

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 |

<http://www.springer.com/978-3-658-18549-7>

Verifiable Privacy Protection for Vehicular
Communication Systems

Förster, D.

2017, XV, 150 p. 30 illus., 13 illus. in color., Softcover

ISBN: 978-3-658-18549-7