Future Generation Computer Systems 75 (2017) 46–57

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Evolving privacy: From sensors to the Internet of Things

Javier Lopez [a], Ruben Rios [a,*], Feng Bao [b], Guilin Wang [b]

[a] Network, Information and Computer Security (NICS) Lab, University of Malaga, Spain
[b] Huawei International Pte Ltd., Singapore

HIGHLIGHTS

- Analysis of existing privacy threats in scenarios involving sensing technologies.
- Evaluation of the privacy problems that may be inherited by the IoT.
- Identification of the challenges that emerge as sensors are integrated into the Internet.

ARTICLE INFO

Article history:
Received 23 November 2016
Received in revised form
24 March 2017
Accepted 29 April 2017
Available online 8 May 2017

Keywords:
Privacy
WSN
Internet of Things
Challenges

ABSTRACT

The Internet of Things (IoT) envisions a world covered with billions of smart, interacting things capable of offering all sorts of services to near and remote entities. The benefits and comfort that the IoT will bring about are undeniable, however, these may come at the cost of an unprecedented loss of privacy. In this paper we look at the privacy problems of one of the key enablers of the IoT, namely wireless sensor networks, and analyse how these problems may evolve with the development of this complex paradigm. We also identify further challenges which are not directly associated with already existing privacy risks but will certainly have a major impact in our lives if not taken into serious consideration.

1. Introduction

The Internet of Things (IoT) has been recognised as one of the major technological revolutions of this century [1,2]. Although the IoT is still in its infancy and will only unleash its full potential with the development of a completely distributed approach [3], the importance of this paradigm has already been recognised by the major international standard bodies [4], which have come into play to ensure the correct operation, interoperability and resilience of this paradigm.

Despite the complexities of the scenarios envisioned by the IoT [5], the realisation of this paradigm can be achieved with three main, non-trivial architectural components: smart things, backend servers and communications infrastructure (as depicted in Fig. 1). One of the challenges in these scenarios is to enable the connection of everyday objects to the Internet. However, the IoT is not only about connectivity, it is about the pervasive collection and sharing of data towards a common goal. Therefore, smart sensing technologies are undeniably one of the key enablers of this paradigm.

Since humans are amidst smart things, the deployment of sensing technologies by IoT systems will pose an unprecedented threat to individual privacy. Unlike current Internet scenarios where users have to take an active role (i.e., query for services) to put their privacy at stake, with the increasing number of sensing devices around us, we become targets of data collection without even noticing it and in hitherto unsuspected situations. This has led some companies to analyse the need for security and privacy in these environments [6,7] but in most cases privacy is treated in the narrow sense of data confidentiality. Surprisingly, only a few companies acknowledge the need for more advanced privacy mechanisms, even though the NGMN Alliance [8] explicitly states that no mature solution has been proposed to date.

Also some researchers have looked at privacy problems in IoT environments. Most of them consider privacy as part of a broader security analysis (e.g., [3]) and only a few papers analyse privacy as a problem in its own right. In this respect, some authors have looked at privacy in the IoT from a legal perspective [9]. Other authors have analysed the privacy impact of various enabling IoT technologies [10,11]; however their analyses are horizontal and they leave out some relevant problems inherited from sensor networks. We cover them in this paper in detail.

* Corresponding author.
E-mail addresses: jlm@lcc.uma.es (J. Lopez), ruben@lcc.uma.es (R. Rios), bao.feng@huawei.com (F. Bao), wang.guilin@huawei.com (G. Wang).

http://dx.doi.org/10.1016/j.future.2017.04.045
0167-739X/

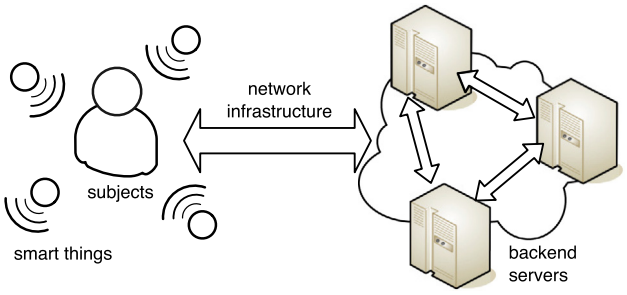

Fig. 1. Simplified IoT architecture.

These privacy problems (see Fig. 2) can be classified into two main categories according to the entity whose privacy is being threatened, namely the user or the network itself [12]:

- In *user-centric* privacy, the problem comes from the ability of sensors to detect the presence of humans or relevant assets and capture sensitive information about them. Therefore, sensor networks can be used as a mechanism to inadvertently spy on anyone or anything. Moreover, user-centric privacy cannot be easily achieved by technological means alone as the privacy perpetrator is the owner of the network and he/she may secretly use the surveillance capabilities of the network to profile and track users.
- In *network-centric* privacy, the attacker is an external entity who wants to learn information about the network itself or the elements being monitored by the network. In this case, the first line of defence is the use of confidentiality mechanisms to protect the content of data packets. However, this is usually not sufficient to provide network-centric privacy as the attacker may gain access to the cryptographic material. In addition, the attacker may be able to extract relevant information by means of traffic analysis attacks.

This classification can be broken down into several subcategories depending on the type of information or asset to be protected. A natural question at this point is whether computer-based anonymity solutions for current Internet scenarios may be suitable to tackle the aforementioned problems. After an extensive analysis [13] we concluded that most of these systems are too costly, and even when some of them are lightweight enough, they do not meet the anonymity requirements for sensor networks or they limit their functionality. However, it is worth noting that they will be indispensable for protecting the traffic to/from the outside infrastructure.

In this paper we concentrate on analysing how the privacy problems that have appeared in sensor networks, as isolated systems, will evolve when they are integrated into the Internet. We also identify new challenges that the evolution of these technologies will possibly entail. The main goal of this paper is thus to highlight privacy problems as well as potential solutions and, in this way, encourage the scientific community to continue researching and delving into the various challenges identified in this paper. This will, in turn, facilitate the development of solutions to address privacy threats thus giving rise to a more privacy-conscious IoT.

The structure of this paper is organised according to the classification in Fig. 2. First, in Section 2 we focus on problems and challenges caused by the ability of sensor networks to surreptitiously collect information about individuals. Subsequently, Section 3 and Section 4 deals with two different privacy problems that affect the network itself and the assets and entities being legitimately monitored by the network. Section 5 describes further challenges that may arise due to the integration of sensing technologies in the IoT but are not a direct evolution of problems already existing in sensor networks. Finally, Section 6 summarises the main contributions of the paper.

2. User-centric privacy

This section describes the privacy problems associated with the ability of sensing technologies to collect information about individuals within their monitoring range without them even being aware of this situation. We also briefly look at the typical approach to privacy in the Internet era, which is based on legislation and fair information practices. Finally, we present the reasons why legislation is not the way to a privacy-friendly IoT and discuss some related challenges.

2.1. Introduction

User-centric privacy concerns people being the target of data collection by ill-intentioned network operators or data-hungry businesses. In fact, Camenisch [14] describes personal information as the "new currency on the Internet" due to the change in the business model over the last few years. Now services are offered in exchange for personal information instead of money. Regardless of the claims of service providers, in many cases personal data are not only used to provide value-added services to the users but also to improve their products or are shared with third parties for different purposes, such as targeted advertisement [15,16].

With sensing technologies all around us, the opportunities for data collection reach new orders of magnitude. Prior to sensing technologies, it was relatively difficult to violate individual privacy unless a user was actively involved in Internet communications. Unfortunately, in a world covered with all types of sensors, privacy can be breached at anytime regardless of being an active user or not, of the system. Moreover, these invasions of personal privacy may appear in all sorts of everyday situations, even in the intimacy of our own home. This represents an unprecedented loss of privacy as sensing technologies will be ubiquitous. There will be sensors at the office, at the supermarket, at home and also attached to our bodies or even implanted [17]. Consequently, it is paramount to set barriers on the collection, processing, storage and dissemination of personal data.

Until recently, the most common approach to privacy protection has been through legislation. Indeed, one of the most well-known privacy definitions was given by Alan F. Westin [18], a legal scholar, who talks about privacy as the right of individuals to determine how much personal information is disclosed to other entities, and how it should be maintained and disseminated.

2.2. Privacy legislation

The aforementioned definition is probably the basis for modern information privacy law as it encapsulates important notions which were later included in some major pieces of legislation, such as the US Privacy Act of 1974, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995. Some of these guidelines and directives have been recently revised or are in the process of revision and awaiting for adoption at the time of writing.

Thereafter, any collection of personal information should conform to the fair information practices (FIPs) as the basis for confidence and trust in online transactions. The FIPs establish a number of principles including user awareness, consent, access and control, purpose specification, data minimisation, and secure storage. In other words, individuals must be aware of being subject to data collection and they must explicitly allow the collection, processing, storage and dissemination of data about themselves. Also, the data collector must clearly specify the purpose of data collection and use the data for no other purposes. Moreover, the collection of personal information must be minimised and retained only for as long as is necessary to fulfil the original purpose