Pervasive and Mobile Computing 14 (2014) 71–82

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Towards privacy-driven design of a dynamic carpooling system

Jesús Friginal [a,b,*], Sébastien Gambs [d], Jérémie Guiochet [a,c], Marc-Olivier Killijian [a,b]

[a] CNRS, LAAS, 7 Avenue du Colonel Roche, F-31400 Toulouse, France
[b] Univ de Toulouse, LAAS, F-31400 Toulouse, France
[c] Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France
[d] Université de Rennes 1, Avenue du Général Leclerc 35042 Rennes Cedex, France

ARTICLE INFO

Article history:
Available online 4 June 2014

Keywords:
Carpooling
Privacy
Mobility
Location-based systems

ABSTRACT

Dynamic carpooling (also known as instant or ad-hoc ridesharing) is a service that arranges one-time shared rides on very short notice. This type of carpooling generally makes use of three recent technological advances: (i) navigation devices to determine a driver's route and arrange the shared ride; (ii) smartphones for a traveller to request a ride from wherever she happens to be; and (iii) social networks to establish trust between drivers and passengers. However, the mobiquitous environment in which dynamic carpooling is expected to operate raises several privacy issues. Among all the personal identifiable information, learning the location of an individual is one of the greatest threats against her privacy. For instance, the spatio-temporal data of an individual can be used to infer the location of her home and workplace, to trace her movements and habits, to learn information about her centre of interests or even to detect a change from her usual behaviour. Therefore, preserving location privacy is a major issue to be able to leverage the possibilities offered by dynamic carpooling. In this paper we use the principles of privacy-by-design to integrate the privacy aspect in the design of dynamic carpooling, henceforth increasing its public (and political) acceptability and trust.

1. Introduction

The automotive and transport sector presents an enormous potential for the exploitation of mobiquitous systems, as seen for example in the research around Vehicular Ad-Hoc Networks (VANETS) [1]. According to recent studies [2], this sector is expected to generate business opportunities of $202 billion until 2020. In this context, the industry is already fostering novel and innovative transports modes that improve comfort and efficiency.

Carpooling, also known as ridesharing, is a solution that could enable private cars to become part of the public transportation system, thus benefiting both users and environment [3]. Passengers benefit by having an alternative when their usual transportation mode is unavailable, and by possibly eliminating the need for an additional car for occasional use. Drivers benefit by having someone to share the cost of the trip or to gain enough passengers to qualify for high occupancy

[*] Corresponding author at: CNRS, LAAS, 7 Avenue du Colonel Roche, F-31400 Toulouse, France. Tel.: +34 96 3877007.
E-mail addresses: jefrilo@gmail.com, jesus.friginal@laas.fr (J. Friginal), sebastien.gambs@irisa.fr (S. Gambs), jeremie.guiochet@laas.fr (J. Guiochet), marco.killijian@laas.fr (M.-O. Killijian).

http://dx.doi.org/10.1016/j.pmcj.2014.05.009
1574-1192/© 2014 Elsevier B.V. All rights reserved.

vehicle lanes. Finally, the environment benefits from a reduction of greenhouse gases emissions. Although different implementations can be found,[1] carpooling is typically characterised by four stages: a system registration where some personal information is required, (ii) a negotiation where users finally agree sharing the same car for a determined itinerary, (iii) the trip execution, and (iv) the assessment of the carpooling experience. While first commercial carpooling solutions are already a reality on the Internet, there are privacy aspects that affect the trust of users, consequently limiting their definitive takeoff.

Privacy, defined as the state or condition of being free from being observed or disturbed by other people [4], has become a real concern of users in the last years. Indeed, after the several espionage incidents involving the National Security Agency (NSA) [5], users have started to gain awareness of the importance of their *privacy assets*, that is, the sensible information related to their daily lives. Carpooling systems are not alien to this mistrust. So, their successful exploitation will depend on the ability of system providers to offer not only functionally appealing but also trustworthy and privacy-aware carpooling solutions.

To date, carpooling systems present two main characteristics:

- Static nature: trips are scheduled several days in advance, but no interaction between users (such as picking up a new passenger on the fly) is possible once the trip has started.
- Centralised infrastructure: applications rely on fixed pre-established Trusted Third Parties (TTP) in charge of collecting and storing sensitive information from carpooling users (such as their identity, location, and usual trips).

Although the static nature of carpooling remains effective, it does not allow the continuous interaction between users. Conversely, a dynamic approach would offer passengers a more flexible ride in just a few minutes. However dynamic carpooling presents a problem of privacy, as it implies a major data exchange between the driver and the passenger. This increases the risk that attackers may infer private information from both participants.

Regarding the second characteristic, TTPs act as guarantors for trust between users. Despite that, the security of carpooling systems may be compromised by those attackers that are able to gain access to centralised TTPs [6]. The adoption of a distributed architecture would make more difficult for an attacker to find the information about users, as it would be scattered around the network. However, the development of distributed TTPs architectures is still a challenging problem that limit the trust of users.

The goal of this paper is to promote the concept of a dynamic and distributed carpooling system, taking into account the non-functional requirements of privacy and trust. In consequence, this paper focuses on answering these challenging questions: (i) what is the critical information required by dynamic carpooling systems to work, (ii) how to exchange such information between drivers and passengers in an infrastructureless context while offering them trust in the information and the service they receive? and (iii) how to protect the privacy of carpooling users from potential attackers? By addressing such issues, this paper aims at integrating the principles of the privacy-by-design [7] for dynamic carpooling systems.

The rest of this paper is structured as follows: Section 2 presents current challenges in dynamic carpooling systems, highlighting the importance of privacy. Section 3 identifies the most important privacy assets from the viewpoint of users as well as the security and privacy properties that need to be addressed to protect them. Section 4 identifies the most important functional entities of dynamic carpooling and how they relate to one another. Then, Section 5 proposes the mechanisms to protect the system from a privacy viewpoint. Section 6 discusses the need of covering the gap between design and final prototypes. Finally, Section 7 concludes the paper.

2. Challenges of dynamic carpooling

Carpooling was early introduced in 1970s, but it is in the last 5 years that it has gained momentum in our society, especially in countries with high population density. For example, recent studies carried out in China [8]state the increasing interest of society in carpooling solutions, highlighting the cost saving and congestion reduction as the most important benefits. However, to address its dynamic decentralised deployment it is necessary to face some issues. The AMORES project[2] [9] is an initiative that addresses the challenges of dynamic carpooling from a cooperative and distributed way. In overall, they involve improving the performance and the comfort of the carpooling experience while protecting the user privacy.

2.1. Scheduling the meeting point

One of the main bottlenecks of carpooling is scheduling the meeting point. In traditional carpooling this decision is taken jointly between the driver and the passenger days before the trip. However, in practice, the system does not provide effective mechanisms to warn users about delays. This problem, identified as complex for carpooling [8], has been explored in European projects such as Eureka-Celtic WiSafeCar[3] from a dynamic perspective. This project focused on studying the

[1] http://www.carpooling.com, http://www.blablacar.com.

[2] http://projects.laas.fr/AMORES.

[3] http://wisafecar.gforge.uni.lu.