A STRIDE-Based Threat Model for Telehealth Systems

Mohamed Abomhara, Martin Gerdes, Geir M. Køien
Department of Information and Communication Technology
University of Agder, Norway
{mohamed.abomhara, martin.gerdes, geir.koien }@uia.no

Abstract

In this study, the most widely accepted threat modeling process, that has been proposed by Microsoft, is used to identify all possible threats to telehealth systems. Security threats to a telehealth trial system at the Center for eHealth and Healthcare Technology, University of Agder, are analyzed and discussed. Moreover, a list of countermeasures is suggested to better design and implement system protection solutions against telehealth insider threats.

1 Introduction

Advances in telehealth systems will likely reduce cost and improve quality of care in general [1–3]. Although telehealth systems may improve the quality of healthcare, the digitalization of health records, the collection, evaluation and provisioning of patient data, and the transmission of patient data over public networks (the Internet) pose new privacy and security threats to patients and healthcare providers [4–7].

As a result, telehealth system security is of paramount significance [8]. If developers do not take into account all possible threats against telehealth systems, they will be unable to provide sufficient security to prevent threats, allowing systems to be vulnerable to security breaches [8, 9]. Therefore, threat modeling serves as a foundation for the analysis and specification of security requirements [10, 11]. It involves understanding of system complexity and identification of all possible threats to the system. Identified threats are further analyzed based on their criticality and likelihood, and decisions are made whether to mitigate the threats or accept the associated risks [12]. Once system designers determine which security mechanisms must be available to the system, the development of these mechanisms follows the general software engineering cycle of design, implementation, testing and maintenance [10].

The main objective of this work is to describe and better understand potential threats to telehealth systems in the following way:

1. An overall threat analysis process is provided by characterizing threat information (assets, adversary and adversary action) originating from various threat actors, to better comprehend all types of threats to a telehealth system.

This paper was presented at the NISK-2015 conference.

2. As a proof of concept, the threats to the telehealth trial system at the Center for eHealth and Healthcare Technology, University of Agder, were analyzed with support of Microsoft Threat Modeling Tool 2014 [12, 13], and potential countermeasures for various threats were listed.

Paper Structure

The remaining parts of this study are organized as follows. In section 2, a brief description of the telehealth system and related work on threat modeling is provided as background information. Section 3 presents the system architecture and the threat modeling process. Conclusions and aspects for future work are presented in section 4.

2 Background

In this section, relevant work underlying the current study is discussed. First, telehealth systems are briefly introduced, followed by an overview of threat modeling and threat modeling methodologies.

Telehealth Systems

Telehealth comprises the use of information and communication technologies (ICT) to offer different, user-group specific healthcare services to participants (patients, doctors and nurses, etc.) who are in different locations [2]. The remote health service provision serves a variety of purposes, such as remote patient monitoring (e.g. home telehealth), specialist referral services and medical education [2, 3]. However, telehealth raises security and privacy concerns. The number of potential threats in the field of health information systems has increased dramatically, and the lack of adequate security measures allows for numerous data breaches [9], leaving patients and healthcare providers vulnerable to security threats [14]. In order to exploit the full potential of telehealth services, protection against threats and vulnerabilities is required.

Threat Modeling Overview

Threat modeling helps to understand system security threats and vulnerabilities, and how those threats potentially impact users and organizations, and to determine the most cost-effective security solutions to mitigate attacks [12]. Due to the extensive cost, time and resources needed for the development on the one side, and due to the fast emergence of new kinds of threats on the other side, it is almost impossible to develop a completely secure system. Thus, it is important to decide on the priority of each asset, and balance between security and cost throughout the system development. The priority of an asset is determined according to its value and risk potential to it. Therefore, threat modeling is used to analyze system threats and vulnerability scenarios in order to evaluate the risk.

Threat modeling methodologies

Academia and industries have undertaken extensive research on the process of threat modeling. This includes, among many others, Microsoft's development of the security life cycle (SDL) [13], the Open Web Application Security Project (OWASP) [15], the Process for Attack Simulation and Threat Modeling (PASTA) [16], Trike methodology [17] and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [18]. The mostly used tool of modeling is that of Microsoft, which encompasses all aspects of security to offer documentation as a guide through the remaining process.

SDL is geared more towards the identification of potential threats through identifying assets and understanding the target application by creating use cases, and identifying threats based on the Microsoft STRIDE model [12, 19]. Subsequently, the identified threats are ranked based on the security risk posed using a DREAD threat-risk ranking model [11].

3 Threat Model for Telehealth Systems

In this section, the main threat components are identified: assets, users, threat agents and threats to the system.

The process of threat modeling is divided into the three main phases as following: (1) identifying assets and access points, (2) listing all potential threats and (3) building a mitigation plan.

1. Identifying assets and access points: An asset is something valuable, owned by an entity, and that attackers are interested in, and wish to access, control or destroy. Identifying assets is the primary, most critical step in threat modeling, because assets are essentially threat targets. Access (or entry) points are interfaces through which potential attackers can interact with the system to gain access to assets. Examples of access points include user login interfaces, file systems and hardware ports. Upon identifying the access points, it is very important to define the trust boundaries in the system. A trust boundary is a boundary across which there are varied levels of trust [12]. Trust levels indicate how much trust is required to access a component of the system.

2. Listing all potential threats: Threats may come from authorized users (insiders) or unauthorized users (outsiders). All the information gathered from phase 1 will help to identify all possible threats and threat sources. Adversaries goals, capabilities and what they might do to the system are all defined as threats. Threats to the system can be identified by reviewing each asset and access point in the system, and creating threat hypotheses regarding violations of asset confidentiality, integrity or availability. In general, threats can be classified into six classes, following the Microsoft STRIDE model [12, 19]:

   - **Spoofing** is attempting to gain access to a system by using a false identity.
   - **Tampering** is the unauthorized modification of data.
   - **Repudiation** is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions.
   - **Information disclosure** is the unwanted exposure of private data.
   - **Denial of service** is the process of making a system or application unavailable.
   - **Elevation of privilege** occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an asset.

3. Building a mitigation plan of countermeasures: Once the basic assets and all potential threats are understood and identified, setting a control mechanism to prevent or mitigate threats is proposed in phase 3 of the mitigation plan.

System Description: Telehealth Reference System Overview

In Figure 1 the system architecture of the studied telehealth reference system is illustrated. The reference system includes the following main system domains:

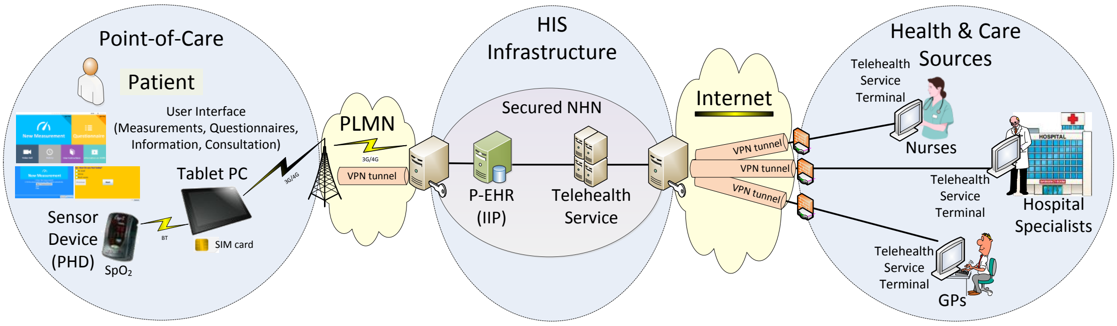

Figure 1: Architecture overview of the telehealth trial system for patients.

Point-of-Care: The Point-of-Care environment includes devices and applications for patients in their personal environment (e.g. their home), to facilitate regular measurements of certain health and care status data, to support self-reporting of health symptoms along questionnaires, to enable remote consultations (video or telephony), and to obtain information and follow-up support.

Health & Care Services: Based on the health and care status of the remotely monitored patients, different healthcare professionals provide collaborative services to follow-up on the patients according to their individual needs.

Health Information Services (HIS) Infrastructure: The health and care status information from the patient, which is reported by the devices and applications in the point-of-care, is collected, stored and provisioned by Electronic and Personal Health Record systems (EHRs, PHRs). Dedicated monitoring services utilize and evaluate the patient data, in order to determine value-added information about the patients' health condition, and to provide decision support information for the patient follow-up by the health and care service providers. The automatic data evaluation includes the triage calculation as explained above.

The typical use case scenario looks like following: in the point-of-care, e.g. the patients' home, the patients carry out certain measurements of healthcare relevant parameters with corresponding wireless body sensors, supported by an application on the tablet PC. Furthermore they do a self-reporting of their individual subjective health condition via electronic questionnaires on the tablet PC. The data from measurements and questionnaires are transmitted to the health information services infrastructure, and stored in electronic / personal health records (EHRs / PHRs). A monitoring service utilizes the data from the EHRs/PHRs to evaluate the patients' healthcare condition, and provides both value-added information as well as the raw data through a Web-based information portal for cooperating health and care services, in order to facilitate an optimal and efficient follow-up.

As part of the European funded FP7 project United4Health (U4H) [20] a telehealth trial system for COPD patients had been developed [21] . End-to-end security and privacy protection requirements and the solution approach for the trial system had been analyzed and published [4].

Threat Model Components

1. Identify Assets: An asset is anything that has business value and that must be protected from misuse by adversaries. The business value of an asset can range from very high to very low. The value of the identified assets is defined as the security services to be protected. There are three conventional security services known as CIA (confidentiality, integrity and authentication). Other security services considered are authorization and accountability.

   Figure 1 illustrates the main components of the studied telehealth trial system and the information flow between its components. Table 1 represents the identified assets according to system domain and asset name.

Table 1: Identified assets and their descriptions

Assets		
ID	System Domain, Asset Name	Description
A1	Point-of-Care	Assets relating to the underlying system at the patient point-of-care
A1.1	Patient credentials	The login credentials used by a patient to log into the system (via a UI-application on a device).
A1.2	Patient communication devices	A typical device (e.g. smartphone, tablet, PC, etc.) used by patients at the Point-of-Care (PoC) to display (output-UI), collect (input-UI), store or transmit patient-specific data. It supports communication with, and controlling medical devices (e.g. used to read data from a sensor device, to control an insulin pump, or to get/send parameters from/to a pacemaker).
A1.2.1	Communication devices credentials	Device-related information, such as a device identifier and key.
A1.2.2	Application on patient communication devices	A software application on a patient communication device supports the patient with carrying out daily measurements of certain life signs as required by the telecare service providers for follow-up decision support (e.g. in the U4H trial system, a user interface (UI) with questionnaire forms for daily reporting of COPD patient symptoms).
A1.2.3	Patient-related data	The patient communication device will store information related to the patient. This information can include the patients name, identifier and answer values for the daily self-reporting of certain disease-specific symptoms.
A1.3	Patient medical devices	A medical device is any instrument, apparatus, implementation, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related hardware component, intended to be used, alone or in combination, by people for one or more of the specific purposes of diagnosis, prevention, monitoring, and treatment of disease or other conditions [22] (e.g. peak flow meter, blood pressure device, pulse oximeter, etc.).
A2	Health Information Services (HIS) Infrastructure	Assets related to the underlying HIS infrastructure
A2.1	Personal / Electronic Health Record (PHR/EHR) Servers	All patient-related data (A1.2.3) from all remotely supervised patients are transmitted and stored in PHRs/EHRs. Data from medical devices (A1.2 and A1.3) are also stored in PHRs/EHRs.
A2.2	Telehealth Service Server	A dedicated telehealth service provides a Web-based information portal for telehealth and care service providers. This service takes patient data from the PHR/EHR system, evaluates the data according to red (critical), yellow (attention), or green (normal) conditions (Triage), and provides overview pages with the triage results of all supervised patients, as well as detailed condition pages with all information from a specific patient collected during supervision.
A3	Health & Care Sources	Assets related to the underlying systems of health & care service providers
A3.1	User credentials	Login credentials used by healthcare service members (e.g. doctors and telehealth nurses) to log into the system (through a website or dedicated device).

A3.2	Telehealth service terminals	Communication devices (tablets, smartphones, workstations) provide information for all support sources, including the formal and informal health & care service providers. With a telehealth service terminal the health and care service providers get access to the Web-portal containing the overview of patient status and history of detailed monitoring data provided by the telehealth service in the HIS infrastructure.
A3.3	Patient-related data	Information related to the patients (A1.2.3) retrieved by healthcare professionals through telehealth terminals. Certain patient-related data and information can be added or modified by a healthcare service member (e.g. notes related to diagnoses, the follow-up plan, etc.), according to the responsibility of the individual healthcare professional (e.g. nurse, doctor, administrator, family member, friends, etc.).

2. Defining the Trust Levels of System Users: Trust levels represent the access rights granted to entities (human users, devices and services) as shown in Table 2, and enforced by the system. Generally, threats can originate from two primary sources: internal agents (someone with authorized access) and/or external agents (someone with unauthorized access). In this study, only internal entities are considered threat agents (Figure 2). The three types of threat agents considered are: the patients themselves, authorized users (e.g. formal healthcare professionals and other health and care support staff such as system administrators) and informal healthcare assistants, such as friends and family members who provide support to patients and have very limited access to the system. The protection against internal agents is much more challenging than against external agents, because insiders are wholly or partially trusted subjects with legitimate access keys to resources.

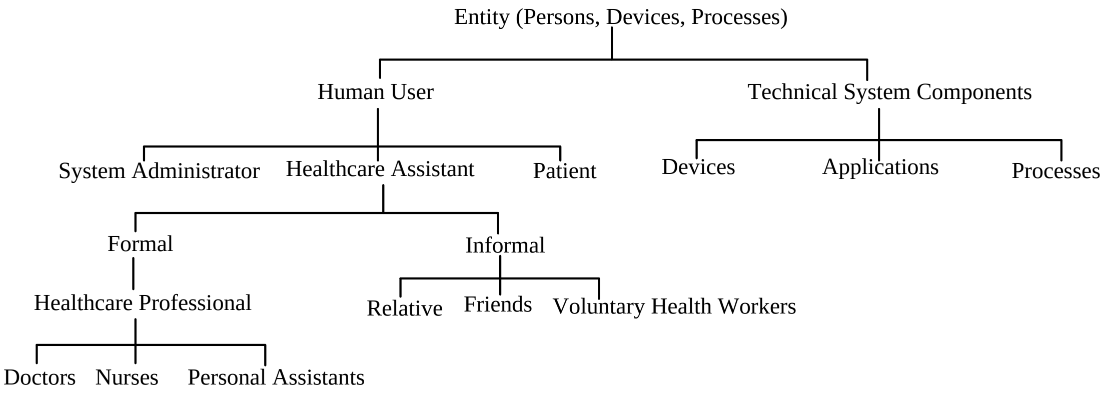

Figure 2: Entities of telehealth trial system.

Moreover, insiders have different motives, resource levels, skills, access privileges and risk tolerance, leading to the high probability that an attack will occur [23]. Resources are defined as assets that can be drawn on by an entity and the degree of access privilege an entity has to them. For instance, an administrator typically has unlimited access to some or all components (or parts) of a system as well as physical access to equipment, which is beyond what other users have access to. Knowledge implies data or information someone possesses about a particular system. For example, knowing critical information about a system, such as the security firewall employed for a particular sever, weak points in the system, and how the system works, can help to exploit vulnerabilities that allow attacks. Legitimate users such as administrators have greater ability to obtain knowledge of the target system without arousing suspicion. Knowledgeable insiders will always have the skills to undertake an attack that is usually limited to systems they are very familiar with. The more privileges and skills a person has, the more risk he or she represents. The motives and goals of insiders vary from one individual attacker to another. Insiders' motives range from identity theft to profit or sabotaging the target system. Some may conduct an attack for personal reasons, such as revenge on the enterprise or even fulfill plans to invoke policy changes within a system.

Table 2: Trust levels for threat agents

Trust Levels		
ID	Name	Description
TA1	Patient	
TA1.1	Patient with valid login credentials	A patient who uses A1.2.2 and has logged in using valid login credentials.
TA1.2	User with invalid login credentials	A user (impersonating a patient) who uses A1.2.2 and is attempting to log in using invalid login credentials.
TA2	Healthcare Assistant	
TA2.1	Formal healthcare professional with valid login credentials	A user (e.g. doctor, nurse, personal assistant, etc.) who is connected to A3.2 and has logged in using valid login credentials.
TA2.2	User with invalid login credentials	A user (impersonating a formal healthcare professional) who has connected to A3.2 and is attempting to log in using invalid login credentials.
TA2.3	Informal healthcare professional with valid login credentials	A user (e.g. relative, friend, etc.) who is connected to A3.2 and has logged in using valid login credentials.
TA3	Administrator	
TA3.1	Server administrator	The database server administrator has read and writes access to the database used to store PHRs/EHRs (A2.1).
TA3.2	Website administrator	The Website administrator can configure the Web-based information portal for telehealth and care service providers (A2.2 and A3.2).
TA4	Other system components	
TA4.1	Patient communication device	A device that provides applications and user interfaces for the patients to support the collection, transmission and illustration of data and information from the patient and the healthcare provider(s), transmitted via PHRs/EHRs.
TA4.2	PHR/EHR servers	A device used to store patient-related data (A1.2.3) from all remotely supervised patients.

The following entities of the telehealth trial system are shown in Figure 2:

(a) *System Administrator* - is responsible for system operation and/or maintenance. It is assumed that the system administrator has access to all system components, in order to ensure the correct operation of hardware and software. However, they should not have access to any health-related information of the patient. Administrators have sufficient resources and high IT skills. On the one hand, administrators are generally very trustworthy, but administrators who are not well-trained might unintentionally threaten the system. On the other hand, administrators who are dissatisfied or have been bribed may become spiteful and intentionally cause harm to the system.

(b) *Patient* - has access to his/her own medical devices, communication devices and personal medical records. Generally, patients have enough resources to attack a system, but those who are not IT experts have low skills to analyze and attack a system. Patients may act maliciously or non-maliciously to access privileges not assigned to them.

    (c) *Formal Healthcare Professionals - Doctors:* have access to their own patients' data, but not that of another doctor's patients; *Nurses or Personal Assistants:* have access to the information of patients they are responsible for. Healthcare professionals may also have adequate resources to attack a system because they have access to it, but their attack skills may be low since they are unlikely to be IT experts.

    (d) *Informal Healthcare Assistants* - friends, visitors and voluntary health workers have very limited access rights to the system (e.g. read only access to some of patients' data). Their role is only that of patient assistants at the point-of-care, or supporting the remote supervision and follow-up of the patient based on information about the patients' health status.

    (e) *Technical System Components* - devices (e.g. sensors, actuators), applications and/or processes that act on behalf of the patient, for instance patient communication devices and medical devices.

3. Data Flow Diagrams (DFD): DFD is a high-level way of disassembling the system and focusing on its functional components, and to analyze the flows of data through the system components [11]. DFD makes it easier to identify threats, to follow and analyze the adversary's data and commands throughout the system, and to identify which assets they interact with [10]. Figure 3 shows the DFD for the telehealth trial system, which was modeled with Microsoft threat modeling tools 2014.

4. Identifying Threats

   Table 3 summarizes the identified threats, which are categorized according to the following types: authentication, authorization and access, privacy, as well as auditing and logging threats.

   For authentication threats, all possible threats related to user identity and login credentials that would possibly enable others to gain access to the system are defined. The main concerns are loss (or theft) or sharing of user identities and login credentials, and authenticating patient devices. Patients sharing their login credentials with friends, relatives and/or healthcare providers may cause potential impact, like identity misuse, tampering with patient data, or private information disclosure, among others. Potential damage is classified as low, medium or high, according to the distribution of the business functions and processes. For instance, if one patient's login credentials were lost (or stolen), the impact would be low, because the damage would only affect one patient; but if a healthcare provider's identity was stolen, the impact would be very high, because this may affect more than one patient.

   Moreover, patient device authentication is very important. When a patient's communication device wants to communicate with the patient's medical device, both devices must authenticate each other, and ensure that they are what/who they claim to be, and are not compromised by an attacker. Similarly, when the patient's communication device wants to send or receive data from the PHR/EHR system, both require mutual authentication. Then the PHR/EHR can trust that it is receiving/sending data from/to the correct device (the right patient respectively), and the patient's communication device can trust that it is sending/receiving data to/from the correct server (the right healthcare provider respectively).

In the second category (authorization and access threats) threats related to unauthorized access to system components are listed. These threats include elevation of privilege, data tampering and/or disclosure of confidential data. With elevation of privilege threats, insiders may attempt to elevate their privileges in order to gain additional access to system components. For example, a patient or healthcare provider may impersonate the context of administrators in order to gain additional privileges and more control over the application or system. Data tampering refers to intentionally or accidentally modify, add and/or delete data, caused by insiders having over-privileges or inapplicable access control of a resource. Confidential data disclosure potentially occurs if sensitive data, such as patient health records and login credentials, can be viewed by unauthorized users due to improper data protection. The potential damage of such threats is stated as low, medium or high, depending on the distribution of business functions and processes. According to Table 3 (Threat Class 2 (T2)), the majority of threats are rated high, because for instance, gaining access to powerful accounts such as those of members of local administrator groups or local system accounts may cause massive damage to patients or healthcare providers.

In the third section of the table, threats related to privacy are identified. Privacy is subject to a variety of threats, including access to sensitive data in storage and data tampering. Threats to sensitive data in storage can affect data stored in the patients' communication devices or on PHR/EHR servers. Improper data protection on patient communication devices may allow attackers to read information not intended for disclosure.

In the final section, threats related to auditing and logging are listed. Auditing and logging should be used to help detecting suspicious activities, such as footprinting or possible password cracking attempts before exploitation actually occurs. These can also help dealing with the threat of repudiation. It is much harder for a user to deny performing an operation if a series of synchronized log entries on multiple servers indicate that the user indeed performed the transaction. Threats related to auditing and logging include potential data repudiation, log tampering and insufficient auditing. Data repudiation concerns users denying they had performed an action or initiated a transaction. For example, a patient or healthcare professional denies or claims that he/she did not receive, write or edit data. Log tampering entails an insider attacking logs via log files. For threats due to insufficient auditing, the logs must capture enough data to display what happened in the past and they must be well-protected to ensure that attackers are not able to cover their tracks.

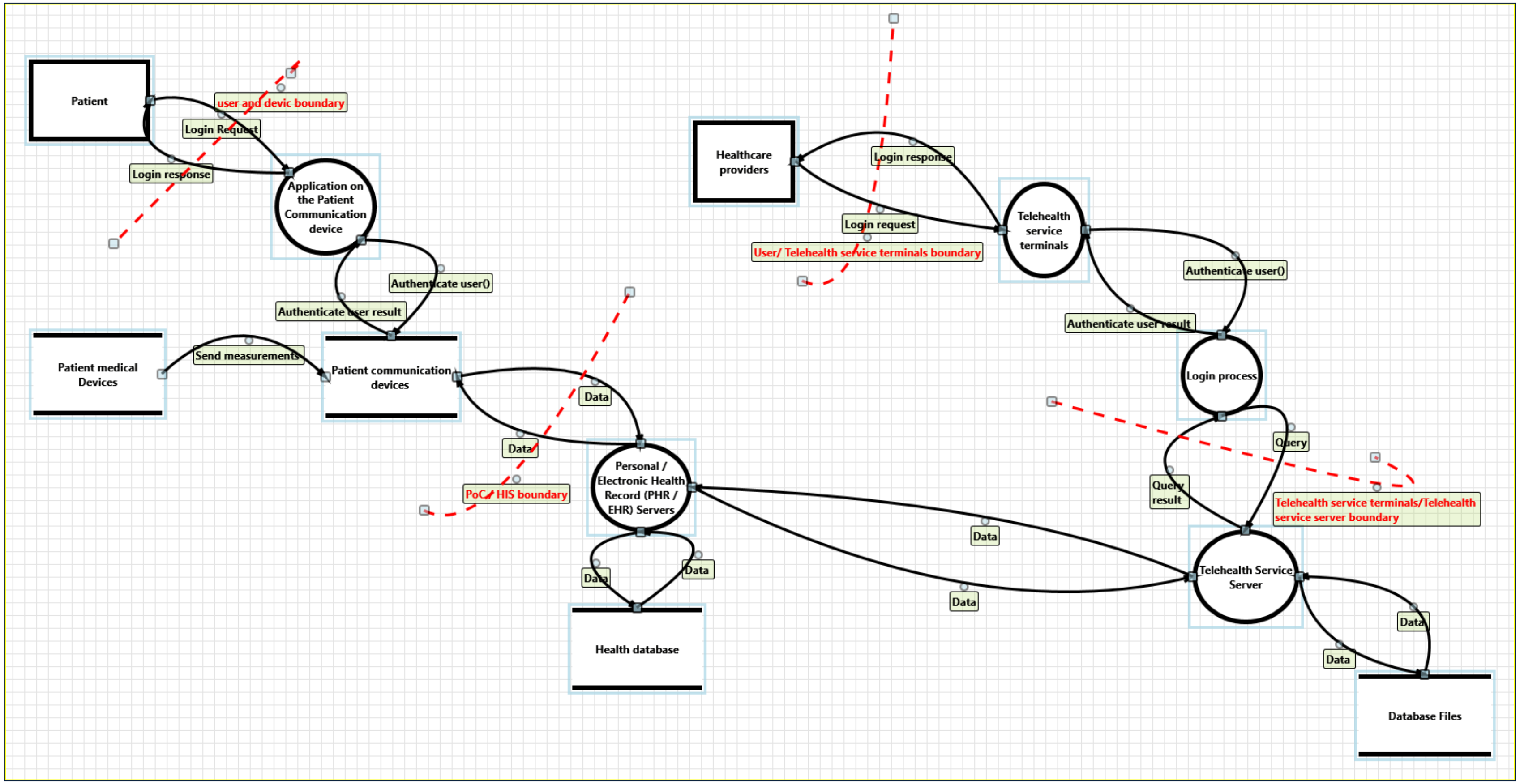

Figure 3: Data Flow Diagram for telehealth trial system.

Table 3: Classification of Threats

Threat/ID	**Threat Class 1 (T1): Authentication Threats** *Description:* unauthorized use or misuse of authorized user identities and login credentials			
ID	Description	Threat agent	STRIDE	Impact
T1.1	**Patient identity loss or identity sharing:** the patients leave their login credentials on a public place (e.g. write them down on a piece of paper) or share them with family, friends or relatives.	TA1.1	**S**	Low
T1.2	**Personnel identity loss or identity sharing:** healthcare providers, and/or system admins leave their login credentials in public places or share them with others.	TA2.1, TA3.1,TA 3.2	**S**	High
T1.3	**Identity spoofing:** patients reveal login credentials to someone (e.g. social engineering attack).	TA1.1, TA2.2, TA2.3	**S**	Low
T1.4	**Identity theft and misuse:** informal healthcare assistant (e.g. friends or family members) misuse patient identity to obtain medical services.	TA2.3	**E**	Medium
T1.5	**Identity theft and misuse:** system admins misuse patient identity for malicious acts (e.g. curiosity, disclosure, fraud and/or sabotage).	TA3.1, TA3.2	**S**	High
T1.6	**Spoofing of source:** patient medical devices may be spoofed by attackers, which may lead to incorrect data being delivered to patient communication devices.	T4.1, T4.2	**S**	High
T1.7	**Spoofing of source:** patient communication devices may be spoofed by attackers, which may lead to data being written to the attacker's target instead of the patients communication device.	T4.1	**S**	Medium
T1.8	**Spoofing of source:** Personal/Electronic Health Record (PHR/EHR) servers or telehealth service servers may be spoofed by attackers, which may lead to incorrect data being delivered to PHR/EHR servers or telehealth service servers.	TA4.2	**S**	High
Threat/ID	**Threat Class 2 (T2): Authorization and Access Threats** *Description:* unauthorized access (including read, write, modify, delete) to confidential data			
ID	Description	Threat agent	STRIDE	Impact
T2.1	**Unauthorized access:** unauthorized access to system data using shared (or stolen) passwords.	TA 1.1, TA 2.1, TA 2.3,	**E**	High
T2.2	**Unauthorized access:** patient intentional or accidental access beyond authorized privileges.	TA 1.1	**E**	Low
T2.3	**Unauthorized access:** system admins and informal healthcare professionals gain intentional unauthorized access to patient data for malicious acts (e.g. curiosity, disclosure).	TA 2.1, TA3.2, A3.3	**E**	High
T2.4	**Data tampering:** patients intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	TA 1.1	**T**	Medium
T2.5	**Data tampering:** formal healthcare professionals and system admins intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	TA 2.1, TA 3.2, A3.3	**T**	High
T2.6	**Elevation using impersonation:** informal healthcare professionals (e.g. friends or family members) may impersonate the patients context in order to gain additional privileges.	TA 2.3	**E**	Medium
T2.7	**Elevation using impersonation:** formal healthcare professionals or system admins may impersonate the context of other healthcare professionals or system admins in order to gain additional privileges.	TA2.1, TA 3.2, A3.3	**E**	High
T2.8	**Unauthorized access to administration interfaces:** malicious users may be able to gain access to configuration management through administration interfaces.	TA 1.1, TA 2.1, TA 2.3, TA3.2, A3.3	**E**	High

Threat/ID	**Threat Class 3 (T3): Privacy threats** *Description:* unauthorized disclosure to sensitive data			
ID	Description	Threat agent	STRIDE	Impact
T3.1	**Unauthorized disclosure:** patients accidentally access some confidential data via malware or file-sharing tools installed on their communication devices.	TA 1.1	**I**	Low
T3.2	**Unauthorized disclosure:** formal healthcare professionals and system admins intentionally or accidentally access some confidential data via malware or file-sharing tools installed on their communication devices.	TA 2.1, TA3.2, A3.3	**I**	High
T3.3	**Lost device:** patients losing their communication devices would cause exposure of sensitive data such as login credentials and PHR.	TA 1.1	**I**	Medium
T3.4	**Stolen device:** theft of patient communication devices that would cause exposure of sensitive data such as login credentials and PHRs.	TA2.3	**I**	Medium
T3.5	**Weak access control:** improperly protected data stored in patients' communication devices could allow attackers to read information not intended for disclosure.	TA3.2	**I**	Medium
Threat/ID	**Threat Class 4 (T4): Auditing and Logging Threats** *Description:* suspicious activities detected, such as footprinting or possible password cracking attempts before exploitation actually occurs			
ID	Description	Threat agent	STRIDE	Impact
T4.1	**Potential data repudiation:** patient denies or claims not receiving, writing or editing data.	TA 1.1	**R**	Medium
T4.2	**Potential data repudiation:** formal healthcare professionals or admins deny or claim not receiving, writing or editing data.	TA 2.1, TA3.2, A3.3	**R**	High
T4.3	**Log files tampering:** patients, system admins or formal or informal healthcare providers delete or update log files in any way.	TA 1.1,TA 2.1, TA 2.3, TA3.2, A3.3	**T**	High
T4.4	**Insufficient auditing:** logging sufficient and appropriate data to handle repudiation claims.	TA 1.1, TA 2.1, TA 2.3, TA3.2, A3.3	**R**	High

5. Mitigation Plan

   Up to this point, all potential threats have been identified and analyzed. To reduce the threats' risk, the mitigation strategy to each threat must be identified. According to the security and privacy protection requirements in [4] and countermeasure techniques corresponding to STRIDE [12], Table 4 suggests a list of countermeasures to address the identified threats. Moreover, security awareness is very paramount. All authorized users (patient, healthcare provider and admins) should have an awareness program in which they should learn about all types of security threats and their consequences.

4 Conclusions and Future Work

The motivation behind creating a threat model for telehealth systems is to help enhancing system security in terms of protecting healthcare information from security threats, such as patient data disclosure and/or unauthorized access or modification by attackers, among others. In this work, a threat model process for telehealth systems using Microsoft threat modeling tool 2014 was established. In order to prepare for threat mitigation, system assets, threat agents, adverse actions, threats and their effects as well as a list of countermeasures were identified and analyzed.

This work will be used to develop security requirements [4] and to better design and implement system protection solutions against telehealth application threats. In the future, the system security will be further investigated at the Center for eHealth and Health Care Technology at the University of Agder. The plan is also to analyze the outsider threats in the telehealth trial system and verify whether implemented system protection solutions will perform effectively and efficiently on identified threats.

Table 4: Threats and Countermeasures

STRIDE	Threat	Countermeasures
Spoofing	T1.1, T1.2, T1.3, T1.5 T1.6, T1.7, T1.8	• Strong authentication: User must be authenticated to the system using a strong password policy, biometrics or multi-factor authentication mechanisms. • Encryption: All credentials must be encrypted, and it has to be ensured that credentials do not traverse the wire in clear text form. • Cryptographic protocols: Cryptographic protocols such as TLS/SSL must be used to ensure a secure (encrypted) communication between system components.
Tampering	T2.4, T2.5, T4.3	• Strong authorization: Appropriate access control mechanisms such as role-based access control (RBAC) must be deployed with least privileges and separation of duties principles. Users must be assigned to access with minimum privileges. • Data hashing and signing: All confidential data must be hashed and signed to ensure that the data is valid (untampered and came from the correct/expected source). • Secure communication links: The communication links between system components must be ensured by using protocols that provide message integrity and confidentiality.
Repudiation	T4.1, T4.2, T4.4	• Secure audit trails: All activities (such as successful and unsuccessful authentication) and sensitive data (e.g. cookies and authentication credentials) must be logged and recorded.
Information disclosure	T3.1, T3.2, T3.3, T3.4, T3.5	• Strong authorization: Ensure that an appropriate access control mechanisms is deployed and only authorized users can access to data. • Encryption: Ensure that all sensitive data is encrypted (in storage or during transit) and only authorized users can read this data. • Secure communication links: Ensure that all communication links are secured with protocols that provide message confidentiality.
Elevation of privilege	T1.4, T2.1, T2.2, T2.3, T2.6, T2.7, T2.8,	• Principle of least privilege : All authorized user must have a least privilege and minimum required access.

References

[1] S. Silow-Carroll, J. N. Edwards, and D. Rodin, “Using electronic health records to improve quality and efficiency: the experiences of leading hospitals,” *Issue Brief (Commonw Fund)*, vol. 17, pp. 1–40, 2012.

[2] A. T. Association *et al.*, “Telemedicine, telehealth, and health information technology: The american telemedicine association (ata) issue paper,” *Washington, DC: American Telemedicine Association, May 2006, at http://www. american-telemed. org/files/public/policy/HIT_Paper. pdf, accessed*, vol. 8, 2012.

[3] B. Fong, A. C. M. Fong, and C. K. Li, *Telemedicine technologies: Information technologies in medicine and telehealth.* John Wiley & Sons, 2011.

[4] M. Gerdes and R. Fensli, “End-to-end security and privacy protection for co-operative access to health and care data in a telehealth trial system for remote supervision of copd-patients.” *Proceedings of the 13th Scandinavian Conference on Health Informatics, Troms, Norway*, 2015.

[5] M. Meingast, T. Roosta, and S. Sastry, “Security and privacy issues with health care information technology,” in *Engineering in Medicine and Biology Society, 2006. EMBS’06. 28th Annual International Conference of the IEEE.* IEEE, 2006, pp. 5453–5458.

[6] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: current state of research,” *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279–314, 2010.

[7] S. Avancha, A. Baxi, and D. Kotz, “Privacy in mobile technology for personal healthcare,” *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 3, 2012.

[8] J. C. Pendergrass, K. Heart, C. Ranganathan, and V. Venkatakrishnan, “A threat table based assessment of information security in telemedicine,” *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 9, no. 4, pp. 20–31, 2014.

[9] C. W. Group, “Healthcare and public health cybersecurity primer: Cybersecurity 101.” [Online]. Available: http://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf

[10] S. Myagmar, A. J. Lee, and W. Yurcik, “Threat modeling as a basis for security requirements,” in *Symposium on requirements engineering for information security (SREIS)*, vol. 2005, 2005, pp. 1–8.

[11] S. F. Burns, “Threat modeling: A process to ensure application security,” *GIAC Security Essentials Certification (GSEC) Practical Assignment*, 2005.

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

[13] Microsoft, “Microsoft security development lifecycle (sdl).” [Online]. Available: https://www.microsoft.com/en-us/sdl/

[14] S. K. Vashist, E. M. Schneider, and J. H. Luong, "Commercial smartphone-based devices and smart applications for personalized healthcare monitoring and management," *Diagnostics*, vol. 4, no. 3, pp. 104–128, 2014.

[15] t. o. w. a. s. p. OWASP, "Application threat modeling." [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling

[16] M. S. U. LTD, "Process for attack simulation and threat analysis engineering attack resilient software and applications," 2014. [Online]. Available: http://www.infosecurityeurope.com/__novadocuments/87663?v=635684093624900000

[17] P. Saitta, B. Larcom, and M. Eddington, "Trike v. 1 methodology document [draft]," *URL: http://dymaxion.org/trike/Trike_v1_Methodology_Documentdraft. pdf*, 2005.

[18] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," *Pittsburgh, PA, Carnegie Mellon University*, 2003.

[19] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, *Improving web application security: threats and countermeasures.* Microsoft Redmond, WA, 2003.

[20] United4Health, "P7 eu project united4health 2013." [Online]. Available: Umbrellaproject:http://www.united4health.eu/;Norwegianproject:http://www.united4health.no/.

[21] M. Gerdes, B. Smaradottir, F. Reichert, and R. Fensli, "Telemedicine and cooperative remote healthcare services: Copd field trial." *Studies in health technology and informatics*, vol. 210, pp. 455–457, 2014.

[22] W. H. Organization *et al.*, "Medical device regulations: Global overview and guiding principles," 2003.

[23] J. Hunker and C. W. Probst, "Insiders and insider threats- an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4–27, 2011.