Keyless car sharing system: A security and privacy analysis

DOI:
10.1109/ISC2.2016.7580758

Document Version
Accepted author manuscript

Keyless Car Sharing System: A Security and Privacy Analysis

Iraklis Symeonidis(✉), Mustafa A. Mustafa, and Bart Preneel
KU Leuven, ESAT-COSIC and iMinds,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Email: {firstname.lastname}@esat.kuleuven.be

***Abstract*—This paper proposes a novel physical keyless car sharing system where users can use and share their cars without the need of physical keys. It also provides a comprehensive security and privacy analysis of such a system. It first presents a high-level model for a keyless car sharing system, describing its main entities and specifying the necessary functional requirements to allow users to share their cars (with other users) without exchanging physical keys. Based on this model and functional requirements, the paper presents a comprehensive threat analysis of the system. It focuses on the threats affecting the system's security and the users' privacy. This analysis results in a specification of an extensive set of security and privacy requirements for the system. This work can be used as a guide for a future keyless car sharing system design and as a mean to assess the security and privacy risks imposed on users by such systems.**

I. Introduction

Keyless car systems allow users to access (i.e., lock and unlock) and drive a car without the need of a physical key, as these keys can be replaced by access credentials on portable devices such as smartphones, or tablets. Keyless car sharing systems allow users to share digital car keys with other users such as family members, friends and acquaintances. The combination of car sharing systems and dynamic key distribution offers a high potential for smart cities.

Nowadays, the smart city concept has been gaining widespread attention as it would allow cities to manage their available resources and assets in a more effective, efficient and sustainable manner [1]. Managing efficiently the usage of transportation assets is one of the biggest challenges in modern cities. One way to address this challenge is to reduce the number of cars by better utilising the already available cars: note that the average time utilization of a car is 5%, which implies that on average 95% of the time cars are standing in a parking lot or garage. Encouraging users to share their cars with others can help to decrease the number of cars in cities. This could be achieved via car sharing systems. Such systems provide individuals with access to cars of other users. Users can reserve one of the available cars parked somewhere in the city and pay based on the time traveled and distance covered. In contrast to traditional car rental companies, car sharing systems can provide a relatively inexpensive alternative to users who occasionally need a car [2].

Appeared at IEEE International Smart Cities Conference (ISC2), 2016

Even if car sharing systems exist today, they are not flexible enough in terms of users' convenience. For example, if a car owner is willing to share her car, the user (or another designated person) has to hand over the physical keys to the user who wants to use the car. In some situations, handing a physical key may not even be possible.

To address the aforementioned issue, we propose a novel physical Keyless car Sharing System (KSS) which would allow car owners to generate digital keys for accessing their cars, and to share these keys with other users. It aims to eliminate the need for a physical key hand-over. However, such a KSS can introduce several privacy and security challenges. Currently, there is no prior work that analyses the security and privacy implications of physical Keyless car sharing systems. Additionally, there is no work that methodologically specifies the security and privacy requirements. The main contributions of this paper are the following:

- Firstly, we propose a novel high-level model for a KSS which allows a car owner to share her car by generating and distributing digital car keys to other users.
- Secondly, we define a threat model and perform a security and privacy threat analysis of the proposed KSS.
- Thirdly, based on this threat analysis, we specify the security and privacy requirements that need to be fulfilled, to allow owners to share their cars as well as users to book and use cars in a secure and privacy-preserving manner.

The remainder of this paper is organised as follows: Section II provides the background information and discusses the related work. Section III proposes a novel KSS. Section IV analyses the potential security threats and attacks on the proposed system. Section V specifies a set of security and privacy requirements. Section VI provides further discussions before concluding the paper in Section VII.

II. Background and Related Work

Weikl and Bogenberger [3] first analysed and evaluated different relocation algorithms for car sharing systems. They proposed a model for optimal vehicle positioning and relocation. Their model has an off-line and on-line demand module. The offline demand module calculates the optimal car pick-up location based on yearly data, whereas the on-line demand module performs the calculations several times per day based on real-time data. Shaheen and Cohen [4] provided a global perspective of markets and emerging trends in car

sharing services. They concluded that car sharing services are becoming popular and that they provide significant benefits for society such as reduced CO_2 emissions and fewer sold cars. Shaheen et al. [5] investigated personal car sharing systems and explored the business models, market opportunities and service barriers of such systems. They concluded that personal car sharing systems have the potential to impact the transportation sector and provide greater alternatives to vehicle ownership. They also pointed out that the most challenging issues such systems face are efficient key transfers between users and reliable reputation mechanisms to rate users. Shaheen and Chan [6] discussed the evolution and feasibility of electric vehicle in car sharing business models. Ferrero et al. [7], [8] reviewed different car sharing systems in terms of their business models and modes of operation. However, none of the above work has explored the idea of physical keyless car sharing systems.

Martínez-Ballesté et al. [9] introduced the concept of citizen privacy in smart cities by distinguishing the following five dimensions: identity privacy, query privacy, location privacy, footprint privacy and owner privacy. Li et al. [10] analysed the data over-collection by users' smartphones, and raised an alarm for the privacy implications on users. Pan et al. [11] analysed the smart city concept from a data mining point of view. They explored different methods for users' trace analysis (from location to behaviour inference) and emphasised the privacy risks of such analysis. Mustafa et al. [12] performed a security analysis on smart electric vehicle charging system that allows users to recharge their vehicle on other users' properties. However, no prior work has analysed the privacy implication of KSSs.

To fill this research gap, we propose a novel keyless car sharing system and perform an extensive security and privacy analysis of such a system.

III. Physical Keyless Sharing System (KSS)

This section details the system model, functional requirements and interactions among entities for a high-level model for a KSS.

A. High-Level Model for a KSS

Our high-level model for KSS consists of the following entities (see Fig. 1).

- *Users* are individuals, who are willing to share their cars (i.e., *owners*) or use cars which are available for sharing (i.e., *consumers*). Car owners can provide consumers such as family members, friends and acquaintances with permanent or temporary (on demand) access to their cars.
- *Keyless Sharing Management Server (KSMS)* is a server (or a complex of servers) that manages the entire KSS. It aims to provide 1) administrative support such as cars and users registration, 2) operational functionalities such as post/search of offers and requests, and car bookings, 3) key management such as generation, distribution, update and revocation of keys, and 4) car access management such as assign, update and revoke access rights for users to access and use cars.
- *Car manufacturer* is a company that manufactures cars and provides car owners with static physical and digital keys (bounded to the physical key) for their cars. It is also responsible for the generation, distribution and revocation of such keys.
- *Keyless Sharing On Board Unit (KS-OBU)* is an embedded or standalone hardware/software component that is part of the access management system of the car. It has a wireless interface such as WiFi, Bluetooth and LTE.
- *Keyless Sharing Application (KSApp)* is a software application developed for mobile devices. Users can interact with the KSMS via this application.
- *Portable Device (PD)* is any mobile device such as smartphone or tablet that can run the KSApp.
- *Authorities* are any governmental agencies that keep records of cars' and their owners' information such as car ownership, blacklists for stolen cars, cars' safety certificates and users' driving licence certificates.
- *Third Parties (TPs)* are any organisations, institutions or companies that might request data from the KSMS, such as insurance companies.

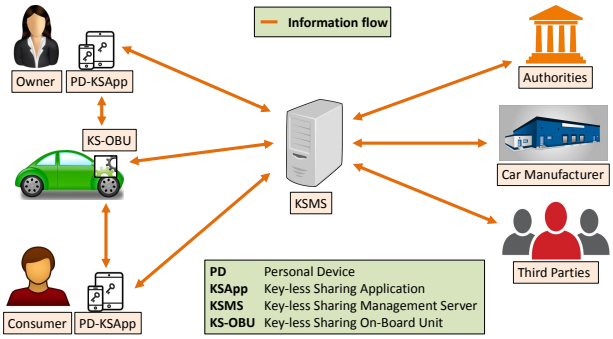

Fig. 1. The proposed physical Keyless car Sharing System (KSS).

B. Functional Requirements

In order to be acceptable to users, our proposed system should satisfy the following functional requirements.

- Users should be able to share their cars with other users. In detail, a car owner and a consumer should be able to:
  - create a profile (register),
  - update and withdraw her profile,
  - post car sharing offers and requests,
  - search for offers and requests,
  - accept or rejects requests,
  - use the KSApp on her PD to access a car,
  - pay (be paid) for using (sharing her) a car and
  - assign/receive reputation scores to/by other users.
- A car owner should be able to:
  - generate, update and revoke a temporary digital key to lock/unlock and drive her car,
  - distribute keys to the selected consumers,

  - retrieve the car's drop-off location, and
  - determine the car's location when the car is not returned and/or stolen.
- A consumer should be able to:
  - book a car,
  - receive a temporary digital key for the car, and
  - retrieve the pickup location of the car.
- The KSMS be should able to manage the following operations:
  - *Users' registration*: validate users' identity and driving licence.
  - *Car registration*: validate cars' profile information, ownership and safety conditions.
  - *Users' profile management*: manage users' profile access, search, update and withdraw.
  - *Operational management*: post and inquire car sharing offers, requests and bookings.
  - *Key management*: generate, distribute, update and revoke digital keys to the selected users.
  - *Access management*: assign, update and revoke access rights to the selected users.
- PDs should not perform computationally heavy operations as most PDs are resource-constrained devices.
- KS-OBUs should perform all the necessary operations to allow the selected users to access the reserved cars.

C. Interactions among Entities

The message types and interactions among the entities are described next.

1) System Setup: A KSS performs all the necessary steps in order to start offering the car sharing service in order to obtain the necessary cryptographic keys and certificates.

2) Initialisation Phase: takes place when a user enrolls.

- *Users' registration*. A user provides the KSMS with all the necessary information for the service registration such as an email address, a proof of her identity (e.g., passport, identity card), and her driving licence.
- *Car registration*. An owner provides the KSMS with all the necessary information for registering her car such as the type, model, colour, engine and certificates.

3) Pre-sharing Phase: takes place before a car is shared.

- *Users profile management*. A user may access, store, update or delete her profile information on the KSMS via the KSApp on her PD such as her username, age, contact details and friend circles.
- *Operational management*. Users may communicate with the KSMS to perform the following actions.
  - An owner (consumer) posts a car sharing offer (request) which includes: her profile data, her (preferred) car's profile data, her (preferred) car's pickup and drop-off location, the car's availability (preferred) period and the asking (offering) price.
  - Users send inquiries to the KSMS for the available offers or requests. These inquiries contain the same information as users' offers or requests.
  - If a user is interested in booking a car, the following operations are performed: (i) a consumer submits a request to book the car, (ii) the owner receives one or more requests for the car and (iii) the owner accepts one of the requests and notifies the selected consumer or rejects all of the requests.
- *Key and access management*. The owner generates and distributes temporary digital keys and assigns access rights for the car to the selected consumers. Additionally, the car owner can update and revoke on demand the keys and privileges for the "misbehaving" consumers. These actions could be performed with the assistance of the KSMS.

4) Car-sharing Phase: takes place while a car is shared.

- *Accessing the car*. The selected consumer uses the received key to access the car via the KSApp on her PD.
- *Using the car*. The car's KS-OBU monitors whether the car follows the agreed car sharing conditions such as duration, distance and region of traveling.
- *Returning the car*. The car's KS-OBU and/or the consumer via her PD-KSApp, notifies the owner and the KSMS for the time and drop-off location of the car.

5) Post-sharing Phase: takes place after a car is shared.

- *Billing*. The consumer pays the owner the agreed fee for using the car with the assistance of the KSMS.
- *Reputation scores management*. The car's owner (consumer) assigns/receives a reputation score for sharing (using) a car with the assistance of the KSMS.

IV. Threat Analysis

This section describes the threat model in detail for each of the KSS entities and provides an extensive analysis of the security and privacy threats to the proposed KSS model.

A. Threat Model

Users are untrustworthy or even malicious. A malicious user might try to passively and/or actively collect and alter the information stored and exchanged within the KSS in an attempt to lower the credibility of the system. For instance, she might try to manipulate the car's availability period, car's profile information (e.g., type, and the number of seats) and location, in an attempt to gain financial advantages and/or extract information about other users of a KSS. Such a malicious user can be a script kiddie, a motivated adversary, or even a governmental agency. Depending on the resources and capabilities, a malicious user might try to corrupt a fixed set of users or either any user of the KSS. However, we assume that an adversary cannot break the underlying cryptographic primitives.

KS-OBU is untrustworthy but tamper-evident. An adversary through the car's KS-OBU might try to infringe the users' privacy by means of collecting the passengers' personal data during a vehicle's operation such as car's location and passengers' behaviour [13]. However, we assume that KS-OBU is equipped with hardware and software security mechanisms

such as the Trusted Platform Module (TPM) [14], [15] to safely store cryptographic keys, perform cryptographic operations and validate software updates [14]. Moreover, a KS-OBU needs to be tamper-evident to detect and keep irrefutable evidence when an adversary attempts to break or alter the hardware and software components of the device. We also assume that the KSMS and the car manufacturers patch software bugs [16], [17] regularly in order to preclude intrusive attacks [18], [19] which could make KS-OBUs hazardous to passengers life [20].

PD-KSApp are untrustworthy but tamper-evident. We assume that PD-KSApp is equipped with security mechanisms to provide access control and protection against data breaches and/or malware. For instance, a PD-KSApp should be equipped with a credential management mechanisms [21] on the mobile device which can encrypt and store users' private keys, passwords and certificates. The PD-KSApp should also be tamper-evident. Moreover, we assume that only the legitimate user of a PD-KSApp can access the KSS through the device using authentication mechanisms. However, an adversary might try to disturb the KSS functionality by sending invalid requests, or executing only a fraction of the KSS operations [22].

KSMS and car manufacturer are honest-but-curious or even semi-honest. Both the KSMS and the car manufacturer might try to learn and extract information about the KSS users such as booking preferences of a user, with whom a car owner is sharing her car with, and with which frequency. However, we assume that is not in their interest to alter the messages exchanged and to disrupt the protocol operations of a KSS. Moreover, the car company and/or the KSMS may try to disturb the KSS functionality by executing only a fraction of the KSS operations honestly.

Authorities, third parties and external entities are untrustworthy or even malicious. They may try to eavesdrop and collect information exchanged withing the KSS. Their aim might be to gain access, collect and/or modify information exchanged within a KSS, in an attempt to disrupt, and extract information for users and the KSS. An adversary can be sophisticated hackers, organized crime or even governmental agencies that might be capable of taking control of a fixed set of users or any user of a KSS. However, we assume that such adversaries are not yet able to break the underlying cryptographic primitives.

B. Security and Privacy Threat analysis

This section analyses the possible threats for a KSS. The threat analysis is based on two well-known frameworks: STRIDE [23]–[25] and LINDDUN [26]. STRIDE mainly covers the security threats, whereas LINDDUN focuses on privacy threats. Both of the frameworks are heavily used by the industry and the research community.

Security Threats

Spoofing. An adversary may attempt to illegally access a legitimate KSS entity such as a user's PD-KSApp or the KSMS. Spoofing attacks introduce functional and trust related issues, and may have an economic impact to the KSS. For instance, an adversary may raise the chances of a booking request to be accepted by impersonating a trusted (for the car owner) user such as a family member, or a close friend. Regarding the economic implications, an adversary may attempt to benefit from (i) eliminating other car sharing offers, thus making available only a selected offer, and (ii) making an impersonated profile to pay for the car she booked and used. Therefore, it is important to have thorough user registration procedures and strong entity authentication.

Tampering with data. An adversary may attempt to modify the information stored and exchanged within the KSS such as manipulating the car's availability period, car's profile information (type, number of seats) and location. By stating inaccurate information, an adversary may attempt to lower the credibility of users or the KSMS. For instance, a user may try to modify the car's KS-OBU information for her own benefit; to alter the travel duration and distance affecting the sharing cost. Therefore, the integrity and authenticity of the messages should be guaranteed.

Information disclosure. An adversary may attempt to eavesdrop messages sent through the KSS. By eavesdropping messages exchanged among the KSMS, the users' PD-KSApps, and the cars' KS-OBUs, an adversary may attempt to retrieve critical information about the system such as the digital keys to access a car, the booking details and the location of a car. For instance, by collecting such information, an adversary may aim to reuse the valid messages and the digital keys she obtained to access a car without the need to prove that she is a legitimate user. Hence, confidentiality of information must be guaranteed. Information disclosure also constitutes a privacy threat to users posing additional risks, such as user profiling.

Repudiation. Disputes may arise when entities (do not) perform an action and claim the opposite such as stating inaccurate information about the travelled period and location of the car. Hence, the non-repudiation of messages exchanged and actions performed must be guaranteed and disputes must be consistently resolved.

Denial-of-Service (DoS). DoS attacks aim to make the car sharing services inaccessible to on or more users. For the KSS, an adversary may target the KSMS, the cars' KS-OBUs, and the users' PD-KSApps in an attempt to make any KSS operation unavailable to its users such as post offers/requests, bookings, and generating, distributing and revoking access car keys. Moreover, an adversary may attempt to perform a spear attack targeting specific users. For instance, an adversary may attempt to raise the likelihood of her offer(s) to be selected by blocking offers from other users. Therefore, the KSMS should be safeguarded by network security tools. Furthermore, users' PD-KSApps and cars' KS-OBUs should be protected from malware using software security tools.

Elevation of privilege. An adversary may attempt to gain elevated access to the resources of the KSS. For instance, an elevated access can imply that an adversary may attempt to elevate her profile privileges from (i) consumer to car owner

gaining unlimited access to a car, and (ii) from passenger to car driver. Moreover, an escalated privilege at KSMS incurs that an adversary may attempt to execute operations as a system administrator aiming to retrieve users' information, alter car sharing offers/requests and bookings. Thus, to mitigate privilege escalation attacks, authorization mechanisms that comply with the principle of least privilege for users' accounts and processes should be deployed.

Privacy Threats

Linkability. An adversary may attempt to distinguish whether two or more Items of Interest (IOI) such as messages, actions and subjects are related to the same user. For instance, an adversary may try to correlate and deduce whether a user posted a car sharing request, booked a car, and drove to a particular location. Hence, unlikability among IOIs must be guaranteed.

Identifiability. An adversary may attempt to correlate and identify a user from messages exchanged and actions performed. For instance, an adversary may try to identify a user by analysing the messages the user exchanges with the KS-OBU, KSMS and PD-KSApp to access a car. Thus, the anonymity and pseudonymity of users must be preserved.

Non-repudiation. In contrast to security, non-repudiation can be used against users' privacy. An adversary may attempt to collect evidence stored and exchanged through the KSMS and the car's KS-OBU to deduce information about a user. It may, for example, deduce whether a user drove to a particular location (clinic). Hence, plausible deniability over non-repudiation must be guaranteed.

Detectability. An adversary may try to distinguish the type of IOIs such as messages exchanged among the KSS entities from random noise. For instance, an adversary may attempt to identify when a user's PD-KSApp communicates with a KSMS and the car's KS-OBU. Thus, undetectability and unobservability of IOIs must be guaranteed.

Information disclosure. An adversary may attempt to eavesdrop and passively collect information exchanged within the KSS. Information disclosure may affect not only the system's security but also users' privacy such as the profiling of users. For instance, an adversary may attempt to learn the location and availability of a car, whether a user is absent from home and with whom a user is traveling with. Moreover, the user's behaviour may be inferred by a systematic collection of the user's information [13] by an adversary. For instance, an adversary may infer the (i) car owners' sharing preferences by collecting information about their sharing patterns such as rental time, duration, and car location, (ii) consumers' free time activities by analysing the history of pickup, drop-off, and drive locations, and (iii) circles of trust by analysing with whom, when and how often they share their cars, such as family members, friends and acquaintances. An adversary may even attempt to infer sensitive information about users such as their health condition, by identifying users who use cars for handicap people, or regular visits to hospitals and clinics. Profiling constitutes a high risk for users' privacy. Therefore, the confidentiality of information must be guaranteed.

Content Unawareness. A misbehaving KSS may attempt to collect more information than necessary from users aiming to use such information for unauthorised purposes such as advertisement. For instance, the KSMS may only need to know whether a user is eligible to drive a car without necessarily the need to collect personal information about a user such as her birthday, gender and the country that issued the user's driving licence. Moreover, the car's KS-OBU should only collect the consumers' location when necessary such as when a car is not returned on time or it exceeds the geographical restrictions agreed during the booking. Hence, the content awareness of users must be guaranteed.

Policy and Consent Noncompliance. A misbehaving KSS may attempt to collect, store, and process users' personal information in contrast to the principles described in the European General Data Protection Regulation 2016/680 [27]. For instance, a misbehaving KSMS may attempt to (i) collect sensitive information about users such as sexual orientation, religion and political opinions, (ii) export users' information to data brokers for revenue, (iii) read users' contacts from their PDs, and their Online Social Network profiles on e.g. Facebook or Google+, and (iv) not allow users to opt out from the KSS service. A misbehaving KSS may also attempt not to comply with the Privacy policy that it advertises [28]. Thus, privacy policies and consent compliance should be guaranteed.

V. Security and Privacy Requirements

Based on the threat analysis, this section specifies a set of security and privacy requirements for the proposed KSS.

A. Security Requirements

To mitigate the aforementioned security threats, security requirements needs to be put in place aiming to safeguard and protect the messages exchanges, actions performed and information stored within the KSS.

Entity Authentication assures to an entity that the identity of a second entity is the one that is claiming to be. It aims to mitigate spoofing attacks. Entity authentication is achieved when a user proves that she (i) knows something such as passwords, PIN and passcode, (ii) possesses something such as token, ticket and specific device, (iii) has specific properties (i.e. use of biometrics), or (iv) with a combination of these. Regarding passwords, it is important for the KSS to support strong password policies, and that passwords are sent encrypted and always stored as salted hashes within the KSS databases.

Integrity ensures that the information stored and exchanged within the KSS have not been altered. It aims to mitigate tampering with data attacks. Integrity is achieved with the use of hash functions, MAC algorithms and digital signatures.

Confidentiality ensures that only the intended users will be able to read the information stored and transferred within the KSS. It aims to mitigate information disclosure attacks. For instance, confidentiality of the exchanged information needs

to be provided while (i) a user's PD-KSApp communicates with a car's KS-OBU and the KSMS, and (ii) the KSMS communicates with a car's KS-OBU. Confidentiality can be achieved with the use of encryption schemes such as symmetric, asymmetric and homomorphic encryption schemes. Confidentiality can also be combined with message authentication when authenticated encryption is used.

Non-repudiation is achieved when an entity cannot deny her action or transaction such as post an offer, book a car and drive to a particular location. It aims to mitigate repudiation attacks (disputes). Non-repudiation can be achieved with the use of digital signatures, timestamps and audit trails.

Availability ensures that the resources of the KSS are available to legitimate users. It aims to mitigate DoS attacks. To safeguard availability, network tools are necessary to be put in place such as firewalls, Intrusion Detection Systems and Intrusion Prevention Systems. To protect the users' PD-KSApp and cars' KS-OBU from malware, software security tools are necessary such as anti-virus and anti-bot tools.

Authorisation ensures that an entity has access rights to read, write, and execute resources of the KSS such as files and operations. It aims to mitigate elevation of privilege attacks. For authorisation, access control mechanisms need to be used such as Access Control Lists, and Role Based Access Control. Moreover, the access control policies should follow the principle of least privilege for user accounts and processes.

B. Privacy Requirements

To mitigate the specified privacy threats, Privacy Enhancing Technologies (PETs) need to be put in place aiming to safeguard and protect users' personal data which will be exchanged, processed and stored within the KSS.

Unlinkability ensures that two or more IOIs such as messages exchanged and actions performed cannot be linked to the same user [29]. It aims to mitigate linkability attacks. Unlinkability can be achieved with the use of pseudonyms [30], anonymous credentials [31] and private information retrieval [32].

Anonymity ensures that messages exchanged and actions performed can not be correlated to a user's identity. It aims to mitigate identifiability attacks. Anonymity can be achieved using Mix-nets [33] and multi-party computation [34].

Pseudonymity ensures that a pseudonym is used instead of a user's real identity within the KSS. As anonymity, it aims to mitigate identifiability attacks. Pseudonymity can be achieved by using random generators to generate unique and highly random pseudonyms.

Plausible deniability over non-repudiation ensures that an adversary cannot prove that a user has performed a specific action and operation such as drove to a particular location, or booked a car for a selected period. It aims to mitigate non-repudiation privacy threats. Plausible deniability, unlike non-repudiation, is achieved with the use of off-the-record messaging [35]. However, we have to stress that non-repudiation service should be provided when necessary such as when more than one entities agreed to trace and identify an action performed, or a message sent.

Undetectability and unobservability ensures that messages exchanged and actions performed cannot be distinguished from others by an adversary as the adversary observes only noise. It aims to mitigate detectability attacks. Undetectability and unobservability can be achieved with the use of Mix-nets and dummy traffic [33].

Confidentiality apart from security is also an important privacy requirement. It can be achieved using multi-party computation and private information searches.

Content Awareness aims to raise users' awareness by better informing them of the amount and the quality of information they submit within the KSS. It aims to mitigate the content unawareness privacy threats. Content awareness can be achieved with the use of Transparency Enhancing Technologies such as privacy nudges [36], dashboards [37], [38] and privacy risk metrics [39].

Policy and consent compliance aims to ensure the compliance of the KSS with the existing privacy legislations such as the European General Data Protection Regulation 2016/680 [27] before users accessing the system. It aims to mitigate the Policy and consent non-compliance privacy threats. Policy and consent compliance can be achieved with the use of Data Protection Impact Assessments [40] and Privacy Impact Assessments [41] analysis of the system such as data flows, data stores, and processes by data controller bodies.

VI. Further Discussions

Although a KSS may provide benefits for users, it also introduces several security and privacy issues. Concerning the security issues, the most challenging task is the key management such as generation, distribution and revocation of temporary digital keys to a car. The desired property for this task should be that the temporary keys are user-car-period specific, i.e., these keys should be valid only for (i) the selected users (owner and consumers), (ii) the selected car, and (iii) the agreed period for sharing the car. Most of the threats can be mitigated by using well-known techniques such as end-to-end encryption, MAC algorithms and digital signatures. Moreover, it is important to make this task multi-party dependent. The owner, consumers, the car and the KSMS should all be involved in the generation and distribution process of these keys. Thus, any single party should not be able to generate the access keys and abuse the system. Multiparty computation and homomorphic encryption could be used to achieve these properties. However, developers should take into account the communication and computational costs of these mechanisms.

Regarding the privacy issues, protecting users' privacy against authorised insiders such as the KSMS is probably the most challenging task. A curious KSMS may be able to infer personal data about users by analysing (i) consumers' booking history such as type of cars, manufacturers and engine power, (ii) owners' sharing history such as the rental time, duration and car location history, and (iii) user friends circles of trust by analysing how often and with whom an owner (consumer) share (use) a car such as to (with) family members, friends and

acquaintances. These privacy concerns call for PETs solutions to be used in the KSS. An example of cost effective and commonly used PETS are pseudonyms and anonymity systems (e.g., Tor).

However, a KSS should be able to perform the necessary operations aiming to provide users with a "good" service. Therefore, to satisfy all the requirements specified, the protocol designers should find the "right" balance between the system's security and users' privacy in combination with the KSS functionality.

VII. Conclusion and Future work

In this paper, we presented a novel keyless car sharing system that allows users to share their cars with others more conveniently. First, we devised a high-level model of our system and described the possible functional requirements and interactions among system entities. Based on this model and taking the STRIDE and LINDDUN frameworks as a reference, we performed a comprehensive threat analysis. Finally, to mitigate the identified threats, we specified a set of security and privacy requirements for such systems. These requirements can be used as a guide (i) to design secure and privacy-preserving protocols that support keyless car sharing systems, and (ii) to perform a risk/threat assessment of protocols that supports such systems. As a future work, we plan to design a protocol satisfying all the requirements specified.

Acknowledgment

We would like to thank the privacy group members of COSIC who helped us shape the idea. This work was supported in part by the Research Council KU Leuven (C16/15/058).

References

[1] M. R. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris, "Smarter cities and their innovation challenges," *IEEE Computer*, vol. 44, no. 6, pp. 32–39, 2011.

[2] M. Duncan, "The cost saving potential of carsharing in a US context," *Transportation*, vol. 38, no. 2, pp. 363–382, 2011.

[3] S. Weikl and K. Bogenberger, "Relocation strategies and algorithms for free-floating car sharing systems," *IEEE Intell. Transport. Syst. Mag.*, vol. 5, no. 4, pp. 100–111, 2013.

[4] S. A. Shaheen and A. P. Cohen, "Carsharing and personal vehicle services: worldwide market developments and emerging trends," *Int. Journal of Sustainable Transportation*, vol. 7, no. 1, pp. 5–34, 2013.

[5] S. A. Shaheen, M. A. Mallery, and K. J. Kingsley, "Personal vehicle sharing services in north america," *Research in Transportation Business & Management*, vol. 3, pp. 71–81, 2012.

[6] S. A. Shaheen and N. D. Chan, *Electric Vehicle Business Models: Global Perspectives*. Springer International Publishing, 2015, ch. Evolution of E-Mobility in Carsharing Business Models, pp. 169–178.

[7] F. Ferrero, G. Perboli, A. Vesco, V. Caiati, and L. Gobbato, "Car-sharing services–part a taxonomy and annotated review," Tech. Rep., 2015.

[8] F. Ferrero, G. Perboli, A. Vesco, S. Musso, and A. Pacifici, "Car-sharing services–part b business and service models," Tech. Rep., 2015.

[9] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 136–141, June 2013.

[10] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1339–1350, May 2016.

[11] G. Pan, G. Qi, W. Zhang, S. Li, Z. Wu, and L. T. Yang, "Trace analysis and mining for smart cities: issues, methods, and applications," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 120–126, June 2013.

[12] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Smart electric vehicle charging: Security analysis," in *IEEE ISGT*, Feb 2013, pp. 1–6.

[13] Uber. New App Features and Data Show How Uber Can Improve Safety on the Road. Accessed July, 2016. [Online]. Available: https://newsroom.uber.com/safety-on-the-road-july-2016/

[14] J. Noorman, P. Agten, W. Daniels, R. Strackx, A. V. Herrewege, C. Huygens, B. Preneel, I. Verbauwhede, and F. Piessens, "Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *USENIX, Washington, DC, USA, August 14-16, 2013*, 2013, pp. 479–494.

[15] Trusted Computing Group. TPM 2.0 Library Profile for Automotive-Thin. Accessed June, 2016. [Online]. Available: http://tinyurl.com/jrklfqj

[16] Tesla. Bugcrowd. Accessed June, 2016. [Online]. Available: https://bugcrowd.com/tesla

[17] K. Mahaffey. The new assembly line: 3 best practices for building (secure) connected cars. Accessed June, 2016. [Online]. Available: http://tinyurl.com/omgkvkc

[18] DEF CON 2013. How to Hack a Tesla Model S. Accessed June, 2016. [Online]. Available: http://tinyurl.com/ovve3wq

[19] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, 2014.

[20] Tesla. Blog. Accessed June, 2016. [Online]. Available: https://www.teslamotors.com/blog/tragic-loss

[21] L. J. Janczewski, H. B. Wolfe, and S. Shenoi, Eds., *Security and Privacy Protection in Information Processing Systems, IFIP SEC, Auckland, New Zealand, July 8-10, 2013*.

[22] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in *IEEE ICC, Ottawa, ON, Canada, June 10-15, 2012*, 2012, pp. 917–922.

[23] M. Howard and S. Lipner, *The security development lifecycle*. O'Reilly Media, Incorporated, 2009.

[24] OWASP. Application Threat Modeling. Accessed May, 2016. [Online]. Available: http://tinyurl.com/zrt2j9l

[25] Microsoft. Improving web application security: threats and countermeasures. Accessed May, 2016. [Online]. Available: http://tinyurl.com/zewb9nz

[26] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, 2011.

[27] Regulation 2016/680 of the European Parliament and of the Council. http://tinyurl.com/h76amd8. Accessed July, 2016.

[28] I. Symeonidis, P. Tsormpatzoudi, and B. Preneel, "Collateral damage of Online Social Network Applications," in *ICISSP*, 2016, pp. 1–8.

[29] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (v0.34). tech. rep." pp. 1–98, 2010.

[30] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *IEEE SmartGridComm*, Nov 2014, pp. 939–945.

[31] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *CRYPTO*, 2004, pp. 56–72.

[32] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of the ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[33] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Com. of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[34] A. C. Yao, "Protocols for secure computations," in *Foundations of Comp. Science*. IEEE, 1982, pp. 160–164.

[35] N. Borisov, I. Goldberg, and E. Brewer, "Off-the-record communication, or, why not to use pgp," in *ACM workshop on Privacy in the electronic society*. ACM, 2004, pp. 77–84.

[36] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor, "Privacy nudges for social media: an exploratory facebook study," in *IW3C2*, 2013, pp. 763–770.

[37] I. Symeonidis, F. Shirazi, G. Biczok, C. Perez-Sola, and B. Preneel, "Collateral damage of facebook apps: Friends, providers, and privacy interdependence," in *IFIP SEC*, vol. 31. LNCS, 2016, pp. 1–14.

[38] M. Nebel, J. Buchmann, A. Ronagel, F. Shirazi, H. Simo, and M. Waidner, "Personal information dashboard: Putting the individual back in control," *Digital Enlightenment*, 2013.

[39] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," in *ICDM '09*, ser. ICDM '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 288–297.

[40] E. Commission. Test phase of the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems. Accessed May, 2016. [Online]. Available: http://tinyurl.com/j7xro7f
[41] D. Wright and P. De Hert, *Privacy impact assessment*. Springer Science & Business Media, 2011, vol. 6.