Chapter 76
A Threat Table Based Assessment of Information Security in Telemedicine

John C. Pendergrass
University of Illinois - Chicago, USA

C. Ranganathan
University of Illinois - Chicago, USA

Karen Heart
Tagmata Software Security, USA

V. N. Venkatakrishnan
University of Illinois - Chicago, USA

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 proposes a threat table approach to assess security threats pertaining to telemedicine applications. The concept and its usefulness are illustrated using a case study. This case study focuses on the capture and representation of salient security threats in telemedicine. To analyze the security threats to an application, it presents a threat modeling framework utilizing a table driven approach. The study 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.

1. INTRODUCTION

Advances in healthcare information technology, like telemedicine, has the potential to improve patient quality of care, reduce costs, and advance medicine in general. However, with these 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 identity theft, costing patients, providers, and payers. As the very nature of telemedicine is vulnerable to a number of security breaches, the security

DOI: 10.4018/978-1-4666-8473-7.ch076

of personal health information in telemedicine applications is of paramount importance to the aforementioned parties (Hall & McGraw, 2014).

Examining security vulnerabilities and privacy threats in telemedicine is non-trivial. These problems get further compounded due to advances in wireless and mobile technologies that are becoming increasingly prevalent in telemedicine applications (Ameen, Liu, & Kwak, 2012; Harvey & Harvey, 2014). The complex and evolving nature of healthcare, government policies and regulations, public concern, and the rise of cyber related crimes make identifying and mitigating threats to patient health information difficult. In an effort to prevent the erosion of privacy and confidentiality of patient health information, federal and states government have created policies and regulatory requirements for patient's protected health information (PHI). Notable are the federal policies and regulations laid out in the Health Information Portability and Accountability Act (HIPAA) of 1996, and the more recent Health Information Technology for Economic and Clinical Health (HITECH) Act; itself a part of the American Recovery and Reinvestment Act of 2009. These, along with varying and often disparate state regulations, make compliance challenging.

There are a number of challenges to consider. One major challenge is the implementation of information security while minimizing disruption to workflow. By its very nature, telemedicine has a more vulnerable data communication and IT operations architecture, and a workflow that must accommodate parties in different localities. Adequate, but non-disruptive, information security measures are definitively more challenging in a telemedicine environment than those within a physically secure location with an inherently more secure IT architecture. In such an environment, identifying threats to information security and PHI are critical for developing secure information systems and operating environments. Identifying and classifying threats allows developers and managers to craft countermeasures. We classify the goals of countermeasures as prevention, detection, mitigation, and elimination.

A number of frameworks for addressing information and software security risks have been developed. Three of better known approaches are: the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework created in 2001 by the Software Engineering Institute at Carnegie Mellon University (Alberts, Dorofee, Stevens, & Woody, 2003); the Open Web Application Security Project (OWASP), an open community project, also created in 2001 (Curphey, 2010); and the Security Development Lifecycle (SDL) method developed in 2004 by Microsoft (Swiderski & Snyder, 2004). While all of these approaches have vulnerability and threat identification as part of their framework, they fall short in providing detailed direction for identify and classifying vulnerabilities and specific threats to system components.

To address shortcomings in generalized frameworks, and the need for greater scrutiny of information security threats and vulnerabilities in telemedicine, this research provides a generalized method of threat and vulnerability identification, classification, and goal determination with high applicability to telemedicine. Drawing on several techniques from the research literature, we construct a threat table that lists security vulnerabilities and potential remedies for any identifiable threat to a system or software application. The threat table was devised through a repetitive process of documenting system operation and functionality at increasing levels of detail. Hence, our process incorporates a cross section of all available information regarding potential threats, beginning with a high level, conceptual understanding of the system and ending with the concrete details of threats that are required for designing and implementing necessary remediation. We feel