Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 627–632

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.

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

10.1016/j.procs.2017.08.314

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: