Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people

Full Text

Title: **Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people**

Authors: **I K Poyner, R S Sherratt**

Biomedical Engineering, University of Reading, UK,
i.poyner@pgr.reading.ac.uk,
r.s.sherratt@reading.ac.uk

Conference: Living in the Internet of Things: Cybersecurity of the IoT
Publisher: IET
Location: London
Date: 28 - 29 March 2018
Accepted Date: 8th December 2017
pp.: not yet assigned
DOI: not yet assigned

Keywords: IoT, healthcare, security, privacy, encryption.

Abstract

The Internet of Things (IoT) promises highly innovative solutions to a wide range of activities. However, simply being a technology company does not exempt an IoT company from needing to comply with the legislation applicable to their operating region that safeguards personal information. This will result in security and privacy requirements for healthcare solutions. There are several mature frameworks that address these issues, but they have been developed within the context of organised hospitals and care providers, where there is the expertise, processing power, communications and electrical power to support highly robust security. However, for IoT solutions aimed at vulnerable people, either at home or within their local environment, there are significant additional constraints that must be overcome. These include technical (low processing capability, power constrained, intermittent communications) organisational (how to enrol and revoke users and devices, distribution of cryptographic keys) and user constraints (how does a patient with physical and/or mental challenges configure and update their devices).

This paper considers at the legal frameworks and the security and privacy requirements for healthcare solutions. An overview of some of the primary frameworks is then provided followed by an assessment of how this is constrained within an IoT system.

1 Introduction

IoT technologies promise many benefits in pervasive health monitoring. Individuals can have multiple attributes measured continuously over an extended period, including environmental and lifestyle factors, compared to occasional measurements during visits to a clinic. Across the wider population, data aggregation and big data analysis may reveal insights not discoverable from individual records, helping to achieve better, more tailored patient treatments whilst also enabling more efficient use of limited resources. However, a patient's health data must be treated with respect and privacy. This is not optional. For care providers, protecting data is not only a reputational or ethical imperative, it is enshrined in law with heavy penalties for not effectively controlling data. Patients' concerns over the security and privacy of their data is also a barrier to the adoption of new technology [1].

Failure to consider safeguarding privacy at the outset of an IoT project could result in significant re-design effort, recall of deployed devices, or inadvertent breaches resulting in large fines (potentially £17M or 4% of global turnover).

Today, many of the standards regarding health monitoring are aimed towards patients in hospital or health-care environments where physical, personnel and procedural security all contribute to the overall data security. Importantly, many of the monitoring systems in hospitals can be configured and maintained by competent persons and are not overly constrained in terms of electrical power, communications and local processing capability. This is however in stark contrast to the resource constrained IoT devices typically used to support people interacting with environments inside/outside of their home. Another complication arises when consumer devices and apps aimed at digital natives for health and fitness tracking are re-purposed for monitoring vulnerable people for whom interaction with technology is largely alien. For example, vulnerable people are less likely to implement the most important protective behaviours [2] such as updating devices and changing default passwords and may be more susceptible to falling victim to social engineering and counterfeiting.

This paper assesses the applicability of current privacy and security models in the context of supporting and monitoring vulnerable people (e.g. early onset dementia, cognitive impairment, children) interacting with their wider environments outside of the home. A key aspect is the range of users who may need differing levels of access to the information – the patient, family carers, social care providers and medical staff such as GPs and paramedics.

2 Legal safeguarding of personal information

IoT solutions will need to comply with applicable legislation protecting health data; being a technology company does not exempt a company from regulations in the sector that it operates. The European Court of Justice signalled this in their ruling of 20 December 2017 against Uber that it should be classified as a taxi service and not a technology intermediate. Similarly, innovative technologies and applications will need to comply with the privacy requirements of handling patients' medical records which have largely evolved around health service and care providers. This will be a challenge for small start-up companies who do not structure their enterprise and technology to meet these constraints.

The need for the protection and privacy of personal data has long been recognised. One of founding guidelines was issued in 1980 by the Organisation for Economic Co-operation and Development (OECD). OECD has published a set of guidelines to harmonise the flow of personal data across frontiers, but also to establish a common approach to privacy across participating nations. Guidelines were updated in 2013 with the explicit need to establish 'privacy enforcement authorities'. In the UK, the Information Commissioner's Office (ICO) is the independent authority set up to uphold information rights in the public interest {Information Commissioner's Office (UK), 2017 #360}.

2.1 GDPR

The General Data Protection Regulation (GDPR) will come into force within the EU on 25 May 2018, replacing the Data Protection Directive 95/46/EC. Its scope also covers personal data transferred outside of the EU. In the UK, the Data Protection Bill, once passed into law, will implement GDPR in the UK with additional provisions.

Privacy by design has always been an implicit requirement of data protection, but the GDPR core principle of 'data protection by design and default', places a general obligation to implement technical and organisational measures to integrate data protection [3].

The UK ICO advocates the seven 'foundational principles of privacy by design' developed by the Information & Privacy Commissioner of Ontario [4] which lists seven principles, four of which are very relevant to IoT:

- Privacy as the default setting,
- Privacy embedded into design,

- End-to-end security,
- Respect for user privacy (user-centric).

These have been further described against a number of user health data scenarios [5] and design guidelines [6]. It is further worth nothing that children are also afforded additional protection.

2.2 HIPAA

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) 1996, mandated the adoption of Federal privacy protections for individually identifiable health information. This has since been enhanced with a Privacy Rule (2003) and Security Rule (2005) setting national standards for compliance. It is applicable to any company that deals with Protected Health Information (PHI), including business associates and subcontractors who support treatment, payment or operations. PHI has to be carefully controlled and data has to be 'de-identified' by removing 18 specified identifiers or by using a statistical expert to determine that data cannot be associated with individuals.

2.3 Impact on IoT solutions

An IoT service that handles personal health information is subject to a long and detailed set of legal requirements. Furthermore, security requirements are dynamically developing and tend to become more stringent over time [7, 8].

Not taking due regard of these frameworks could jeopardise the service and healthcare operator. The provider must protect their own networks, storage and processing, and also potential liabilities arising from intermediate systems and third-party partners also need to be risk assessed and managed.

3 Security and privacy requirements for healthcare

Having recognised that IoT healthcare systems will need to comply with healthcare legislation, this paper now considers how regulations levy requirements for security and privacy. The detailed requirements will be somewhat dependent upon the regulatory environment, but the general requirements can be summarised below.

Security of data is often expressed in the three characteristics of confidentiality (privacy), integrity and availability. In a healthcare application, the following additional requirements may also be necessary [7]:

i. Confidentiality – data is accessible only to those who have the right to know (ISO 17799).
ii. Integrity - assurance that data has not been tampered with or modified in any way to undermine its authenticity.
iii. Availability – having timely access to information. Some applications also require the ability to withstand attacks aimed at denying availability (e.g.: denial-of-service flooding the communications channel or rapidly depleting the battery).
iv. Identity management - management of user identities across the end-to-end architecture, hence associating health information with the right individuals.
v. Nonrepudiation of origin – is provided through the use of digital signatures and guarantees that the sender of information cannot later deny (or repudiate) having sent the information.
vi. Consent management - enables patients to provide and manage their consent preferences, which serves as a basis for governing access to and usage of their individual identifiable health information.

Additional requirements may also be required [9, 10]:

vii. Freshness – the data is still relevant to analysis and treatment.
viii. Audit – recording user activities of the healthcare system in chronological order, such as maintaining a log of every access to and modification of data. Enables prior states of the information to be faithfully reconstructed.
ix. Archiving - moving healthcare information to off-line storage in a way that ensures the possibility of restoring them to on-line storage whenever it is needed without the loss of information.

Privacy is defined in several different ways, such as by the ITU [7] as:

> *"an aspect of system security (preventing undesired system use) that deals with providing access to the parties to which the information belongs and to parties that have explicitly been allowed access to certain information (also known as confidentiality).* A simpler purpose is that privacy *should protect a user's personally identifiable information and keep a certain degree of anonymity, unlinkability and data secrecy"* [9].

Zhang and Liu [10] argue that three principles are necessary in a cross-institutional patient records system to ensure privacy of patients and the content authenticity and source verifiability of electronic medical records:

- All electronic medical should be guarded through ownership controlled encryption, enabling secure storage, transmission, and access.
- The creation and maintenance of records should preserve not only content authenticity but also data integrity and customizable patient privacy throughout the record integration process.
- Access and sharing of records should provide end-to-end source verification through signatures and certification process against blind subpoena and unauthorized change in healthcare critical data content and user agreements.

A recurring principle in the literature is that a patient should be able to control (provide consent) as to what data is divulged to different care providers / health applications. Vulnerable patients may also need further safeguards, such as a guardian proxy.

'Secure by Default' (SbD) principles, as espoused by the UK National Cyber Security Centre (NCSC) [14], are highly applicable in systems for vulnerable people. SbD addresses the entire system including hardware, firmware, software, services, applications and configuration. However, a principle is that default configuration settings are usually set to the most secure possible, which may frustrate usability, especially where users have special needs (e.g.: large font, audio- visual accessories). The relevant principles include:

- security should be built into products from the beginning, it can't be added in later,
- security should be added to treat the root cause of a problem, not its symptoms,
- security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product,
- security should never compromise usability – products need to be secure enough, then maximise usability,
- security should not require extensive configuration to work, and should just work reliably where implemented,
- security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build,
- security through obscurity should be avoided,
- security should not require specific technical understanding or non-obvious behaviour from the user.

Addressing security throughout the whole lifecycle of an end-to-end service, especially when devices are upgraded, is vital as the devices become more capable to counter evolving threats. The last point is particularly pertinent to vulnerable patients who should not be relying on untrained family or carers to configure their systems.

4 Healthcare frameworks

IoT system developers need to consider existing frameworks for connected health devices, especially where they wish to sell a service to an established health or care provider who expects data to be secured in accordance with frameworks with which they have experience. A large organisation may place greater emphasis on the potential liabilities and reputational impact of a data breach than the opportunities offered by an innovative IoT solution.

Several health security models have resulted from hospital and community health care environments, or from personal health and fitness devices operated around the home. Some of these have now been incorporated into international and open standards which help to create a stable market for devices compared to the wide diversity of embryonic technologies currently promoted across the IoT community.

3.1 HL7

HL7 (Health Level Seven International) provides international standards for the transfer of clinical and administrative data between software applications used by healthcare providers. Its name is derived from the application level of the ISO OSI (Open Systems Interconnect) network model, and it aims to provide semantic interoperability between systems. The NHS Direct Interoperability Tool Kit (ITK) is based upon HL7.

HL7 privacy and security classification system [11] includes fields for confidentiality, sensitivity, integrity, compartment and handling caveat (purpose of use, obligations and refrain policies). The privacy rule is applied to composite information extracted from a health record; for example, if a treatment is prescribed for HIV then this will apply a restricted access rule to the record and require patient consent for onward release. A user accessing the system without a need to see the restricted information (for example a nurse entering temperature and blood pressure readings) would see only the incomplete information with details of HIV treatment either masked, encrypted or redacted (removed).

3.2 Continua

The Continua Design Guidelines (CDG) [12] are published and promoted by the Personal Connected Health Alliance (PCHAlliance). It is a framework based upon *open standards to create a secure and interoperable health data exchange in personal connected health*. The CDG are recognised by the International Telecommunication Union (ITU), which is the United Nations agency in the field of ICT, in ITU-T guidelines H.810 [7].

The CDG builds upon the ISO/IEEE 11073 [13] series for personal health device communication, HL7 standards and the technical specifications for USB, Bluetooth, Bluetooth LE, NFC and ZigBee.

In addition to the normal security C,I,A requirements of confidentiality (privacy), integrity and availability, the CDG/H.810 add requirements for identity management (management of devices across the end-to-end architecture), non-repudiation of origin (using digital signatures) and consent management (to individually identifiable health information).

5 Challenges for IoT systems

Characteristics of many of today's IoT eco-systems include heterogeneity of devices, a profusion of architectures and standards and very low resources (battery power, processing, memory, fault tolerance etc).

Fault-tolerant architectures need to accept that IoT devices, software and communications do not have the same reliability as that found within a clinical or hospital environment. Intermittent data loss has to be assumed and designed into the overall system.

Many of the security and privacy implementations used in healthcare are not constrained by processing power, memory or battery energy. When these are transferred into IoT systems the performance is often not acceptable in terms of response speed, reliability and robustness to loss of nodes or communication errors. Instead, a series of new protocols have been developed for IoT which are more suited to constrained devices. The security solutions in IoT {Malina, 2016 #320} have to provide authentication and authorization of nodes (things, users, servers, objects) and data authenticity, confidentiality, integrity and freshness. The security solutions are usually implemented at net- work, transport and application layers in IoT. These include:

- Constrained Application Protocol (CoAP);
- IPSec;
- Host Identity Protocol(HIP);
- Transport Layer Security (TLS) protocol and Datagram Transport Layer Security (DTLS) protocol;
- Slim Extensible Authentication Protocol Over Local Area Networks (SEAPOL);
- Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM).

A further complication is the distribution of secret cryptographic keys to users and devices that are geographically separated and may not be physically present to be authenticated when they are enrolled or registered onto a system. Revocation of a user or a device is also important, for example when a patient moves from a doctor or care provider, or when a device is lost, discarded or temporarily loaned.

Several communication and authentication protocols are assessed by Malina et al [9]. A recurring problem is that many security approaches offload computationally intensive operations to trusted unconstrained devices, but this overlooks the need for authentication, key establishment and the protection of user privacy. A main finding from the paper is that the selection of the security schemes has to consider the constraints of the IoT nodes, including processing power and memory, which will impact other factors such as cost, battery life and the need for user interaction and configuration. For example, asymmetric encryption may not introduce noticeable delays when implemented on a smartphone, but is an order of magnitude worse when implemented on a more constrained device, such as Raspberry Pi (Model B+). For very low-cost, highly-constrained devices, such as microcontrollers and smart cards, symmetric encryption and hashing can be performed in only a few milliseconds provided that the choice of algorithm is carefully chosen, such as AES-128b or RND 160b/ RND 560b random number generation, and there is sufficient RAM.

Other energy-saving techniques have been demonstrated using AES-128 and SHA-2 algorithms, such as encompression (encryption + compression) {Zhang, 2013 #359}. The authors claimed a reduction of up to 78% was achieved by increasing the compression ratio and can even be lower than an uncompressed system without any encryption.

Privacy schemes examined by Malina et al. include k-anonymity; homomorphic encryption; group signatures and ring signatures; and attribute based signatures and attribute based encryption.

Encryption of data on the end user device, as recommended by HL7, has considerable implications for an IoT system, including computation resources and key management where many heterogenous, remote devices may be joining or leaving the service. Identity management and non-repudiation may require devices to be enrolled into a service and the use of digital signatures and a certificate authority.

6 Acknowledgements

This research is funded by the University of Reading Research Endowment Trust Fund.

7 References

1. Dhukaram, A.V., et al. *End-User perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust*. in *2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*. 2011.
2. Blythe, J.M., et al., *Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours.* Frontiers in Public Health.
3. Information Commissioner's Office. *Data protection by design and default* 2017 [cited 14 December 2017]; Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.
4. Information & Privacy Commissioner of Ontario, *Privacy by Design.* 2013.
5. Mihailidis, A., et al., *Sensors and In-Home Collection of Health Data: A Privacy by Design Approach*. 2010.
6. Information and Privacy Commissioner Ontario, et al., *Privacy Engineering: Proactively Embedding Privacy, by Design.* 2014.
7. ITU, *H.810 Interoperability design guidelines for personal connected health systems: Introduction* 2017.
8. Continua, *H.810 Interoperability design guidelines for personal connected health systems* 2016.
9. Malina, L., et al., *On perspective of security and privacy-preserving solutions in the internet of things.* Computer Networks, 2016. **102**(Supplement C): p. 83-95.
10. Zhang, R. and L. Liu. *Security Models and Requirements for Healthcare Application Clouds*. in *2010 IEEE 3rd International Conference on Cloud Computing*. 2010.
11. HL7 International, et al., *Guide to the HL7 Healthcare Privacy and Security Classification System (HCS).* 2013.
12. Continua, *Introduction to the Continua Design Guidlines 2017*. 2017.
13. IEEE, *IEEE 11073-00103:2015 Health informatics Personal health device communication Part 00103: Overview*. 2015.
14. NCSC. *Secure by Default*. 2017 2 May 2017 [cited 9 January 2018]; Available from: https://www.ncsc.gov.uk/articles/secure-default.