Micah Wieburg - Week 3 - Research Paper

Micah L Wieburg

School Of Computer Information Sciences, University of The Cumberlands

ITS834 - B04: Emerging Threats & Countermeasures

Dr. James Webb

November 3, 2022

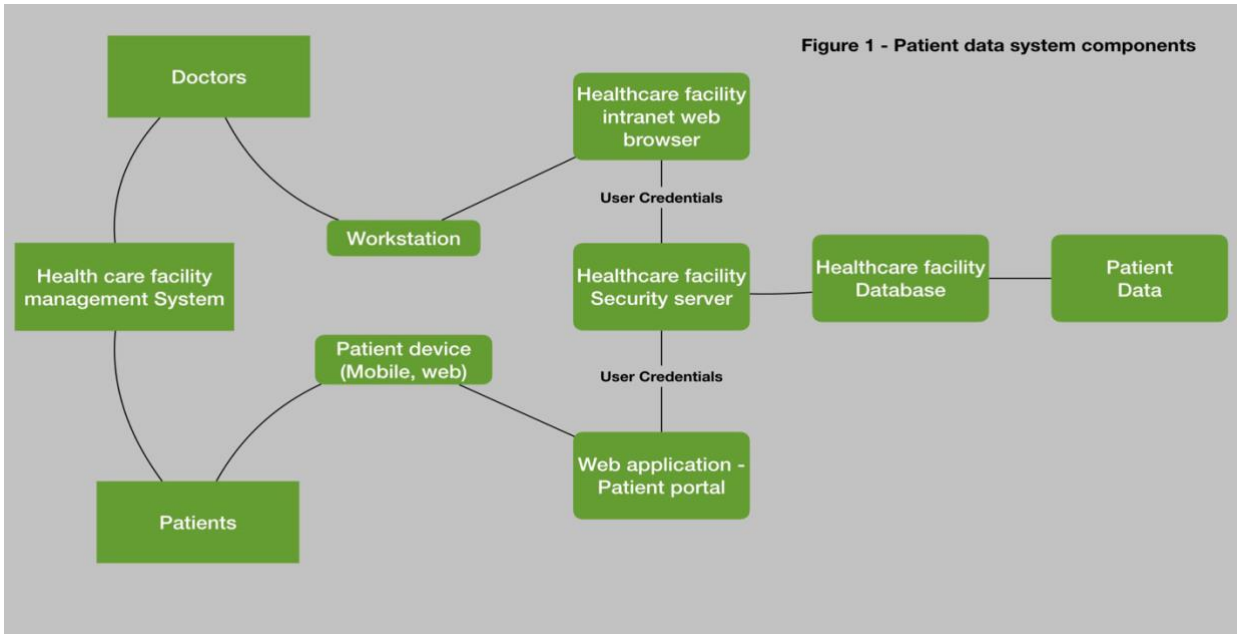
System threat analysis is an activity cemented into the overall security of software and hardware. In developing the proper conclusions concerning threats, threat modeling is a practical approach to threat discovery. Threat modeling aims to identify assets, discover possible threats, and create mitigation efforts against threats (Cagnazzo et al., 2018). The threat modeling process brings understanding to system security threats, vulnerabilities, and the impact that these threats can inflict on users and organizations. (Abomhara et al., 2015). Threat modeling is a process that requires continuous reevaluation to maintain the accuracy of threat findings and mitigation efforts (Loadenthal et al., 2021). Due to the evolving nature of cyber threats, the ability to create a fully secure system is greatly hampered. Furthermore, threat modeling must be approached with asset prioritization as a primary objective. Value and risks must be evaluated and ranked to arrive at conclusions on priority. (Loadenthal et al., 2021) Identified threat modeling as attempting to answer three questions, "What am I trying to protect?, What do I need to protect against?, How much time, effort, money, decreased functionality, additional steps, etc., am I willing to expend to obtain adequate protections?". Identified assets, known possible threats, and practical mitigation efforts allow organizations to understand their security domain and build a foundation for protection. In this report, we will present the research findings of three threat models and provide a recommendation based on the results suggested.

LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness of content, and Non-compliance of policy) threat modeling is primarily focused on privacy threats and mitigation. Using this model will giveaway to private threat assumptions in the early phase of system architecture concepts and reveal flaws in privacy design (Van Landuyt & Joosen, 2020). The assumptions and critical threats identified during LINDDUN serve as the core for building the proper plans. LINDDUN gives aid to knowledge

and process. The knowledge is organized concerning the categories of threats that make up LINDDUN (Wuyts et al., 2020). Three steps are generally followed for this modeling process. Step one is to model the system via flow diagrams or other visual representations (Wuyts et al., 2020). Step Two of LINDDUN performs threat analysis by reviewing diagrams presented in step one and identifying any applicable threats in the data flow interactions (Wuyts et al., 2020). Step three of LINDDUN is oriented toward managing threats. In this step, threat management should prioritize threats based on the associated risk and spawn mitigation objectives for each ranked threat (Wuyts et al., 2020).

The PASTA threat model (Process for Attack Simulation and Threat Analysis) focuses on risk threat modeling techniques that encompass risk analysis in the initial stages to establish the security of high-priority infrastructure (Singh et al., 2022). Sequential modeling is the core of PASTA which consists of seven stages. At stage one, risk analysis goals are defined to provide solid objectives related to business and reports from the analysis. Stage two of PASTA consists of determining the technology's scope while understanding potential attacks through comprehensive technical information. In stage three, diagrams, assets, and access lists are given as part of the analysis performed in this stage. PASTA stage four is reserved for risk analysis and reports covering threats, incidents, and attack variables. PASTA stage five creates Common Vulnerability Scoring System scores after executing assessments of vulnerabilities. PASTA stage six will model attacks and mock-ups of common threats, which are used to provide attack strategy projections. Stage seven is the final stage of PASTA and is accompanied by risk analysis to develop profiles and mitigation plans for the identified threats.

For the purposes of this report, the recommendation is to utilize the STRIDE threat model. STRIDE is a widely used threat model and stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial Of Service, and Elevation of Privileges (Hasan & Hasan, 2021). This threat model uses these categories to label each identified threat during the modeling process. STRIDE has gained notoriety as a Microsoft created threat model and is widely used by several others, having the ability to find threats from the developers' perspective (Hasan & Hasan, 2021). For the categories noted in STRIDE, risk reduction is supplied by a defined group of countermeasure techniques. Figure 1 diagram illustrates system components related to patient data and access inside of the healthcare facility. The assets identified in Table 1 require threat analysis in order to rank the potential impact. As noted in Table 2, each asset is susceptible to some variant of exploitation or misuse.



The criteria for labeling an asset are rooted in the business value of the subject entity. Each asset is subject to value investigation and generally receives a ranking from very low to very high (Abomhara et al., 2015). The investigation will primarily revolve around data access and the components that handle access control concerning the healthcare facility. These components are subject to potential intrusion threats due to their sensitive nature. Mitigation resources will garner a significant focus to safeguard these high-priority assets.

Table 1 - Healthcare Facility Assets

Healthcare Facility - Asset	Description
Staff User Credentials	Login credentials used by facility members to access data via intranet access
Patient Credentials	Login credentials used by patients to access data via personal devices
Patient Data	Data pertaining to healthcare facility patient records (visits, labs, medication) access via intranet or patient portal
Facility devices	The workstation or other facility devices used by staff to access necessary system components
Facility Security Server	Security system component that regulates access requests

Table 2 - Healthcare Facility - Threats

Threat	Description	Impact	STRIDE - Category
Spoofing attack: Staff/ patient credentials	Credentials of staff members or patients are disclosed to unauthorized sources via spoofing attack	Medium	Spoofing
Patient device misplaced/stolen	The patients' device used to access healthcare facility data could contain credentials used to access the system	High	Information Disclosure
Data access violation: Access configuration	Staff members are able to view patient data that is outside of their relational access controls	Low	Elevation of Privelege
Patient Session Hi-Jacking	Security vulnerabilities on patients device subject the valid portal sessions to session hi-jacking and exposure of sensitive data	High	Information Disclosure

The threats in Table 2 are categorized based on the six categories defined by the STRIDE threat model. Based on the impact on system security, each threat is rated as either high, medium, or low. Losing patient or staff credentials to unauthorized parties could result in exposure to private health data. With regulations related to HIPPA and facility integrity, this type of threat evaluates to a high impact ranking. Threats related to the spoofing category are largely preventable at the facility level, therefore receiving a medium rating. Elevation of privilege threats identified concerning the facility is limited to internal exposure and timely resolution, encouraging low ranking.

Threat modeling is a valuable means of planning for system security. After researching the available options, the conclusion is that STRIDE threat modeling is the optimal choice. Using

STRIDE for threat modeling will serve the need to have a granular view of the threats that have the potential to impact system elements. There are significant benefits of having a deep analysis of assets and how essential these assets are to the well-being of the overall system. These details provide clear direction for comprehensive security measures to safeguard data integrity and reliance.

References

Cagnazzo, M., Hertlein, M., Holz, T., & Pohlmann, N. (2018). Threat modeling for mobile health systems. *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 314–319. https://doi.org/10.1109/WCNCW.2018.8369033

Abomhara, M., Køien, G., & Gerdes, M. (2015). *A STRIDE-Based Threat Model for Telehealth Systems*.

Loadenthal, M., Nielsen, P., & McCarthy, D. (2021). *Risks, Dangers, and Threat Models: Evaluating Security Analysis for Conflict Practitioners* [Technical Report]. Better Evidence Project. http://mars.gmu.edu/handle/1920/12716

Van Landuyt, D., & Joosen, W. (2020). A descriptive study of assumptions made in LINDDUN privacy threat elicitation. *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 1280–1287. https://doi.org/10.1145/3341105.3375762

Wuyts, K., Sion, L., & Joosen, W. (2020). LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 302–309. https://doi.org/10.1109/EuroSPW51379.2020.00047

Singh, J., Patel, C., & Chaudhary, N. K. (2022). *Resilient Risk based Adaptive Authentication and Authorization (RAD-AA) Framework*. http://arxiv.org/abs/2208.02592

Hasan, R., & Hasan, R. (2021). Towards a Threat Model and Security Analysis of Video Conferencing Systems. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–4. https://doi.org/10.1109/CCNC49032.2021.9369505

Sgandurra, D., & Lupu, E. (2016). Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems. *ACM Computing Surveys*, *48*(3), 1–38. https://doi.org/10.1145/2856126

Alshehri, S., Mishra, S., & Raj, R. (n.d.). *Insider threat mitigation and access control in healthcare systems*. 15.