Data Security Overview for Medical Mobile Apps

Assuring the Confidentiality, Integrity and Availability of data in transmission

Ceara Treacy, Fergal McCaffery
Regulated Research Centre & Lero
Dundalk Institute of Technology,
Dundalk, Ireland
e-mail: {ceara.treacy, fergal.mccaffery }@dkit.ie

Abstract— **Mobile medical apps are a growing mechanism for healthcare delivery through an increasingly complex network of information technology systems connecting patients, doctors, nurses, pharmacists and medical devices. Characteristically, these apps are designed to gather measure and transmit sensitive personal health data, which is required to be kept secure through regulations and legislation. With the integration of mobile medical apps into the healthcare industry, the multitude of sensitive personal health data transmitted across various applications, technologies and networks is increasing. This raises questions about compromised patient privacy and the security of the data associated with the mobile apps. The detections of increased app hacking by security companies and researchers are especially significant amidst today's rapid growth in healthcare mobile apps. Consequently, security and integrity of the data associated with these apps is a growing concern for the app industry, particularly in the highly regulated medical domain. Until recently, data integrity and security in transmission has not been given serious consideration in the development of mobile medical apps. This paper provides an overview of existing mobile medical apps data security issues and security practices. We discuss current regulations concerning data security for mobile medical apps. The paper introduces our current research in data security for mobile medical apps. There are currently no procedures or standard practices for developers of mobile medical apps to assure data integrity and security. The paper introduces the concept of a process model to assist mobile medical app developers to implement data security requirements to assure the Confidentiality, Integrity and Availability of data in transmission. The research is grounded on the only published medical device security standard IEC/TR 80001-2-2:2012.**

Keywords- Mobile Medical Apps; data security; Mobile Medical Apps data regulations.

I. INTRODUCTION

In mHealth, mobile apps are in general classified into mobile health/wellbeing apps (MHAs) and mobile medical apps (MMAs) [1]. This classification is predominantly driven by the Food and Drug Administration (FDA) Mobile Medical Applications Guidance [2] and is outlined in Table I. Medical professionals and the general public use mobile apps to perform many tasks, such as: sharing medical videos, photos and x-rays; health and fitness tracking; blogs to post medical cases and images; share personal health information; and keep track of alerts on specific medical conditions and interests [3].

MMAs are evolving quickly coinciding with the processing capabilities of mobile devices and are currently one of the most dynamic fields in medicine [4]. The use of mobile apps enables dynamic access to personal identifiable information and the collection of greater amounts of sensitive data relating to personal health information (PHI). The use of mobile apps implicates changes in the way health data will be managed, as the data moves away from central systems located in the services of healthcare providers, to apps on mobile devices [5]. MMAs by design collect process and transmit large quantities of information and data. Increasing reliance on mobile apps raises questions about compromised patient privacy [6] and the security of the data accompanying the apps [5]. There is continued mistrust in mobile apps in healthcare handling personal identifiable information and PHI in a secure and private manner. The 2015 PwC's Health Research Institute's survey, claims 78% of surveyed consumers were worried about medical data security, while 68% were concerned about the security of their data in mobile apps [7].

The impact of data breaches in the medical industry is far-reaching in terms of costs, losses in reputation [8] and potential risk to patient safety. Reasons for obtaining access to PHI can be for monetary gain, to inflict harm and for personal intention [9]. An example of the importance of cybersecurity can be seen with the health insurer Anthem in the US. A reported breach involved hackers obtaining personal identifiable information and PHI for about 80 million of its customers and employees [10]. The information stolen falls under the Health Insurance Portability and Accountability Act (HIPAA), which is the federal law governing the security of medical data and could result in fines of up to $1.5million. A data breach that maliciously makes changes to a medical diagnosis or prescribed medication has serious consequences in terms of physical harm and patient safety. With PHI breaches, either through physician diagnosis or a treatment plan, the possibility of personal harm or loss is pronounced. In 2014 the SANS Institute, a leading organization in computer security training, indicates health care security strategies and practices are poorly protected and ill-equipped to

TABLE I. FDA CATEGORIZATION FOR REGULATORY PURPOSES [2]

Medical Mobile Apps - Focus of FDA Regulatory Oversight	Mobile Apps which FDA Intends to Exercise Enforcement Discretion	Mobile Apps that are NOT Medical Devices
Mobile apps that: • Are extensions of one or more medical devices • Provide patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations • Transform the mobile platform into a regulated medical device • Become a regulated medical device (software)	Mobile apps that: • Provide or facilitate supplemental clinical care • Provide patients with tools or access to information • Specifically marketed to help patients document, show, or communicate to providers potential medical conditions • Perform simple calculation. • Interact with PHR systems or EHR systems	Mobile apps that: • Provide access to electronic records, textbooks or other reference materials or educational tools • Are for medical training, general patient education and access, automate general office operations, are generic aids or are general purpose products

handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property [11].

It is largely assumed MMAs are not typically deployed in "hacker rich" mobile environments [12]. The detection of increased app hacking by security companies and researchers is significant amidst today's rapid growth in healthcare mobile app usage [7], [11]–[13]. An Arxan report states that many sensitive medical and healthcare apps have been hacked with 22% of these being FDA approved apps [12]. In the MMA domain, developers do not have extensive experience with the types of threats other consumer app industries (e.g., banking) are familiar with. Consequently, privacy has not been given serious consideration until recently, while the importance of security is getting recognized little is yet being done [14]. The FDA regulates medical devices in the U.S and are alert to the cybersecurity of medical devices. In July 2015, the FDA issued a cybersecurity alert to users of a Hospira Symbiq Infusion System pump, where it strongly recommended discontinued use, as it could be hacked and dosage changed [15]. In September 2015, the FBI issued a cybersecurity alert, outlining how Internet of Things (IoT) devices may be a target for cybercrimes and may put users at risk [16]. If a cyber-thief changes patient medical information or a physician diagnosis, serious medical harm or even death can result. An article that references the DarkNet, describes how it is now possible to purchase a medical identity that mirrors individual ailments, size, age and gender, to seek "free" medical services that would not be suspicious to a clinician [17]. According to CISCO the estimated cost associated with medical identity theft in the US, to the healthcare industry in 2015 is $12 billion [18].

Development of MMAs is picking up momentum as many companies are lured into the domain by the explosion of the market and the potential financial gains. However, issues arise such as: many of these developers do not have a background in the highly regulated domain of medical devices and are not aware of the data protection and privacy requirements of electronic PHI (ePHI). Developers coming from the medical device domain are discovering the technical complications of entering the mobile domain. The job of securing mobile apps in health care is primarily up to those building them, which also has its challenges because the developers tend not to be security experts [19]. The European Commission's 'Green Paper on mHealth' findings are that this market is dominated by individuals or small companies, with 30% being individuals and 34.3% are small companies (defined as having 2-9 employees) [20]. This would advocate a lack of experience, knowledge and financial means to address the issues outlined above. The survey conducted by research2guidance [21] highlights that MHA developers regard the main market barrier for the next five years to be the lack of data security. The health industry is reaching out for help in designing security into mobile apps in healthcare that go beyond simple encryption to meet the potential sophistication of future threats [16]. This research aims to assist developers address privacy and security of data for MMAs, drawing from the standards and best practice perspectives.

The rest of this paper is organized as follows. Section II covers background on MMAs, data transmission and MMA data security. Section III, outlines the privacy and security laws for health data. In Section IV, we introduce our research on the development of a process model to assure the Confidentiality, Integrity and Availability (CIA) of data in transmission for developers of MMAs. The concept of a corresponding testing suite is also introduced in this section. Finally, we conclude the paper and present the future work in Section V.

II. MOBILE MEDICAL APP DATA

A. MMAs and Data Transmission

In July 2011, the FDA issued draft guidance for MMAs and defined a "mobile medical app" as a software application run on a mobile platform (mobile phones, tablets, notebooks and other mobile devices) that is either used as an accessory to a regulated medical device or transforms a mobile platform into a regulated medical device and can be used in the diagnosis, treatment, or prevention of disease [2]. Thus, a MMA is an app that qualifies as a medical device and is therefore required to follow the applicable medical device regulatory requirements. Mobile devices, on which MMAs run, now provide many of the capabilities of traditional PCs with the additional benefit of a large selection of connectivity options [22]. Data is transmitted to and from the MMA through various approaches depending on the goal of the

application. There are numerous MMA deployment scenarios that require consideration to ensure data is secure. As a result, MMAs use a variety of channels, wired or wireless, for transmission in a point-to-point, point-to-multipoint and multipoint-to-multipoint setting, to communicate information. Transmission of data may occur between the MMA and for example: remote Health/Service Centers; Medical Professionals; or Health Record Networks. In some cases, the information sent to the MMA is processed on the app and retransmitted to the specified device or center. Through MMAs the collection of significant medical, physiological, lifestyle and daily activity data [20] is greatly amplified and transmitted via varied and numerous networks. Data in transit has a higher level of vulnerability to both losses through oversight and to misappropriation. Misappropriation in the context of this research is the unauthorized use of another's name, likeness, or identity without that person's permission, resulting in harm to that person. Consequently, particular attention is necessary to protect information made accessible in transmission, particularly when it is personal data and ePHI.

Common technologies used for data transmission in MMAs include: Wireless Sensor Networks (WSNs) [23]; Body sensor networks (BSN) [24]; Wireless Body Area Network (WBANs) [25]; Bluetooth/ Bluetooth Low Energy (BLE) [24]; ZigBee [26]; UWB [27]; Wireless Medical Telemetry Service (WMTS) [28]; communication networks such as Wi-Fi [22]; wired communication (internet access, broadband and fiber-optic communication) [14]; and mobile networks 3G/4G and as it becomes more widely available 5G [26]. MMAs are predominantly executed from mobile devices and connect to wireless sensor networks. Consequently the data transmission to and from the MMAs will be predominantly via wireless technologies [24].

B. Mobile Medical Application Data Security

Security and privacy related to patient data are two essential components for MMAs. The fundamental concepts when considering data security are confidentiality, integrity and availability (CIA). Confidentiality is protection of the information from disclosure to unauthorized parties. Integrity refers to protecting information from being modified by unauthorized parties. Availability is ensuring that authorized parties are able to access the information when needed. The intention of health data security and protection is to assure patient privacy through confidentiality, within the development of functional devices, while sustaining the data integrity and availability necessary for use [29].

When considering data security risks for MMAs it is necessary to specify what types of security threats they should be protected against. Deployment of MMAs involves security threats from multiple threat sources which include: attacks; the user; other mobile apps; network carriers; operating systems and mobile platforms. These security risks are further extended when consideration is given to the unauthorized access to the functionality of supporting devices and unauthorized access to the data stored on supporting devices [30]. Given the context in which MMAs are deployed and used, the information going to and from the MMA travels across potentially many different and varying networks in diverse operation settings [31]. In addition, consideration that wireless networks and channels are accessible to everyone [32] and have shared features, means information and network security is equally important in this domain [33]. The potential for breaches of CIA of data in transmission is consequently greatly amplified by these circumstances. The 2015 Ponemon report on mobile app security, emphasized that not enough is spent on mobile app security [34].

1) Attacks: Attacks are techniques that attackers use to exploit vulnerabilities in applications. There are numerous tools available for hacking into MMAs and wireless networks. Hackers target mobile apps to gain entry into servers or databases in the form of malware attacks. A recent list of these tools can be found in the Appendix of the Araxan Report [12]. This report examined 20 sensitive medical and healthcare apps and discovered 90% of Android apps and no iOS apps have been subject to hacking [12]. When data travels across a network, they are susceptible to being read, altered, or "hijacked". Potential for breaches of confidentiality of data occurs during collection and transmission of data. Data in transmission to and from the MMAs must be protected from hacking. Some of the most common issues (but not inclusive) are Easvesdropping, Malware, Node Compromise, Packet Injection, Secure Localization, Secure Management, Sniffing Attacks, Denial of Service (DoS), SQL injection attacks, Code Injection and Man-in-the Middle attacks. The consideration of WBANs for MMAs must satisfy rigorous security and privacy requirements [35]. Wireless channels are open to everyone. Monitoring and participation in the communication in a wireless channel can be achieved with a radio interface configured at the same frequency band [36]. This may cause severe damage to the patient since the cybercriminal can use the attained data [35] for many of the illegal purposes mentioned above. The ISO/IEEE 11073 standard deals only with mutual communication protocols and frameworks exchanged between and has never considered security elements until recently, irrespective of all sorts of security breaches [37]. Security issues must be resolved while designing medical and healthcare apps for sensor networks to avoid data security issues [24].

2) Users: Many of the mobile devices will be personal and bypass the majority of inbound filters normally associated with corporate devices which leaves them vulnerable to malware. It is important that the user has good knowledge of the security safeguards, what measures

to follow and what precautions to take [38]. A key challenge with MMA data is the lack of security software installed on mobile devices [39]. Many mobile device users do not avail of or are unacquainted with basic technical security measures, such as firewalls, antivirus and security software measures. Mobile device operating systems are very complex and therefore demand additional security controls for the prevention and detection of attacks against them [40]. The accessibility of social media and email make it easy to post or share information in violation of HIPAA regulations. An example being, a New York nurse was fired because she posted a photo to Instagram of a trauma room after treating a patient [41]. Mixed with the availability to mobile phone cameras and social media apps, the risk of employees divulging PHI and violating HIPAA requirements has increased [42]. One of the greatest threats to MMA data security lies with the fact that most are on mobile devices which are portable, making them much more likely to be lost or stolen [43]. Potentially any data on the device is accessible to the thief, including access to any data and hospital networks. Due to the regulatory protection of PHI, it is important that even when the app is on a stolen device the security of the data remains protected and is regularly backed-up [40]. Measures should be available to remotely lock the MMA, disable service, completely wipe out the data [40] and restrict access to supporting devices.

Not all users' password-protect their devices. Even when passwords are used because of the lack of physical keyboards with mobile devices, users tend to not use complex passwords to secure their information. The use of more than one type of authentication technique suggested by Alqahtani, would afford better data security for MMAs [40]. The difficulty is requesting lengthened authentication requirements from a busy medical professional. Inputting numerous passwords, or waiting for an authentication code in a pressurized situation is not desirable.

3) Other mobile apps: Unfortunately, many users download mobile apps often without considering the security implications. Unintentionally, a user can download malware in the form of another application, an update or by downloading from an unauthorised source. The difficulty in detecting the attack was due to the fact that there currently is no mobile device management application programming interface (API) to obtain the certificate information for each app [44]. An attacker can use Masque Attacks to bypass the normal app sandbox and get root privileges by attacking known iOS vulnerabilities [44]. Cloned apps are a concern, over 50% of cloned apps are malicious and therefore pose serious risks. A recently discovered iOS banking app malware, Masque Attacks, replace an authentic app with malware that has an identical UI. The Masque Attacks access the original app's local data, which was not removed when the original app was replaced and steal the sensitive data [44]. The mobile device management interface did not distinguish the malware from the original as it had used the same bundle identifier.

4) Operating systems & development: Consideration with handling data on mobile devices includes unintended data leakage. It is essential that the MMA is not susceptible to analytic providers that will sell the data to marketing companies. The app stores are attempting to address this, e.g., Apple is banning app developers from selling HealthKit data or storing it on iCloud. Google insists that the user is in control of health data as apps cannot be accessed without the user providing permission. Developers could include analytics that report how often a section of the MMA was viewed, similar to the analytics credit card provider's use to flag unwanted access to data. It is equally important to consider the intentional or unintentional sharing of personal information. Leakage of personal data from the device to the MMA and the leakage of MMA data onto personal devices are key considerations. The bypass of outbound filters elevate the risk of non-compliance with data privacy laws and requirements, e.g., the use of personal Dropbox.

A basic requirement such as encryption is not used in many MMAs. Data is encrypted so that it is not disclosed whilst in transit. Data encryption service provides confidentiality against attacks. The requirement of encryption is stressed, not only for the data, but for the code in development to assure data security [24][40]. Data encryption of passwords and usernames if they are to be stored on the MMA is essential; many apps store this information in unencrypted text. This means that anyone with access to the mobile device the MMA resides on can see passwords and usernames by connecting the device to a PC. If the MMA is hacked, the information encrypted will be useless to the cybercriminals. Many apps send data over an HTTPS connection without checking for revoked certificates [45]. MMA developers should ensure that back-end APIs within mobile platforms are strengthened against attacks using state of the art encryption. As discussed above a MMA could expose healthcare systems that had not previously been accessible from outside their own networks. In MMA data security consideration developers should always use modern encryption algorithms that are accepted as strong by the security community.

Hackers are aware that just because a patch was released does not means it was applied, which, in turn make the app vulnerable for attacks [46]. Some recommend the installation of "Prevention and Detection" software for defending and protecting against malware as essential [40]. Consequently, software that tracks detection and anticipates attacks would require consideration in MMA development.

It is essential that developers research the mobile platforms they are developing for. Each mobile OS offers different security-related features, uses different APIs and

handles data permissions its own way. Developers should adapt the code accordingly for each platform the MMA will be run on. There are no standards that straddle development or security testing across the different platforms. Developers design security for each individual OS.

III. REGULATIONS FOR HEALTH DATA

This section of the paper highlights some of the difficulties MMA manufacturers encounter understanding PHI data security and privacy requirements. It describes the key regulations on data security and privacy, MMA developers are required to observe in Europe and the United States.

Increasingly, MMA developers must deal with a range of international regulations if they want to perform business in more than one country. The absence of privacy laws in some countries, in addition to inconsistency or even conflicting laws means PHI is often misused and treated superficially. In the rush to market the aspects of privacy and security are not properly considered [47]. Some MMA providers find they are in breach of regulation only when they are warned or fined, blindsided by regulatory issues, due to the complexity [48]. Due to the surge in value of PHI on the black-market, owing to the lack of security controls within healthcare and the increase in the security of credit card data [17], privacy and security policy issues relating to data with MMAs are now of primary importance. The Thomas Reuters Foundation and mHealth Alliance published a global landscape analysis of the privacy and security policies to protect health data [48]. The report states, that most jurisdictions agree, data security is essential. The report proposes the world of privacy law is divided into three major groups: Omnibus data protection regulation in the style of the European laws that regulate all personal information equally; U.S.-style sectorial privacy laws that address specific privacy issues arising in certain industries and business sectors, so that only certain types of personal information are regulated; The constitutional approach, whereby certain types of personal information are considered private and compelled from a basic human rights perspective but no specific privacy regulation is in place otherwise [48].

A. European Union

Data protection and privacy has always been a strong concern for European law makers. Within the EU, the EU Data Protection Directive (Directive 95/46/EC) [49] is the key piece of regulation that will affect how you manage health data. This Directive is currently implemented in laws of Member States and requires establishment of supervisory authorities to monitor its application. However, at the beginning of 2012, the EU approved the draft of the European Data Protection Regulation (EDPR) [50], and will be enforced by 2018. This means the law will apply generally over all states in the EU, it will not require individual Member States implementation. With this progression in regulation, all Member States will be at the same stage of security and data protection [47].

The Directive enables ease in definition of terms. Health data is regarded in the Directive under the 'special category of data' known as sensitive data [49]. The Directive has specific sections in relation to sensitive data which include: Rules on lawful processing of sensitive data, Article 8 (1- 7); Rules on secure processing, Article 17, Article 4 (2), and Article 16. The sections stipulate specific rules about sensitive data, the processing, protection and the requirement that this data is not transferred to an end point that does not have acceptable levels of protection. The Directive is now the international data protection metric against which data protection adequacy and sufficiency is measured [51], [52].

Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 [53], known as the ePrivacy Directive, is concerned with the processing of personal data and the protection of privacy in the digital age. It is now law in all EU countries and covers all non-essential cookies, and tracking devices. This Directive principally concerns the processing of personal data relating to the delivery of communications services. It provides rules on how providers of electronic communication services, should manage their subscribers' data. It also guarantees rights for subscribers when they use these services. The key parts that MMA developers are concerned with in the directive are: processing security; confidentiality of communication; processing traffic and location data; cookies and controls.

B. United States

The key law that applies to health data in the US is HIPAA. HIPAA was established to classify security policies and privacy rights across the healthcare spectrum [29]. As a result, new federal standards were implemented to assure patient's medical information privacy, in addition to security procedures for the protection of privacy [54]. HIPAA is organized into separate Titles and the security and privacy of health data is addressed in Title II, referred to as the 'Privacy Rule' and the 'Security Rule' [55]. The HIPAA Privacy Rule covers all PHI in any medium while the HIPAA Security Rule covers ePHI. The Security Rule necessitates security controls for the physical and ePHI to ensure the CIA of the data. The US does not have any centralized legislation at the federal level regarding data protection and follows a fragmented approach, which requires looking at a number of laws and regulations to form the definition of terms [55]. The basic HIPAA requirements for MMA developers include: Secure access to personal health information via unique user authentication; Encryption of data that will be stored; Regular safety updates to protect from any breaches; A system to audit the data and ensure that it hasn't been accessed or modified in any unauthorized way; A mobile wipe option that allows personal health information to be wiped if the device is lost; Data backup in case of a device loss, failure, or other disaster [56].

HIPAA was updated in the HIPAA Omnibus Rule required by The Health Information Technology for Economic and Clinical Health Act of 2010, (HITECH Act). The HITECH Act established new information security breach notification requirements that apply to businesses that handle personal health information and other health data [57]. The FDA released guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" [58]. This provides a list of recognized consensus standards dealing with Information Technology and medical device security [58].

The circumstances in which MMAs may transmit information wirelessly places them in the domain of Federal Communications Commission (FCC) regulation, to ensure consumer and public safety [59]. Recognizing the need for regulatory clarity, the FCC, FDA, Office of the National Coordinator (ONC) and the Department of Health and Human Services (HHS) came together in a grouping called the Food and Drug Administration Safety and Innovation Act (FDASIA) Working Group. The group, through the FDA, released a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology including MMAs [60].

IV. CURRENT RESEARCH

A. Research Perspective

As the MMA domain grows and becomes a standard established mechanism for healthcare delivery, both the security and privacy of health data will be essential. The reference [12] report, which included investigation of MHAs and MMAs, highlighted that hacks are on the rise in mobile apps. Mobile apps in healthcare are being developed persistently without proper data security functionality. This is largely due to the lack of understanding of current standards and regulation requirements pertaining to data security and partly due to the fact that many of these apps are developed by businesses not familiar with the medical device industry. Consequently, a gap exists as there is no standardized way to assist mobile app developers in the healthcare domain and particularly the highly regulated MMA domain, to observe security related requirements of regulation or assure data security in operation. A study analyzing security vulnerabilities explicitly in mobile health apps, highlighted the lack of a global security standard for mobile devices [13]. There are no specific MMA standards for cybersecurity, which are visible in other industries where standards and guidance are available, e.g. the NIST Special Publication 800-82 Guide to Industrial Control Systems Security [61]. For mobile apps in healthcare, existing regulation and standards must be applied in a patchwork method to address security.

The aim of this research is to investigate this gap further and provide a solution to assist clarity in relation to data security and regulation for MHA and MMA app developers. The intention of this research is to develop a Process for identifying the most applicable objective evidence to assist MMA developers to assure data security for MMAs during development, with specific focus upon data transmission. Due to the nature of MMAs and their use of public and open networks for data transmission, data is particularly exposed at this stage.

B. Research Setting

1) International standards, technical reports and best practice: This section briefly outlines the international standards, technical reports and best practice literature, in which the research is to be grounded. The research leverages on two medical device standards, IEC/TR 80001-2-2:2012 [62] and IEC/TR 80001-2-8 [63]. The overall objective of the research is to develop a process in order to establish security controls pertinent to MMAs for all 19 security capabilities outlined in the IEC 80001-2-2:2012 standard. IEC/TR 80001-2-2:2012 is the only published medical device security standard and presents 19 high-level security-related capabilities in understanding the type of security controls to be considered and the risks that lead to the controls [64]. It is the only guidance available that specifically addresses security requirements for networked medical devices [65]. IEC/TR 80001-2-8 (currently at a committee draft stage) is a catalogue of security controls developed relating to the security capabilities defined in IEC/TR 80001-2-2. The security controls support the maintenance of confidentiality and protection from malicious intrusion [66]. The report provides guidance to healthcare organizations and MD manufacturers for the selection of security controls to protect the CIA and accountability of data and systems during development, operation and disposal [66].

This research proposes using the applicable security controls in IEC/TR 80001-2-8 relating to two of the capabilities directly associated with data transmission from IEC/TR 80001-2-2, as an exemplar. The intent is to use the measured applicable security controls outlined in IEC/TR 80001-2-8, with further research completed to assemble security controls pertinent to the mobile aspect, with comparative expert validation, by means of analysis of applicable standards and best practices. In addition, the research aims to establish a corresponding testing suite to assure data CIA in data transmission for MMAs against the developed security controls.

The two specific capabilities from IEC/TR 80001-2-2 that relate to data transmission are, TXCF – Transmission Confidentiality and TXIG – Transmission Integrity. Each capability comes with recommended reference material and a common standard to consider when developing and establishing security controls. The security controls established in IEC 80001-2-8 associated to the TXCF and TXIG capabilities will be mapped through the common standard and reference materials to establish security control objectives and technical strategies for MMA developers. Additionally, the security controls will be mapped to wireless network and healthcare standards to

determine if further controls are required for MMAs. The standards currently being mapped to the IEC 80001-2-8 established security controls are: ISO/IEC 27033-2:2012; ISO/IEEE 11073; NIST SP 800-153.

2) Threat Modeling Analysis (TMA): The research revealed Threat Modeling Analysis (TMA) assists in understanding and assessing the security risks an asset can be exposed to. A key part of TMA is threat modeling. The research revealed that threat modelling analysis and threat modelling are established methods considered in National Institute of Standards and Technology (NIST) standards and best practice (OWASP) in relation to mobile app security risk assessment. Threat modeling is an important basis for defining security requirements of information systems [67] and information protection. Threat modeling is widely acknowledged in NIST standards [68] and recognised as being best practice [69] in risk assessment for network and mobile app security. Threat modeling is widely recognized as an effective means to establish a solid basis for the specification of security requirements in app development and is considered as a significant step in the security requirement model [70].One of the objectives of this research is to develop an operational threat model from the developed security controls for MMA data transmission. Therefore, an understanding of best practices in threat modeling is essential for this research. The aim of the research is to create a threat modelling analysis framework that incorporates a threat model which is aligned with the developed security controls from the process model. Primary research has established the recommended TMA and threat modeling methods. This will be the foundation for the development of a threat modelling analysis framework, developed through focus groups and validation in two MMA development companies and the standards community.

3) Threats and attacks: The introduction of risk assessment requires an understanding of the threats and how they exploit vulnerabilities to alter or attack an asset from the position of MMA data security. To establish this understanding, additional investigation was conducted in the area of threats and attacks on mobile apps. The research on the classification and some of the most common threats and corresponding attacks in the mobile app field for data in transmission can be seen in Table II, [22], [31], [34], [71]–[73], [74]. This section of the research is currently being written into a conference paper. By understanding the threats and corresponding attacks in this domain, this research will leverage on the existing understandings in app security to the MMA field.

4) Testing suite: The dynamic nature of mobile app development creates difficulties for inexperienced developers and small organizations, particularly in the medical device domain. This is partially due to the budgetary resources or motivation to conduct extensive testing and this in turn can leave an app, the user's device, and the user's network vulnerable to exploitation by attackers [75]. Security testing of mobile apps is largely a manual, expensive and difficult process[76] and security testing is seen as primarily a manual process, with little hybrid or automation testing available for use or used by developers and a significant challenge [77]. Complexity of testing the application security itself and consideration relating to the security requirements of open platforms in which apps transmit data is an additional emphasized difficulty [78]. Investigation has commenced in the area of transmission security testing methodologies and testing methods and mobile apps, to fully review the landscape of transmission security testing. This research was undertaken with the collaboration of data security experts within a specialist testing company. The company and experts have vast experience in working in both network and app data security. In collaboration with the testing company, their experts and academic experts the expectation is to develop a testing suite against the considered security controls. The testing suite will be developed to follow the information discovery process, which includes the threat modeling analysis that was developed to address the MMA security controls. A diagrammatic summary of the adapted OWASP Testing Guide 4.0 [79] and researched considerations required when completing mobile app security testing, concerning this research, can be seen in Figure 1.

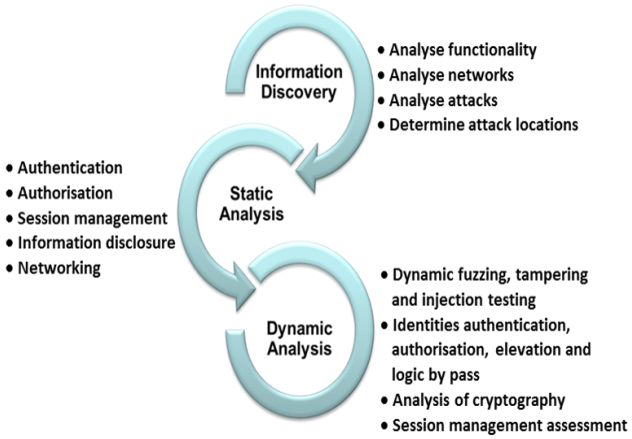

Figure 1. Diagrammatic summary of requirements for mobile app security testing.

OWASP highlight the need to have a clear understanding of the testing objectives and, therefore, the security requirements to have a successful testing program. The information discovery step would be accomplished with the completion of the first step in TMA, the collection of background information, and the first two steps of threat modeling. Both static analysis and dynamic analysis are standard requirements in any software testing process,

neither analysis approaches are sufficient alone to address all testing limitations [79]. In recent years much research and development has been completed in the field of static source review tools, called code scanners. These scanners automatically look for coding errors that can determine some security issues. Many organizations are using static source code scanners, however this approach is not effective when used alone [79]. The limitations of dynamic analysis are, it only monitors the behavior of the app during runtime and lacks the ability to identify potential vulnerabilities [80]. The dynamic approach is therefore generally used in the second step of the testing process [75], [80].

5) Validation and trailing: Validation will combine expert opinion from the standards community, recognized experts in mobile data security, testers and developers from within the MMA industry. The trailing will be completed in two identified MMA companies, which are currently collaborating with the research to assure data security of their MMAs. Action Design Research (ADR) was considered the most appropriate approach for this research. ADR methodology was developed to facilitate a useful approach to benefit the interests of both IS research and organisational research [81] and the evaluation of an IT artifact. It was chosen in order to accommodate the development of IT artifacts, in collaboration with industry and stimulate organisational change when addressing transmission security in the development of MMAs. This research involves collaborative development of artifacts through theory- ingrained research and practice inspired research. ADR can account for both technological and organisational contexts, shaping of the artifact via design and use and influences of designers and users [82]. Additionally, consideration of the dynamic setting and development environment in which this research will be conducted, ADR was considered appropriate methodology to facilitate these challenges.

TABLE II. DIFFERENT TYPES OF ATTACKS IN THE MOBILE APP FIELD

Grouping of Attack Vectors	**Description**	**Examples**	**Security Concern**			**Classification**	
			Confidentiality	***Integrity***	***Availability***	***Passive***	***Active***
Reconnaissance Attacks	Referred to as information gathering, an activity that does not noticeably interfere with the regular operation of the device. They often serve as preparation for further attacks.	Eavesdropping Sniffing Port Scans Distributed Network Services Queries	x	x	x	x	x
Access Attacks	Gaining unauthorized access to a device and its resources.	Spoofing Man-in–the-Middle SSL-stripping SQL Injection Session hijacking/replaying Re-ordering/rerouting Port redirection Backdoor Tampering Cross-site scripting Security Misconfiguration Privilege Escalation Attack	x	x			x
Denial of Service Attacks	Based on the layers Attacks on networks, in order to bring them to a stop or interrupt the system by saturating communication links or by flooding hosts with requests to deny access to the user.	Distributed Denial of Service Attack Physical Layer Jamming/ De-synchronization Tampering Data Link Collision Exhaustion Neglect and greed Homing Misdirection Black holes Transport		x	x		x

Grouping of Attack Vectors	Description	Examples	Security Concern			Classification	
			Confidentiality	*Integrity*	*Availability*	*Passive*	*Active*
		Flooding					
Malware Attacks	A program covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs.	Worms (Mass Mailing) Bot/Botnet /Malicious Mobile Code Viruses (Compiled, Interpreted) Trojan Rootkits		x	x	x	x
Network Attacks	MANET	Re-ordering/Rerouting Path Traversal Byzantine Wormhole Attack Byzantine Attacks Black Hole Attack Worms (Network Services) Flood Rushing Attack Floor Rushing Attack	x	x			x
	WSN	Bluesnarfing Port Scan	x	x		x	x

V. Conclusion and Future Work

This paper examined existing data security issues and practices in relation to MMAs. A summary of regulations relating to data privacy and security MMA providers are mandated by law to adhere to, were outlined. Compliance and improved understanding of data security regulations and best practices will assist developers to meet the security requirements for data in transmission. The security gaps in MMAs are exploited due to lack of knowledge, understanding or amalgamated regulation for data security with MMAs.

The mobile app industry claim innovation is stifled, due to the lack of clarity in regulations and security concerns. Developers will need to find the optimal balance between data security and privacy as MMAs expand and PHI enters into new aspects. The lack of consistent data security to assure privacy, to allow interoperability, and to maximize the full capabilities [83], presents a significant barrier to the industry. The primary focus for the continued research in this area will be two fold. The development of a framework to establish security controls for transmission of PHI to assist MMA developers assure CIA. The security controls will be completed in examining and mapping the referenced standards and best practices currently recognized in the medical, applications and data security domains. The intention is to fill the gap in knowledge and understanding for MMA developers, through ease of accessibility to the most appropriate information. The second objective of the future research is the establishment of a practical testing suite for the MMA developers in the data transmission domain. The testing suite will be developed against the validated mobile transmission security controls for PHI. The aim is to test the implemented transmission security controls during development, use and security patch updates to assure data CIA. The implementation of the transmission security controls would be encouraged from the preliminary development stage with the future research providing a checklist for developers with MMAs in the market.

Validation of the research will be completed in collaboration with two identified MMA development companies. The MMAs being developed will have different transmission requirements and capabilities to assure diversity.

Acknowledgment

This research is supported by the Science Foundation Ireland Research Centres Programme, through Lero - the Irish Software Research Centre (http://www.lero.ie) grants 10/CE/I1855 & 13/RC/2094.

References

[1] C. Treacy and F. McCaffery, “Medical Mobile Apps Data Security Overview,” in *SOFTENG : The Second International Conference on Advances and Trends in Software Engineering*, 2016, pp. 123–128.

[2] FDA, “Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff,” *U.S. Deapartment of Health and Human Services Food and Drug Administration*. U.S. Department of Health and Human Services, USA, p. 44, 2015.

[3] B. M. Silva, J. J. P. C. Rodrigues, F. Canelo, I. C. Lopes, and L. Zhou, “A data encryption solution for mobile health

apps in cooperation environments," *J. Med. Internet Res.*, vol. 15, no. 4, p. e66, Jan. 2013.

[4] A. W. G. Buijink, B. J. Visser, and L. Marshall, "Medical apps for smartphones: lack of evidence undermines quality and safety," *Evid. Based. Med.*, vol. 18, no. 3, pp. 90–2, Jun. 2013.

[5] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, "Security Concerns in Android mHealth Apps," in *AMIA Annual Symposium Proceedings*, 2014, no. November, pp. 645–654.

[6] Y. Yang and R. . Sliverman, "Mobile health applications: the patchwork of legal and liability issues suggests strategies to improve oversight," *Health Aff.*, vol. 33, no. 2, pp. 222–7, 2014.

[7] Price Waterhouse Cooper - Health Research Institute, "Top Health Industry Issues of 2015 - A new health economy takes shape," 2015.

[8] "Data breach results in $4.8 million HIPAA settlements," *U.S. Department of Health and Human Services*, 2014. [Online]. Available: http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html. [Accessed: 01-Dec-2016].

[9] N. H. Ab Rahman, "Privacy disclosure risk: smartphone user guide," *Int. J. Mob. Netw. Des. Innov.*, vol. 5, no. 1, pp. 2–8, 2013.

[10] G. S. McNeal, "Health Insurer Anthem Struck By Massive Data Breach - Forbes," *Forbes*, 2015. [Online]. Available: http://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/. [Accessed: 30-Nov-2016].

[11] B. Filkins, "Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon," SANS Institute, 2014.

[12] Araxan, "State of Mobile App Security : Apps Under Attack - Special Focus on Fincial, Retail/Merchannt and Healthcare/Medical Apps," 2014.

[13] Y. Cifuentes, L. Beltrán, and L. Ramírez, "Analysis of Security Vulnerabilities for Mobile Health Applications," *Int. J. Electr. Comput. Energ. Electron. Commun. Eng.*, vol. 9, no. 9, pp. 999–1004, 2015.

[14] J. Kabachinski, "Mobile medical apps changing healthcare technology," *Biomed. Instrum. Technol.*, vol. 45, no. 6, pp. 482–6, 2011.

[15] FDA, "Safety Communications - Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication," *WebSite*, 2015. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm?source=govdelivery&utm_medium=email&utm_source=govdelivery. [Accessed: 30-Nov-2016].

[16] G. M. Snow, "FBI — Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism," *FBI Website*, 2011. [Online]. Available: https://archives.fbi.gov/archives/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. [Accessed: 19-Nov-2016].

[17] J. Williams, "Don't Mug Me For My Password! - InformationWeek," *Information Week Healthcare*, 2014. [Online]. Available: http://www.informationweek.com/healthcare/security-and-privacy/dont-mug-me-for-my-password!/a/d-id/1318316. [Accessed: 29-Nov-2016].

[18] Cisco, "Combating cybercrime in the healthcare industry." pp. 1–7, 2015. [Online]. Available: https://www.google.ie/search?q=Cisco,+%E2%80%9CCombating+cybercrime+in+the+healthcare+industry.%E2%80%9D&ie=utf-8&oe=utf-8&gws_rd=cr&ei=Su0-WJXTNKGBgAaM1rKoCg. [Accessed: 29-Nov-2016].

[19] FDA, "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication," *FDA Website*, 2013. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm. [Accessed: 25-Nov-2016].

[20] European Commission, "Green Paper on mobile Health ('mHealth')," Brussels, 2014.

[21] "mHealth App Developer Economics 2014 The State of the Art mHealth Publishing." research2guidance, Continua Health Alliance, mHealth Summit Europe, Berlin, pp. 1–43, 2014.

[22] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[23] J. N. Al-Karaki and a E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wirel. Commun.*, vol. 11, no. December, pp. 6–28, 2004.

[24] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[25] J. Y. Khan and M. R. Yuce, "Wireless Body Area Network (WBAN) for Medical Applications," in *New Development in Biomedical Engeneering*, D. Campolo, Ed. InTech, 2010, pp. 591–623.

[26] T. V. Ngoc, "Medical Applications of Wireless Networks," Washington University, St. Louis, Student Reports on Recent Advances in Wireless and Mobile Networking (2008). [Online]. Available: http://www.cse.wustl.edu/~jain/cse574-08/ftp/medical/. [Accessed: 18-Nov-2016].

[27] Y. Gao *et al.*, "Low-power ultrawideband wireless telemetry transceiver for medical sensor applications," *IEEE Trans. Biomed. Eng.*, vol. 58, no. 3 PART 2, pp. 768–772, 2011.

[28] J. Ahmad and F. Zafar, "Review of body area network technology & wireless medical monitoring," *Int. J. Inf.*, vol. 2, no. 2, pp. 186–188, 2012.

[29] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 1–54, 2012.

[30] J. L. Hall and D. McGraw, "For Telehealth to Succeed, Privacy and Security Risks Must be Identified and Addressed," *Health Aff.*, vol. 33, no. 2, pp. 216–221, 2014.

[31] D. Fischer, B. Markscheffel, S. Frosch, and D. Buettner, "A Survey of Threats and Security Measures for Data Transmission over GSM/UMTS Networks," *7th Int. Conf. Internet Technol. Secur. Trans.*, pp. 477–482, 2012.

[32] S. Singh, M. Singh, and D. Singhtise, "A survey on network security and attack defense mechanism for wireless sensor networks," *Int. J. Comput. Trends Tech*, no. May to June, pp. 1–9, 2011.

[33] M. Li, W. Lou, and K. Ren, "Data Secutiry and Privacy in Wireless Body Area Networks," *IEEE Wirel. Commun.*, vol. 17, no. 1, pp. 51–58, 2010.

[34] Ponemon Institute, "The State of Mobile Application Insecurity," 2015.

[35] S. Saleem, S. Ullah, and K. S. Kwak, "A study of IEEE 802.15.4 security framework for wireless body area networks," *Sensors (Basel).*, vol. 11, no. 2, pp. 1383–95, 2011.

[36] V. Mainanwal, M. Gupta, and S. Kumar Upadhayay, "A Survey on Wireless Body Area Network : Security Technology and its Design Methodology issue," in *2nd International Conference on Innovations in*

Information,Embedded and Communication systems (ICIIECS)2015, 2015, no. I, pp. 1–5.

[37] S. S. Kim, Y. H. Lee, J. M. Kim, D. S. Seo, G. H. Kim, and Y. S. Shin, "Privacy Protection for Personal Health Device Communication and Healthcare Building Applications," *J. Appl. Math.*, vol. 2014, pp. 1–5, 2014.

[38] M. Souppaya and K. Scarfone, *NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Gaithersburg, USA: National Institute of Standards and Technology, 2013, pp. 1–29.

[39] D. Nyambo, Z. O. Yonah, and C. Tarimo, "Review of Security Frameworks in the Converged Web and Mobile Applications," *Int. J. Comput. Inf. Technol.*, vol. 3, no. 4, pp. 724–730, 2014.

[40] A. S. Alqahtani, "Security of Mobile Phones and their Usage in Business," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 11, pp. 17–32, 2013.

[41] C. Wiltz, "Mobile App Developers to Congress: HIPPA is Stifling Innovation | MDDI Medical Device and Diagnostic Industry News Products and Suppliers," *Mobile Health*, 2014. [Online]. Available: http://www.mddionline.com/article/mobile-app-developers-congress-hippa-stifling-innovation-140918. [Accessed: 19-Sep-2016].

[42] FierceHealthIT, "Mobile & HIPAA Securing personal health data in an increasingly portable workplace," FierceHealthIT, pp. 1–4, 2014.

[43] P. Ruggiero and J. Foote, "Cyber Threats to Mobile Phones," United States Computer Emergency Readiness Team, 2011.

[44] H. Xue, T. Wei, and Y. Zhang, "Masque Attcak: All Your iOS Apps Belong to US," *FireEye*, 2014. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html. [Accessed: 18-Nov-2016].

[45] M. B. Barcena, C. Wueest, and H. Lau, "How safe is your quantified self?," Mountain View, 2014. [Online]. Available: https://www.google.ie/search?q=%E2%80%9CHow+safe+is+your+quantified+self%E2%80%AF%3F,%E2%80%9D&ie=utf-8&oe=utf-8&gws_rd=cr&ei=KO4-WO6vEcrGgAbpranwBg. [Accessed: 30-Nov-2016].

[46] Y. S. Baker, R. Agrawal, and S. Bhattacharya, "Analyzing Security Threats as Reported by the United States Computer Emergency Readiness Team," in *2013 IEEE International Conference on Intelligence and Security Informatics (ISI 2013)*, 2013, pp. 10–12.

[47] B. Martinez-Perez, I. Torre-Diez de la, and M. Lopez-Coronado, "Privacy and Security in Mobile Health Apps: A Review and Recommendations," *J. Med. Syst.*, vol. 39, no. 1, p. 181, 2015.

[48] Thomas Reuters Foundation and mHealth Alliance, "Patient Privacy in a Mobile World a Framework to Address Privacy Law Issues in Mobile Health," Thomas Reuters Foundation, London, 2013. [Online]. Available: https://www.google.ie/search?q=%E2%80%9CPatient+Privacy+in+a+Mobile+World+a+Framework+to+Address+Privacy+LawIssues+in+Mobile+Health,%E2%80%9D&ie=utf-8&oe=utf-8&gws_rd=cr&ei=Dvw-WNvHB4XmgAb18r7IDg. [Accessed: 30-Nov-2016].

[49] European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EU, 1995.

[50] European Commission, Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), vol. 11. 2012, p. 118.

[51] European Commission., "Communication fom the Commission to the European Parliament the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)," 2015.

[52] P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals," *Comput. Law Secur. Rev.*, vol. 28, no. 2, pp. 130–142, 2012.

[53] European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). EU, 2002.

[54] J. Li and M. J. Shaw, "Electronic medical records and patient privacy," *Int. J. Inf. Secur. Priv.*, vol. 2, no. 3, pp. 45–54, 2008.

[55] B. Malin, "A De-identification Strategy Used for Sharing One Data Provider's Oncology Trials Data through the Project Data Sphere® Repository," Nashville, 2013.

[56] A. Wang, N. An, X. Lu, H. Chen, C. Li, and S. Levkoff, "A Classification Scheme for Analyzing Mobile Apps Used to Prevent and Manage Disease in Late Life," *JMIR mhealth uhealth*, vol. 2, no. 1, pp. 1–11, Feb. 2014.

[57] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, "Privacy and Data Security Risks in Cloud Computing," *Electron. Commer. Law Rep.*, vol. 186, pp. 1–6, 2010.

[58] FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," 2014.

[59] A. Atienza and K. Patrick, "Mobile Health: The Killer App for Cyberinfrastructure and Consumer Health," *Am. J. Prev. Med.*, vol. 40, no. 5S2, pp. 151–153, 2011.

[60] Food and Drug Administration and Safety and Innovation Act, "FDASIA Health IT Report Proposed Strategy and Recommendations for a Risk-Based Framework," 2014.

[61] K. Stouffer and J. Falco, "Guide to Industrial Control Systems (ICS) Security," 2015.

[62] IEC, "TR 80001-2-2 Application of risk management for IT-networks incorporating medical devices Part 2-2 : Guidance for the disclosure," European Commission, pp. 1–54, 2012.

[63] IEC/DTR, "80001-2-8 Health informatics, Application of risk management for IT-networks incorporating medical devices: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC/TR 80001-2-2," no. June 2014. 2015.

[64] IEC, TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices Part 2-2 : Guidance for the disclosure and communication of medical device security needs, risks and controls. BSI Standards Publication, 2012.

[65] A. Finnegan and F. McCaffery, "A Security Argument Pattern for Medical Device Assurance Cases," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, 2014, pp. 220–225.

[66] A. Finnegan and F. McCaffery, "A Security Argument for Medical Device Assurance Cases," in *Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on*, 2014, pp. 220–225.

[67] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat Modeling as a Basis for Security Requirements," in *Proceedings of*

the 2005 ACM workshop on Storage security and survivability, 2005, pp. 94–102.

[68] NIST, "Special Publication 800-30 Guide for Conducting Risk Assessments," 2012.

[69] OWASP, "Threat Risk Modeling," *The Open Web Application Security Project (OWASP) webpage*. [Online]. Available: https://www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE. [Accessed: 07-Mar-2016].

[70] E. A. Oladimeji, S. Supakkul, and L. Chung, "Security threat modeling and analysis: A goal-oriented approach," *Proc 10th IASTED Int. Conf. Softw. Eng. Appl. SEA 2006*, pp. 13–15, 2006.

[71] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *2011 Proceedings of the 34th International Convention MIPRO*, 2011, pp. 1468–1473.

[72] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and responses," *Inf. Syst.*, vol. 36, no. 3, pp. 675–705, May 2011.

[73] J. Agbogun and F. A. Ejiga, "Network Security Management," *Netw. Secur.*, vol. 2, no. 4, pp. 617–625, 2013.

[74] K. Scarfone, "SP 800-153 Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)." NIST, p. 24, 2012.

[75] S. Quirolgico, J. Voas, T. Karygiannis, C. Michael, and K. Scarfone, "NIST Special Publication 800-163 Vetting the Security of Mobile Applications," U.S. Department of Commerce NIST, U.S., pp. 1–44, 2015.

[76] R. Mahmood, N. Esfahani, T. Kacem, N. Mirzaei, S. Malek, and A. Stavrou, "A whitebox approach for automated security testing of Android applications on the cloud," in *7th International Workshop on Automation of Software Test (AST)*, 2012, pp. 22–28.

[77] M. E. Joorabchi, A. Mesbah, and P. Kruchten, "Real challenges in mobile app development," in *International Symposium on Empirical Software Engineering and Measurement*, 2013, pp. 15–24.

[78] A. I. Wasserman, "Software Engineering Issues for Mobile Application Development," *ACM Trans. Inf. Syst.*, pp. 1–4, 2010.

[79] M. Meucci *et al.*, OWASP Testing Guide 4.0. The OWASP Foundation, 2014. [Online]. Available: https://www.owasp.org/index.php/OWASP_Testing_Project. [Accessed: 30-Nov-2016].

[80] S.-H. Seo, A. Gupta, A. Mohamed Sallam, E. Bertino, and K. Yim, "Detecting mobile malware threats to homeland security through static analysis," *J. Netw. Comput. Appl.*, vol. 38, pp. 43–53, Feb. 2014.

[81] R. Cole, S. Purao, M. Rossi, and M. K. Sein, "Being Proactive: Where Action Research meets Design Research," in *ICIS 2005 Proceedings*, 2005, pp. 1–21.

[82] J. Iivari and J. Venable, "Action Research and Design Science Research," in *17th European Conference on Information Systems*, 2009, pp. 1–13.

[83] European Commission, "Commission Staff Working Document: on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document Green Paper on mobile Health ('mHealth')," Brussels, SWD(2014) 135 Final Commission, 2014.