Security on Wheels: Security and Privacy for Vehicular Communication Systems

Tutorial

Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
www.ee.kth.se/nss

ABSTRACT

There is already a significant body of work on security and privacy for vehicular communication systems and the conditions for deploying the technology are maturing. This tutorial provides a crystalized and easily accessible view of the state of the art.

Keywords

Security; privacy; vehicular networks

1. INTRODUCTION

Modern cars are already equipped with many on-board sensors and computers (micro-controllers), navigation systems, multiple user interfaces, and short-range wire replacements (e.g., Bluetooth). More recently, wireless communication devices (cellular and Wi-Fi) have been integrated enabling new user services enabled (e.g., car manufacturers announcing top-tier "connected" models). At the same time, intelligent transportation systems have been evolving, with roadside sensors now deployed in new highways and in urban settings (e.g., through smart-city initiatives). Meanwhile, the industry and authorities have substantiated, over the past few years, significant interest in car-to-car communications. This is a leap forward, with lots of research already done in academia and in industry: additional on-board computing and communication capabilities will connect vehicles to each other, to road-side infrastructure, and to back-end servers, enhancing in new ways transportation safety and transportation efficiency and catering to users (driver and passenger needs). In fact, vehicles will be central in a more complex landscape that includes intelligent transportation, location based services, novel applications (e.g., urban sensing) and, eventually, automation of transportation. Concerned primarily with vehicular communications and the related platforms, technologies, and standards, we term these vehicular communication (VC) systems.

While developing VC systems, academia, industry, including standardization and harmonization working groups, and authorities, came to clearly understand that VC systems couldn't be deployed without securing them and without safeguarding the privacy of their users (drivers and passengers). If we did, VC systems and their users would be exposed to all kinds of attacks, ranging from "innocent" hacks and modifications to full-fledged adversarial behavior. This would lead to abuse, disruptions and even significant damages. This is not simply a prediction: there have been already attacks demonstrated on currently available connected vehicles (e.g., disabling the driver's control, remotely unlocking them, or installing fraudulent software). As the VC sophistication and penetration increases, the stakes will only get higher. This is also true in terms of privacy: we would not want VC systems constantly giving away our whereabouts and identity, through our activities and transactions, without our agreement.

The way forward is clear: only with strong security and privacy protection we will be able to reap the benefits of VC systems. There has been a multitude of efforts (academia, industry) with a large number of proposals. Although there is convergence on some basic matters, it is often the case that the community has built on diverse assumptions and then designed mechanisms with differing characteristics and reaching conclusions that may even be contradictory. At the same time, the problem at hand is multifaceted, VC systems are being concretized in field operational tests, and there is increasing 'pressure' to roll out their next versions.

2. TUTORIAL OUTLINE

This tutorial is concerned with the design of appropriate security and privacy mechanisms and their integration with VC functionality, especially in the light of strict requirements of VC-enabled safety applications. We consider architectural issues, a wide range of protocols, their analysis, and related implementation aspects. The focus will shift as needed: from an in-depth technical treatment to broader applicability and organizational matters; from the current common understanding in industry and standardization bodies to future enhancements and developments, to the latest on implementation and field operational testing. We will first introduce the basics of VC systems and identify related vulnerabilities and threats. Then, we will outline requirements and present the state-of-the-art solution space. In brief, the following will be covered:

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2976752

1. System assumptions and enabling technologies, adversarial models, security and privacy requirements

2. Basic concepts and architectures for secure and privacy enhancing VC systems

3. Security mechanisms, facilities, and protocols

   (a) Identity, key, and credential management

   (b) In-car communication and platform security

   (c) Secure and privacy preserving VC protocols

      i. Vehicle-to-vehicle/vehicle-to-infrastructure

      ii. Single/multi-hop

      iii. Transportation safety- and efficiency-related

      iv. Adaptive and scalable validation mechanisms

   (d) Data validation and wrong-doer eviction

4. Outlook on the evolving broader landscape

3. TUTORIAL AUDIENCE

The potential audience includes researchers from academia and industry, including PhD and graduate students. Some background in wireless networking and knowledge of basic security principles would help participants to fully benefit from this tutorial. However, the tutorial will be self-contained, introducing briefly all basic concepts of security, networking and VC system functionality. To benefit attendees with more advanced relevant knowledge, additional references and material to probe further for deeper technical coverage will be provided. Where possible/relevant, the tutorial will also reflect organizational, policy, and societal considerations, to cater to relevant interests, e.g., of representatives of public authorities or industry.