Proceedings of the 51^{st} Hawaii International Conference on System Sciences | 2018

MedDevRisk: Risk Analysis Methodology for Networked Medical Devices

Katherine A. Seale
University of South Alabam
kas908@jagmail.southalabama.edu

J. Todd McDonald
University of South Alabama
jtmcdonald@southalabama.edu

William B. Glisson
University of South Alabam
bglisson@southalabama.edu

J. Harold Pardue
University of South Alabam
hpardue@southalabama.edu

Michael B. Jacobs
University of South Alabam
mjacobs@southalabama.edu

Abstract

The prolific integration of technology into medical environments is continuously generating new attack vectors. This continuous amalgamation of technology into the medical field prompted the idea that risk assessment models can be utilized to identify cyber security vulnerabilities in medical settings. This research presents an initial investigation into the application of risk assessment frame works, i.e., STRIDE, Common Vulnerabilities and Exposures, and a Common Vulnerability Scoring System to identified networked medical devices that are currently employed in an operational medical simulation lab. The contribution of this research is twofold and culminates in a novel proof-of-concept system known as MedDevRisk. First, it demonstrates an approach to incorporating existing threat models into a relational database schema based on Threat-Vulnerability-Asset (TVA) relationships. Second, it provides an initial empirical analysis of the risk associated with networked medical devices along with providing the foundation for future research.

1. Introduction

In today's world, medical devices have transitioned from isolated, stand-alone systems into networked medical devices that are heavily dependent on software. In 2013, Alemzadeh et al. [1] discerned a 70% increase in medical device recalls reported to the United States Food and Drug Administration (FDA) along with a 103% increase in adverse events between 2006 and 2011. The authors also noted that 23% of all medical device recalls were computer-related failures, which include any malfunction of the device's hardware, software, input, output, or battery.

Complicating matters, many medical devices contain and transmit patient data to other devices and network servers [2], which levies the requirement on organizations and manufacturers to protect such data in transit and at rest [2, 3]. The use of software in a networked environment also opens the risk for malware to infect computers that control medical devices [4]. Due to the reliance on medical devices and control software, many new vulnerabilities are being introduced into patient care environments, with consequences of compromise ranging from loss of essential equipment necessary to treat patients, to data integrity being violated [5].

Healthcare organizations that use and manage medical devices face potential problems if outdated or unsupported software is not kept updated on a regular basis. Likewise, knowing which preventative measures to apply so that risk will be mitigated long-term is typically left to the expertise or experience of the network administrators and information technology (IT) staff [2, 5, 6]. Such variability can pose severe problems in safety critical environments, like medical devices, which require constant contact while in service [7]. Current research also indicates that there are risks associated with networked medical devices that could, potentially, lead to further patient injury or even death, if unresolved [8]. This is further highlighted by academic activity investigating ways to compromise surgical environments [9] along with the development of solutions that integrate forensic principles into the design and development of Medical Cyber-Physical Systems [10].

In order to address the need for actionable threat assessment criteria for healthcare organizations to govern the use of medical devices on their networks, this research poses a novel framework known as *MedDevRisk* with the following key features: 1) use of a relational data model capturing medical device threats, assets, and vulnerabilities, 2) use of conventional risk assessment standards, and 3) data from a real-world health-related organization. This framework provides a relational integration of network device information with their attendant security threats

URI: http://hdl.handle.net/10125/50302
ISBN: 978-0-9981331-1-9

and potential remediation steps. The consolidation of these data provide underlying relationships which can answer risk assessment questions pertinent to both lower-level administrators and higher level managers that make decisions on money and resources.

The remainder of the paper is structured in the following manner. Section two provides background on risk modeling along with relevant related work. Section three elaborates on the fundamental motivations and assumptions associated with the development methodology. Section four highlights key features of the framework implementation and section five provides conclusions and plans for future work.

2. Background and Related Work

The continued amalgamation of technology into the medical field raises concerns about risk and how that risk is perceived in a medical context [9, 11, 12]. Pairing the growing concerns about risk with the impact that residual data appears to have, in legal context, serves to escalate interest in risk mitigation solutions [13-15]. Hence, this interest has prompted previous work in databases and proposed frameworks [16, 17] for assessing risk.

2.1. Governing Organizations and Law

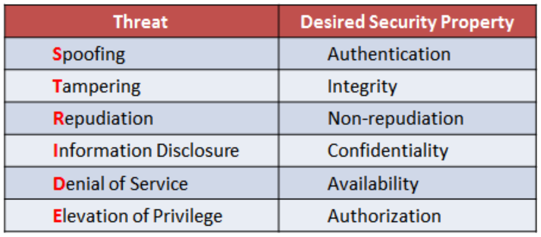
The U.S. Food and Drug Administration (FDA) is responsible for the protection of the public's health by regulating the medical device safety and security [18]. In 2013, the FDA released the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices concerning how manufacturers and the healthcare industry should approach cybersecurity in medical devices [18]. The FDA guidelines require lists of cybersecurity risks, controls, countermeasures, and instructions for medical devices from the manufacturers. In the United States, the healthcare industry must implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which mandates the privacy of protected health information of patients by covering information privacy, information security, and standardization of data [19]. Though most of the healthcare industry already has problems ensuring good practices, there are information security issues, such as vulnerable networks, that frequently remain overlooked [19].

2.2. Risk Assessment

The tacit understanding of risk is the possibility that a vulnerability will be exploited by a threat to cause damage to an asset [20]. Risk is, commonly, calculated as a combination of the probability that an adverse event will occur and the impact (severity), if the event actually does occur. Overall, the entire objective of security is essentially risk prevention through the removal of vulnerabilities and preventing threat agents from endangering assets [20]. Hence, risk assessment and analysis encompass methods for the categorization and distribution of information concerning the security risks related to the organization's infrastructure [21]. A risk assessment, as defined by the National Institute of Standards and Technology (NIST), is a "process of identifying, estimating, and prioritizing information security risks" [22, 23]. Brown [24] agrees and expands this definition to include cultivating mitigation strategies. Gerber's research [25] concluded that after completing a risk analysis, security controls can effectively decrease risks. Ultimately, risk analysis should result in greater protection for technology-related assets and data. Yue et al. [26] further state that security risk management has developed into a crucial obligation for IT managers and staff. Thus, the *MedDevRisk* framework derives its inspiration from the need to provide relevant risk assessment for health and health-care related organizations.

2.3. Conventional Risk Models

MedDevRisk leverages several nomenclatures promoted by Microsoft and MITRE that are in common use in government and industry. These include the STRIDE threat model, Common Vulnerabilities and Exposures (CVE), and the Common Vulnerability Scoring System (CVSS). The STRIDE threat model (Figure 1) is a mnemonic that categorizes threats into spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges [27, 28]. According to Shostack [28], each of the six threat classifications are attack methods that could exploit the components of information assurance and each has an attendant security property that would address the threat. The STRIDE model is used extensively as part of Microsoft's Security Development Lifecycle (SDL) to help define the attack surface [27, 28].



Threat	Desired Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Figure 1. STRIDE threat model.

CVE is a public dictionary created by the MITRE Corporation that encompasses a collection of known information security vulnerabilities and exposures with the purpose of offering common identifiers for cybersecurity threats [29]. CVSS is a risk assessment framework for modeling cybersecurity vulnerabilities quantitatively, in addition to providing impact scores based on three metric groups: base, temporal, and environmental exposures [30]. The CVSS model is presented in Figure 2. These standard nomenclatures and models provide a real-world context for how the *MedDevRisk* framework formulates and presents risk assessment evaluations.

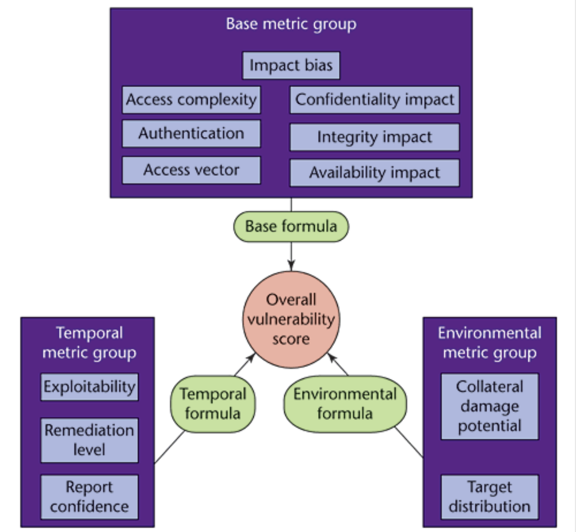


Figure 2. CVSS metric groups [30].

2.4. MeDRa

One of the few published frameworks that evaluates medical device risk is documented by Brown [24]. His electronic medical devices risk assessment tool (MeDRa) is healthcare environment centric. MeDRa creates a risk profile for each device classification and each potential device setting that is connected to an intranet. Device assessment in MeDRa is based on clinical environment usage. For example, a medical device that is frequently used in large hospitals by well-trained staff has a lower risk value than the same medical device that is not commonly used in smaller environments [21]. The risk referenced in Brown's research is based on the Australian Standard As/NzS4360, statistical analysis, and risk observations as defined by healthcare professionals. In primary contrast to our proposed framework, MeDRa creates a risk assessment for each medical device based on user responses from a series of yes/no questions concerning organizational communication and culture, staff skills and knowledge, device operation and use, and device maintenance. Users that are considered in the published evaluation of MeDRa include nurses, allied health professionals, consultants, and other medical staff. The MeDRa tool outputs a medical device risk assessment report and a mitigation plan as raw data in Microsoft Excel.

Brown's [24] major finding focused on how the use of the risk assessments, compiled from feedback from healthcare professionals and analyzed using statistical methods, compared to the Australian Risk Standard. The official risk ratings for most devices are defined as very low, whereas the results from the MeDRa tool and analysis proved that the devices could potentially have a higher risk rating. According to Brown [24], the major limitation of the MeDRa study is that risks identified by healthcare professionals could be biased [24]. In contrast, the *MedDevRisk* framework utilizes CVE and CVSS nomenclature as the qualitative basis for assigning vulnerability exposures and scores.

While there is research in the broader area of risk assessments that utilize relational databases, minimal research exists that successfully integrates multiple risk models into a database framework using real-world data. The *MedDevRisk* framework brings these key features together into a unified context.

3. Methodology

In order to investigate the key features of the *MedDevRisk* framework, this research conducted a case study as defined by Yin [31] and discussed by Oates [32]. The following approach was implemented to identify real-world risks faced by medical and health organizations based on their networked medical devices.

1. **Schema Selection:** A database schema was selected from prior work, modified to utilize several security nomenclatures and implemented.
2. **Normalization:** The selected database schema was then examined for normalization.
3. **Data Acquisition:** A list of medical devices was acquired from the College of Nursing Human-Patient Simulation Unit at the University of South Alabama (USA).
4. **Schema Adaptation:** The database was examined for appropriate tables, columns, rows, and data fields. It was then expanded, where necessary.
5. **Threat Model Categorization**: Threat models were applied to categorize the data. This paper reports only the STRIDE model integration.
6. **Asset Data Entry**: The data acquired from the simulation lab was entered into the database to populate assets.
7. **Vulnerability Categorization:** The models were then applied to identify vulnerabilities.

8. **View Generation:** The database was then modified to create schema views to support multiple levels of query.
9. **Vulnerability Data Entry:** The vulnerabilities were then input into the database.
10. **Query Development:** Queries were then developed to highlight vulnerabilities that targeted two managerial perspectives: low-level IT managers of technology and high-level decision makers like CTOs, CISOs, and CIOs.
11. **Result Analysis:** The queries were executed and the results were collected for analysis.

Figure 3 diagrams the flow of the *MedDevRisk* framework and its components. More specifically, the flow diagram illustrates how the database schemas, threat models, the case study data collected from the simulation unit and any additional research ties into the flow of the new database and its outputs. As noted in the data relationships portion of Figure 3, the STRIDE threat model and use of the National Vulnerability Database (NVD) risk data may be included as part of the inclusion of existing threat modelling techniques into the database.

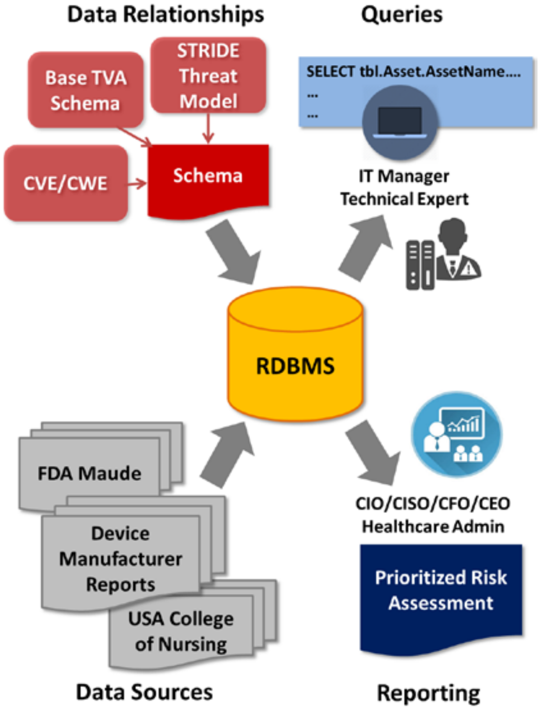


Figure 3. *MedDevRisk* framework.

3.1. Schema Selection and Normalization

The *MedDevRisk* relational framework builds upon the work of Pardue et al. [16], which uses a database-driven approach to assess risk. This work implemented a threat-vulnerability-asset (TVA) model using healthcare-related threats and countermeasures. As a proof-of-concept, the authors populated a relational database with hypothetical data involving security vulnerabilities in healthcare.

Pardue et al.'s [16] schema, as seen in Figure 4, was based on the TVA model and included entities such as threat, vulnerability, asset, control, threat source, cause, and domain. They organized threats by ranking how much risk is associated with a particular threat. They extracted data through the use of the structured query language (SQL) to manipulate the data and execute queries to identify threats, controls and countermeasures. As a proof-of-concept model, their solution formed pertinent risk assessment outcomes using query capabilities. In Cerkovnik's unpublished thesis work [17], the TVA-based approach proposed by Pardue et al. [16] was investigated as a potential framework for integrating various threat and vulnerability data associated with medical devices. This study collected a small data sample from various sources including the Manufacturer and User Facility Device Experience (MAUDE) database [33], the FDA Medical Product Safety Network (MedSun) [34], Shodan [35], and FDA's 510(k) database Pre-Market Notification database [36].

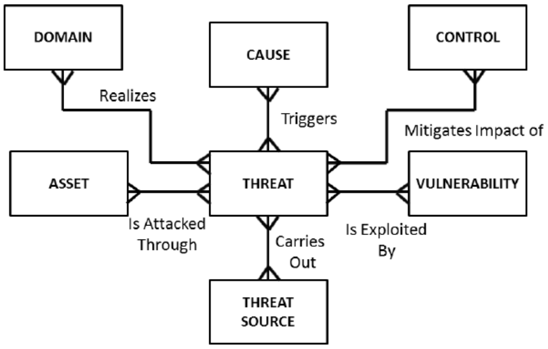


Figure 4. Base TVA schema [15].

Although Cerkovnik's [17] work provided an experimental basis for how to tailor the TVA approach for specific medical terminology and categories, the resulting schema was independent from the base TVA relationships. As our contribution, the *MedDevRisk* framework and database (seen in Figure 5) provides a unifying schema with new tables, fields, underlying views, underlying queries, and context-specific relationships that captures a broader set of features for analyzing risk in medical devices. For instance, two new tables were added to the initial schema in order to normalize the database and include new categories of medical devices, i.e. *tblDevice* and *tblInventory*.

The new *tblDevice* table is connected to the risk assessment database using a one-to-many relationship to *tblAsset.* Because the attributes in the table *tblAsset* is composed of general terms used for cyber assets or devices (e.g. an operating system, smart phone, or electronic patient health record), “Medical Devices” was inserted, as a new item, into the *tblAsset*. The `AssetID` field is used to categorize the types of devices, whether it is the server, router, laptop, or medical device.

The device table, *tblDevice*, was created to hold cyber asset data types so that multiple devices could be associated with any type of asset. For instance, an electrocardiogram and a defibrillator are both medical device assets, but would be listed as separate devices in the *tblDevice* table. The table *tblDevice* contains attributes related to the types of the devices and the descriptions of those devices.

In addition to *tblDevice*, a new table was created that is designed to contain the location and the actual device’s specific information for individual devices called *tblInventory*. This table is used for each device that is on-site in the facility and can account for multiple devices of the same type of device. The idea is that each facility or hospital could have more than one of the same type of device, such as multiple laptops or multiple patient monitors.

3.2. Data Acquisition

To validate and exercise the enhanced relational schema, an experimental case study was performed based on the collection of real-world data from the USA’s School of Nursing, Human–Patient Simulation Program. The Simulation Unit contains high-quality medical simulators and devices used for realistic training in healthcare clinical scenarios. These scenarios are used to train future doctors, nurses, and healthcare professionals. They are also routinely used to assist with continuing education efforts for practitioners.

The USA Simulation Unit provided a list of networked medical devices. The list of medical devices was, initially, evaluated and three networked medical devices were input into the relational database model. The devices selected include LifeSync Wireless Electrocardiogram (ECG) Systems, Physio-Control LIFEPAK Defibrillators, and Laerdal VitalSim Vital Signs Simulators. The LifeSync Wireless Electrocardiogram (ECG) System transmits ECG signals and patient data wirelessly from the patient to the ECG monitor. The LifeSync Wireless System uses “a radio-frequency signal transmitter and receiver of diagnostic electrocardiographic physiological signals which are displayed on the ECG monitors of various manufacturers’ systems” [37]. A Physio-Control LIFEPAK Defibrillator is a wireless acute cardiac care response system in a single, portable device. Each of medical device type in the device list has at least one model number and may be listed on the list more than once (i.e., multiple devices in inventory).

3.3. Schema Adaptation

Based on the starting TVA schema, three specific adaptations were chosen that extend the core entities based on their relevance to risk assessment and availability of current data: 1) **Threat:** Applied SQL views using STRIDE; 2) **Vulnerability:** Applied SQL views using NVD (CVE/CVSS/CWE); and 3) **Asset:** Modified database to include device-specific data. Existing threat and vulnerability frameworks were integrated into the relational database model, including the STRIDE [27] threat model, Common Vulnerabilities and Exposures (CVE) [29], Common Weakness Enumeration (CWE), and Common Vulnerability Scoring System (CVSS) [30].

The STRIDE model [27] is the threat categorization model applied towards the threat component of the TVA-based relational database. CVE [29], which is a cybersecurity vulnerability identifier, and CVSS [30], which is a risk assessment of the CVE cybersecurity vulnerabilities, are the vulnerability threat modeling techniques and resources applied to the vulnerability component of the database. The National Vulnerability Database (NVD) provides the CVSS for CVE entries. To account for assets in the TVA model, the asset component of the relational database was expanded by adding the device and inventory tables. The table tblDevice plays another role as well. Each CVE and CVSS reflects the vulnerabilities and risk score of medical devices, this information is recorded in *tblDevice*.

Device vulnerabilities were identified using reports, manuals, and U.S. Government resources such as FDA MedSun reports [34] and the National Vulnerability Database [38]. To reduce complexity in the database, SQL views are used to pull the attributes needed from tables to model threats. This allows the examination of the data through a diverse threat model lens.

3.4. Threat Model Categorization

In order to support threat assessment, each category of the STRIDE threat model was researched in order to assign threat actions appropriately. Each threat was classified by two STRIDE categories based directly on the `ThreatCategoryID` and the `ThreatAction`. Two primary threat actions that were used include 1) “Disclose Patient Health Information”, which is directly related to information disclosure in STRIDE, and 2) “Manipulate Patient Health Information”, which is tampering in STRIDE.

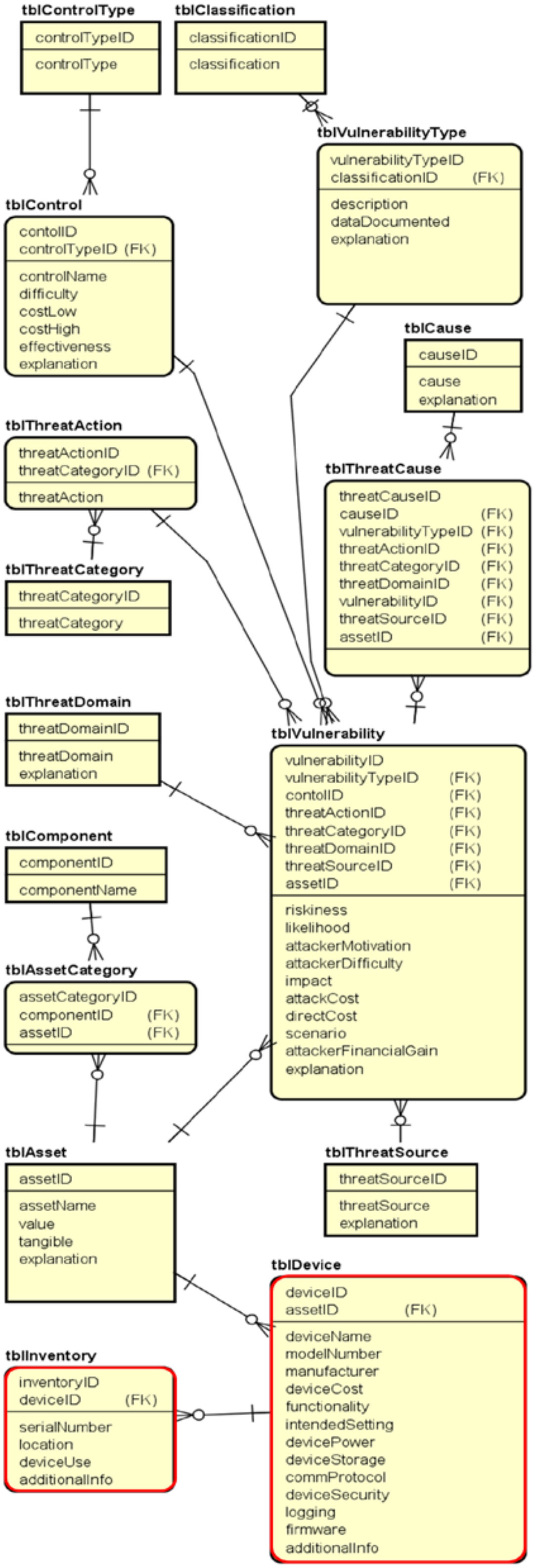
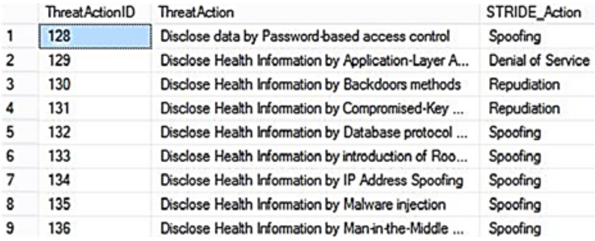


Figure 5. *MedDevRisk* database schema.

STRIDE categories were created based on attacker motivation and threat actions: 1) `STRIDE_Motivation` relates what happened to the data or the motivation for the threat, i.e. whether disclosure or data manipulation was in view, and 2) `STRIDE_Action` relates how the threat happened or what action occurred, e.g. Man-in-the-Middle attack or IP Spoofing. One type of threat action (SQL Injection attacks) covered more than two STRIDE categories. This attack affects Spoofing, Tampering, Repudiation, Information Disclosure, and Elevation of Privilege [39]. The attacker could potentially steal an identity, remove logs, change their privileges, or perform data leakage and alteration. Figure 6 provides a partial view of STRIDE categories.



	ThreatActionID	ThreatAction	STRIDE_Action
1	128	Disclose data by Password-based access control	Spoofing
2	129	Disclose Health Information by Application-Layer A...	Denial of Service
3	130	Disclose Health Information by Backdoors methods	Repudiation
4	131	Disclose Health Information by Compromised-Key ...	Repudiation
5	132	Disclose Health Information by Database protocol ...	Spoofing
6	133	Disclose Health Information by introduction of Roo...	Spoofing
7	134	Disclose Health Information by IP Address Spoofing	Spoofing
8	135	Disclose Health Information by Malware injection	Spoofing
9	136	Disclose Health Information by Man-in-the-Middle ...	Spoofing

Figure 6. STRIDE view mapping.

3.5. Asset Data Entry

A SQL Server database was used to implement the *MedDevRisk* schema, associated views, and queries. The database was populated with the network medical devices from the Human-Patient Simulation Unit. The list contains ten (10) different types of medical devices, a total of twenty-seven (27) different models of the types of medical devices collectively, and a total of forty-five (45) medical devices in inventory. Of the ten (10) different types of medical devices, eight (8) devices are high-fidelity or medium-fidelity medical simulators. High-fidelity medical device examples include the CAE iStan Adult Simulators and the Gaumard Noelle Birthing Simulators, which are full-sized, wireless adult medical mannequins. The other two types of medical devices are electrocardiograms and defibrillators.

Device-specific data for *tblDevice* was collected using manufacturer reports, user manuals, and technical specification sheets issued by the manufacturer. The collected data was then matched to appropriate attributes in *tblDevice* for each device. Rows were inserted into *tblInventory* for each item by serial number. Identified vulnerabilities and CVSS Metric values from NVD Vulnerability Summaries for CVEs for each device were also matched to the *tblVulnerability* attributes [30, 38].

3.6. Vulnerability Categorization & Entry

In addition to device manuals, user guides, and technical specifications released by the manufacturer, the following online resources were utilized to collect device-specific data and vulnerabilities: FDA MAUDE, FDA Medical Product Safety Network (FDA MedSun), Shodan, FDA's 510(k) Pre-Market Notification database, FDA Recalls, and the NVD, which contains information for CVE, CVSS, and CWE. Vulnerability data was inserted into *tblVulnerability* for each device for a total of 31 vulnerabilities. The `AssetID` for Medical Devices and the `ThreatDomainID` for Healthcare was used for all vulnerability entries.

For each vulnerability, at least one potential threat action was identified. For each threat action, potential controls were identified that could be implemented as mitigation strategies. Each combination of vulnerability type, threat action, and control received its own vulnerability entry in *tblVulnerability*. Additionally, some vulnerabilities were identified that could be exploited by different threat sources: a human-deliberate insider, human-deliberate outsider, or human unintentional insider. If a vulnerability had more than one threat source, it was listed multiple times.

Often, one attribute affected another. For example, if a human-unintentional insider exploits the Laerdal VitalSim Vital Signs Simulator's vulnerability by disclosing health information through the extraction of data through a USB drive, the main control is identified as educating the Medical Staff about the severity, consequences, fines and penalties related to a data breach. However, if the same vulnerability is exploited by a human-deliberate insider, by using malware to attack the device through a USB drive, then more evasive controls should be implemented, such as applying security patches and software updates.

3.7. View Generation

SQL VIEWs were developed to extract relevant data from *tblVulnerability* and to provide renaming of attributes to match our acquired CVE, CVSS, and CWE data. Essentially, the same database data is examined differently using multiple vulnerability and risk assessment frameworks. Similarly to the data insertion process, the database attributes were translated into NVD-based attributes that focused on CVE and CVSS values.

The National Vulnerability Database (NVD) provides the CVSS for CVE entries and includes the CWE into each Vulnerability Summary for the CVE. The NVD Vulnerability Summary for a CVE was applied to the database using SQL VIEWs. CVEs were then searched for that included networked medical devices in the vulnerability database using search terms like medicine, medical device, insulin pump, infusion pump, defibrillator, and pacemaker.

As a result, we found a total of eight (8) CVEs for infusion pumps (e.g. Hospira LifeCare PCA Infusion System), five (5) CVEs for insulin pumps (e.g. Johnson & Johnson Animas OneTouch Ping and Medtronic Paradigm wireless insulin pump), two (2) CVEs for pacemakers (pacemaker management system), and two (2) CVEs for defibrillators (e.g. ZOLL Defibrillator).

Examining multiple CVE examples online allowed for the translation of the CVE data into our database from metrics into table attributes. The following vulnerability attributes were identified from the CVE data: `Vulnerability Type ID`, `Threat Action ID`, `Threat Domain ID`, `Threat Source ID`, and `Scenario`.

Relevant information from the Scenario attribute was included in *tblVulnerability* as a baseline. ControlIDs were then selected based on the identified vulnerabilities and threats. For instance, countermeasures were identified that should be implemented to aid in prevention of a future application-layer or denial of service attacks, such as inspecting database traffic and implementing network precautions.

CVSS data in the NVD entry were used to identify the impact values for the device and decided how to implement the values in *tblVulnerability* in the database. Based on the CVSS data in the Impact section of the NVD entry, the following *tblVulnerability* attributes were identified: `Riskiness`, `Likelihood`, `Attacker Motivation`, `Attack Difficulty`, `Impact`, and `Explanation`. The `Explanation` attributes contains additional descriptions of impact metrics such as `Access Vector`, `Access Complexity`, `Authentication`, and `Impact Type`.

After determining vulnerability values to insert into the database for testing, SQL INSERT queries were written to insert the vulnerability data into *tblVulnerability*. Because *tblVulnerability* does not contain device-specific attributes and only contains an `AssetID`, the device's name, manufacturer, and model number(s) that apply to the vulnerability in the `Scenario` attribute were included. To link the `Vulnerability ID` to a `Device ID`, a LIKE expression is used in the WHERE clause to match the `Device Name`, `Manufacturer`, and `Model Number` to the vulnerability.

3.8. Query Development

SQL queries were written to retrieve the case study networked medical devices and highlight each networked medical device's vulnerabilities using the TVA Model, the STRIDE Threat Model, and the NVD Vulnerability Summary for CVEs. For the STRIDE model and NVD framework, SQL VIEWs were utilized to select data.

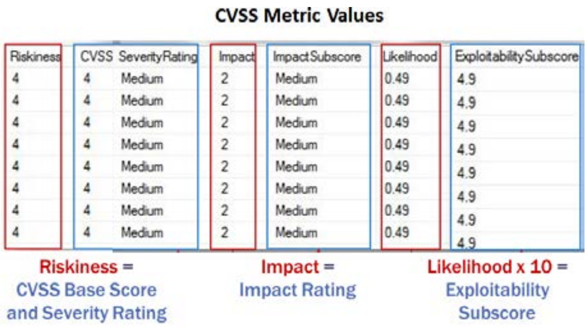
An SQL query that focuses on the STRIDE categories was developed to highlight the vulnerabilities of our case study medical devices. STRIDE was implemented by selecting the `Threat Action ID` first, the `STRIDE Action` categories second, the `STRIDE Motivation` categories third, the description of the `Threat Action` fourth, and the device-related attributes fifth. Then, additional attributes from *tblVulnerability* like riskiness, likelihood and impact were included in the query.

4. MedDevRisk Result Analysis

The research successfully identified existing relational database-driven system research, originally proposed by Pardue et al. [16], that could be modified and expanded for the purposes of integrating a prioritized risk mitigation strategy for networked medical devices. In the expanded system, attributes were selected using a ranking methodology to organize the threats, to assess the risk of a threat, and prioritize resources as part of the risk assessment. Threat risk modeling and vulnerability frameworks were successfully incorporated into the risk assessment by using our STRIDE and CVE VIEWs. The results of the implementation for the STRIDE view are presented in Figure 6.

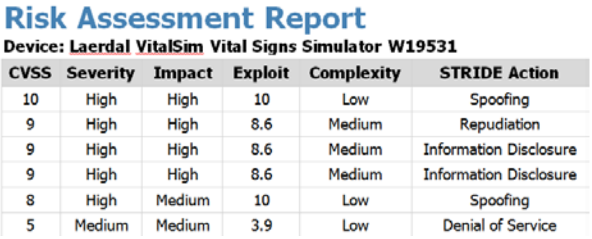
A proof-of-concept case-study, using real-world data from a practicing medical simulation training unit was successfully implemented using the developed model. The reports generated, as a result of the case study, contain a ranked list of medical devices and associated vulnerabilities. Specialized SQL queries and views were initially developed to conveniently access information from multiple perspectives and then they were implemented in reports. Figure 7 provides a sample view of the mapping between NVD reported vulnerability scores and database specific fields where risk score, impact, and likelihood are tied together.

The *MedDevRisk* framework provides ability to directly tie reported vulnerability risk scores from CVSS rankings directly into reporting features. The SQL queries for the Risk Assessment reports focus on a list of devices with each device's CVSS Metrics, vulnerability data, and STRIDE categorizations of the related threat actions. The main Risk Assessment Report combines all threat risk modeling and vulnerability frameworks that were incorporated into the database. A Risk Assessment Report is provided in Figure 8.



Riskiness	CVSS	SeverityRating	Impact	ImpactSubscore	Likelihood	ExploitabilitySubscore
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
4	4	Medium	2	Medium	0.49	4.9
						4.9

Figure 7. Database values to NVD values.



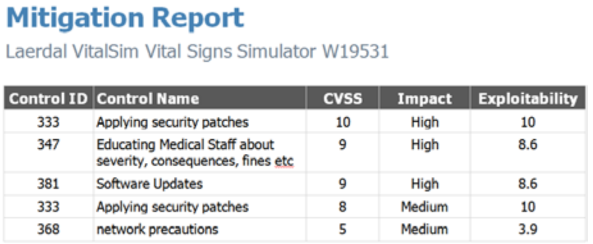
Risk Assessment Report

Device: Laerdal VitalSim Vital Signs Simulator W19531

CVSS	Severity	Impact	Exploit	Complexity	STRIDE Action
10	High	High	10	Low	Spoofing
9	High	High	8.6	Medium	Repudiation
9	High	High	8.6	Medium	Information Disclosure
9	High	High	8.6	Medium	Information Disclosure
8	High	Medium	10	Low	Spoofing
5	Medium	Medium	3.9	Low	Denial of Service

Figure 8. *MedDevRisk* risk assessment report.

The SQL queries for the Mitigation Report contain a list of ranked controls by number of vulnerabilities, a list of medical devices matched to their controls, and a list of controls and devices ranked by CVSS Metrics to determine the order of implementation. The final Mitigation Report is organized by device and contains ranked controls per device by CVSS Metrics. Therefore, a total of five reports was created. An example of a Mitigation report is provided in Figure 9.



Mitigation Report

Laerdal VitalSim Vital Signs Simulator W19531

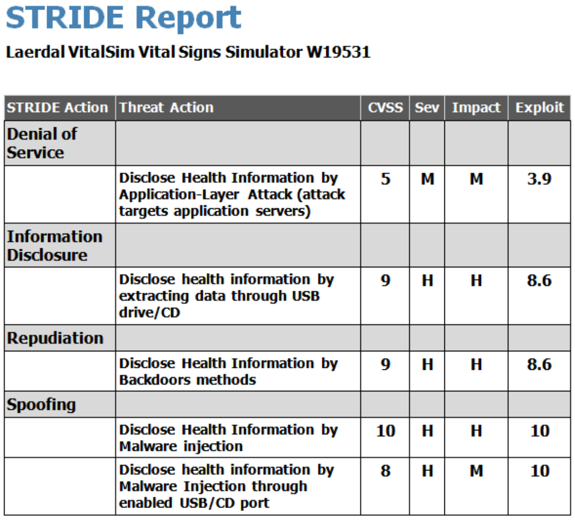
Control ID	Control Name	CVSS	Impact	Exploitability
333	Applying security patches	10	High	10
347	Educating Medical Staff about severity, consequences, fines etc	9	High	8.6
381	Software Updates	9	High	8.6
333	Applying security patches	8	Medium	10
368	network precautions	5	Medium	3.9

Figure 9. *MedDevRisk* mitigation report.

Three specialized Risk Assessment Reports were then created that reflect the TVA Model, STRIDE Model, and NVD Summary for CVEs were created during the course of this research. An example of a STRIDE report is available in Figure 10. The report presents each device on a separate page, provides the STRIDE Motivation, the STRIDE Action, ranked vulnerability risk, NVD-Based and STRIDE Data

5. Conclusions and Future Work

The unrelenting amalgamation of technology into healthcare organizations creates an environment that is conducive to an attack. Hence, the risk that technology is presenting to medical situations is generating interest in industry and academia.



STRIDE Report

Laerdal VitalSim Vital Signs Simulator W19531

STRIDE Action	Threat Action	CVSS	Sev	Impact	Exploit
Denial of Service					
	Disclose Health Information by Application-Layer Attack (attack targets application servers)	5	M	M	3.9
Information Disclosure					
	Disclose health information by extracting data through USB drive/CD	9	H	H	8.6
Repudiation					
	Disclose Health Information by Backdoors methods	9	H	H	8.6
Spoofing					
	Disclose Health Information by Malware injection	10	H	H	10
	Disclose health information by Malware Injection through enabled USB/CD port	8	H	M	10

Figure 10. *MedDevRisk* STRIDE report.

The overall results of the case study support the idea that relational data models can be utilized for medical devices to generate actionable threat assessment criteria for healthcare organizations. The results of the technical aspects of this research indicate that it is possible to successfully integrate relational data models with threat vulnerability asset associations. The implementation of the *MedDevRisk* model with data from an operational medical simulation training unit demonstrates that the model can be used to generate actionable threat assessment criteria for healthcare organizations.

Future research in this area will extend the existing research to include larger data samples and more diverse medical facilities. It will also explore automated data collection from static documents or web-based reports, schemas that acquire data in real–time from multiple sources, along with the incorporation of more diverse attack models.

6. Acknowledgements

This material is based in part upon work supported by the National Science Foundation under grant DUE-1241675.

7. References

[1] H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk, and J. Raman, "Analysis of Safety-Critical Computer Failures in Medical Devices," *IEEE Security & Privacy*, vol. 11, pp. 14-26, 2013.

[2] V. Cehlot and E. B. Sloane, "Ensuring patient safety in wireless medical device networks," *Computer,* vol. 39, pp. 54-60, 2006.

[3] U.S. Food and Drug Administration (FDA). (2013, May 1). *FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks.* Available: http://www.fda.gov/medicaldevices/safety

[4] D. E. Gobuty, "Defending medical information systems against malicious software," *International Congress Series,* vol. 1268, pp. 96-107, 2004/06/01/ 2004.

[5] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Commun. ACM,* vol. 56, pp. 35-37, 2013.

[6] U.S. Food and Drug Administration (FDA). (2013). *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*. Available: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

[7] J. C. Knight, "Safety critical systems: challenges and directions," in *Proceedings of the 24th International Conference on Software Engineering. ICSE 2002*, 2002, pp. 547-550.

[8] S. R. Rakitin, "Networked medical devices: essential collaboration for improved safety," *Biomedical instrumentation & technology*, vol. 43, pp. 332-338, 2009.

[9] M. Van Devender, W. Glisson, M. Campbell, and M. Finan, "Identifying Opportunities to Compromise Medical Devices," in *Americas Conference on Information Systems*, San Diego, 2016.

[10] G. Grispos, W. B. Glisson, and K.-K. R. Choo, "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 2017, pp. 108-113.

[11] P. Luckett, J. McDonald, and W. Glisson, "Attack-Graph Threat Modeling Assessment of Ambulatory Medical Devices," in *50th Hawaii International Conference on System Sciences*, Waikoloa, HI 2017.

[12] W. B. Glisson, T. Andel, T. McDonald, M. Jacobs, M. Campbell, and J. Mayr, "Compromising a Medical Mannequin," in *Americas Conference on Information Systems (AMCIS)*, Puerto Rico, 2015.

[13] M. S. V. Devender, W. B. Glisson, R. Benton, and G. Grispos, "Understanding De-identification of Healthcare Big Data," in *Twenty-third Americas Conference on Information Systems*, Boston, 2017.

[14] K. Berman, W. B. Glisson, and L. M. Glisson, "Investigating the Impact of Global Positioning System (GPS) Evidence in Court Cases," in *Hawaii International Conference on System Sciences (HICSS-48)*, Kauai, Hawaii 2015.

[15] J. McMillan, W. B. Glisson, and M. Bromby, "Investigating the Increase in Mobile Phone Evidence in Criminal Activities," in *Hawaii International Conference on System Sciences (HICSS-46)*, Wailea, Hawaii, 2013.

[16] J. Pardue, J. Landry, and S. Purawat, "A Database-driven Model for Risk Assessment," 2014.

[17] J. Cerkovnik, "Managing Vulnerabilities and Risk in Networked Medical Devices," MSc, School of Computing, University of South Alabama, 2015.

[18] US Food and Drug Administration, "Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and food and drug administration staff," *Retrieved May,* vol. 1, p. 2014, 2013.

[19] J. Collmann, D. Lambert, M. Brummett, D. DeFord, J. Coleman, T. Cooper, K. McCall, D. Seymour, C. Alberts, and A. Dorofee, "Beyond good practice: why HIPAA only addresses part of the data security problem," in *International Congress Series*, 2004, pp. 113-118.

[20] J. M. Stewart, M. Chapple, and D. Gibson, *CISSP: Certified Information Systems Security Professional Study Guide*: John Wiley & Sons, 2012.

[21] Z. I. Saleh, H. Refai, and A. Mashhour, "Proposed framework for security risk assessment," *Journal of Information Security,* vol. 2, p. 85, 2011.

[22] E. Aroms, "NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems," 2012.

[23] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," National Institute of Standards and Technology2012.

[24] A. S. Brown, "Identifying risks using a new assessment tool: the missing piece of the jigsaw in medical device risk assessment," *Clinical Risk,* vol. 13, pp. 56-59, 2007.

[25] M. Gerber and R. Von Solms, "From risk analysis to security requirements," *Computers & Security,* vol. 20, pp. 577-584, 2001.

[26] W. T. Yue, M. Çakanyıldırım, Y. U. Ryu, and D. Liu, "Network externalities, layered protection and IT security risk management," *Decision Support Systems,* vol. 44, pp. 1-16, 2007.

[27] Microsoft. (2005, 06/13). *The STRIDE Threat Model*. Available: https://msdn.microsoft.com/en-us/default.aspx

[28] A. Shostack, *Threat modeling: Designing for security*: John Wiley & Sons, 2014.

[29] MITRE. (2017, 06/13). *Common Vulnerabilities and Exposures*. Available: http://cve.mitre.org/

[30] P. Mell, K. Scarfone, and S. Romanosky. (06/13). *A Complete Guide to the Common Vulnerability Scoring System*. Available: https://www.first.org/cvss/v2/guide

[31] R. K. Yin, *Case Study Research: Design and Methods*, Third Edition ed. London: Sage Publications, Inc, 2002.

[32] B. Oates, *Researching Information Systems and Computing*. London: Sage Publications, 2006.

[33] U.S. Food and Drug Administration. (2017, 06/13). *MAUDE - Manufacturer and User Facility Device Experience*. Available: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Search.cfm

[34] U.S. Food and Drug Administration. (2017, 06/13). *MedSun: Medical Product Safety Network*. Available: https://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/default.htm?source=govdelivery

[35] Shodan. (06/13). *Shodan is the world's first search engine for Internet-connected devices.* Available: https://www.shodan.io/

[36] U.S. Food and Drug Administration. (2017, 06/13). *510(k) Premarket Notification*. Available: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/pmn.cfm

[37] R. Jugo, "510(k) Summary GMPlWireless Medicine LifeSyncTM System " 2003.

[38] National Institute of Standards and Technology. (06/14). *National Vulnerability Database*. Available: https://nvd.nist.gov/

[39] Open Web Application Security Project. (2016, 06/14). *SQL Injection*. Available: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project