publicly, discoverers can also make vulnerability information available through other informal sources such as vendor sites, blogs, and social media. We contend that vulnerability management will require extraction of knowledge from different sources and then presented in a form that will allow security analysts to assess the severity of vulnerabilities and thereby prioritize the remediation efforts.

In this study, we propose an ontology-based conceptual model for the formal knowledge representation of the cybersecurity vulnerability domain and intelligence. Although prior research has proposed several vulnerability ontologies, there are two shortcomings. First, the existing ontologies are based on generic information security concepts (see An Wang et al. 2010; Elahi et al. 2009) and lack the context of vulnerabilities as provided by CERT/CC and Common Vulnerability Scoring System (CVSS) framework. CVSS is a published standard used by organizations worldwide to properly assess and prioritize vulnerability management process. Second, there is a lack of research on integrating social media intelligence for vulnerability management. Although few recent studies have proposed conceptual models to integrate social media for cyber intelligence (Joh and Malaiya 2010; Mittal et al. 2016; Sabotkke et al. 2015), these studies does not account for the concepts of vulnerability domain as described in the National Institute of Standards and Technology (NIST) (Bowen et al. 2007; Fenz and Ekelhart 2009). It is important to integrate social media intelligence as research suggests that severe vulnerabilities that receive high

2 https://www.first.org/cvss/
exposure on social media are quickly exploited (Sabottke et al. 2015). In this study, we address the noted gaps by proposing a conceptual ontology model that integrates the vulnerability concepts defined by NIST, CERT/CC, and CVSS with social media intelligence.

**Background Literature**

**Cybersecurity Vulnerabilities**

CVE defines cybersecurity vulnerability as a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, or availability of information assets. There are several pathways to vulnerability disclosure (see Kannan and Telang 2005; Ransbotham et al. 2012). A discoverer may choose to report the vulnerability to U.S. CERT/CC. Two major entities sponsored by CERT/CC are CVE and National Vulnerability Database (NVD). Usually, CERT/CC provides a protected window of 45 days to the affected vendors for releasing the patch. At the end of 45 days, CERT/CC discloses the vulnerability information to the public. This pathway is referred to as deferred disclosure. Alternatively, the discoverer may choose to disclose the vulnerability immediately by sharing it through mailing lists such as BugTraq. A discoverer may also choose to sell the vulnerabilities for some rewards to agencies such as iDefense and Tipping Point. Finally, a hacker may sell a vulnerability on the black market or may use it to exploit the system. Such vulnerabilities are disclosed after the exploit is published, or security analysts detect an intrusion.

Recently, few studies have begun to explore the role of social media in vulnerability disclosure. Messages with the root-cause, patch, advisory or exploit information are retweeted more than the messages that simply alert about a new vulnerability. Further, vulnerabilities shared by influential users are found to generate more retweets (Syed et al. 2018). Although social media provides intelligence about vulnerabilities, it is time-consuming to gather and integrate intelligence from multiple heterogeneous sources. Hence, few scholars have also proposed approaches for social media monitoring. For instance, Trabelsi et al. (2015) proposed a vulnerability monitoring system based on the security intelligence collected from Twitter. The authors found that Twitter users disclose vulnerabilities before the official sources. Few other studies have proposed methods to detect exploits, calculate risk, and prioritize response action based on social media feeds (Joh and Malaiya 2010; Mittal et al. 2016; Sabottke et al. 2015). In a related study, Benjamin et al. (2015) proposed a machine-learning approach to collect information from hacker forums, Internet-Relay-Chat (IRC), and carding shops for detecting cyberattacks. Finally, Lippmann et al. (2016) proposed a human language technology classifier to detect cyber discussions on Stack Exchange, Reddit, and Twitter.

**Ontologies and Vulnerability Management**

Guarino (1998) defines ontology as “... an engineering artifact, constituted by a specific vocabulary used to describe a certain reality, plus a set of explicit assumptions regarding the intended meaning of the vocabulary words [...] In the simplest case, an ontology describes a hierarchy of concepts related by subsumption relationships; in more sophisticated cases, suitable axioms are added in order to express other relationships between concepts and constrain their intended interpretation” (p.2). Ontologies allow formalized knowledge representation implemented in an ontology language (Guarino and Poli 1993). Guarino (1998) further notes that “an ontology is a logical theory accounting for the intended meaning of a formal vocabulary, i.e., its ontological commitment to a particular conceptualization of the world” (p. 7). The formal logic is specified using ontological vocabulary organized into a taxonomic class hierarchy. The vocabulary consists of concepts or classes, relationships, axioms, properties (attributes), and instances. The hierarchy is defined by a single root concept, referred to as “Thing” to which other concepts (classes) are related. The concepts are related to each other by “is-a” relation. Further, the concepts can be initiated by creating instances, which are referred to as individuals. The class instances can also be related by defining relations other than “is-a”, which are referred to as object properties. While relations between classes leads to a hierarchical domain representation, the relations between instances lead to a network domain representation. The range and domain of object properties can be set as directed or restricted. The range and domain specify the individual types that define object property. Finally, axioms can be added to object properties to represent the principles in the conceptual domain and limit the possible interpretations of defined concepts (Arbanas and Ćubrilo 2015).

In this study, we conceptualize an ontological representation of cybersecurity vulnerability domain, which is a specialized application domain of information security. In the literature, few vulnerability ontologies
have been proposed. For instance, Fenz and Ekelhart (2009) present a generic information security ontology with some focus on vulnerabilities. The ontology presents the security and vulnerability concept referencing German IT Grundschutz Manual by Federal Office for Information Security (2004) and the NIST Handbook (Bowen et al. 2007). The main concepts include asset, threat, vulnerability, and control. Few other studies have also proposed ontologies to integrate knowledge for vulnerability management (An Wang et al. 2010; Elahi et al. 2009; Sahoo et al. 2010). Similar to generic security ontologies, the vulnerability management ontologies include concepts such as vulnerability product, attack, and countermeasures. Finally, Salini and Shenbagam (2015) proposed a vulnerability ontology-based system to predict and classify the web application attacks.

In conclusion, the existing research has enhanced our understanding of vulnerability and security domain. The need for ontological representation of vulnerability domain has also been noted in the literature. However, there are two gaps. First, the existing vulnerability ontologies are modeled on generic information security concepts (see An Wang et al. 2010; Elahi et al. 2009) and lack the context of vulnerability domain as specified by CVE and NVD, both sponsored by the US CERT/CC. Further, vulnerability ontologies do not model the vulnerability characteristics as provided by CVSS framework, an industry standard to assess the severity of the vulnerabilities. Second, there is a lack of research on integrating social media intelligence for vulnerability management. Although Mittal et al. (2016) proposed a conceptual model to integrate Tweets for cyber intelligence, their model does not account for the concepts of vulnerability domain as described in the National Institute of Standards and Technology Special Publication 800-12 (Fenz and Ekelhart 2009). Further, the model does not account for tweet author details, which is important to establish the trustworthiness of tweets (see Trabelsi et al. 2015) and to assess the likelihood of retweeting vulnerabilities (Syed et al. 2018). We address the noted gaps by proposing a conceptual ontology model that integrates the concepts of NIST with CERT/CC (i.e. CVE, NVD), CVSS framework, and social media intelligence.

**Design Science Research Methodology**

In information systems literature, several techniques are used to design and develop artifacts. A design artifact refers to "a thing that has, or can be transformed into a material existence as an artificially made object (e.g., model, instantiation) or process (e.g., method, software)" (Gregor and Hevner 2013, p. 341). In this study, we follow Peffers et al. (2007) methodology, which is a generalized design science research approach (Gregor and Hevner 2013) The research is motivated by the fact that prevention of cybersecurity exploits requires timely intelligence of threats and vulnerabilities. Our primary objective is to construct a conceptual ontology-based model for representing cybersecurity vulnerability domain. The ontology integrates the vulnerability concepts from both formal sources (such as CVE, NVD) and informal sources such as social media. Further, the ontology could be used to issue cyber alerts by reasoning on the relationships between entities to help security analysts analyze and manage vulnerabilities.

The resources required to move from research objectives to design and development requires knowledge of theory that can be brought to bear in a solution (Peffers et al. 2007). At the design stage, we ensured that the ontological model is grounded in theory. We systematically reviewed the literature to ensure that the mapping of vulnerability constructs with the security domain. We conducted an in-depth review of the research on vulnerability and security ontologies and taxonomies, and software vulnerability literature to identify appropriate techniques and concepts that could be used to inform the design of the ontology. Next, we designed a conceptual ontology to build a formal representation of cybersecurity vulnerability domain. We develop the ontology using Protége software. Next, we, instantiate the ontology with the representative data collected from multiple sources. Finally, we implement the predefined reasoning rules to issue cyber alerts. The details of the application serve as a proof-of-concept for the vulnerability alert system (Peffers et al. 2007). The adequacy of the conceptual model is assessed by checking with domain experts. The utility and usefulness of the alert system are assessed through summative evaluation of the artifacts using both artificial and naturalistic approaches (March and Smith 1995; Venable et al. 2016).

**Conceptual Model of Vulnerability Ontology**

Figure 1 illustrates our conceptual model. The vulnerability ontology consists of five core concepts: vulnerability, threat, product, intelligence, and countermeasures. The ontology complies with the information security standards and taxonomy provided by NIST information security handbook (Bowen et al. 2007), CERT/CC, and CVSS framework. Further, the ontology is enhanced with the concepts pertaining to social media.
NIST defines vulnerability as the weakness in the computational logic which could be exploited by a threat (Bowen et al. 2007). Following CVSS metrics specifications\(^3\), the vulnerability concept consists of nine subconcepts: Attack Vector (i.e., the context by which vulnerability exploitation is possible), Attack Complexity (i.e., conditions under which an attacker can exploit the vulnerability), Privileges Required (i.e., privileges required by an attacker to successfully exploit the vulnerability), User Interaction (i.e., whether user interaction other than that of hacker is required to exploit a vulnerable system), Scope (i.e., whether exploiting the vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component), Impact (i.e., impact on the confidentiality, integrity, and availability of the system), Exploit Code Maturity (i.e., the probability that a vulnerability will be attacked), Remediation Level (i.e., the extend that the vulnerability can be solved), and Report Confidence (i.e., amount of information about the vulnerability that is known). Further, based on the vulnerability information provided by NVD and CVE, we added four more subconcepts: Severity (i.e., the base score ranging from 0 to 10 and qualitative ranking on severity), Exploit (i.e., the number of times a vulnerability is exploited), Vulnerability Type (i.e., the vulnerability type provided by CVE\(^4\)), and Disclosure (i.e., whether the vulnerability has immediate or deferred disclosure, and the date of disclosure).

**Figure 1: Conceptual Vulnerability Management Ontology**

Our Intelligence concept is informed by Twitter attributes (Mittal et al. 2016; Syed et al. 2018). We defined four subconcepts: Content-Type (i.e., whether a tweet text contains alert, patch, exploit, advisory, or root-cause information), Posting time (i.e., first time and the latest time a vulnerability is tweeted); Technical Details (i.e., the URL and Hashtags referred in tweet posting), and Source (i.e., the attributes of the tweet author) (see Syed et al. 2018). The Threat concept consists of three subconcepts: Threat Type (i.e., the cause of vulnerability as specified in Common Weakness Enumeration (CWE) Specifications\(^5\)) and CWE ID. The Product concept consists of four subconcepts: Product Type (i.e., the product classification provided by CVE\(^5\)), Vendor, Version, and Patch Availability. Finally, following Fenz and Ekelhart (2009), the Countermeasure concept has two subconcepts: Control Type (i.e., corrective, detective, and deterrent) and Control (i.e., the measures to mitigate a vulnerability).

**Conclusion**

In this study, we proposed a conceptual ontology for cybersecurity vulnerability management. In doing so, we expect to contribute to information security literature. While prior research has proposed several vulnerability ontologies, those are limited to generic information security concepts. Our ontology integrates cybersecurity vulnerability concepts from several sources including NIST, CVE, NVD, CVSS framework, and social media. Second, we expect to contribute by designing an ontology-based cyberalert system for security analysts to analyze and manage vulnerabilities. Using reasoning rules, the ontology could be useful for reasoning about the relationships between entities to issue cybersecurity alerts. For example, which countermeasure protects the confidentiality of data? Which product vulnerabilities are most shared on

---

\(^3\) [https://www.first.org/cvss/specification-document](https://www.first.org/cvss/specification-document)


\(^5\) [https://nvd.nist.gov/vuln/categories](https://nvd.nist.gov/vuln/categories)

Twitter? Finally, the conceptual ontology sets the grounds for scholars to explore further the effective means to present and integrate vulnerability information from heterogeneous sources.

REFERENCES


