Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 00 (2017) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

The fourth International Workshop on Privacy and Security in HealthCare 2017 (PSCare17)

Towards Composable Threat Assessment for Medical IoT (MIoT)

Salaheddin Darwish[a], Ilia Nouretdinov[a], Stephen D. Wolthusen[a,*]

[a] *Information Security Group (ISG), Royal Holloway University of London, Egham, Surrey, TW20 0EX , UK*

Abstract

The Medical Internet of Things (MIoT) has applications beyond clinical settings including in outpatient and care environments where monitoring is occurring over public networks and may involve non-dedicated devices. This poses a number of security and privacy challenges exacerbated by a heterogeneous and dynamic environment, but still requires standards for handling personally identifiable and medical information of patients and in some cases caregivers to be maintained. Whilst risk and threat assessments generally assume a stable and well-defined environment, this cannot be done in MIoT environments where devices may be added, removed, or changed in their configuration including connectivity to server back ends. Conducting a complete threat assessment for each such configuration changes is infeasible. In this paper, we seek to define a mechanism for prioritising MIoT threats and aspects of the analysis that are likely to be affected by composition and related alterations. We propose a mechanism based on the UK HMG IS1 [1] approach and provide a case study in the form of the Technology Integrated Health Management (TIHM) [2] test bed.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Medical IoT ; Security ; Privacy ; Threat and risk analysis ; Federated Network Systems

1. Introduction

The flexibility of collecting data and eventually also integrating medical devices into a Medical Internet of Things (MIoT) to permit integrated views and interaction with data is highly alluring not only in clinical settings but particularly where outpatients and care environments are concerned[3,4]. With continuous and varied data available to monitor symptoms over the longer term and the ability to analyse such time series that may also include further important clues such as on the ambient environment, more informed diagnostic and therapeutic decisions can be reached, especially in areas such as dementia where effects of different stimuli must be understood and will vary over time. However, both the sensors used and their configuration such as aggregation devices and back end services is likely to change over time, rendering any initial risk and threat assessment on security and privacy rapidly obsolete.

Risks and threats may e.g. result in compromise of devices, violations of data quality and integrity, breaches of privacy expectations or policy violations as well as information governance requirements. Moreover, as devices and software configurations or the way data is processed by intermediate systems may change frequently, this raises the problem of continued validity of any risk and threat assessment.

* Corresponding author. Tel.: +44-178-444-3270 ; fax: +44-178-443-0766.
E-mail address: Salaheddin.Darwish@rhul.ac.uk ; I.R.Nouretdinov@rhul.ac.uk ; Stephen.Wolthusen@rhul.ac.uk

Peer-review under responsibility of the Conference Program Chairs.

Taking cognizance of this set of problems, the present paper seeks to propose a methodology for enhancing the efficiency of risk and threat assessments under updates and composition. As a point of departure, the UK HMG IS1[1] method was chosen as it provides a detailed, structured, and reproducible approach, which also explicitly captures distinctions of threat sources and threat actors. *The main contribution of this paper is to structure the threats into static and dynamic classes within a taxonomy, allowing the identification of areas requiring renewed or new analyses and of cascading effects*. Clearly, as the concept of MIoT requires interconnection of edge devices with consumers such as monitoring and diagnostic systems, such cascading effects must be understood in a timely manner. We also outline an application of the aforementioned approach for the case study of the UK NHS Technology Integrated Health Management (TIHM)[2] Test Bed studying home-based dementia care as its target environment.

In Section 2, we introduce the MIoT system definition. In Section 3, we examine security challenges in MIoT. In Section 4, we discuss the standard UK HMG IS1 method and composability properties,for the threats analysis of MIoT. In Section 5, we present our TIHM threat model addressing composability features. In Section 6, we conclude the paper highlighting the importance of composability features in threat analysis for MIoT and the work limitation.

2. Medical IoT Systems

Medical IoT is another wave of IoT technologies to support public healthcare domain by providing an efficient medical care to a growing population especially for patients requiring long-term monitoring[5]. Typical medical devices, undergo a massive transformation from unconnected equipment, through to wirelessly reprogrammable devices including some medical software applications installed in current mobile devices[6,7]. A MIoT system is defined as a healthcare system consisting mainly of monitoring devices. These devices track the patient's condition remotely by recording particular health measurements systematically and sending them to a back-end system. Then, the back-end system examines this collected data to generate appropriate alerts to clinicians. These alerts enable clinicians to detect health issues earlier, and immediately react for any emergencies[8]. For the discussion purpose, a monitoring device can be a medical device but also can be alternative devices (e.g. a smart watch) or cellular phones which can hook to the people. Also, it is worth pointing out that the data created by this type of device appears to be very sensitive as it is typically interpreted against the health record of a certain patient. This system can be exploited in domestic care environments, clinic settings or outpatient control. Eventually, a MIoT System represents a sophisticated ecosystem, which includes heterogeneous components and systems (i.e. medical devices, smart devices, hubs/gateways, Cloud services, databases, Big-Data and clinical information systems) collaborating to leverage for healthcare improvement.

3. Security and Privacy Medical IoT Challenges

Like any new technologies, MIoT encounters several challenges such as interoperability, performance, device constraints, and security. According to our scope, we propose the priority list of security and privacy goals[8] as shown in Table 1:

Table 1. Security goals

Index	Security Goal	Description
G1	Device Integrity	Information has to be correctly collected and transferred by medical devices and sensors.
G2	Data Integrity	Non-existence of information flows that may have been subject to modification by entities at different levels of integrity than the originating principal (e.g. integrity of data-in-flight).
G3	Confidentiality	A principal does not disclose information to unauthorised entities allowing the deduction of the state of the principal.
G4	Availability	Information or the means to process these must be available when they are requested/required.
G5	Privacy	Correct sharing of information among group where membership may vary over time.
G6	Security Usability	Convenience and adaptability of particular security features to users (i.e. some security mechanisms accomplish their objectives even they are not used properly)[9].

Integrity is the most important goal because accuracy, consistency and value of the data handled by this system are pivotal. Device integrity comes before data integrity as the data must not be generated by a compromised device.

Amongst specific challenges caused by MIoT systems, we can mention the following ones related to security goals:

- Validation of the measurements due to device diversity, misusage, mistakes [10](*Sec. Goals G1*,*G2*).
- Valuableness of the information related to patient's health for data understanding [4] (*G2*).
- Heterogeneity, agreement and synchronisation among the sensors by different producers [5] (*G1*,*G2*,*G4*).
- Various aims of access to the data entries that may be used by doctors, carers, researchers and others (*G3*,*G4*,*G5*).
- Different protocols and technologies of communication [11] (*G2*,*G3*,*G5*).
- Dynamic network topology, and multiplex data transfer between providers, home, central back-ends [11] (*G2*,*G3*,*G4*).
- Computational, memory, energy, mobility limitations [11] (*G1*,*G2*,*G4*).
- Special threats for the privacy because of big data collections [5] (*G5*).
- Dynamic security updates and tamper-resistant packages required for IoT devices [11] (*G3*,*G4*).
- Complex human interactions [4], e.g. it is vital to adopt usable passwords due to patient's health (*G6*).

4. Threats Identification

Noticeably, IoT especially for the medical one forms a new unique landscape of security threats which attracts more adversaries [12,13,14]. This stems from that fact that the MIoT system usually consists of hybrid and dynamic collaborative services and subsystems (WSN, WLAN, database, Cloud, etc.), which may be maintained by different providers and susceptible to a range of security attacks. Therefore, this requires regular thorough threat assessment by security analysts in order to mitigate potential breaches.The next two subsections discuss the approach adopted to identify security threats for MIoT system and the notion of composability for more effective threat re-assessment.

4.1. Approach

As a part of the risk and threat analysis stream, it is essential to consider a standard method for assessing and managing threats and risks in IoT systems like other ICT systems such as HMG IS1 [1] and ISO/IEC 27033 [15] allowing largely reproducible analysis. We have broadly used an adapted version of the HMG IS1 method [1] for MIoT which includes the case where a source may directly or indirectly drive an actor to facilitate an attack on their behalf. Moreover, this particular assessment would typically be referred to the known security and privacy goals, taking into account the specific features of MIoT system that are known to be vulnerable and sophisticated [13]. We have relied on this specific method because it provides a well-structured approach and the standard explicitly distinguishes between threat sources and actors. According to this model, the threat analysis goes through the stages shown in Fig. 1.

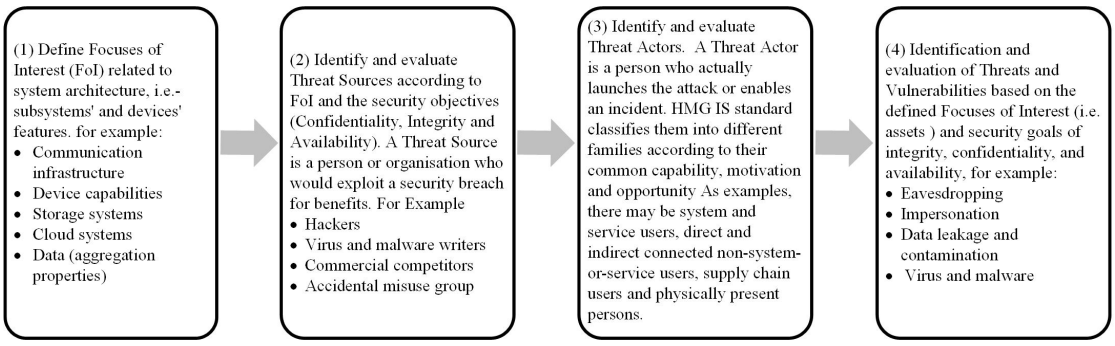

Fig. 1. The HMG IS1 method for assessing security threats

4.2. Composability in Threat Identification

Due to volatile and diverse components of MIoT system, it is vital to regularly conduct threat identification for such a system especially in the case of upgrade. However, performing this assessment frequently for the same multifaceted

system instigates effort, time and resource challenges. Therefore, we have studied the potential threats for the MIoT system and the related components in the system to extract the features of composition. The principal point in the threat analysis is how the result of previous threat assessment is affected by adding a new device to the system. Therefore, it is important to consider what components of the system (devices, data back-ends) are involved in a scenario of a threat or an attack, and what type of data are being handled (measurements, control, etc.). We propose a composability property for the threats encountered by the MIoT components: (1) **static** and (2) **dynamic** properties. A static attribute refers to threats that need consideration only in newly added MIoT devices. Whereas, dynamic attribute indicates that the check is demanded not just for newly fitted MIoT devices but also for all other associated devices. Indeed, these specific threats appear to be strongly related to data being handled (e.g. clock poisoning, corruption and contaminated information, privacy breaches from information leakage). On the other side, for effective threat analysis, we propose also a taxonomy, which includes four main classes based on the type of targeted data: data disclosure (1), alternation (2), inaccessibility (3), and another category for process/control/code manipulation (4) equally violating all the goals. This threat classification along with defined FoIs, will be used as means to facilitate analysis of threats and vulnerabilities and defining their composability property as shown in Table 1. For viability purpose, we present a scenario of MIoT system which includes a blood pressure device.This device is connected to the hub to take measurements of a given patient and both the device and hub already have threat assessment (i.e. ensure that the device generates a correct sequence of measurements with no data corruption). Then, another new device for measuring heartbeats needs to be added to the hub. Obviously, two devices are collecting correlate time-based data (symptoms), it is necessary to ensure time synchronisation between the two. In addition, as the different measurements will be aggregated and stored in the hub, this combined information may entail information leakage.

5. TIHM Threat Assessment (Case Study)

To realise significance of considering composability properties in threat assessment of MIoT, we have taken advantage of our existing threat analysis conducted in our Technology Integrated Health Management (TIHM) project[2]. In fact, this project is devoted to exploiting major innovative technologies for support of people with dementia and their carers. The TIHM architecture is a hybrid of systems and components, which provide services as an aggregate at different interfaces for the overall architecture, and additional components serving to integrate the aforementioned subsystems. TIHM system building blocks and connections are shown by Fig. 2. The system building blocks comprise MIoT devices, hub/gateway/based-station and three back-end infrastructures; at the TIHM data center all data is saved. Different communication systems are exploited in TIHM such as Bluetooth, Wi-Fi, GPRS, Message Bus and WAN.

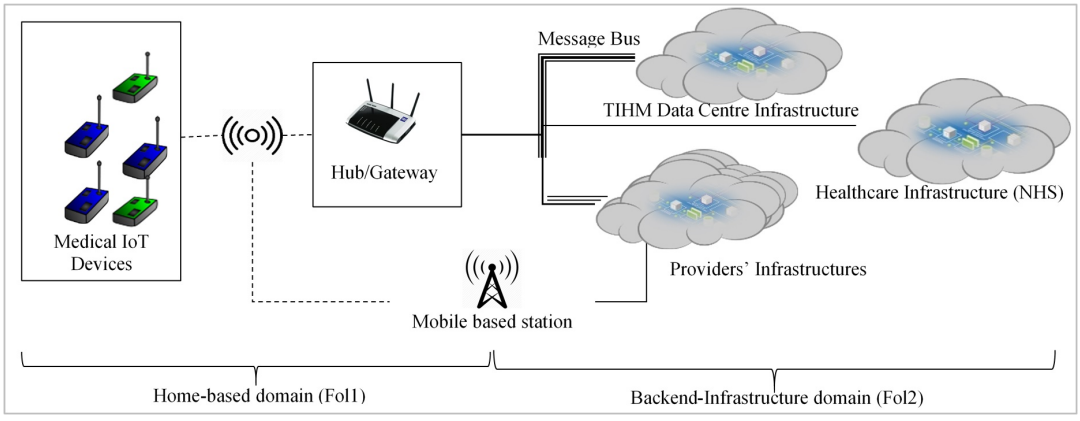

Fig. 2. The TIHM System Architecture and its Focus of Interests (FoIs)

Based on the TIHM system architecture, we have defined two Focus of Interests (FoI): home-based and back-end. According to our analysis of *Threat Sources*, at severe level there are targeted criminal groups. Moderate level has non-targeted criminal groups, professional hackers, malware writers, insider groups. Low level includes amateur

hackers whereas negligible level has academic and researchers and accidental misuse. In our analysis of *Threat Actors*, at FoI.1, the severe level represents compromised devices with malware and virus while the moderate level includes device technicians and physical intruders. The low-level has normal users, suppliers, person within range and internet users. In FoI.2, the severe level has compromised devices with malware and virus. While, the substantial level contains TIHM testbed admin users and the moderate level has service consumers, handlers, service providers and physical intruders. In low level have Internet users whereas negligible level includes TIHM project researchers and analysts, NHS nurses. The result of our TIHM *Threat Identification* is presented in the Table 2. The last column assists whether adding an IoT is static (related to a new IoT only) or dynamic (data-related, affecting other IoT kits).

Table 2. TIHM threat analysis and availability of composability properties

Threat Analysis				**Availability of Composability Properties**
Vulnerability/Attack			**Level**	**Update needed after adding a new IoT**
Data Disclosure Group	FoI 1	Unauthorised access to the IoT and Hub\Gateway	Very High	Static
		Eavesdropping	Low	Static
		Home user impersonation	Medium	Static
		Information leakage or release	Low	Dynamic (patient identification by collected data)
	FoI 2	Unauthorised access to TIHM databases/storages.	Very High	Not changed by unless IoT has extra connections
		Unauthorised access to non-secure Cloud services	Very High	Static (checking whether the service is secure)
		Back-end infrastructure user impersonation.	Very High	Not changed by IoT addition
		Cross contamination (from shared resources)	High	Not changed unless a shared storage is used
		Information leakage or release	Low	Dynamic (patient identification by collected data)
Data Alternation Group	FoI 1	Home user impersonation	Medium	Static
		Information corruption or disruption	Medium	Static (for IoT misusage), with possible dynamic elements (comparing records)
		Connection interference	Medium	Dynamic
	FoI 2	Data staleness or non-Freshness	Low	Dynamic (comparing time records)
		Invalid data suppression	Very Low	Static (for IoT misuse), with possible dynamic elements (comparing records)
		Information Injection	Medium	Not changed by IoT addition
		Back-end infrastructure user impersonation	Medium	Not changed by IoT addition
		Cross contamination	Medium	Not changed by IoT addition
Data Inaccessibility Group	FoI1	Energy draining	Low	Static
		Accidental fault	Low	Static
		Network congestion	Low	Dynamic
	FoI 2	Denial of Service (DoS)	Very High	Not changed by IoT addition
		Accidental system failure	Very High	Not changed by IoT addition
Process/Code Manipulation Group	FoI 1	Virus and malware	Very High	Static (for IoT devices) Dynamic (for the network)
		Clock Poisoning	Medium	Static (for IoT misusage), with dynamic elements
		Misconfiguration	Medium	Static (for IoT devices)
	FoI 2	Virus and malware	Very High	Not changed by IoT addition

According to the analysis conducted in the Table 2, adding a new IoT to a hub may require the following checks.

1. Checks related to the sensor itself and its connection to the home hub:
   (a) Prevention of unauthorised access, eavesdropping, user impersonation.
   (b) Prevention of information corruption at the collection stage.
   (c) Check for physical threats such as energy draining, possible faults.
   (d) Check for anti-virus protection, correction configuration, clock synchronisation.
   (e) Check for security of cloud storages and other extra connections of the sensor if used.
2. Checks related to the hub and other sensors connected to it:
   (a) Check the security of connection between the hub and the new sensor.

(b) Check for network or connection congestion, connection interference, signal delays.

3. Checks related to collecting information at the hub and central back-end infrastructure:
   (a) Check whether the whole data collected for a patient may have a threat for the patient's confidentiality.
   (b) Check synchronisation between the records from different sensors.
   (c) Possibly, check the information from different sensor of the same patient for contradiction.

Moreover, new threat sources and actors should be examined to update the main list in the analysis.

6. Discussion and Conclusion

This work would encourage threat analysts to conduct composable threat analysis by determining the interactive features (static or dynamic) in the components of their MIoT systems when tackling threats re-assessment. This is because these features would have an impact on the space and dependencies of threats once updating the system is taking place (i.e. adding new equipment may entail cascading effects). This will arguably save time and efforts in performing threat identification for such a system. The challenges instigated by the medical system complexity were observed in Sec. 3. The principal solution is creating a federalised line of interaction between the system elements. It allows to reduce the number of vulnerabilities, and to share responsibility for remaining issues by the subsystems in an effective way. In fact, this work is considered as a preliminary model for further developing a concrete, effective compos-able methodology for threat analysis which can be utilised in the domain of MIoT. One limitation in this work is that assessing threats, which affect the safety of medical devices in the MIoT system, is out of this paper scope as there is a well-known framework regulated by Medical Device Directives (MDD) developed for that purpose.

7. Acknowledgements

This work was supported by Technology Integrated Health Management (TIHM) project[2] awarded to the Department of Information Security at Royal Holloway as part of an initiative by NHS England supported by InnovateUK.

References

1. HMG IA Standard No. 1 & 2 Supplement Technical Risk Assessment and Risk Treatment , issue No 1 Apr 2012, Available at:https://www.ncsc.gov.uk/content/files/guidance_files/IS1 %26 2 Supplement - Technical Risk Assessment and Risk Treatment - issue 1.0 April 2012 - NCSC Web.pdf, (Accessed : 2017-05-13) (2012).
2. TIHM (Technology Integrated Health Management) for dementia, Available at: http://www.sabp.nhs.uk/tihm, (Accessed : 2017-05-13).
3. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, J. J. C. de Santanna, Internet of Things in healthcare: Interoperatibility and security issues, in: 2012 IEEE Int. Conf. Commun., IEEE, 2012, pp. 6121–6125.
4. P. A. H. Williams, V. McCauley, Always connected: The security challenges of the healthcare Internet of Things, in: 2016 IEEE 3rd World Forum Internet Things, IEEE, 2016, pp. 30–35.
5. A. W. Atamli, A. Martin, Threat-Based Security Analysis for the Internet of Things, in: 2014 International Workshop on Secure Internet of Things, IEEE, 2014, pp. 35–43.
6. P. A. Williams, A. J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem., Med. Devices (Auckl). 8 (2015) 305–16.
7. IoT Healthcare Market by Component (Medical Device, Systems & Software, Service, Connectivity Technology), Application (Telemedicine, Work Flow Management, Connected Imaging, Medication Management), End User, and Region - Global Forecast to 2022, Available at:http://www.researchandmarkets.com/reports/4213883/iot-healthcare-market-by-component-medical, (Accessed :2017-05-16) (2017).
8. Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (7) (2012) 1497–1516.
9. E. Schultz, R. W. Proctor, M.-C. Lien, G. Salvendy, Usability and Security An Appraisal of Usability Issues in Information Security Methods, Computers and Security 20 (7) (2001) 620–634.
10. Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for Internet of Things, J. Netw. Comput. Appl. 42 (2014) 120–134.
11. S. M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, Kyung-Sup Kwak, The Internet of Things for Health Care: A Comprehensive Survey, IEEE Access 3 (2015) 678–708.
12. S. Dixit, Opportunity vs risk with the Internet of Things, Netw. Secur. 2016 (12) (2016) 8–10.
13. M. O'Neill, The Internet of Things: Do more devices mean more risks?, Comput. Fraud Secur. 2014 (1) (2014) 16–17.
14. M. J. Covington, R. Carskadden, Threat Implications of the Internet of Things, in: Cyber Confl. (CyCon), 2013 5th Int. Conf., 2013, pp. 1–12.
15. ISO/IEC 27033-3:2010 - Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues, Available at:https://www.iso.org/standard/51582.html, (Accessed :2017-05-16) (2010).