Western Michigan University
ScholarWorks at WMU

Transactions of the International Conference on Health Information Technology Advancement

Center for Health Information Technology Advancement

10-2013

A Threat Table Based Approach to Telemedicine Security

John C. Pendergrass
University of Illinois at Chicago, john.cecil@gmail.com

Karen Heart
University of Illinois at Chicago, kheart2@uic.edu

C. Ranganathan
University of Illinois at Chicago, ranga@uic.edu

V.N. Venkatakrishnan
University of Illinois at Chicago, venkat@uic.edu

WMU ScholarWorks Citation

Pendergrass, John C.; Heart, Karen; Ranganathan, C.; and Venkatakrishnan, V.N., "A Threat Table Based Approach to Telemedicine Security" (2013). *Transactions of the International Conference on Health Information Technology Advancement*. 38.
http://scholarworks.wmich.edu/ichita_transactions/38

A Threat Table Based Approach to Telemedicine Security[i]

John C. Pendergrass
University of Illinois at Chicago
University Hall, Room 2404
Chicago, IL 60607-7124
312-996-2672
jpender2@uic.edu

Karen Heart
University of Illinois at Chicago
851 S. Morgan, Room 1120 SEO
Chicago, IL 60607-7053
312-996-3422
kheart2@uic.edu

C. Ranganathan
University of Illinois at Chicago
University Hall, Room 2404
Chicago, IL 60607-7124
312-996-2672
ranga@uic.edu

V.N. Venkatakrishnan
University of Illinois at Chicago
851 S. Morgan, Room 1120 SEO
Chicago, IL 60607-7053
312-996-3422
venkat@uic.edu

Abstract: Information security within healthcare is paramount and telemedicine applications present unique security challenges. Technology is giving rise to new and advanced telemedicine applications and understanding the security threats to these applications is needed to ensure, among other things, the privacy of patient information. This paper presents a high level analysis of a telemedicine application in order to better understand the security threats to this unique and vulnerable environment. This risk analysis is performed using the concept of threat tables. This case study focuses on the capture and representation of salient security threats in telemedicine. To analyze the security threats to an application, we present a threat modeling framework utilizing a table driven approach. Our analysis reveals that even in a highly controlled environment with static locations, the security risks posed by telemedicine applications are significant, and that using a threat table approach provides an easy-to-use and effective method for managing these threats.

INTRODUCTION

Advances in healthcare technology, like telemedicine, will likely improve quality of care, reduce cost, and advance medicine in general. However, with technological advances comes increased information security and privacy risks. The digitization of health records, data transmission over public networks, and an assortment of client side devices increases the opportunity for privacy invasion and medical identity theft, costing patients, providers, and payers. As the very nature of telemedicine is vulnerable to security breaches, the security of personal health information in telemedicine applications is paramount.

This work-in-progress study seeks to analyze information security threats in telemedicine applications using a threat table model developed by the authors. Drawing on various techniques from the research literature, we construct a threat table that lists security vulnerabilities and potential remedies for various threats to a system or software application. We feel that this threat table approach to modeling will prove a valuable addition to risk analysis, system analysis, or audit of any information system. To examine its usefulness, we analyzed a telemedicine application used at a Midwestern college of medicine (CoM) to provide remote clinical care for hepatitis-C and HIV patients at state penitentiaries. The CoM system has one provider location serving 22 remote locations within the state.

BACKGROUND

Telemedicine

Telemedicine is a technology-based method to provide clinical healthcare at a distance. It is considered a sub-category of telehealth, which is, generally, the remote delivery of health related services. Technological advances and the digitization of data have given rise to numerous telehealth applications. Such is the usefulness of modern telehealth that the federal government created the Office for the Advancement of Telehealth, part of the Office of Rural Health Policy within the U.S. Department of Health and Human Services, to promote the use of telehealth technologies for health care delivery, education, and health information services.

Health Information Security

With forthcoming legislation that became HIPAA, one of the first definitive works on threats to information in healthcare came in response to a request in October 1995 from the U.S. National Library of Medicine (NLM) by the Computer Science and Telecommunications Board who produced the report, For the Record: Protecting Electronic Health Information (National Research Council, 1997). Subsequently, NLM awarded projects that included the assessment of various approaches to ensuring the confidentiality of health data transmitted via electronic networks (National Library of Medicine, 2012).

A core requirement of telemedicine system analysis and development should include analysis of risk to both information security and patient privacy. Advanced risk analysis methods have long been used within many fields, such as insurance, military, finance, aviation, and others. However, only in recent years did the software industry finally develop workable frameworks to address security. This is exemplified by the development of the Open Web Application Security Project (OWASP) in 2001 and Microsoft's development of the Security Development Lifecycle (SDL) in 2004. Additionally, other risk methods have also been applied to information systems. Such methods include CRAMM (CCTA Risk Analysis and Management Method; Central Computing and Telecommunications Agency of the U.K. government), LAVA (Los Alamos Vulnerability Assessment), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) developed at Carnegie Mellon, and others.

Threat modeling is often done in conjunction with risk analysis. When done so, it provides a deeper quantification of risk. Indeed, this approach is seen within Microsoft's SDL. Threat modeling of information systems or computer software is most often used for identification of vulnerabilities at entry points to a system, application, or their components. A threat model developed during the design phase can be used for verification during the test phase. A threat model may also be used to analyze existing systems and software to identify vulnerabilities.

Frameworks for information security have been proposed for decades. When information security professionals and researchers realized that the classic triad of confidentiality, integrity, and availability was inadequate to describe what security practitioners think about, they began proposing more extensive frameworks. Many have attempted to overcome the dominant technologist view of information security by focusing more holistically on security, including information assets, potential sources of loss, types of loss, controls to avoid loss, remediation selection methods, and the overall objectives in protecting information. For example, one approach included that of dividing information security into a technological component addressing logical aspects and one addressing physical aspects (Eloff, Labuschagne, and Badenhorst, 1993). Their concepts include: risk identification, risk analysis, risk assessment, risk resolution, and risk monitoring. More recently, the six security elements of availability, utility, integrity, authenticity, confidentiality, and possession have been proposed by Parker (2002) and used in his Threats, Assets, and Vulnerabilities Model. It is from the development of such frameworks that risk analysis methods such as CRAMM, LAVA, and OCTAVE arose, intending to encompass the calculation of risk in both the technical and physical aspects of risk analysis.

In contrast, OWASP and SDL focuses less on calculating risk and more on the identification of potential threats during the design and development of software. In such an environment, assigning risk to defined threats is only useful as far as prioritizing work, but not necessarily part of a calculus to determining remediation. Given the adage that information security is only as good as the weakest link in a system, the goal of system and software design is to identify all potential vulnerabilities and provide countermeasures to remove or mitigate risk.

The literature also contains numerous studies on formal approaches to threat modeling. These protocols typically employ graph-based state modeling. Some rely on UML (Kong, Xu, and Zeng, 2010; Lund, Hogganvik, Seehusen, and Stolen, 2003), and others on Petri Net notation (Mirembe and Muyeba, 2008; Xu and Nygard, 2005; Youn, Park, and Lee, 2011). Microsoft, on the other hand, developed the SDL framework utilizing data flow diagrams to identify asset entry points necessary for an attack based on their STRIDE model (Hernan, 2006). STRIDE is an acronym for the six threat categories of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

Related Work

A systematic study that identified 58 published articles that in some manner concerned security in telemedicine (Garg and Brewer, 2011) reflects the scarcity of studies in this area. However, of these 58 articles, few mentioned formal standards for security. In the literature of telemedicine system development there is research that develops a secure videoconferencing system for use in diagnosis and treatment (Tulu, Chatterjee, Abhichandani, and Li, 2003), secure texting in healthcare (Bones, Hasvold, Henriksen, Strandenoes, 2007), a handheld device for diagnosis and treatment of soldiers in the field (Morris, Pajak, Havlik, Kenyon, and Calcagni, 2006), a Web-based system for managing diabetic patients at home (Bellazi, Montaini, Riva, and Stefanelli, 2001), remote sensors that monitor patient health (Chowhurry 2012; Mirembe 2006; Xiao, Shen, Sun, and Cai, 2006), and applications akin to enterprise systems (Chen, Yu, and Feng, 2000; Liu, Lu, Hong, and Wang, 2008; Maji, Mukhoty, Majumdar, Mukhopadhyay, Sural, Paul, and Majumdar, 2008). Of these articles, only Maji et al. and Bones et al. devoted significant attention to threat models. Whereas, Bones et al. concentrated on demonstrating a risk assessment of approximately thirty potential threats synthesized from an ad-hoc brainstorming session utilizing the OCTAVE method, Maji et al. used OWASP and other resources to address fourteen specific threats most commonly experienced by Web applications. As such, we see that threat modeling in telemedicine has received scant attention.

A THREAT TABLE METHOD

Our approach is based on the work of Swiderski and Snyder (2004) and consists of five aspects: (1) Identification of the points at which an attack could occur, (2) identifying the potential vulnerabilities using STRIDE, (3) listing the specific attack types for the given vulnerabilities, (4) providing proposed countermeasures and, (5) classifying the goal of the countermeasure as either Prevention, Detection, Mitigation, or Elimination. Our contribution is the development of a meaningful and easy-to-use tool absent the need for learning a formal method or needing an automated tool. This table based approach captures concise information needed for threat identification and classification, and countermeasure proposal and classification. Stored electronically in a spreadsheet or relational database, the information is easily segmented, sorted, or reported in a manner conducive to the task at hand. The simplicity of the method allows those not versed in formal threat modeling, like subject matter experts, to participate in the process of threat management.

We begin with a simple listing of the conceptual tasks that a system is envisioned to perform. This listing, which can be readily achieved using a common spreadsheet, is essentially free-form, using vocabulary and terminology that is familiar to the domain for which the system is to be used. The list of primary tasks is then decomposed into component tasks until all tasks are described. For each task, potential vulnerabilities are surmised and possible countermeasures proposed. Using this simple, straightforward approach, we believe that a threat table can capture all necessary information for threat modeling while arming software developers and their managers with sufficient guidance to address security breaches to the extent possible. We note that data flow diagrams could be utilized as the starting point of constructing a threat table since they can be used to visually identify entry points into a system or application. However, our model does not require their use.

Specifically, our threat table is composed of five columns. The first column contains task information with each task described generally and its component tasks listed underneath. This process is completed when the component tasks cannot logically be reduced any further. These conceptual and concrete tasks comprise the rows of the threat table with conceptual tasks serving as row headings. The remaining four columns are Vulnerability, Attack description, Countermeasure, and Goal of countermeasure. Vulnerability is noted used the STRIDE nomenclature described above. Attack description and Countermeasure are nominally described though a previously defined taxonomy could be used. The Goal of the countermeasure is noted as Prevention, Detection, Mitigation, or Elimination (P, D, M, or E). Notating the goal of a countermeasure is useful to later risk analysis efforts.

Once the conceptual tasks have been decomposed, each component task is analyzed for vulnerabilities in accordance with the STRIDE model. For each category of STRIDE vulnerability, potential attacks against the task are considered. Each potential attack, along with the STRIDE classification, is then listed on a separate row. For each attack listed, countermeasures are then listed in order of preference, one per row, followed by the countermeasure goal. Thus, a task may be followed by several attack descriptions, each on a separate row. Each attack may be addressed by multiple countermeasures, again with each described on a separate row.

Although the names of the goals have obvious associations, the intent of each is specific and not always apparent. Prevention refers to the idea that changes can be made in the system that prevent the possibility of a particular threat from ever occurring. For example, an interface to a system could be browser-based and use SQL statements to retrieve and store data in a database. If the code executing the SQL is not written well, an SQL injection attack is possible. By rewriting the code carefully, such as by using prepared statements, this type of attack could be entirely prevented. Of course, attacks used against certificates would be possible and would have to be addressed by other means. Detection comes into play when it is necessary for the remediation of a threat by the system, user, or some administrator. Mitigation refers only to reducing the likelihood or impact of the attack, and Elimination characterizes complete removal of the threat.

The threat table approach is arguably simpler than formal models. It is also equally capable of modeling multiple path threats due to its hierarchical nature. Each task is denoted as a starting point in the threat table, and multiple threats may be listed as being applicable to the task. As such, the threat table forms a tree but without the graphical interface. For example, an attacker might wish to obtain sensitive information about a particular patient. If a task of “View sensitive information” were listed in the table, one threat might be “Spoof identity” while another might be “Unattended screen.” Thus, the table can depict multiple threat paths to the same task. Alternatively, the table approach also permits one to list the paths separately. Hence, one task could be listed as "Logging In" and the spoofing threat identified as a potential attack on that task, while "View sensitive information" is listed as a separate task and the "unattended screen" attack listed as its potential threat. Thus, the tabular nature of our approach provides functionality that is equivalent to paths provided by formal modeling approaches.

ANALYSIS

Architecture of System

The CoM began providing remote clinical services to 22 state penitentiary locations for Hepatitis C and HIV clinical care in July 2010. This application of telemedicine serves remote and static locations using a system from Polycom to provide encrypted transmission of audio, video, and clinical instrumentation between the penitentiaries and CoM facility.

There are two examination rooms at the CoM facility designed and equipped specifically for using the Polycom system. A room contains a large high-definition screen, a remote controlled high-definition room camera mounted on top of the screen, microphones, speakers, controls for the remote (penitentiary) examination room camera, audio equalization for the stethoscope, and a PC providing access into CoM’s electronic medical record (EMR) system and a third-party laboratory. A PC-based application for connecting into the Polycom system is typically used by a caseworker and pharmacist from their respective office. A high level schematic is shown in figure 1.

When a session is initiated, the patient is accompanied by a nurse in the examination room at the prison facility. A caseworker, physician, and pharmacist are present at the CoM facility for each session. Any medical data needed from the prison are either faxed, held up to the camera to be viewed, or communicated by phone. There is no electronic interoperability between the prison and CoM EMR systems. The physician at CoM manually creates and updates an EMR record for each patient. The examination begins with the caseworker validating the identity of the patient visually and with the on-site nurse. A high-definition camera sits above the monitor at each location and is remotely controlled by the viewers. A small hand-held, high-definition camera is used by the nurse to provide close up dermatological examination of the patient. An electronic stethoscope and otoscope that plug into the Polycom system provide remote instrumentation. The physician listens to the stethoscope using headphones that are tuned with audio equalization for optimum auscultation. Finally, the otoscope provides remote visual examination into the ears, nose, and throat.

If labs are needed, the nurse collects the appropriate sample(s) and sends to a third-party lab. Using a Citrix application on his PC, the physician has remote login privilege in order to view lab results. As with the prison EMR, there is no interoperable system connection between CoM and the third-party lab. If medication is prescribed, the pharmacist participating in the session, typically from their office, orders the medication using a CoM Hospital system. The medication is packaged from a central location and shipped overnight to the prison.

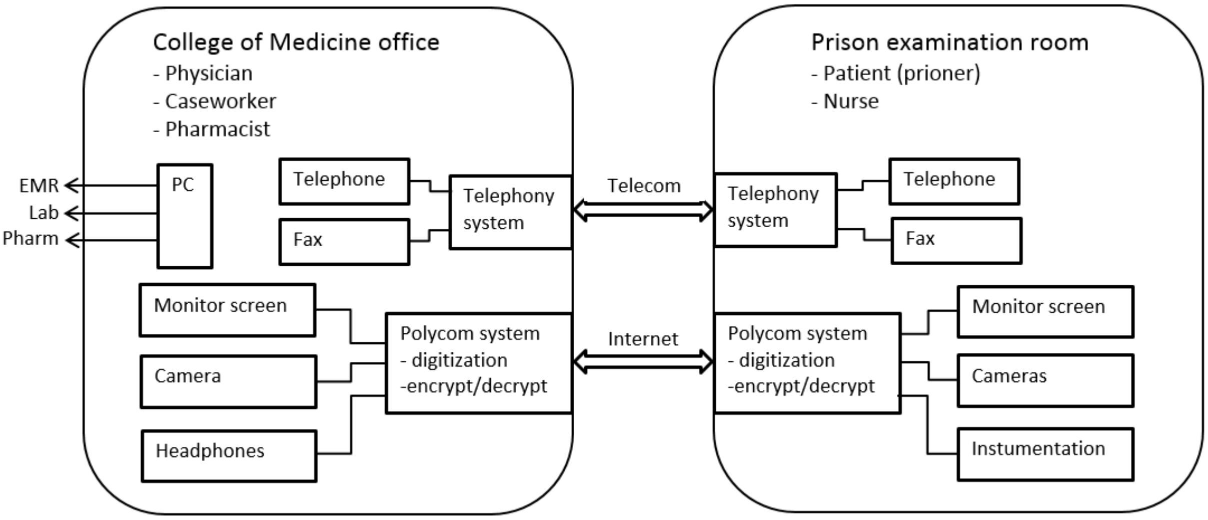


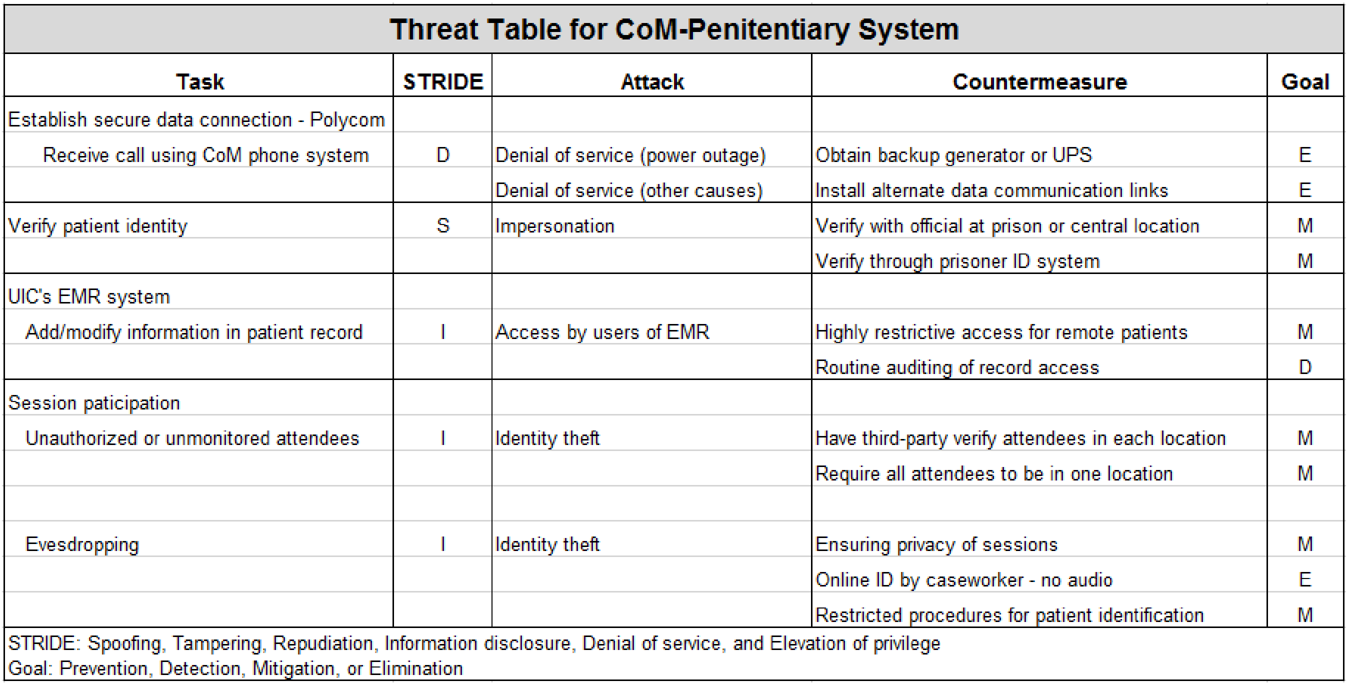
Figure 1. College of Medicine to Penitentiary telemedicine system

Results

This application of telemedicine consists of teleconferencing and digitized instrumentation. The environment is static and highly controlled, all but alleviating location privacy issues that can be problematic with telemedicine. With the Polycom system encrypting data end-to-end, any risk to information security during transmission is essentially eliminated. Furthermore, with equipment located in secure facilities and configured to use a fixed network, physical risk is minimized. Although the caseworker and pharmacist may be located in separate rooms from the physician, their data connections are on the internal CoM network and data is encrypted to their local computer. In general, the security risks to the CoM system are not as much technical as they are social.

Despite the highly controlled environment for this telemedicine application, the risk for identity theft, as well as fraud, exists. The exact procedures used during a session were not disclosed and we were prohibited from viewing a session as it would be a violation of the patient’s rights. However, without proper checks and balances several social born threats are possible. For instance, a patient and a nurse at a prison facility could collude to falsify the patient’s medical condition in order to obtain medications, such as narcotics, that could then be sold to other prisoners or on the black market. Such a scheme can work because the nurse is relied upon to identify a new patient to the caseworker and samples taken from the patient and sent to a third-party lab are also controlled by the nurse. Cross-checking of patient identity using a connection to the prison's identification system would reduce this risk. Moreover, obtaining the patient's prior medical history by connecting to external healthcare systems would further minimize this risk.

It is also possible for the prisoner to become the victim of identity theft. Rather than the patient being examined by a physician onsite with the physician using a single EMR system, the patient’s identity is now revealed remotely to at least three people outside of the prison system, namely, the physician, the caseworker, and the pharmacist. Other personnel within earshot of a session or inappropriately in attendance of a session could also obtain the patient’s identity. Additionally, a medical record for the patient is maintained in two EMR systems, increasing the risk of unauthorized access. Though these are but simple examples of threats, our threat table demonstrates the utility of modeling both technical and social born threats to patient privacy. A partial threat table demonstrating these threats is shown in table 1.



Threat Table for CoM-Penitentiary System

Task	STRIDE	Attack	Countermeasure	Goal
Establish secure data connection - Polycom				
Receive call using CoM phone system	D	Denial of service (power outage)	Obtain backup generator or UPS	E
		Denial of service (other causes)	Install alternate data communication links	E
Verify patient identity	S	Impersonation	Verify with official at prison or central location	M
			Verify through prisoner ID system	M
UIC's EMR system				
Add/modify information in patient record	I	Access by users of EMR	Highly restrictive access for remote patients	M
			Routine auditing of record access	D
Session paticipation				
Unauthorized or unmonitored attendees	I	Identity theft	Have third-party verify attendees in each location	M
			Require all attendees to be in one location	M
Evesdropping	I	Identity theft	Ensuring privacy of sessions	M
			Online ID by caseworker - no audio	E
			Restricted procedures for patient identification	M

STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
Goal: Prevention, Detection, Mitigation, or Elimination

Table 1. Partial Threat Table Example

DISCUSSION

Analyzing information security threats in telemedicine applications requires analysis at a system level and software application level. The telemedicine system analyzed for this project mostly consisted of disparate software applications and other components. From our literature review we believe this to be generally the case in practice. As such, the need for information security and privacy analysis during the design, development, and operational phases of telemedicine applications is all the more salient given the very nature of information vulnerability in telemedicine.

Previous studies of telemedicine information security have generally discussed vulnerabilities in terms of risk. Several studies simply list threats and categorized them in a risk matrix by likelihood and consequence. Though useful for risk analysis purposes, this approach does not provide an understanding of the types of threats and potential countermeasures for specific threats to a given vulnerability. In contrast, our method of using threat tables is focused on the threat, not the risk. That is, if a goal in the design of a system or application is to minimize, or eliminate, a specific type of vulnerability then it is an understanding of all forms of attack on that vulnerability that is of interest. Simply knowing the level of risk of a given vulnerability does not provide as rich an understanding as knowledge of all forms of attack on the vulnerability. It is an understanding of threats at this level that is the contribution of our approach.

Using our threat modeling approach gives practitioners an intuitive and simple method of listing vulnerabilities, threats to these vulnerabilities, and potential remedies to these threats. This is particularly useful to those developing or analyzing applications with high concern for security and privacy, like telemedicine. Threat tables are useful as-is or as a component of some system development methodology or risk analysis method. Here, we developed an example of a threat table using functional and task dimensions to illustrate identification of threats. Use of data flow diagrams or other system modeling methods could provide useful identification of vulnerabilities and potential entry points for an attack. Compared to using formal-based methods that can require specialized knowledge and software, our method is intuitive and easily implemented.

The CoM staff was very concerned about security, although they did not describe any breaches that may have occurred. CoM had not adopted a protocol or identified a process for threat modeling. Our simple protocol of using a threat table identified all of the potential problems that had been identified by CoM staff, and more.

Notably, the physician in charge of the CoM system explained how the identity of the patient could pose a challenge and remarked that he therefore took steps to confirm the identity. This concern is readily deduced using the threat table, as demonstrated above. Another prominent concern was the potential disclosure of information because conversation and video are transported over the Internet. This common threat is dealt with readily by the threat table. Indeed, the set of potential threats mentioned by CoM was easily exceeded using a short demonstration of the threat table.

CONCLUSION

We performed a high level analysis of information security threats to a telemedicine application. Using a framework that utilizes threat tables developed by the authors, we demonstrated a method of defining vulnerabilities and proposing countermeasures. Our analysis of the CoM telemedicine application reveals that even a telemedicine application in a physically static and electronically controlled environment is vulnerable to some of the same threats as seen in mobile environments utilizing public communication channels, demonstrating the usefulness of threat modeling to telemedicine applications.

Because of its simplicity, the threat table approach appears to be a salient option for providers of telemedicine. The fact that telemedicine can involve a composite of systems and applications does not detract from the value that this method brings to modeling threats. Ensuring the security of telemedicine is not only necessary for legal and financial reasons but also for providing the peace of mind required for productive relationships between patients and medical professionals.

Notably, our table-based approach to modeling threats and responsive actions is intentionally open-ended; it is capable of accommodating the analysis of any type of potential threat. This flexibility is necessary when constraints such as governmental regulations come into play. In particular, security in systems that handle medical information is regulated by HIPAA and the HITECH Act. In 2013, the Department of Health and Human Services published a final rule on security measures that must be incorporated within such systems. These requirements address such fundamental security measures as user authentication, encryption, and transaction logging, among others. Threats that potentially are remediated by such measures, or, more importantly, that impact their implementation, may readily be modeled using our approach. Therefore, table-based threat modeling that relies on STRIDE is consistent with both the spirit and text of HHS regulations.

Our investigation into modeling the threats in this project was limited by our knowledge and understanding of the telecare systems analyzed. CoM was kind enough to demonstrate their system to us and discuss the details at an introductory level, but we did not have the opportunity to conduct an exhaustive audit of all elements of this system. Nonetheless, we gained enough knowledge during our visit to synthesize an initial, high-level threat model. Due to the limitations of the interview, little information was obtained about how the CoM staff views standardized approaches to threat modeling, but it appeared that the addition of a formalized protocol, such as our threat table approach, would potentially benefit their organization.

With this initial understanding we will continue exploring the identification of security threats and how the traits of these threats and their countermeasures should be represented in a threat table. Our next step is to analyze a multifarious telemedicine system and consider refinement to the structure of the threat table. Our goal is to develop a practical and useful method of addressing security threats in the design and analysis of telemedicine systems with applicability to information systems in general.

Future work could include studying threat tables in practice, as well as studying other threat modeling approaches, particularly formal methods, compared against this method for usability, effectiveness, and feasibility. Further, we could explore the utility of incorporating the threat table approach into an overall risk analysis of a telemedicine system. Finally, we would like to expand our threat analysis of telemedicine applications into unconventional environments, such as disaster relief environments, where telemedicine applications might be used with ad-hoc or hastily formed networks.

REFERENCES

Bellazi, R., Montani, S., Riva, A, & Stefanelli, M. (2001). Web-based telemedicine systems for home-care: technical issues and experiences. *Computer Methods and Programs in Biomedicine,* 64, 175-187.

Bones, E., Hasvold, P., Henriksen, E., Strandenoes, T. (2007). Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International Journal of Medical Informatics,* 76, 677–687.

Chen, Z., Yu, X., & Feng, D. (2000). A Telemedicine System over the Internet. *Proceedings of the Sixth Pan-Sydney Workshop on Visualisation*, 2, 113-118.

Garg, V. & Brewer, J. (2011). Telemedicine Security: A Systematic Review. *Journal of Diabetes Science and Technology*, 5(3), 768-777.

Hernan, S., Lambert, S., Ostwald, T., and Shostack, A. (2006). Uncover Security Design Flaws Using The STRIDE Approach. *MSDN Magazine*, *November 2006*. Retrieved from http://msdn.microsoft.com/en-us/magazine/cc163519.aspx on Dec. 11, 2012.

Kong, J., Xu, D., & Zeng, X. (2010). UML-Based Modeling and Analysis of Security Threats. *International Journal of Software Engineering and Knowledge Engineering*, 20(6), 875–897.

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. (1993). A comparative framework for risk analysis methods. *Computers & Security,* 12(6), 597-603.

Liu, Q., Lu, S., Hong, Y., Wang, L., & Dssouli, R. (2008). Securing Telehealth Applications in a Web-Based e-Health Portal. In Proceedings *Availability, Reliability and Security*, 3-9.

Lund, M. S., Hogganvik, I., Seehusen, F., & Stolen, K. (2003). UML profile for security assessment (Technical report STF40 A03066). SINTEF Telecom and Informatics, Trondheim, Norway.

Maji, A. K, Mukhoty, A., Majumdar, A. K, Mukhopadhyay, J., Sural, S., Paul, S., & Majumdar, B. (2008). Security Analysis and Implementation of Web-based Telemedicine Services with a Four-tier Architecture. *Proceedings of Second International Conference on PervasiveHealth 2008*, 46-54.

Mirembe, D. P. (2006). Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services. (Master thesis). Radboud University Nijmegen, the Netherlands.

Mirembe, D. P. and Muyeba, M. (2008). Threat Modeling Revisited: Improving Expressiveness of Attack. *Proceedings of Second UKSIM European Symposium on Computer Modeling and Simulation,* 93-98.

Morris, T. J., Pajak, J., Havlik, F., Kenyon, J., and Calcagni, D. (2006). Battlefield Medical Information System–Tactical (BMIST): The Application of Mobile Computing Technologies to Support Health Surveillance. *Telemedicine Journal and e-Health,* 12(4), 409-416.

National Library of Medicine, National Institutes of Health. (2012). NLM National Telemedicine Initiative. Retrieved from www.nlm.nih.gov/research/telemedinit.html, accessed February 21, 2013.

National Research Council, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board. (1997). *For the Record: Protecting Electronic Health Information*. Washington, D.C: National Academy Press.

Parker, D. B. (2002) Toward a new framework for information security, in, S. Bosworth and M. E. Kabay (Eds.) *Computer Security Handbook.* New York: John Wiley & Sons.

Swiderski, F., and Snyder, W. (2004). Threat Modeling, Redmond, WA: Microsoft Press.

Tulu, B., Chatterjee, S., Abhichandani, T., and Li, H. (2003). Secured Video Conferencing Desktop Client for Telemedicine. *Proceedings of Enterprise Networking and Computing in Healthcare Industry*, 61-65.

Xiao, Y., Shen, X, Sun, B., and Cai, L. (2006). Security and Privacy in RFID and Applications in Telemedicine. *IEEE Communications Magazine*, 44(4), 64-72.

Xu, D. and Nygard, K. (2005). A threat-driven approach to modeling and verifying secure software. *Proceedings of IEEE/ACM International Conference on Automated Software Engineering*, 342-346.

Youn, H., Park, C., and Lee, E. (2011). Security based survivability risk analysis with extended HQPN. *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication,* article 25.

[i] This work has been funded with support from NSF under the IGERT Grant Number 1069311.