An Overview of Privacy and Security Issues in the Internet of Things

Carlo Maria Medaglia and Alexandru Serbanati

1 Introduction

The trend of having ever more objects included in the IT data flows and ever more connected devices, moving toward mobile and decentralized computing is evident. The Internet and ancillary technologies are the base that provide the needed connectivity. In the last few years, the idea of connecting existing computing devices gave place to the concept of "connecting things." The Internet of Things, as it is called, has drawn a lot of attention from many academics and public research institutions. While there is no global consensus on the meaning of the term [1–3], it is clear that the main idea behind the IoT concept is the ability to connect loosely defined smart objects and enable them to interact with other objects, the environment, or more complex and legacy computing devices. The communication infrastructure will be based on an extension of the Internet, which will enable transparent use of the object resources across the globe. Smart objects will densely populate human life and human environment [4], interacting with both by providing, processing, and delivering any sort of information or command. Objects and environment will be able to tell us about them, their state, or their surroundings and can be used remotely. Sensors will be integrated in buildings, vehicles, and common environment, carried by people and attached to animals and will communicate among them locally and remotely in order to provide integrated services.

For example, mobile devices could adopt silent mode when entering a meeting room if this is the request of the meeting moderator, alert the user and turn off the radio before entering sensitive medical areas or detect when the user enters the car and connect to its sound system. Wireless sensors could let people check where their pet is in real-time as well as control the temperature of each room of their house while they are out. Emergency services could be remotely and automatically alerted if fire is detected in a building or if a patient's medical parameters drop beyond a critical threshold.

C.M. Medaglia (✉) and A. Serbanati
Centro per le Applicazioni della Televisione e delle Tecniche di Istruzione a Distanza (CATTID), University "Sapienza", Rome, Italy
e-mail: carlomaria.medaglia@uniroma1.it

D. Giusto et al. (eds.), *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*, DOI 10.1007/978-1-4419-1674-7_38,

With such a deep penetration of technology, which will introduce a new kind of automation and remote interaction, it is likely that new security and privacy issues will rise.

2 Short Term

The first steps of this process are already ongoing, with autoID and sensor and actuator networks as peripheral enabling technologies. In this context, only presence and sensor data can be provided by the peripheral part to the central structure. Radio Frequency Identification (RFID) tags are passive (powered by the RF field emitted by the RFID reader) while more complex objects are battery powered. Their battery lifetime is in inverse proportion to that of their processing and communication potential. Self- and context-awareness, provision of web services[1] as well as mobility inside a global, morphologically dynamic network are still missing at this stage. Also, a fundamental lack is the absence of a unified communication standard across the different parts of the Internet of Things network.

Even if some of the auspicated enabling technologies for the IoT are still missing, it is evident that the resulting overall number of connected devices will be very large and the Internet, as we nowadays conceive it, would soon be overwhelmed. One of the shared ideas about the possible solution is the adoption of the IPv6 standard, which will provide a sufficient number of available unique addresses for many years to come, thanks to a 128 bit addressing instead of current 32 bit of IPv4. This scenario, dominated by current technological limits, is what the authors call the short-term scenario.

The current scenario follows two main ways of collecting information in the environment: RFID and Wireless Sensor Networks (WSN). Note that while authors have chosen a technology from each of the aforementioned peripheral enabling technologies, both are wireless because: (a) this is the current IoT forecast trend in order to provide mobility and service portability, and (b) wireless devices are more challenging from a security point of view as they share the physical medium with other, potentially malicious devices.

2.1 RFID and Identification

The most common RFID implementations use passive tags, which uniquely and wirelessly identify the items to which they are attached, enabling they presence

[1] Authors use the term "services" when referring to high level services provided by business systems to their users, while the term "web service" is properly used for a software capable of providing a standard interface with other computing devices across the network. The term "infrastructure service" will be used referring to a software run by the governance of the IoT providing smart objects critical information for the operation of the IoT itself.

monitoring. Recent tags, especially UHF ones because of their higher data throughput and widespread, also have a small amount of memory in which business data can be stored, but usually this data is either unprotected or read-only locked. EPC Global Gen-2 tags also provide a wider range of primitive functions onboard though labels provide no security feature by default. *Kill* and *Lock* commands are available. The former feature is not useful in the IoT context and, as seen in [5], it may lead the way to other threats as eavesdropping the communication session could give an attacker the 16bit PIN needed to kill the tag which, usually, is the same for all the tags in a given system.

In RFID systems, the reader never authenticates and tags are by default set to respond to the interrogation of any compliant reader, which poses a concrete threat to privacy. Not only authorized readers can read the tag, but also rogue ones. Also, even readers that should be authorized in a context could read the tag on unsolicited occasions. Approaches to this issue in logistics envisage the killing of tags, use of active jamming or even Faraday cages [6], but these are not compliant with such a pervasive architecture as that of IoT.

Also, the authentication of the RFID tags itself is subject to issues: while the primary goal of this technology is to provide a means of identification, it is not a secure way of. ID-writable tags are available in case of simpler RFID technologies. More recent standards (such as the aforementioned Gen-2) provide the primitives for developing more complex authentication features and a good amount of academic research is drawn by this subject [7]. Yet, the shared communication, physical medium, and the reduced computational capabilities make it difficult to develop an absolutely secure system [8] based on passive RFID.

Currently, RFID solutions should be used in noncritical contexts: in the IoT, RFID can provide information about object presence and, eventually sensor-collected data but system designers should address the risk malicious alteration of such information. Also, for RFID solutions to be integrated in the IoT, a special middleware must be used to provide a suitable, possibly web service based, interface to remote interaction. In this case, services will of course be provided by a central architecture or by the middleware. Security issues for this part of the network are out of the scope of this work.

13.56 MHz RFID-based Near Field Communication (NFC) is sometimes seen as an answer to some of the security issues of RFID. Mifare and NFC compliant devices provide authentication and symmetric cipher, though it has been already demonstrated that reverse engineering is practicable and can compromise the entire system [9].

The fact that the technology is usually embedded in mobile devices also provides interesting options for enhancing overall system security. As seen in [10], the availability of network communication and consequent access to a Public Key Infrastructure (PKI), together with the peer-to-peer NFC operation mode and a programmable environment may give place to secure applications.

2.2 WSN and Networking

The first and most important architectural differences between WSNs and RFID are the networking and processing capability. Nowadays, the greater part of WSNs are based on different implementations of the IEEE 802.15.4, a standard for low-rate WPAN, which provides different network topologies, among which mesh networking.

WSNs were born for field survey or control in military and ecological contexts. Such battery-powered computing devices had long autonomy and small form-factor requirements and thus usually had constrained hardware (low processing power, limited connection and storage capabilities) while compared to other devices.

These requirements very well suit the idea of IoT and mesh networking is also very interesting because, in this way, devices are not bound to operate in a specific area. Albeit the processing power is minimal, it is sufficient to provide some automation. WSN-based systems are still centralized, being controlled or used by more complex and powerful devices. Sometimes [11] such devices can be attached to the system to act as a gateway or provide services to users across the Internet. Home automation is one of the most widespread applications of such technology.

WSNs are a key enabling technology in the evolution of IoT as the presence of a network architecture facilitates the integration in a larger framework (i.e., the IoT infrastructure) and the provision of services. Services that could be technically provided through the means of WSNs are very appealing and pervasive of human life. Being potentially very pervasive and directly impacting users' lives, securing such systems must be taken into account. A general overview of security in WSNs is given in [12].

Authorization prior to inclusion of nodes in a WSN is very important as, even if other (higher level) security mechanisms could prevent rogue nodes from deciphering or injecting packets, they could easily provoke Denial of Service (DoS), for example, by overwhelming the (reduced) network bandwidth.

Authentication should also be taken into account as, failing that, there is a concrete risk of running business processes or providing services on top of malicious data. Authentication should be done against secure PKIs, probably run by Certification Authorities. This will become particularly important for mobile devices as these could provide mobile gating capabilities for less complex smart objects, which cannot have a dedicated connection to the Core Infrastructure. Creating the tools for enabling trust in such a scenario will likely speed the adoption of the IoT paradigm.

Data confidentiality and integrity are also issues for the possible consequences on user privacy and safety. Failing this, private sensor data could be available to malicious users, actuators could be commanded to perform unauthorized actions or the correct functioning of the system could be altered by corrupting packet loads.

Talking about the IEEE 802.15.4 standard, it provides some security features. This standard defines Physical and Medium Access Control layers. First of all, an Access Control List (ACL) can be defined and only frames from the nodes listed in it are admitted to be received. Basic access control, message integrity, message confidentiality and replay protection are provided.

There are different implementation of the 802.15.4, the most interesting of which are ZigBee and SunSPOT. ZigBee provides an application layer security (APS) while SunSPOT users (still at version 0.4) provide SSL. SunSPOT is an exception to the reduced resources characteristic of WSN devices as it works on a 200 MHz ARM7, its OS is open source, it can be programmed in Java, and thus could implement any potential security feature. The only limit is that security features usually draw upon the reduced processing power and bandwidth, producing a significant overhead over the business logic and the messages' payload respectively.

Evolutions in IoT will likely see the presence of PKIs to establish trust between different component devices. According to the current architecture, which is still centralized, object to object connectivity is not contemplated. The 6LoWPAN project [13] aims to bridge this gap providing IPv6 address compression and communication gating low-rate WPANs (i.e., 802.15.4 compliant). PKIs assume a critical role in this context as security features implemented on WSNs must be forwarded to the entire IoT or, where possible, protocols for scaling Internet (i.e., computer) level security features to low rate WPANs (i.e., smart objects) should be provided. Though current devices are not yet sufficiently powerful, this would also open the way to policy regulated service providing as authentication could be provided in both directions.

3 Long-Term Vision

Future devices will likely be as powerful and resourceful as any current mobile or even fixed device and they will have all the privacy and security issues that such current devices have. Miniaturization and increase in spectrum efficiency will enable a denser use of devices which, in turn, will be more sophisticated.

In this new scenario, standardization, semantics, and the availability of smart-object-based services will very likely be the key to the success of this paradigm. In this context, many new private, public, and business services can be conceived. An interesting set of visionary scenarios explored by a high-level visionary Panel of experts of the European Commission can be found in [4]. These efforts toward understanding the future scenario should serve as a base for better extending the current legislation to the new issues brought by the IoT paradigm. Such architecture also poses a great challenge for what concerns its governance. In [14], the European Commission places

> the definition of a set of principles underlying the governance of the Internet of Things and the design of an architecture endowed with a sufficient level of decentralized management

as the first action to be undertaken to promote the evolution of the IoT.

Privacy is also one of the main concerns: issues will arise as data collection, storage, mining, and provision will be completely different from what we now know and legislation shall change accordingly. The number of entities providing services as well as the occasions in which personal data could be collected by such entities

will be greater than what the human user could manage by himself. The solution will be a personal policy-based privacy management system that will automatically negotiate and handle privacy issues for the user according to the rules set by the governance. It will be very important though to provide the user with the right tools for letting him ultimately in control of his own privacy. Such a system might be somehow compared to the identity management system, which is under development by the PRIME project [15].

For example, in order to enforce privacy, devices should have at least two context-based operating modes: public and personal. In the former state, the object should advertise its presence and provide its services to all nearby devices. In the later, it should listen only for other object's presence advertisement and inform about the services it provides only those objects with which a close relationship subsists and public key is already possessed (for example, those belonging to the same user).

In a wider view, smart objects should be able to transparently manage interaction with the environment by using user-defined policies. As previously mentioned, it will be important to have the user in control and that he feels so.

Also, a new set of issues will rise from the high mobility of smart objects and the services they provide. Devices will travel across the world, always and transparently providing the user with their functionalities. To this end, they will locally connect to other objects or gateways. They will have to manage both situations in which they – either directly or not – can access the IoT infrastructure and relative services, and contexts in which they will only be able to communicate with nearby devices. Ad hoc security solutions and policies should be developed for managing mutual authentication, policy enforcement, and basic communication security in both situations.

Security management of nomadic devices will also be an issue. Mobile or worn smart objects, for example, will be able to connect to the infrastructure through different connections in time (some of which may be public while other may be provided by TLC for example). These devices though will need to safely interact with other devices spread across the word, which are not aware of their movement, connection status, etc.

The services too will have to be redesigned as they will become probably portable from one device to a possibly completely different one. It is too soon though to understand how services will actually evolve.

4 Conclusions

It is certain that many other new solutions are needed in order to enable the long-term vision. As for all the newborn visions, there is little agreement in the scientific community about the architectural and technical solutions to adopt. There is though a common feeling that standardization will be one of the key enabling factors. Thus, IoT security design should also follow this trend in order to enable an open, pervasive and interoperable yet secure infrastructure. For the sake of privacy and

flexibility, smart objects should be capable of implementing individual, user set policies. Infrastructural security services should also be accessible transparently and regardless of the connection used by nomadic smart objects.

References

1. Gershenfeld N, Krikorian R, Cohen D (2004) The Internet of things. Sci Am 291(4):76–81
2. Furness A (2008) A Framework Model for The Internet of Things. In: GRIFS/CASAGRAS Workshop, Hong Kong, December 2008
3. Presser M et al. (2008) Real World Internet (Position Paper). Future Internet Assembly, Madrid, Spain, December 2008
4. Hourcade JC, Nuevo Y, Wahlster W, Saracco R, Reinhard P (2009) Future Internet 2020: visions of an industry expert group. Future Internet Final Report, Belgium, May 2009
5. Duc DN, Park J, Lee H, Kim K (2006) Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning. The 2006 symposium on cryptography and information security, Hiroshima, Japan
6. Korkmaz E, Ustundag A (2007) Standards, security & privacy issues about radio frequency identification (RFID). RFID Eurasia, 2007 1st Annual, Istanbul, Turkey
7. Chien HY, Chen CH (2007) Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Comput Stand Interfaces 29(2):254–259
8. Peris-Lopez P, Hernandez-Castro JC, Estevez JM, Ribagorda A (2009) Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. Comput Stand Interfaces 31(2):372–380
9. Garcia FD, de Koning Gans G, Muijrers R, van Rossum P, Verdult R, Schreur RW, Jacobs B (2008) Dismantling MIFARE classic. Proceedings of ESORICS 2008, Malaga, Spain, pp 97–114
10. Aigner M, Dominikus S, Feldhofer M (2007) A system of secure virtual coupons using NFC technology. Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth annual IEEE international conference on, 19–23 Mar 2007, pp 362–366
11. Arch Rock. Arch Rock PhyNetTM. http://www.archrock.com/product/
12. Boyle D, Newe T (2008) Securing wireless sensor networks: security architectures. J Netw (JNW) 3(1):65–77
13. Mullingan G (2007) The 6LoWPAN architecture. Proceedings of the 4th workshop on embedded networked sensors, Cork, Ireland, pp 78–82
14. European Commission (2009) When your yogurt pots start talking to you: Europe prepares for the internet revolution. European Commission's Press Release, June 2009
15. Hansen M, Krasemann H (2008) PRIME whitepaper. Available at https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf, May 2008