Privacy Implications of the Internet of Things

Ivan Gudymenko, Katrin Borcea-Pfitzmann, and Katja Tietze

Dresden University of Technology
Department of Computer Science, Chair of Privacy and Data Security
Nöthnitzer Str. 46, 01187 Dresden
ivan.gudymenko@gmail.com, katrin.borcea|katja.tietze{@tu-dresden.de}

Abstract. The Internet of Things (IoT) is likely to become one of the milestones which is going to determine the technological advance for the future. At the same time, new privacy concerns arise which might seriously impede the adoption of such systems. In this paper, we provide for our view on privacy implications of IoT focusing on RFID technology as one of its main enablers and suggest possible solutions to developing IoT systems in a privacy-respecting and secure way.

Keywords: IoT, privacy, RFID.

1 Introduction

The authors of [1] describe IoT as " [...] a world where things can automatically communicate to computers and each other providing services to the benefit of the human kind". It is desirable that communication protocols are standardized since this greatly facilitates the process of worldwide adoption and implementation of IoT and thus encourages the process of transition from numerous local proprietary solutions to the ubiquitous ones with a qualitatively new level of interoperability. Such a process is likely to initially converge into IPv6, namely IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [2], since it has a potential of leveraging the two basic concepts which brought success to the conventional Internet, namely packet switching and the "end-to-end" principle. The latter suggests that "[...] the behavior of the network should be determined by what is connected to it rather than by its internal construction [...]", and given the heterogeneity of end devices of IoT should help to "solve the problem of connecting heterogeneous devices rather than heterogeneous networks" [3].

The very prospective area of IoT, however, raises serious concerns over individual privacy in the new environment of smart things. The reason for this is that thanks to the omnipresent intelligence-integrated artefacts, the process of sampling and distribution of information in IoT can be practically carried out anywhere. Ubiquitous connectivity through Internet access aggravates the problem because, unless special mechanisms are considered (encryption, authentication, etc.), personal information might become worldwide available.

In this position paper we express our concerns over privacy issues of IoT and outline possible solutions to this problem. The main focus is made on privacy

implications of RFID technology as it is fairly considered to be one of the main enablers of the IoT paradigm.

2 Privacy implications of IoT

Privacy issues are often left unconsidered during the development of IT systems and are frequently implemented later as an add-on rather than a built-in solution. That might result in immaturity of privacy compliance of the end product and consequently endanger privacy of its users [5]. Therefore, we argue that it is highly important to pay proper attention to privacy issues because the maturity of privacy management mechanisms and availability of robust security solutions[1] will to a large extent determine the level of acceptance of the IoT concept among users. The authors of [1] claim that "People will resist the IoT as long as there is no public confidence that it will not cause serious threats to privacy". In [5] we have already discussed the privacy implications of UbiComp, which to a large extent intersect with the ones of IoT. In this position paper, we would like to focus above all on IoT and also present our view on its privacy implications.

Radio Frequency Identification (RFID) is quite often seen as the major and possibly the most suitable technology which is going to enable IoT. Low-cost, mass production and the ability to attach RFID tags to almost every possible artefact makes them truly pervasive. This surely raises serious privacy concerns because, in such a scenario, the IoT technology has the potential to penetrate everybody's everyday life and affect not only the individuals who directly use the service, but also those, who are simply unaware of the fact that they are the "passive" users. For example, in [6,7], a scenario of integrating RFID tags into clothes was described. For logistic purposes and returns tracking a chip can be sewn into the garments during the manufacturing process and remain in operation even *once the item has been sold*. This raises serious concerns over privacy of customers who happen to use the RFID system in a subtle way without their consent. Equipping garments with RFID tags may enable remote tracking of customers and therefore paves the way to illegal profiling introducing another case of privacy violation.

That is why Weber mentions in [8] that the EU Commission is going to seriously consider the "right to silence of the chips" and the possibility of the individuals to be able "to disconnect from their networked environment at any time". This closely relates to the problem of the "disability to opt-out" discussed in [5] where it was explicitly mentioned that one of the key requirements to provide for a privacy-respecting system is the support of opt-in/opt-out according to the user's choice (i.e. carefully considering the individual's consent).

The ability of mass producing RFID tags and their wide distribution, which ensures the ubiquitous presence of computing and its pervasive penetration into daily life aggravate the problem. According to [6], around 15 million chips were shipped to the retail company by 2003. This demonstrates the large scale of

[1] Security provides for the necessary basis for implementing and ensuring privacy and is, therefore, an integral part of the underlying mechanisms of privacy management.

this initiative. Moreover, the authors of [7] inform that some firms are going to release *handheld* devices capable of reading RFID tags (including the ones, woven into the garments). That means that it has become much easier not only to disseminate personally identifiable information (PII) to the infrastructure (fixed readers) but also to perform *reading* from mobile[2] readers which have become relatively small and unobtrusive. If such devices are further equipped with the function of transforming the RFID-specific data (obtained from the query) into IP-compatible format (i.e. acting as a gateway) and have access to the Internet, then the queried PII can be made worldwide available without necessarily allowing the affected individuals to have any control over this, or perhaps not even informing them of the data distribution.

The authors of [1] argue that "[...] there will be an amazing number of occasions for personal data to be collected" putting a so-called "right to be forgotten" in question because the intelligent artefacts can now gather the PII and save it for an indefinite length of time.

3 Possible solutions

It is always desirable that privacy and security are considered through a cross-layered approach. That is why we suggest introducing privacy protecting solutions into IoT across several layers[3]. At the application layer, access control policies, and enforcement thereof should enable privacy management, as has been demonstrated in [4]. At the lower layers, privacy middleware should provide for necessary interfaces which can be used up the stack and therefore bridge the specific communication mechanisms between the smart things and their high-level representation.

Finally, inherent privacy implications, which directly result from the specific technology of smart things production, should be considered as well. For example, the ability to perform a remote reading of an RFID tag from a large distance or if it is possible to permanently deactivate a tag with a guarantee that it can not be reactivated in future.

Moreover, the means of technical privacy enforcement applied directly to end devices (e.g. RFID tags) play an important role in privacy protection. The following list describes several techniques, which from our point of view are the main components of technical privacy enforcement in the IoT, focusing on their implementation in RFID:

– *Anonymization.* Given the ubiquity of RFID tags distribution and the constantly increasing likelihood of their pervasive presence in daily life, it is important to provide for protection against data linking and profiling. The authors of [17], for example, described a scheme allowing an RFID tag to answer with a different ID to each new request of the reader[4]. Since a legit-

[2] RFID readers are usually fixed or mobile but not handheld.
[3] Analogous to the OSI Basic Reference Model [16].
[4] This procedure is based on the randomization algorithm implemented in the tag's circuitry.

imate reader is connected to the system database where the ID sets of each tag are stored, tag identification by legitimate parties is enabled while an adversary is prevented from doing so.

- *Encryption.* Personally identifiable information (PII)[5] residing in the tag is subject to protection. Lightweight implementations of encryption can protect sensitive information from illegitimate exposure. The authors of [19,18], for example, have already demonstrated the feasibility of AES[6] and ECC[7] implementation in constrained environment of RFID.
- *Hash functions.* In order to ensure that an RFID tag offers its functionality only to a legitimate reader, hash functions can be utilized. For example, the authors of [22] suggest a concept of an "unlock key" implemented through a hash function, which ensures that only a reader possessing such a key can have its request processed by a respective tag.
- *Tamper resistant modules.* Critical data (e.g. encryption and identification keys) can be stored in the protected memory area of a tag, which has a tamper-resistance property. The utilization of such areas, however, may significantly raise the cost of a tag and given the scale of production process, the overall cost of a system.
- *Disabling a tag.* A very straightforward but effective approach: physically shielding a tag when not in use (e.g. Faraday cage), temporarily disconnecting RFID antenna (by using, for instance, the "clipped" tags principle described in [23]) or plainly killing a tag by destroying its antenna.

Technology alone will not be able to provide for full-fledged privacy protection mechanisms. Additionally, legal issues should be considered. Thus, privacy regulation and *legal enforcement* of privacy rights is an important part of privacy management mechanisms in the IoT.

The European Commission expressed its concerns over privacy in RFID-based applications and issued a recommendation "on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification" — the so-called framework for privacy and data protection impact assessments (PIA) [9]. This framework is targeted at facilitating the process of establishment and maintenance of compliance with the privacy and data protection laws and regulations as well as risk management in RFID systems. It also provides for privacy assessments at early stages of RFID system development. Thus, we consider PIA as one of the key steps for developing IoT systems according to the "Privacy by Design" paradigm [10].

The development of such a framework is a decent step towards the creation of a competent and widely acceptable means of privacy assessment of an RFID

[5] The information stored in the tag which can be used for inference allowing to obtain PII falls into this category as well. Consider an example of a unique ID of a tag woven into clothes combined with the name of a customer who has purchased the respective garment.

[6] Advanced Encryption Standard [20].

[7] Elliptic Curve Cryptography [21].

system, which can be understood by all parties involved. Furthermore, having created the appropriate legal basis, it might be possible to oblige organizations, which utilize RFID technology for business purposes, to carry out PIA assessment with, for example, subsequent certification. The resulted report can be provided for an external review by the respective authorities enhancing the transparency and contributing to the overall process of privacy protection.

Surely, such a framework can be efficient only if it is based on the results of a decent research on underlying technological principles of RFID systems and privacy implications of these.

In order to approach privacy issues in the IoT based on RFID technology, we suggest that the following requirements are considered:

- *Assessment of privacy compliance of the RFID system*: It should be possible to provide for competent privacy assessment (e.g., based on PIA) of the RFID system in question in a way, that can be understood by all parties involved.
- *Ability to opt-out*: By default, the users should be provided with an opportunity to prevent communication of their devices with the RFID infrastructure at any time.
- *Ability to permanently disable the tag* [8]: some of the tags are constructed in such a way that they can be remotely reactivated again after having been sent the deactivation command ("kill" command). Thus, it might be useful to certify the utilization only of those tags the processing and transmission functions of which can be permanently disabled (e.g., by a strong electromagnetic impulse which *physically* destroys the tag's circuitry).
- *Marking the intelligence-enabled artefacts*: The fact of intelligence being integrated into certain artefacts should be made visible to *all* individuals who might be directly and indirectly affected by the RFID system (e.g., attaching special markers to the smart things which indicate their IoT activity. Whenever this is not possible (e.g., in case of RFID transceivers sewn into clothes, see [6,7]), this kind of information should be included into the terms of use supplied along with the goods containing the IoT device/s.
- *Considering M2M Privacy*: Machine-to-machine (M2M) privacy should be specifically addressed. Current EU Directives only consider natural persons as objects of privacy laws [13]. In IoT environments, however, smart artefacts quite often can be directly associated with their owners or even with other individuals in their vicinity and thus to a large extent affect the individual privacy. Moreover, one of the definitions of the IoT itself indirectly introduces the notion of M2M: "Things *having identities* and *virtual personalities* operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts" [1]. This results into smart things possessing their own privacy derived from that of an individual. Since smart things can communicate with each other (M2M communication, see [14,15]), this form of privacy can be called M2M privacy.
- *RFID usage restriction*: Critical areas should be protected by prohibition or at least restriction of the use of RFID technology [8]. This is because

some areas (e.g., AIDS centers, etc) succumb to particular regulations with respect to the privacy of the individuals.
– *Support for security goals*: Confidentiality, integrity, and availability should be provided for in IoT systems. The authors of [12] claim that to a certain extent it is already feasible to solve this problem, for example using the AES/CCM encryption (see [11] for details).

Moreover, the current legal regulation on privacy in the EU is rather coarse-grained and hence inflexible. Weber claims in [8] that "[...] only "extreme" warranties are legally guaranteed [...]". That is why a lot of effort should be targeted at fine-tuning the legal privacy regulations. These, from our point of view, can be realized only in cooperation with IT specialists who can provide for the necessary technological basis highlighting the peculiar privacy threats inherent in the IoT systems.

4 Conclusion

IoT is a very promising and challenging paradigm. Modern communications are steadily evolving and IoT is one of the milestones which is going to determine the technological advance for the future. The dynamic environment of IoT introduces unseen opportunities for communication, which are going to change our perception of computing and networking. At the same time, the privacy and security implications of such an evolution should be carefully considered to prevent the promising technology from being transformed into a pervasive surveillance object.

References

1. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Comput. Netw.*, 54:2787–2805, October 2010.
2. J.W. Hui and D.E. Culler. Extending IP to low-power, wireless personal area networks. *Internet Computing, IEEE*, 12(4):37–45, july-aug. 2008.
3. Rafi Krikorian, Neil Gershenfeld, and Danny Cohen. The Internet of Things. *Scientific American*, pages 76–81, October 2004.
4. E Welbourne, L Battle, G Cole, K Gould, K Rector, S Raymer, M Balazinska, and G Borriello. Building the internet of things using RFID: The RFID ecosystem experience. *IEEE Internet Computing*, 13(3):48–55, 2009.
5. Ivan Gudymenko and Katrin Borcea-Pfitzmann. A Framework for Transforming Abstract Privacy Models into Implementable System Requirements. In *1st International Workshop on Model-based Interactive Ubiquitous Systems*, 2011.
6. Benetton to tag 15 million items. `http://www.rfidjournal.com/article/view/344`, March 2003. Accessed on 18.07.2011.
7. Antone Gonsalves. Privacy concerns hinder RFID rollout. `http://www.itnews.com.au/News/11417,privacy-concerns-hinder-rfid-rollout.aspx` Jan 2000. Accessed on 18.07.2011.
8. Rolf H. Weber. Internet of things - new security and privacy challenges. *Computer Law & Security Review*, 26(1):23 – 30, 2010.

9. Report. Privacy and data protection impact assessment framework for RFID applications., Jan 2011. Accessed on 25.05.2011.
10. Ann Cavoukian. *Privacy by Design. Take a challenge.* Electronic resource, 2009. Availbable at: `http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf`
11. D. Whiting, R. Housley, and N. Ferguson. Counter with CBC-MAC (CCM). *Internet Ingineering Task Force*, 2003.
12. Zach Schelby and Carsten Bormann. *6LoWPAN: the Wireless Embedded Internet.* Wiley, 2009.
13. European Parliament and Council Directive. Directive 2002/58/EC of the European Parliament and of the Council: concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Communities, 2002.
14. Inhyok Cha, Y. Shah, A.U. Schmidt, A. Leicher, and M.V. Meyerstein. Trust in M2M communication. *Vehicular Technology Magazine, IEEE*, 4(3):69 –75, sept. 2009.
15. Geng Wu, S. Talwar, K. Johnsson, N. Himayat, and K.D. Johnson. M2M: From mobile to embedded internet. *Communications Magazine, IEEE*, 49(4):36 –43, april 2011.
16. J.D. Day and H. Zimmermann. The OSI reference model. *Proceedings of the IEEE*, 71(12):1334 – 1340, dec. 1983.
17. Jacek Cichon, Marek Klonowski, and Miroslaw Kutylowski. Privacy Protection in Dynamic Systems Based on RFID Tags. In *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, pages 235 –240, march 2007.
18. Michael Hutter, Martin Feldhofer, and Johannes Wolkerstorfer. A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines. In *WISTP*, pages 144–159, 2011.
19. Michael Hutter, Marc Joye, and Yannick Sierra. Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation. In *AFRICACRYPT*, pages 170–187, 2011.
20. NIST. Specification for the Advanced Encryption Standard (AES). FIPS 197., November 2001.
21. Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):pp. 203–209, 1987.
22. S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *1st International Conference on Security in Pervasive Computing (SPC)*, March 2003.
23. Günter Karjoth and Paul A. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, WPES '05, pages 27–30, New York, NY, USA, 2005. ACM.