Verifiable Privacy Protection for Vehicular Communication Systems

David Förster

Verifiable Privacy Protection for Vehicular Communication Systems

Springer Vieweg

David Förster
Ulm, Germany

Dissertation, Ulm University, Germany

Date doctorate awarded: 16 December 2016

ISBN 978-3-658-18549-7 ISBN 978-3-658-18550-3 (eBook)
DOI 10.1007/978-3-658-18550-3

Library of Congress Control Number: 2017943242

Springer Vieweg

Printed on acid-free paper

This Springer Vieweg imprint is published by Springer Nature
The registered company is Springer Fachmedien Wiesbaden GmbH
The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Acknowledgements

I would like to thank Professor Frank Kargl for supervising this thesis, for providing guidance for my research, and for our many fruitful discussions. Being a part of the Distributed Systems Institute at Ulm University was a great experience and I would like to thank my fellow institute members for their support. I would also like to thank Professor Falko Dressler and Professor Franz J. Hauck for acting as referees for this thesis and for their helpful comments.

The security research group at the Bosch has been an inspiring environment for the last three years. I would like to thank my supervisor Dr. Hans Löhr who spent many hours with me discussing ideas, providing feedback, and sharing his expertise. I would also like to thank Dr. Jan Zibuschka for our discussions about privacy and our research collaboration on privacy-friendly authentication and revocation. Furthermore, I would like to thank Dr. Paul Duplys, Stefan Gehrer, Christopher Huth, Sébastien Léger, Dr. Jamshid Shokrollahi, Hervé Seudié, and Robert Szerwinski for sharing their expertise, providing feedback, and for always being up for a discussion. I would also like to thank Anne Grätz for the work performed during her internship and Dr. Dirk Stegemann and Dr. Dieter Lienert for their ongoing support for my research.

The work presented in this dissertation was conducted at the Corporate Research department of Robert Bosch GmbH in Renningen.

David Förster

Abstract

This dissertation examines privacy protection on various layers of vehicular communication focusing on inter-vehicular communication. Also known as Vehicle-to-X (V2X) communication, the technology will supplement modern vehicles' sensors with information exchanged with other cars or traffic infrastructure via ad-hoc radio communication. V2X communication is expected to deliver significant improvements for traffic safety and efficiency, as well as comfort functions.

Privacy protection is crucial for several reasons: Vehicles are personal items, therefore, the traces they leave via radio communication can be considered personal identifiable information if no protection is implemented. V2X-based safety functions may be required by legislation in the future, leaving drivers no choice whether or not to use them. Therefore, established concepts for data protection, such as the requirement for the user's consent for collection and processing of his data, cannot be applied. For the technology to deliver the expected improvements for traffic safety and efficiency, a significant market penetration is required. However, privacy concerns about "Connected Cars" have been raised in the media repeatedly and need to be addressed to ensure rapid adoption once V2X-equipped vehicles are available.

Upcoming standards consider privacy protection and there is a significant body of previous research, but several points remain unaddressed: 1. A scheme of changing "pseudonym certificates" has been proposed for privacy-friendly message authentication, but it is unclear when and how often vehicles need to change their pseudonym for adequate protection. 2. For revocation of misbehaving participants, it has been suggested that the certificate authorities retain a mapping database of pseudonym holders. This database constitutes a high-value target and a single point of failure that puts drivers' privacy at risk. 3. Modern cars' connectivity facilities enable new applications such as "crowdsourcing" of sensor data. Privacy protection for drivers is required but must be balanced with quality of the collected data.

Recent large-scale security breaches illustrate the difficulty in keeping systems secure that attract motivated and skilled attackers. Furthermore, the revelations by Edward Snowden about extensive governmental surveillance have raised many concerns. Therefore, in the attacker model used throughout this work we assume a powerful adversary that is able to compromise back-end systems. We propose

solutions that do not rely on organizational controls (such as separation of duties) but use cryptographic mechanism to verifiably protect users' privacy even when back-end systems are untrusted or compromised.

We address the research gaps outlined above with the following contributions:

1. We examine the effectiveness of pseudonym changes to protect drivers from tracking attacks. Our goal is to provide guidance on change strategies and change intervals for real-world deployments. We conduct simulations in two different large-scale traffic scenarios and use the realistic model of an adversary with limited coverage. We propose specific change intervals for an urban scenario, which are shorter than the ones foreseen by upcoming standards. In a highway scenario, however, none of the strategies under evaluation achieves satisfactory protection against our tracking algorithm.

2. The privacy protection offered by changing pseudonym certificates depends on their anonymity, which is threatened by the "mapping database" required by currently proposed revocation mechanisms. We propose a privacy-friendly pseudonym system that provides full anonymity for drivers. It is complemented by a revocation mechanism that is based on a trusted component in each vehicle and does not require resolution of pseudonym holders.

3. For privacy-friendly crowdsourcing, we propose a mechanism that balances drivers' privacy with the data quality requirements from a traffic authority. Data is only made available if it satisfies a certain privacy level quantified as k-anonymity. The protection is enforced using a decentralized secret sharing scheme and does not require a central, trusted party.

For a comprehensive assessment of privacy in vehicular networks it is crucial to consider all relevant layers. Privacy protection on a higher layer is only possible if the lower layers do not leak information. In this dissertation, we present several novel protocols that protect drivers' privacy by cryptography and data minimization. We demonstrate that strong privacy protection can be achieved even when central parties are untrusted or compromised.

Privacy protection in inter-vehicular communication systems is challenging due to their unique character (mobile nodes that emit messages with a high frequency) in conjunction with safety requirements. Our results indicate that these challenges are not fully solved yet and that there may be limitations on the level of privacy that can be achieved under certain traffic conditions.

Zusammenfassung

Die vorliegende Arbeit untersucht den Schutz der Privatsphäre in der Fahrzeugkommunikation unter Berücksichtigung mehrerer Systemebenen, mit Fokus auf der sogenannten Car-to-X-Kommunikation zwischen Fahrzeugen untereinander und mit der Verkehrsinfrastruktur. Durch den ad-hoc Austausch von Funknachrichten soll Car-to-X-Kommunikation die sensorische Wahrnehmung der Außenwelt durch Fahrzeuge ergänzen und so zur Erhöhung der Verkehrssicherheit, -effizienz und des Fahrkomforts beitragen.

Der Schutz der Privatsphäre spielt dabei aus mehreren Gründen eine entscheidende Rolle: Fahrzeuge werden oft nur von einer Person benutzt. Deshalb können die Funknachrichten, die sie aussenden, als personenbezogene Daten angesehen werden, wenn keine Schutzmaßnahmen ergriffen werden. Weiterhin wird Car-to-X-Funktionalität in Zukunft möglicherweise gesetzlich vorgeschrieben sein. Deshalb können etablierte Datenschutzkonzepte, wie beispielsweise die Einwilligung des Nutzers zur Verarbeitung seiner Daten, nicht angewendet werden. Damit die Technologie den versprochenen Nutzen liefern kann, ist eine signifikante Ausstattungsrate von Fahrzeugen nötig. Kritische Medienberichte über Datenschutzaspekte vernetzter Fahrzeuge müssen ernst genommen und die geäußerten Bedenken adressiert werden, um eine schnelle Marktdurchdringung zu erreichen.

Aufkommende Standards berücksichtigen den Schutz der Privatsphäre bereits, und es gibt vielfältige wissenschaftliche Untersuchungen zu dem Thema. Trotzdem sind einige Fragen und Probleme ungelöst: 1. Zur datenschutzfreundlichen Authentifizierung wurde ein Verfahren zur Signatur von Nachrichten mit wechselnden Pseudonym-Zertifikaten vorgeschlagen. Allerdings ist unklar, wann und wie oft Fahrzeuge ihr Pseudonym wechseln müssen, um ausreichenden Schutz zu erhalten. 2. Zum Ausschluss von Teilnehmern, die ungültige Nachrichten senden, wurde vorgeschlagen, dass die Betreiber des Car-to-X-Systems eine Mapping-Datenbank mit der Zuordnung von Pseudonym-Zertifikaten zu ihren Besitzern aufbauen. Diese Datenbank ist ein attraktives Ziel für Angreifer und gefährdet die Privatsphäre der Systemteilnehmer. 3. Die Konnektivität moderner Fahrzeuge ermöglicht viele neue Anwendungen, wie beispielsweise das “Crowdsourcing” von Sensordaten. Dabei muss eine Balance zwischen dem Schutz der Privatsphäre der Fahrer und der Qualität der erhobenen Daten gefunden werden.

Die Vielzahl erfolgreicher Hackerangriffe und Datenlecks in letzter Zeit zeigen, wie schwierig es ist, die Sicherheit von Systemen zu gewährleisten, die motivierte und fähige Angreifer anziehen. Weiterhin haben die Enthüllungen von Edward Snowden Besorgnis in der Bevölkerung hervorgerufen. Um diese Bedrohungen abzubilden, nimmt die vorliegende Arbeit einen starken Angreifer an, der auch in der Lage ist, Backend-Systeme zu kompromittieren. Es werden Schutzmechanismen vorgeschlagen, die nicht auf organisatorischen Maßnahmen (wie dem Vier-Augen-Prinzip) basieren, sondern die Privatsphäre der Benutzer durch kryptographische Maßnahmen nachvollziehbar schützen, selbst dann, wenn Backend-Systeme nicht vertrauenswürdig oder kompromittiert sind.

Um die oben genannten Forschungslücken zu schließen, leistet diese Arbeit folgende Beiträge:

1. Eine Untersuchung der Effektivität von Pseudonymwechseln, um Fahrer vor Tracking-Angriffen zu schützen. Das Ziel ist es, Orientierung bezüglich Pseudonymwechselstrategien und Wechselintervallen für den Einsatz von Car-to-X-Systemen in der Praxis zu geben. Dazu wurden Simulationen in zwei großflächigen Verkehrsszenarien durchgeführt und das realistische Modell eines Angreifers mit beschränkter Empfangsreichweite verwendet. Für ein Stadtszenario werden konkrete Wechselintervalle vorgeschlagen, die kürzer sind als in den aktuellen Standards empfohlen. In einem Autobahnszenario konnte jedoch keine der untersuchten Strategien einen zufriedenstellenden Schutz vor dem entwickelten Tracking-Algorithmus erreichen.

2. Der Schutz, den wechselnde Pseudonym-Zertifikate bieten, hängt von deren Anonymität ab und wird durch die Mapping-Datenbank bedroht. Diese wird von aktuellen Verfahren zum Ausschluss von Teilnehmern benötigt. Die Arbeit stellt ein datenschutzfreundliches Pseudonym-System vor, in dem Pseudonym-Zertifikate vollständig anonym sind. Es wird ergänzt durch einen Mechanismus zum Ausschluss von Teilnehmern, der auf einer vertrauenswürdigen Hardwarekomponente basiert und keine Zuordnung von Pseudonym-Zertifikaten zu ihrem Besitzer benötigt.

3. Für datenschutzfreundliches Crowdsourcing schlägt die Arbeit einen Mechanismus vor, der die Privatsphäre der Fahrer schützt und gleichzeitig die bestmögliche Datenqualität sicherstellt. Dabei werden nur Daten veröffentlicht, die ein bestimmtes Datenschutzniveau, gemessen als k-anonymität, nicht unterschreiten. Der Schutz wird dabei durch ein dezentrales Secret-Sharing-Verfahren sichergestellt, das keine zentrale, vertrauenswürdige Partei benötigt.

Eine umfassende Analyse der Privatsphäre in einem Car-to-X-System muss alle relevanten Ebenen einbeziehen. Schutz auf einer höheren Ebene ist nur möglich, wenn die darunterliegenden Ebenen keine Informationen preisgeben. Diese Arbeit stellt mehrere neue Verfahren vor, die die Privatsphäre von Fahrern durch den Einsatz von Kryptographie und Datenminimierung nachvollziehbar schützen. Damit wird gezeigt, dass ein starker Schutz der Privatsphäre auch dann erreicht werden kann, wenn zentrale Parteien nicht vertrauenswürdig oder kompromittiert sind.

Der Schutz der Privatsphäre in Car-to-X-Systemen bringt besondere Herausforderungen mit sich, auf Grund ihres besonderen Charakters (mobile Knoten, die Nachrichten mit einer hohen Frequenz aussenden) in Verbindung mit Safety-Anforderungen. Die Ergebnisse dieser Arbeit zeigen, dass diese Herausforderungen noch nicht vollständig gelöst sind, und legen nahe, dass es Grenzen gibt bezüglich des erreichbaren Schutzes der Privatsphäre unter bestimmten Verkehrsbedingungen.

Contents

1 Introduction **1**
- 1.1 Key results and publications 4
- 1.2 Scope and limitations 8
- 1.3 Structure of this work 8

2 Background **11**
- 2.1 Vehicular communication 11
  - 2.1.1 Motivation and use cases 11
  - 2.1.2 Research, standardization and deployment 12
- 2.2 Privacy 14
  - 2.2.1 Location privacy 16
  - 2.2.2 Location privacy metrics 16
  - 2.2.3 Verifiable privacy protection 18
- 2.3 Security and privacy in vehicular communication 19
  - 2.3.1 Security and privacy requirements 20
  - 2.3.2 Security research projects 21
  - 2.3.3 Pseudonymous authentication 22
  - 2.3.4 Tracking attacks 23
- 2.4 Notation 25

3 Evaluation of Pseudonym Strategies **27**
- 3.1 Motivation 28
- 3.2 Related work 29
- 3.3 System model and scenario 31
  - 3.3.1 Requirements 33
  - 3.3.2 Requirements for pseudonym strategies 33
  - 3.3.3 Attacker model 34
- 3.4 Building blocks 35
  - 3.4.1 Mix-zones 35
  - 3.4.2 Matching in bipartite graphs 36
- 3.5 Evaluation framework 36
- 3.6 Framework implementation 38
  - 3.6.1 Model mobility 38
  - 3.6.2 Apply pseudonym strategy 41

3.6.3 Observe vehicles . . . 43
3.6.4 Learn & attack . . . 44
3.7 Evaluation . . . 47
3.8 Summary . . . 53

4 A Pseudonym System with Strong Privacy Guarantees . . . 55
4.1 Motivation . . . 56
4.2 Related work . . . 58
4.3 System model and scenario . . . 60
4.3.1 Requirements . . . 62
4.3.2 Attacker model . . . 63
4.4 Building blocks . . . 64
4.4.1 The basic pseudonym scheme . . . 64
4.4.2 Zero-knowledge proofs of knowledge . . . 65
4.4.3 Dynamic accumulators . . . 65
4.4.4 Blind signatures . . . 66
4.4.5 CL signatures . . . 67
4.4.6 Periodic n-show credentials . . . 68
4.4.7 Trusted components . . . 69
4.5 PUCA – Pseudonyms with user-controlled anonymity . . . 70
4.5.1 Protocols . . . 71
4.5.2 Extensions and modifications . . . 74
4.5.3 Alternative realization using Brands credentials . . . 75
4.5.4 Alternative realization using Lian et al.'s credential scheme 76
4.5.5 Integration into existing systems . . . 76
4.6 REWIRE – Revocation without resolution . . . 76
4.6.1 R-Tokens for self-identification . . . 78
4.6.2 Protocols and message formats . . . 81
4.6.3 Trusted computing integration . . . 83
4.6.4 Prevent blocking of OSR messages . . . 84
4.7 Evaluation . . . 85
4.7.1 Security and privacy analysis . . . 86
4.7.2 Performance evaluation . . . 88
4.8 Summary . . . 90

5 Decentralized Enforcement of k-Anonymity . . . 93
5.1 Motivation . . . 94
5.2 Related work . . . 95
5.3 System model and scenario . . . 97
5.3.1 Requirements . . . 97

5.3.2 Attacker model 98
5.4 Building blocks 99
5.4.1 K-anonymity 99
5.4.2 Shamir's secret sharing 99
5.5 Decentralized, non-interactive secret sharing 100
5.6 Privacy-friendly traffic analysis 100
5.6.1 Location obfuscation 102
5.6.2 Location- and time-specific keys 102
5.6.3 Key exchange modes 103
5.6.4 Protocols 103
5.7 Evaluation 113
5.7.1 Security and privacy analysis 113
5.7.2 Simulation setup 115
5.7.3 Availability of information 115
5.7.4 Scalability 117
5.8 Summary 120

6 Conclusion and Outlook 123

Acronyms 129

Publications 131

References 133