Chapter XXXVII
Location Privacy in Automotive Telematics

Muhammad Usman Iqbal
University of New South Wales, Australia

Samsung Lim
University of New South Wales, Australia

ABSTRACT

Over the past few decades, the technologies of mobile communication, positioning, and computing have gradually converged. The automobile has been a natural platform for this convergence where satellite-based positioning, wireless communication and on-board computing work in tandem offering various services to motorists. While there are many opportunities with these novel services, significant risks to the location privacy of motorists also exist as a result of the fast-paced technological evolution. These risks must be confronted if trust and confidence are to prevail between motorists and service providers. This chapter provides an overview of the current situation of location privacy in automotive telematics by exploring possible abuses and existing approaches to curb these abuses followed by a discussion of possible privacy-strengthening measures.

INTRODUCTION

The proliferation of location-aware computing devices promises an array of "quality-of-life enhancing" applications. These services include in-car navigation, roadside assistance, infotainment, emergency response services, vehicle diagnostics and prognostics. The key idea is to provide services using "location" as a geographic filter. These services can be triggered by an event, for example, the location of the vehicle can be transmitted to an emergency response center on deployment of air bags. Some services can be explicitly requested by the driver, for example, in-car navigation or road side assistance. While other applications can be quietly running at all times, passing on real-time information of the vehicle's movements such as Global Positioning System (GPS) enabled Pay-As-You-Drive (PAYD) insurance (Grush, 2005).

Although location data is critical to the operation of such applications, there is a precarious balance between the necessary dissemination of location information and the potential for abuse of this private information. Spatio-temporal (location in time) information continuously monitored (and logged) about the places a person visits can reveal a lot about one's persona. Given the current capabilities of inference by combining disparate sources of information, a lot can be inferred about an individual. These derived profiles can then be used to make judgments about a person or used for unsolicited marketing by location-based marketers. Orwell (1949), in his criticism against totalitarianism, would have most likely referred to these "Small Brothers" (location-based retail marketers) had he known about these inference attacks.

In the next few sections a background on location privacy is presented, some possible privacy abuses of telematics services are discussed, and existing approaches to curb these abuses are investigated. The chapter then suggests possible measures to strengthen location privacy.

BACKGROUND

Before delving into the core issue of location privacy, it is important to agree on a definition of privacy itself. Much of the literature pertaining to privacy refers to Westin's precise definition. In the context of telematics, location privacy is a special case of privacy, relating to the privacy of location information of the vehicle, and ultimately the user of the vehicle.

Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others. (Westin, 1967)

How Positioning Systems can be Privacy Invasive?

Positioning systems can be categorized into either being 'Self-positioning' or 'Remote-positioning'. In Self-positioning systems, the vehicle is either fitted with a GPS receiver or Dead-Reckoning system (based on one or more gyroscopes, a compass and odometer) to locate where it is on the road. Remote-positioning systems require a central site to determine the location of the vehicle (Drane and Rizos, 1997). The result is a set of coordinates (or position) of the vehicle expressed in relation to a reference frame or datum. Self-positioning systems inherently protect location privacy because they do not report the location of the vehicle to any other system. On the other hand, remote-positioning systems track, compute and retain the location information at the central monitoring site and creates a risk to the individual's privacy. Self-positioning systems also pose a privacy risk if they report the vehicle's