Engineering and Technology Journal e-ISSN: 2456-3358
Volume 09 Issue 10 October-2024, Page No.- 5329-5331
DOI: 10.47191/etj/v9i10.10, I.F. – 8.227

Threat Modeling for Enhanced Security in the Healthcare Industry with a Focus on Mobile Health and IoT

Rohith Vallabhaneni[1], Vinod Veeramachaneni[2]
[1]School of Computer and Information Sciences, University of the Cumberlands
ORCID: 0009-0003-3719-2704
[2]School of Computer and Information Sciences, Colorado Technical University, USA
ORCID: 0009-0006-6282-6133

ABSTRACT: The advancement of mobile health and the Internet of Things (IoT) promises to enhance healthcare quality while reducing costs, particularly with the transition from inpatient to home and ambulatory care. This shift, driven by an aging population, financial pressures, and a shortage of skilled healthcare professionals, presents significant opportunities and challenges. While mobile health improves access and encourages self-management, it also raises serious concerns regarding security and interoperability, especially with wearable devices equipped with sensors in a patient's Body Area Network (BAN). This paper critically analyzes the security and interoperability risks associated with these technologies, emphasizing the need for robust measures such as configuration and asset management. Utilizing recommendations from ENISA (2016) and conducting a risk and vulnerability assessment, this study develops a comprehensive security model tailored for healthcare architectures. Additionally, it applies the STRIDE threat modeling approach to identify and mitigate potential threats, providing valuable insights for securing healthcare systems and prioritizing critical assets vital to organizational operations.

KEYWORDS: Mobile Health, Internet of Things, Healthcare Security, Threat Modeling, STRIDE, Risk Assessment, Interoperability, Body Area Network, ENISA, Asset Management.

INTRODUCTION

Advancement in mobile health and the Internet of Things is like to improve the quality and reduce costs of healthcare. Especially with the shift from inpatient to home and ambulant care, ubiquitous and mobile technology are inevitable steps. Teixeira et al. (2015) note that the shift is a result of an aging society, cost pressure, and inadequate skilled personnel in health care. As mobile health is increasing access to healthcare, maintaining treatment, and encouraging self-management and the Internet of Things is increasingly defining the health care industry, numerous challenges arise in terms of security and interoperability which should be treated and considered seriously. For instance, security and interoperability risks that are associated with wearables with sensors such as gyroscopic, bioimpedance, heart rate sensors deployed in a patient's Body Area Network (BAN), should be analyzed critically as they may cause death. ENISA (2016) identifies configuration and asset management as key technical measures to prevent attacks. In an attempt to come up with an effective security model, this paper addresses key recommendations identified in ENISA (2016) and conducts a risk and vulnerability assessment for the healthcare industry, particularly health architectures that are deployed in any clinical context. It also models threat modeling using STRIDE based approach.

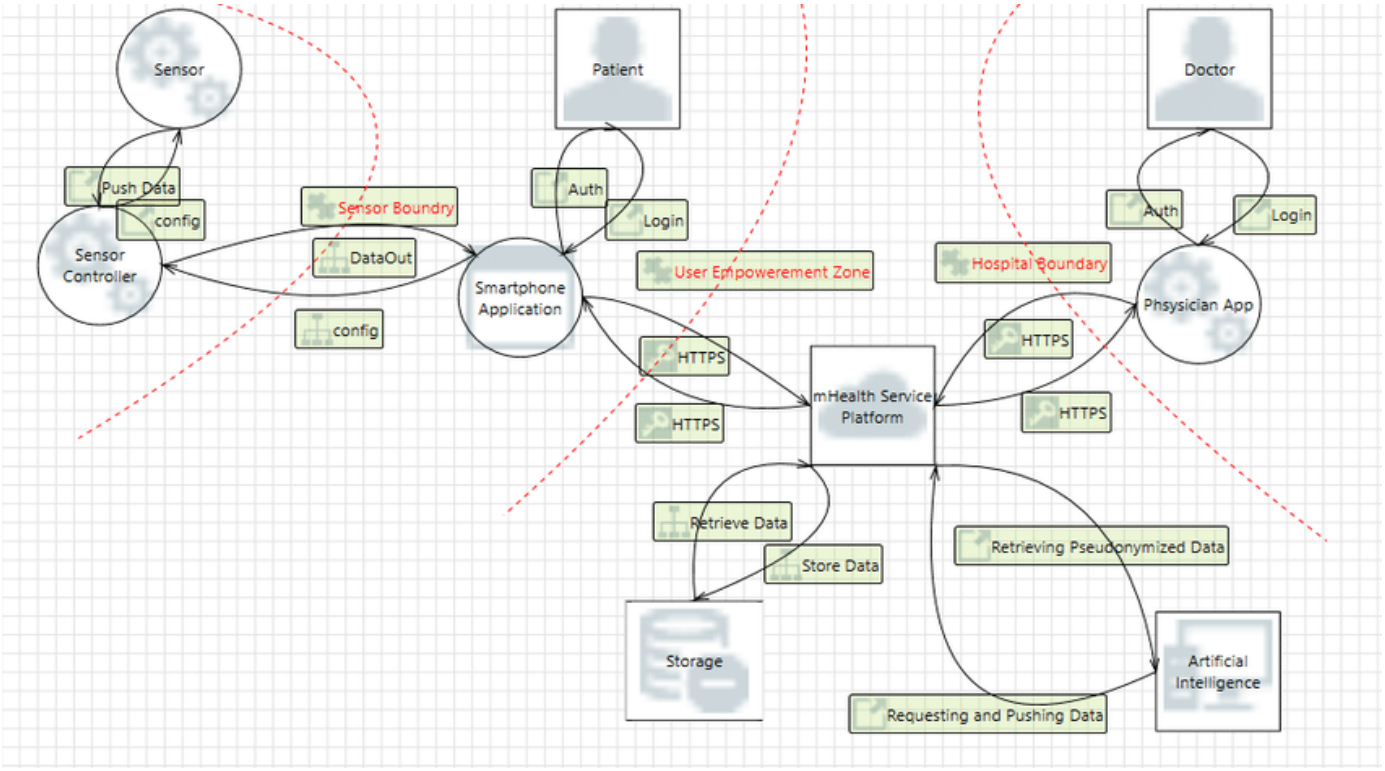
Threat modeling, the process of aiming at building more secure and better software, is an important aspect of the security development lifecycle (Howard & Lipner, 2006). It is a technique of finding assets, analyzing threats, and mitigating them to provide defenders with important security insight, including assessing assets an attacker is attracted to, potential attack vectors, and attack vectors that may be unnoticed. The identified threats are then associated with security risks to prioritize some assets. ENISA (2016) note that an asset is valuable to an organization, its day-to-day business operation, and the community. For instance, an asset to be prioritized can be information resources supporting the main mission of an organization.

STRIDE, an abbreviation for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Shostack, 2014), is highly recommended despite that there are other threat modeling techniques such as PASTA and OCTAVE frameworks. PASTA combines an attacker's perspective with impact analysis and risks to give a complete picture of threats and applications, vulnerabilities, and inform risk and priorities decisions. OCTAVE, on the other hand, defines a risk-based strategic assessment and security planning techniques. The DREAD technique can be used to rank threats according to categories. The table below shows the connection between

STRIDE and the mHealth setting. After addressing the threat, STRIDE requires that risk metrics of an attack are calculated. While using the DEAD model, for instance, we can calculate the likelihood of an attack by exploiting a single threat.

Threat Categories	Attacker's Security Perspective
Spoofing: attacker pretends to be an authorized user	Used user authentication credentials to access patient data
Tampering: an attacker modifies a patient's data	Modify BAN, LAN data
Reproduction: if a proof is missing, an attacker filters malicious information	Authorized staff performs illegal actions without being detected by the system
Information Disclosure: exposing patient's information to an authorized user	Leaking medical data
Denial of Service: attackers ensures valid users are denied access to valuable information	Jamming patient or hospital systems
Evaluation of privilege: manipulate patient systems via gained access rights	Access to system security as a trusted individual.

Low to high values are assigned to each addend, the sum is calculated and the results are categorized in a 5-15 range of value. Afterward, the overall rating of 12-15 can be used to rank threats as high risks, 8-11 medium, and 5-7 low. Threat middling in STRIDE is divided into assets identification, threats listing, and threat mitigation. To define threats and have a more detailed overview of this architecture, a graphical representation of critical data points and flow is illustrated below.



From the diagram, data from one sensor is pushed to the central sensor controller. The collected data is pushed to the application using a Bluetooth LE connection. The application then sends data to the sensor controller. From the above data flow diagram, a patient authenticates himself to access the application. Data is transferred via HTTPS connection and acknowledged after being stored successfully. If a practitioner wants to check a patient's record, he or she authenticate himself to the system and can send interventions over the cloud infrastructure. Assets in the system include network components, identity management, database, and communication means. The associate impacts include confidentiality violation, and data availability and integrity. Since a patient system should offer real-time information, data breach leads to loss of data, safety, and privacy. Depending on a medical scenario, real-time data communication can range from a few seconds to 15 minutes for cardiac monitoring to depression monitoring respectively. Loss of patient information and confidentiality are other key impacts as patient information is highly personal and should

be protected carefully. The health care system should be trustworthy and should provide and maintain patient privacy and confidentiality always.

The table below shows authentication and confidentiality threats. While focusing on spoofing, misuse and credential loss may be severe.

Description	STRIDE	DREAD
Patient identity sharing or loss	S	Medium
Personnel identity sharing or loss	S	High
Identity spoofing	S	Low
Patient and Personnel Identity Theft	E	Medium
Sysadmin Identity Theft	S	High
Sensor Spoofing	S,D	Medium
Smartphone Spoofing	S,D	Medium
EHR/PHR Spoofing	S	High

If users gain unauthorized access to the system, threats are the evaluation of disclosure, privileges, and data tampering. In a STRIDE column, as indicated below, users can evaluate their privileges, gain admin privileges leading to the disclosure of personal data. Authorization threats are medium despite that they can be high because gaining administrative access damages both the patient and the healthcare provider. Spoofed sensor floods the architecture with requests leading to a denial of service as the service or the application is not responding.

Description	STRIDE	DREAD
Unauthorized Access to system data	E	High
Unauthorized Access beyond authorized privileges	E	Medium
Tampering to modify access control	T	Medium
Impersonation of a Patient	E,D	Medium
Impersonation of Personnel	E,D	High
Unauthorized access to admin functionality	E,T	High

Artificial intelligence can also be targeted by threats. Threats targeting Artificial intelligence are medium as they can alter the integrity of the entire system. An attacker can change the training data causing every decision of the system to be false.

Description	STRIDE	DREAD
Potential altering of training data	T	High
Non-targeted adversarial attack	T	Medium
Targeted adversarial attack	T	Medium

Possible mitigation strategies while using this method entail grouping assets into different underlying processes and technologies. For instance, it is easy to classify the attacks as physical attacks and virtual attacks. By doing so, each threat can be conquered using a well-known encryption or authentication approach. Authorization and threats can thus be prevented using a reliable authentication approach and privacy threats can be conquered using proper encryption techniques. Threats that can harm patients or cause mental or physical damage can be prioritized, analyzed, and mitigated using extreme caution. Since the healthcare industry is heterogeneous, STRIDE has proven to be effective in designing secure systems as it performs specific analyses of a threat. Besides, it is iterative and can be developed easily.

REFERENCES

1. ENISA. (2016). "Cyber security and resilience for Smart Hospitals", European Union Agency for Network and Information Security.
2. Howard, M., & Lipner, S. (2006). *The security development lifecycle* (Vol. 8). Redmond: Microsoft Press.
3. Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.
4. Teixeira, R., Frey, W., Griffin, R. (2015): States of Change: The Demographic Evolution of the American Electorate, 1974-2060; American Enterprise Institute, Brookings Institution and Center for American Progress.