Privacy in Smart Cities
A Case Study of Smart Public Parking

Pablo A. Pérez-Martínez, Antoni Martínez-Ballesté and Agusti Solanas
CRISES Research Group, Universitat Rovira i Virgili, Av. Països Catalans 26, Tarragona, Spain

Keywords: Parking, Smart Cities, Privacy, Privacy Enhancing Technologies, Ubiquitous Computing.

Abstract: Cities are steadily growing and the process of urbanisation is prevalent worldwide. With the aim to provide citizens with a better place to live, a new concept of city was born: the **Smart City**.

This concept has gained much attention and many "regular" cities are taking action so as to become "smart". To do so, cities are deploying and using information and communication technologies, with the aim of tackling many local problems from local economy and transportation to quality of life and e-governance.

In this article we recall the concept of smart city and its main areas of interest. We discuss that the ubiquitous use of information and communication technologies within the context of a smart city might lead to the transparent gathering of private data from citizens. We focus on the transportation area and, more specifically, on the parking problems that might arise in big cities. We propose a set of procedures, based on privacy enhancing technologies, that allow the private, secure and efficient management of parking in smart cities.

The main goal of this article is to foster discussion about the privacy issues that might arise in a smart city and to provide an example scenario (i.e. public parking) to demonstrate some interesting ideas and show some open problems.

1 INTRODUCTION

Countries are making great efforts to be competitive, attract investments and talent, reduce debt and be more sustainable. The struggling of countries for competitiveness has a smaller version in their cities, which are competing at an international level for investments, talent and quality of life, and they realise that the most promising path to success is the use of technology. Specifically, information and communication technologies (ICT) allow local governments and companies to develop ubiquitous innovative solutions that improve city operations in a variety of areas, such as transportation, energy, sustainability, e-governance, economy and communications.

In big cities, factors related to economies of scale help to reduce operational costs. However, managing big cities is challenging because the number of inhabitants grows steadily and the infrastructures and operational procedures have to be adapted to a growing and very demanding population.

In this context, local administrations have the need for smart procedures to improve the quality of life and the management of resources in cities. As a result of these needs, the concept of smart city appeared and, although this is pretty new, we can find several examples of cities that pursued this idea applied to a variety of areas (e.g. Amsterdam (Liander and AIM, 2012), Vienna, Toronto, Paris, New York, London, Tokyo, Copenhagen, Hong Kong or Barcelona (Activa, 2012)).

A very relevant area in every city is transportation. On the one hand, the management of public transportation is a very important and difficult issue that has been studied and companies, such as IBM, are proposing solutions to make it smarter (IBM, 2011). On the other hand, private transportation has proved to be a cornerstone for the local government of any big city. The challenges related to private transportation are diverse, namely traffic jam management, tax collection, parking lots management, and so on.

In this article we revise the definition of smart city, which is a concept that has not been fully defined. We show the great advantages of smart cities, such as reduction of CO_2 emissions, improvement of the relations between citizens and administrations, increase of the efficiency of public and private transportation, etc. However, we note that the easy gathering of data that occurs in ICT-based smart cities might open the door to privacy attacks from, at least, two sides: (i) from the infrastructure and (ii) from external attackers. To exemplify this situation we consider the spe-

Pérez-Martínez P., Martínez-Ballesté A. and Solanas A..
Privacy in Smart Cities - A Case Study of Smart Public Parking.
DOI: 10.5220/0004314700550059
In *Proceedings of the 3rd International Conference on Pervasive Embedded Computing and Communication Systems* (PECCS-2013), pages 55-59
ISBN: 978-989-8565-43-3

cial case of parking management within a smart city and we describe a protocol that allows the private and secure management of the information required to control the payments in public parking lots.

The rest of the paper is organised as follows: In Section 2 we provide some background on smart cities, we propose an extended definition for smart city and we describe our case study. In Section 3 we describe our privacy-aware protocol for our case study and, in Section 4, we briefly summarise its main properties from a privacy and security perspective. Finally, the article concludes with some final remarks in Section 5.

2 BASICS OF SMART CITIES AND CASE STUDY

2.1 Smart Cities

In recent years many people have started to use the term "*Smart City*" but in many cases the meaning given to this term changes from person to person. Moreover, the term has gained a kind of marketing value that local governments want to benefit from. Thus, the definition of the term is frequently modified so as to adapt to the needs of the people using it in a particular situation. As a consequence, a number of different definitions and conceptual ideas regarding smart cities can be found in the literature.

From a very general perspective we could say that smart cities are those in which people can make their own choices and have a high quality of life combined with the efficient use of resources and the reduction of emissions. More specifically, a smart city considers six main areas/dimensions that are connected to the neoclassical theories of urban growth and development:

- *Smart Economy.* Improve regional competitiveness and attract talent.
- *Smart Mobility.* Improve the efficiency of public transportation and the management of private vehicles.
- *Smart Environment.* Reduce the energy footprint and to better use natural resources.
- *Smart People.* Promote human and social capital.
- *Smart Living.* Increase the quality of life of citizens.
- *Smart Governance.* Foster the participation of society and the interaction of the citizens with the administration.

According to Caragliu et al. (Caragliu et al., 2009) a city might be considered "smart" when it invests in human and social capital and in traditional (transport) and modern (ICT) communication infrastructures that fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance.

We complement this definition by adding that a city to be "smart" should guaranty the privacy and security of its citizens, in the spirit of the concept of the W^3-Privacy (Pérez-Martínez and Solanas, 2011), so as to foster their participation and avert the *Big Brother* effect, which might raise concerns amongst privacy advocates.

To summarise, our definition of smart city is as follows:
≪ ***Smart Cities** are cities strongly founded on information and communication technologies that invest in human and social capital to improve the quality of life of their citizens by fostering economic growth, participatory governance, wise management of resources, sustainability, and efficient mobility, whilst they guaranty the privacy and security of the citizens.* ≫

2.2 Case Study: Public Parking

Parking a vehicle in a crowded city is a difficult task due to several reasons. First, it is complicated to find a place and people waste a lot of time looking for a parking lot. Second, once a parking place is found, in many cases, drivers are required to pay some money depending on the time that the vehicle is parked. This payment poses several problems:

- *Need for Change.* If the payment method is based on parking meters, drivers need to carry some change: in general, credit cards are not supported; if they are supported, card readers can be easily damaged and therefore become useless. If the payment method is based on pay and display machines, drivers might pay with money or credit cards, but they have to find the machine and then go back to the car to leave the ticket obtained.
- *Have Extra-costs.* In some places prepaid RFID cards (wallet cards) can be used to pay for the service but they are usually not re-usable and drivers pay the extra-cost of the card every time they buy a new one (Ostojic et al., 2007).
- *Pay again to Move the Vehicle to another Area.* In most cases, after paying for parking in a place, if the driver moves to another place (located in a different payment area of the city), he/she must pay again and cannot use the ticket previously issued even if it has not expired.

- *Renew the Ticket.* When pay and display machines are used, if the ticket expires drivers must go back to the machine, buy a new ticket and leave it in the car. This is a very inconvenient procedure, specially if the driver is far from the parking place.

In the context of a smart city we assume that a number of RFID readers are deployed so as to identify vehicles and control their payment status. Thus, in addition to the previously stated problems, we identify some attacks against the privacy of the users that can take place and should be avoided:

- *Attacks from the Infrastructure.* Some of the current parking systems use contactless technology, but in most cases users use an ID. If vehicles are identified with a single ID (e.g. the licence plate, or the like), the infrastructure can obtain a record of the locations that a given driver visits and can obtain extra-information that might endanger the privacy of drivers, namely their habits, their place of residence, their place of work, etc.
- *Attacks from External Attackers.* If RFID technology is used inappropriately, external attackers could obtain the identification of the vehicle and clone it so as to avoid payment by stealing the identity of legitimate users.

In our case study we consider all these problems related to both the payment and identification of the vehicles. We do not consider the problem of finding a parking place because it has been widely studied and several solutions already exist (Lee et al., 2008). Thus, to address the aforementioned problems we need to design a procedure (or a set of protocols) that guaranties the following properties.

- *Anonymity.* Payments should be anonymous so as to avoid the identification of the user by the infrastructure and avoid undesired profiling.
- *Remote payment.* Payments might be done remotely, this is, without the need for change and without the need for going back to the vehicle or the parking meter.
- *Transparent Multi-area Parking.* If users have paid for a given parking time and they change the location of their vehicle, they should be allowed to use the remaining time that they have (if any) in the new parking place.
- *Untraceability.* External attackers and the infrastructure should not be able to distinguish two different payments from the same user. Thus, they cannot infer the habits or the places frequently visited by users.

3 PROTOCOL

In this section we describe our protocol, which uses off-the-shelf privacy enhancing technologies to address the problems identified in the previous section. We assume that users/drivers have an RFID card and a mobile phone that can communicate with this card. First, we describe the procedure to anonymously pay by means of e-cash. Then we describe how to use our protocol within the context of a smart city.

3.1 Anonymous Payment

With the aim to break the link between the identity of the user and the payment he/she makes, we propose the use of anonymous e-cash. To obtain e-cash and proceed with the payment, users operate as follows:

1. **Get e-cash.** A user U_1 gets e-cash (electronic cash) from a bank. To do so, one can use a lot of existing protocols, for example the system proposed in the patent (Simon, 1995), in which a user asks to the bank for a given amount of money in the form of electronic cash. To do that, the user sends a request for some quantity of e-cash to the bank, and the bank sends back to the user the e-cash with the requested value. In this procedure the bank signs the money so as to guaranty its validity. By using this procedure, double spending is averted by the bank.
2. **Pay for the Service.** When U_1 parks a vehicle in a public parking area that requires payment, he uses the previously obtained e-cash to pay the service by using a mobile phone (*cf.* Figure 1). To proceed, the user sends an activation message to the RFID tag located in the vehicle[1]. When the tag receives the activation message it generates a pseudonym using a one-way hash function h$(ID_1||r)$, where ID_1 is the private identifier of the tag, r is a random number generated by the tag, and $(||)$ is the concatenation operator. Then, the tag sends the pseudonym back to the driver, who will use it to make the payment.
3. **Verify the Payment.** Once the service provider receives the payment, it contacts the bank to check the validity of the e-cash. If the e-cash received is valid the bank sends the money to the parking service provider (cf. Figure 2).
4. **Determine and Store Expiration Time.** The parking service provider converts the e-cash re-

[1] This communication can be performed in a variety of ways, but the use of NFC is becoming popular and might be the standard in the near future.

ceived into "parking time" and determines the expiration time for the user. Finally it saves this information in its database and informs U_1 about the expiration time.

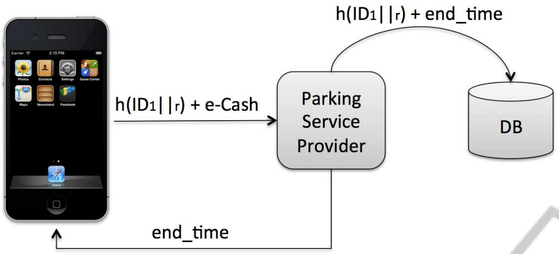

Figure 1: Payment by means of e-cash and a mobile phone.

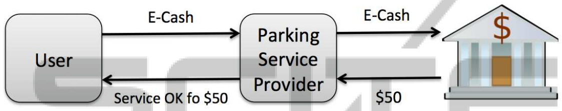

Figure 2: Scheme of the payment and validation procedure.

3.2 Protocol Operation in a Smart City

We assume that the smart city in which our protocol is applied has a number of RFID readers deployed in public parking areas. Those RFID readers are able to identify RFID tags.

- When a user U_1 parks in a monitored parking place, an RFID reader detects the tag in the vehicle and registers its current ID in its database *DB*. As stated before the ID of the tag that the reader will obtain is a pseudonym like h($ID_1||r$) that will be related to the payment issued by U_1. For the communication between the RFID reader (R) and the RFID tag of the user's vehicle (T), we can use the improved randomised hash-locks (IRHL) protocol (Juels and Weis, 2006). IRHL are computationally cheap in the tags side (they only need a pseudo-random number generator and a hash function). In the IRHL protocol, R generates a random number r_1 and sends it to T. Then, T generates another random number r_2 and computes the answer $a = h(r_1||r_2||ID)$ where ID is the secret identifier of T, $(||)$ is the concatenation operator, and $h()$ is a one-way hash function. Finally, when R receives the answer (a) and the nonce (r_2) it determines the ID of the tag by performing an exhaustive search in its database looking for an identifier ID_i such that $a = h(r_1||r_2||ID_i)$. When that happens the tag is identified as ID_i. Figure 3 shows a graphical description of this protocol.
- U_1 proceeds to pay by means of his mobile phone, as we stated before (cf. Figure 1).
- Once U_1 has paid, the parking service provider updates the information about the expiration time in the database.

By using this procedure, users can pay anonymously, they can move from one area to another without paying again (because a centralised database contains all the information), they can extend their parking time by using their mobile phone, and they are not traceable thanks to the use of pseudonyms that can be changed every time a user parks a vehicle in a new location.

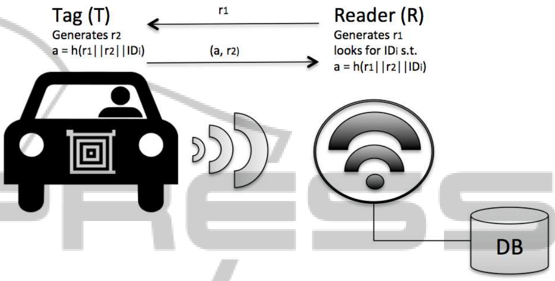

Figure 3: Secure communication between a vehicle and an RFID reader using IRHL.

4 DISCUSSION

We have designed our protocol so as to provide anonymity, remote payment, transparent multi-area parking and untraceability. Next we briefly discuss why our protocol achieves these goals and how they help to protect citizens privacy within the scope of a smart city.

- *Anonymity.* Thanks to the use of e-cash, the infrastructure cannot relate the payments with the identity of the user. This would be only possible if the infrastructure colludes with the bank. However, this does not seem to be a realistic scenario.
- *Remote Payment.* Due to the fact that the payment is no longer linked to a machine or a parking meter, users are able to pay remotely by using their e-cash through a mobile phone.
- *Transparent Multi-area Parking.* Information about payments and identifiers are stored in a centralised database. Thus, if users change the location of vehicles, they do not need new tickets.
- *Untraceability.* At any moment, the user might decide to send an activation message to the RFID tag of the vehicle. By doing so, the user makes the tag generate a new pseudonym that will be used to pay and to identify the vehicle. Due to the fact that pseudonyms change, it is impossible for the infrastructure to trace users by means of their ID.

From a security point of view, the use of the IRHL for the communication between vehicle tags and infrastructure readers guarantees that the pseudonyms generated by tags cannot be cloned. Thus, the security of the drivers is also guaranteed. The down side of IRHL is their computational cost in the readers side. However, it has been shown that it is possible to obtain efficient identifications by using the collaboration of multiple readers (which would be highly applicable in a smart city scenario) (Trujillo-Rasua et al., 2012), (Trujillo-Rasua and Solanas, 2011b), (Trujillo-Rasua and Solanas, 2011a).

5 CONCLUSIONS

Information and communication technologies have opened the door to an unprecedented amount of opportunities for cities to become smart. In this article we have recalled and clarified some concepts related to smart cities. With the aim to show some of the privacy and security problems that might arise within a smart city, we have considered a case study focussed on managing parking payments. We have proposed a protocol that uses private enhancing techniques such as pseudonyms, improved randomised hash-locks and, anonymous payments, to guarantee the privacy and security of the citizens that park their vehicles in public parking areas in a smart city. We have discussed that our protocol allows anonymity, untraceability, remote payment and transparent multi-area parking. Further work includes the implementation of this protocol in a real scenario.

ACKNOWLEDGEMENTS

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 “ARES”, project TSI2007-65406-C03-01 “E-AEGIS”, project TIN2011-27076-C03-01 “CO-PRIVACY”, project INNPACTO 2010 PT-430000-2010-31, project AVANZA I+D 2009 TSI-020100-2009-720, project AVANZA I+D 2010 TSI-020302-2010-153, and by the Government of Catalonia under grant 2009 SGR 1135.

Pablo A. Pérez-Martínez and Agusti Solanas thank the Security and PRivacy INnovation GRoup (SPRINGeR) of the University of Roma Tre for hosting them for a research stay during which this article was written.

The authors are with the UNESCO Chair in Data Privacy, but the views expressed in this paper are their own and do not commit UNESCO.

REFERENCES

Activa, B. (2012). Live barcelona. Website. http://w41.bcn.cat/web/guest.

Caragliu, A., del Bo, C., and Nijkamp, P. (2009). Smart cities in europe. In *CERS’09, 3rd Central European Conference in Regional Science*, pages 45 – 59.

IBM (2011). Integrated fare management for transportation. Website. http://www.ibm.com/smarterplanet/us/en/traffic_congestion/nextsteps/solution/G080151O85496M88.html.

Juels, A. and Weis, S. A. (2006). Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137. http://eprint.iacr.org/.

Lee, S., Yoon, D., and Ghosh, A. (2008). Intelligent parking lot application using wireless sensor networks. In *Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on*.

Liander and AIM (2012). Amsterdam smart city. Website. http://www.amsterdamsmartcity.nl/#/en.

Ostojic, G., Stankovski, S., Lazarevic, M., and Jovanovic, V. (2007). Implementation of RFID technology in parking lot access control system. In *RFID Eurasia, 2007 1st Annual*, pages 1 –5.

Pérez-Martínez, P. A. and Solanas, A. (2011). w^3-privacy: the three dimensions of user privacy in LBS. In *MOBIHOC 2011, Twelfth ACM International Symposium on Mobile Adhoc Networking and Computing*. ACM SIGMOBILE.

Simon, D. R. (1995). Untraceable electronic cash. Patent US005768385A.

Trujillo-Rasua, R. and Solanas, A. (2011a). Efficient probabilistic communication protocol for the private identification of RFID tags by means of collaborative readers. *Computer Networks*, 55(15):3211–3223.

Trujillo-Rasua, R. and Solanas, A. (2011b). Scalable trajectory-based protocol for RFID tags identification. In *RFID-TA*, pages 279–285.

Trujillo-Rasua, R., Solanas, A., Pérez-Martínez, P. A., and Domingo-Ferrer, J. (2012). Predictive protocol for the scalable identification of RFID tags through collaborative readers. *Computers in Industry*, 63(6):557–573.