Threat Modeling for Mobile Health Systems

Matteo Cagnazzo[1] and Markus Hertlein[3] and Thorsten Holz[2] and Norbert Pohlmann[1]

***Abstract*— Mobile Health (mHealth) is on the rise and it is likely to reduce costs and improve the quality of healthcare. It tightly intersects with the Internet of Things (IoT) and comes with special challenges in terms of interoperability and security. This paper focuses on security challenges and offers a mitigation solution especially with a focus on authentication and encryption for resource constrained devices. It identifies assets in a prototyped mHealth ecosystem and classifies threats with the STRIDE methodology. Furthermore the paper identifies associated risk levels using DREAD and outlines possible mitigation strategies to provide a reasonable trustworthy environment.**

I. INTRODUCTION

Advances in mobile health (mHealth), respectively IoT-Health, are likely to reduce costs and improve the quality of healthcare. Especially with the paradigm shift from inpatient care towards ambulant and home care, mobile and ubiquitous technologies are an inevitable step. The shift is due to increasing cost pressure, ageing society and shortage of skilled professionals[24]. Mobile health applications can increase access to healthcare, encourage self-management and maintain treatment. Internet of Things (IoT) devices are used within healthcare systems and form mHealth environments. Wearables with various sensors, for example gyroscopic-, heart rate- or bioimpedance sensors are often deployed in the Body Area Network (BAN) of the patient. These devices come with a lot of challenges in terms of interoperability and security which need to be considered and treated seriously [23]. *ENISA* identifies "asset and configuration management as a relevant technical measure" to prevent attacks [7]. Furthermore, this paper addresses a key recommendation from [7] because it conducts risk and vulnerability assessment for a mHealth architecture which is deployed in a clinical context. This paper discusses most recent related work in chapter II. Afterwards it introduces current developments and background knowledge for mHealth in chapter III-A and threat modeling in chapter III-B. After this we model the threats and define assets in chapter IV. We use a STRIDE-based approach to model threats[22]. To assess the associated risks for specific threats we use the DREAD model [25]. At the end of the paper possible mitigation strategies are discussed in chapter V and conclusions are drawn in chapter VI.

*This work is partly funded by the Federal Ministry of Education and Research in Germany (Grant.Nr: 16SV7775)

[1]M. Cagnazzo and N. Pohlmann are with the Institute for Internet-Security, Westphalian University of Applied Sciences, 45876 Gelsenkirchen, Germany {lastname} at internet-sicherheit.net

[2]T. Holz is with the Horst Gortz Institute for IT-Security (HGI), Ruhr-University Bochum, Germany thorsten.holz at rub.de

[3]M. Hertlein is with XignSys GmbH, Gelsenkirchen, Germany hertlein at xignsys.de

II. RELATED WORK

Several papers on future research direction indicate that privacy and security are key issues to the successful deployment of mHealth[16][3]. [16] defines one research challenge as: "clarify threats and develop security and privacy protections for smartphone apps that handle medical and health data". This paper aims to give an overview of threats and mitigation strategies for current and future mHealth applications. Current work on threat modeling in healthcare is focusing on telehealth and is not paying attention to mHealth specific threats, especially if data is stored in a cloud environment[1]. Works like [19] are defining and mitigating threats for smart home systems and consider parenthetically how mHealth systems and threats interact with it. [5],[21] and others try to solve the authentication, usability and confidentiality problem within the IoT in general. They do not use standardized approaches to identify threats and mitigate them as well. Stationary care telehealth service terminals, as described in [8] and [20] are likely reduce mobile application scenarios for doctors and medical personnel. This stationary approach is something a mHealth ecosystem is aiming to overcome in the future, to empower mobility to doctors and other caregivers.

Common legacy protocols used in medical environments often lack security and privacy aspects. [11] shows that the often used "HL7" protocol has no security or privacy mechanisms specified especially in version two, which is the most deployed solution in production systems.

Figure 1 shows a prototypical mHealth system. It is derived from an architecture which is used in the MITAS-SIST project. The project is funded by the German Federal Ministry of Education and Research. Figure 2 shows a more detailed view of the components, which data has to pass in the architecture. The wearable on which the sensors are deployed will produce huge amounts of data. Analyzing big amounts of data quickly becomes impracticable for humans, therefore an artificial intelligence(AI) is trained during the research project. Current research shows, that the used models can be exploited by an attacker as well, therefore we include the artificial intelligence into our threat model[9][17].

III. BACKGROUND

This section will give a brief definition and introduction of mHealth as well as an architectural overview of an mHealth system. Furthermore threat modeling and the used methodology is introduced.

A. mHealth

mHealth is the combination of computing and internet technologies, with information and communication systems. In addition with sensors it can form a wearable body area network (BAN) with the patients smartphone[15]. Patients as well as health- and careproviders can benefit from mHealth solutions. mHealth applications that run on information systems like smartphones are used by patients and doctors to access data within the health platform as shown in figure 1. Doctors, caretakers and patients access the platform via an application which can either be deployed to a mobile or stationary device. The patient environment consists of devices and applications in personal patient environment, like wearables and smartphones. These are needed to collect measurements of sensor data, support self reporting as well as feedback or intervention from the caretaker. Most sensors that are deployed are also modules in the IoT, therefore mHealth and IoT components intersect each other. The patients send data via mobile or WLAN networks to the health service cloud. The data is stored in an electronic or personal health record systems(EHR/PHR) which is integrated in the hospital cloud service. The most used protocol is HL7[11]. The data can be crawled by monitoring services or an artificial intelligence, which support the doctor in his decision making, offer more granular insights for patient and doctor, as well as providing suggestions how the patient can improve his health. Other health and care providers could get access to the data as well. This yields privacy concerns which are out of scope of our paper, therefore we neglect third party scenarios. Patients benefit from mHealth applications around the world, since the deployment of mHealth applications can be done in a cost effective way. Especially developing countries can benefit from the widespread deployment of mHealth solutions[10]. "Respectively, 50 % and 70 % of the interventions were effective in promoting physical activity and healthy diets" says[18].

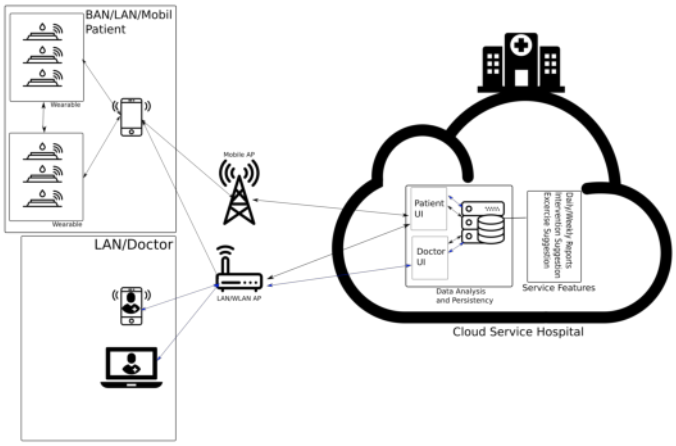

Fig. 1. mHealth Prototype Architecture

B. Threat Modeling

Threat modeling is an important aspect of the security development lifecycle, which is a process aiming to build better and more secure software[13]. It is a technique, which aims to find assets, analyze potential threats and mitigate them. This provides defenders with important insights:

- The most likely attack vectors
- Assets an attacker is attracted to.
- Attack vectors that otherwise would have gone unnoticed

The threats which are found during the threat modeling phase will be associated with a security risk to rank them and prioritize certain assets. An asset is defined by ENISA as "anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission".

TABLE I
CONNECTION BETWEEN STRIDE AND MHEALTH ENVIRONMENT

Threat Categories	mHealth Security Perspective
Spoofing: attacker poses as an authorized user or entity	Attacker using user authentication information to access sensitive medical data
Tampering: Modifying data maliciously	Attacker modifying data in transit (e.g. from BAN to LAN) or at rest
Repudiation: Filtering malicious actions if proof is missing	Authorized user performs illegal operations and system cannot trace it, other parties cannot prove this
Information disclosure: Exposing information to any unauthorized entity	Leaking raw data or medical records
Denial of Service: Denying service to valid users	Attacker jamming BAN or DoS'ing hospital environment
Elevation of Privilege: User gains privilege rights and manipulates the system	Attacker gains access to security systems as a trusted entity

The threat modeling technique used in this paper is STRIDE by Microsoft which is an abbreviation for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege [22]. There are more threat modeling frameworks, for example PASTA or OCTAVE [2][25]. To rank threats we use the DREAD model, which is described in the next section.

Table I defines each threat category and relates it to a specific mHealth attack scenario. After the STRIDE threats are addressed, a metric for the risk of an actual attack needs to be calculated. We will use the DREAD model to evaluate the likelihood of an attack by exploiting a particular threat[14]. The DREAD model consists of Damage potential,

Reproducibility, Exploitability, Affected Users and Discoverability. The DREAD risk can be calculated as follows:

$$Risk_D = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTEDUSERS + DISCOVERABILITY) \quad (1)$$

Values from 1 (low) to 3 (high) are assigned to each addend of equation 1. The sum is calculated and the result can fall in the range of 5-15. Afterwards one can rank threats with overall ratings of 12-15 as high risk, 8-11 as medium risk, and 5-7 as low risk.

IV. STRIDE THREATS

The process of threat modeling according to STRIDE can be broken down into three blocks:

- Identifying assets
- Listing potential threats
- Mitigating threats

To define threats and get a more detailed overview of our architecture, a graphical representation of the data flows and critical points are illustrated with Microsofts Threat Modeling Tool 2017 in figure 2. Data is acquired

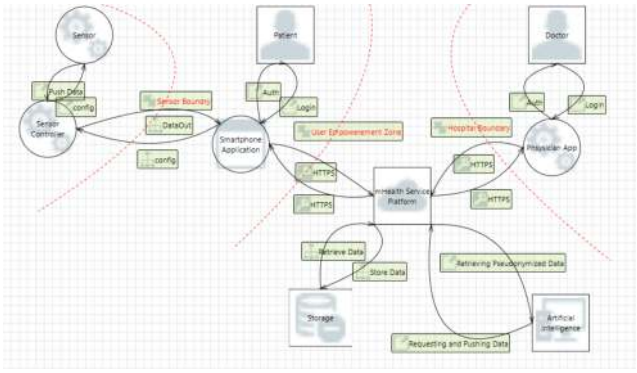

Fig. 2. Data Flow and critical points

from one or more sensors on a wearable and pushed to a central sensor controller. The data is collected and persisted. After a configurable time-interval the data is pushed to the application over a *Bluetooth LE* connection. The application can send configuration data to the sensor controller and acknowledges received and stored sensor data. Configuration data could be, for example the sampling rate of a specific sensor. The patient authenticates himself and gets access to the application. Sensor data is transmitted from the device to the service platform over a *https* connection. This data gets acknowledged, after it is stored successfully. If medical personnel wants to check on a patients condition it authenticates itself on its application and sees selected vital data of the patient. If the medical supervisor wants to send interventions to the patients, these are sent to the patient over the cloud infrastructure and gets an acknowledgement after the patient read the intervention. From the flow of data over the respective components a threat model is generated.

TABLE II
ASSETS AND IMPACT

Asset	Impact
Network components connecting the user to the service	No Availability Loss of information
Network components connecting the sensor to the Application	No Availability Loss of information
Identity management for access control and authentication	User specific information cannot be stored or retrieved
Database and Storage Components	Loss of Availability Loss of Data Integrity Loss of feedback
Eavesdropping on Communication	Confidentiality Violation

Table II shows identified assets and the impact, which a failure of the respective asset would have. Loss of Availability is the most common impact the alteration of an asset could have. Since the mHealth solution should provide close to realtime feedback or intervention to the patient, a loss of availability could be harmful for patient safety not just for security reasons. Depending on the health or monitoring scenario in which the solution is used, close to realtime can range from a few seconds (cardiac monitoring) to 15 minutes (depression monitoring).

Other important impacts are confidentiality violation and loss of information. Since the data is considered medical it is highly personal and must be protected carefully. The mHealth platform should be trustworthy, therefore it should provide and maintain confidentiality wherever possible.

Table III shows threats towards patient or personnel authentication. It focuses on the loss and misuse of credentials, as well as spoofing of sensors. Generally threats are more severe, if an admin or health personnel is compromised because this would alter the whole integrity of the platform whilst an attack against a single user would only put that specific user at risk. If an attacker or user gains unauthorized access to the platform the threats are elevation of privilege, data tampering and disclosure. Table IV shows this in the STRIDE column. A user could try to elevate his privileges and gain admin access to the service component or the PHR. This elevation could lead to disclosure of private data from other users. The associated risks by an authorization threat are at least medium but most of the times high, because gaining administrator or system privileges, even if they are only local, can cause damage to patients as well as healthcare providers. Furthermore spoofed sensors or smartphones can be used to flood the architecture with requests, forcing a denial of service

TABLE III
AUTHENTICATION THREATS

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

because the service or smartphone cannot respond.

Privacy is of huge importance for patients, especially if they suffer from a mental disease. A disclosure of their illness can either be beneficial or hinder the healing process but for most patients it is a dilemma whether they should disclose or conceal it[4].

TABLE IV
AUTHORIZATION AND ACCESS THREATS

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

Nonetheless individuals suffering from any illness should choose for themselves, if they want to disclose their illness, therefore patient data disclosure by an adversary should be prevented at all costs. Lost or stolen devices, especially lost wearables only pose a low risk to private data disclosure, because an attacker cannot read sensitive data from it. Only the last few sensor measurements are stored on the wearable, therefore the information gain is minor. If the smartphone is lost or stolen the information leakage is bigger, but no information from a PHR is exposed.

TABLE V
PRIVACY THREATS

Description	STRIDE	DREAD
Patient Data Disclosure	I	High
Administration Data Disclosure	I	High
Lost Smartphone	I	Medium
Lost Wearable	I	Low
Stolen Smartphone	I	Medium
Stolen Sensor	I	Low
Weak access control smartphone	I	Medium
Weak access control wearable	I	Low

The last threat category are threats that target artificial intelligences. Table VI shows that these threats are at least of medium importance since an altering of the AI would alter the integrity of the whole platform. Someone could try to change the training data which would mean that every decision the AI does is made from false assumptions, therefore this is the main threat and has a high risk, for now. A non targeted adversarial attack has the goal of forcing the classifier to return an incorrect result. If for example heart rate is monitored an attacker could try to make the classifier return the result cardiac disease, even though the patient is healthy. A targeted attack would try to yield a whole class of the AI and make it return this class regardless of the input. A targeted attack could be that every patient where the data looks like a cardiac arrhythmia will be diagnosed with an infarction. Both attacks imply, that an attacker has successfully gained access to the smartphone or is an active adversary in the same network, because he needs to manipulate the data sent to the mHealth service.

TABLE VI
ADVERSARY THREATS

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

V. POSSIBLE MITIGATION STRATEGIES

The assets can be grouped by the different kinds of the underlying technologies and processes. This leads to different

mitigation strategies for each scenario. Even though security and privacy are the main factors in the healthcare environment to focus on, the interoperability between systems and devices is gaining more and more importance, since sensors and smart devices are spreading faster. Therefore, this paper presents a holistic approach as the mitigation strategy covering all parts of the mHealth system. A distributed system like the presented prototypical mHealth system (Fig. 1) can be harmed by two independent classes of attacks.

The first class is physical attacks, for example the physical destruction of a sensor or the disturbing of the interconnection of the sensors, smart devices and cloud services. That kind of attacks cannot be prevented with IT-Security mechanisms.

The second threat class is virtual attacks, like data manipulation. We are only focusing on attacks of the second class. In reverse that means, that Denial of Services through connection jamming or physical destruction is not part of this research. A Denial of Service could also be achieved if an attacker is able to conquer a connection, for example through connection hijacking. That kind of DoS is part of the second class of attacks and can be prevented by using proper authentication and IT-Security mechanisms on different network layers.

The hypothesis is, that each threat of the classes can be conquered with a modern approach of well-known authentication and encryption techniques. That means that threats towards authorization and access can be prevented with a reliable authentication process and that threats towards privacy can be prevented by using proper encryption techniques. Even these processes must be built on a reliable authentication. The reason why encryption without authentication is not enough to gain a high level of privacy, is because of the communication between several entities. Old fashioned networks are usually directly wired. In these kinds of networks there was only a 1:1 communication between entities. Every entity only received the data, that was determined for them. Today we have a n:n communication network where most data are accessed by more than one entity, but with different rights for different reasons. Device authentication is of importance since no adversary should be able to put on the wearable and start transmitting data to the mHealth platform. The Wearable should mutually authenticate against the smartphone and the smartphone mutually against the service platform to ensure correctness of the entities.

In this research we are mainly using XignQR [12]. XignQR is a fully cryptographical based authentication and identity management system, which can manage identities for persons as well as for machines. The concept of XignQR matches the requirements of mutual authentication between every entity perfectly and the encryption of communication and data based on previous authentication process. Every entity is equipped with a public key pair and a corresponding certificate. For sensors with less computing power a symmetric secret is used. If a sensor uses a symmetric key for authentication and encryption, the smartphones acts as gatekeeper. That means, that the cloud infrastructure will only process data from the sensor if the data is signed by the smartphone and the data can be decrypted with a combination of the secret key of the wearable itself and a generated one-time-secret derived from the information of the smartphones public keypair.

In that way data integrity, authenticity and trust can be achieved. Not less important is the liability of the data that is sent to the wearable, e. g. for configuration purpose. Since a sensor may not have enough computing power to perform asymmetric cryptography a chain of trust must be built through the smartphone. To ensure trust, the wearable has to be paired with the smartphone application in a first step. In the pairing process two symmetric keys are derived. One is stored in the smartphone and the other is transmitted to the mHealth cloud environment. That one that is stored in the smartphone is used to calculate a one-time-secret for the authentication of the communication between smartphone and wearable. The other secret sent to the mHealth cloud environment is used for the encryption and integrity check of the data, that is sent from cloud to sensor and vice versa.

With that way of mutual authentication and encryption, based on symmetric and asymmetric cryptography all the key aspects of IT-Security authenticity, integrity, trust, liability can be achieved. The missing part is availability. Even here we are using a system that prevents Denial of Service attacks using the mechanism of mutual authentication. The cloud architecture is protected by a system that filters different kinds of DoS attacks on each of the ISO/OSI layers. Filters are using deep packet inspection to recognize malicious traffic. With that technique DoS can be prevented in the backbone of an infrastructure without entering the application layer. For example, one filter makes a rule based decision. The first message of the communication between entities must initiate the mutual authentication process. If the first message is another type of message as the initiation message, then the traffic is not routed to the infrastructure. On the application layer a machine learning based system is used, which protects the cloud infrastructure, even if an attacker uses its own smart device for the attack. The proper roll-out and management of digital certificates also prevents scaling of an attack that is used by an internal attacker, after a successful authentication. With the concept of mutual authentication we can ensure 1:1 communication on the application layer between smart device and cloud infrastructure.

VI. CONCLUSIONS AND FUTURE RESEARCH

This research paper provides a comprehensive, high-level overview of threats and its mitigations in a classical information security context within a mHealth environment. Certain threats that were identified, have the possibility to harm

patients and cause physical or mental damage. These threats must be prioritized, analyzed and mitigated with extreme caution in real world settings. Since the ecosystem for mHealth is very heterogeneous this work can function as an orientation during the development of a mHealth application but specific threat analysis has to be performed depending on the medical use case. This work should give a high level overview of threats and mitigations that can be used to deploy an at least reasonable secure mHealth ecosystem. Since threat modeling is an iterative process, this work is just a starting point while architectures and technologies used in mHealth still continue to develop.

A remaining research challenge in the mHealth ecosystem is, how replacement devices, or devices which have a high fluctuation, are handled. If a device is going offline due to maintenance or repair reasons, how can it's temporary replacement be integrated in a simple and efficient, yet secure and trusted way. Especially trustworthy authentication becomes a challenge because it is an unknown device, which comes from a vendor and is not integrated in our system. Temporary access needs to be granted and revoked in an easy way, while the high standards for security and privacy must still apply.

Future research has to focus on the exploration, exploitation and mitigation of those vulnerabilities and the correlation between security threats and patient safety. Legacy protocols and standards like *DICOM* or *HL7* need to be evaluated from a security perspective as well. This could be done if the *Common Vulnerability Scoring System* is expanded by possible patient harms. Another important research direction is how to perform soft- and firmware updates on past, current and future devices and architectures so they are resilient to modern and future threats. Another important research step would be to test adversarial input in systems that implement an AI to analyze and diagnose radiologic recordings or other medical exchange formats.

REFERENCES

[1] Abomhara, Mohamed, Martin Gerdes, and Geir M. Kien. "A stride-based threat model for telehealth systems." Norsk informasjonssikkerhetskonferanse (NISK) 8.1 (2015): 82-96.

[2] Alberts, Christopher J., et al. "Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0." (1999).

[3] Arora, Shifali, Jennifer Yttri, and Wendy Nilsen. "Privacy and security in mobile health (mHealth) research." Alcohol research: current reviews 36.1 (2014): 143.

[4] Bril-Barniv, Shani, et al. "A Qualitative Study Examining Experiences and Dilemmas in Concealment and Disclosure of People Living With Serious Mental Illness." Qualitative Health Research 27.4 (2017): 573-583.

[5] Cagnazzo, Matteo, Markus Hertlein, and Norbert Pohlmann. "An Usable Application for Authentication, Communication and Access Management in the Internet of Things." International Conference on Information and Software Technologies. Springer International Publishing, 2016.

[6] European Union Agency for Network and Information Security (ENISA), Glossary, accessed: 08/17 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

[7] ENISA "Cyber security and resilience for Smart Hospitals", European Union Agency for Network and Information Security, 2016.

[8] Gerdes, Martin, and Rune 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." SHI 2015, Proceedings from The 13th Scandinavien Conference on Health Informatics, June 15-17, 2015, Troms, Norway. No. 115. Linkping University Electronic Press, 2015.

[9] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." arXiv preprint arXiv:1412.6572 (2014).

[10] Goel, Sonu, et al. "Bridging the human resource gap in primary health care delivery systems of developing countries with mhealth: narrative literature review." JMIR mHealth and uHealth 1.2 (2013).

[11] Hasselhorst, Dallas "HL7 Data Interfaces in Medical Environments: Understanding the Fundamental Flaw in Healthcare", SANS Reading Room, 2017.

[12] Hertlein, Markus, Manaras, Pascal, and Pohlmann, Norbert: Bring Your Own Device For Authentication (BYOD4A) The XignSystem. In Proceedings of the ISSE 2015 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe 2015 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2015

[13] Howard, Michael, and Steve Lipner. "The security development lifecycle." Vol. 8. Redmond: Microsoft Press, 2006.

[14] Howard, M. and LeBlanc, D. Writing Secure Code, Second Edition, Microsoft Press , December 2002.

[15] Istepanian, Robert SH, and Bryan Woodward. M-health: Fundamentals and Applications. John Wiley & Sons, 2016.

[16] Kotz, David, et al. "Privacy and security in mobile health: a research agenda." Computer 49.6 (2016): 22-30.

[17] Kurakin, Alexey, Ian Goodfellow, and Samy Bengio. "Adversarial examples in the physical world." arXiv preprint arXiv:1607.02533 (2016).

[18] Mller, Andre Matthias, et al. "The effectiveness of e-& mHealth interventions to promote physical activity and healthy diets in developing countries: A systematic review." International Journal of Behavioral Nutrition and Physical Activity 13.1 (2016): 109.

[19] Olawumi, Olayemi, et al. "Security Issues in Smart Home and Mobile Health System: Threat Analysis, Possible Countermeasures and Lessons Learned." International Journal on Information Technologies and Security 9.1 (2017): 31-52.

[20] Ondiege, Brian, Malcolm Clarke, and Glenford Mapp. "Exploring a New Security Framework for Remote Patient Monitoring Devices." Computers 6.1 (2017): 11.

[21] Sicari, Sabrina, et al. "A security-and quality-aware system architecture for Internet of Things." Information Systems Frontiers 18.4 (2016): 665-677.

[22] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.

[23] Tarouco, Liane Margarida Rockenbach, et al. "Internet of Things in healthcare: Interoperatibility and security issues." Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012.

[24] 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.

[25] Uceda Velez, Tony, and Marco M. Morana. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons, 2015.