

Datenschutz in IVS

Anna Sinitsyna

Institut für Programmstrukturen und Datenorganisation (IPD)

Betreuender Mitarbeiter: Ref. iur. Leonie Sterz

Abstract

1 Einleitung

Motivation

Neue Problemstellung, wozu braucht man Datenschutz und Privacy? Was ist das Ziel der Seminararbeit?

2 Verwandte Themen und Hintergrund

Einstiegsliteratur - [12] [7]

Begriff C-ITS - [9], andere Begriffe einführen.

Initiativen in Deutschland und EU, Geschichte und Entwicklung

Car-2-Car Communication Consortium - [2]

Related work - Literatur, die sich mit der Fragenstellung beschäftigt - z.B. [6]

3 Technische Grundlagen

Hier grob den technischen Ablauf beschreiben und die darauf folgenden Themen kurz vorstellen.

3.1 Public-Key Infrastruktur

Im Allgemeinen In Europa - Trust List Managers

[10] - European certificate policy for C-ITS

PKI für V2X Kommunikation - Aufbau EA, AA, EE - [12] Verschlüsselung, Trust and Privacy Management - [5]

ECDSA Algorithmus basierend auf elliptischen Kurven (ECC) - [1]

3.2 Nachrichtenformate

[13] - Security Headers and Certificate Formats

Eventuell ein Schaubild für die Nachrichtenformate erstellen und hier referenzieren

3.3 Angriffsmöglichkeiten

"Big Brother Angreifer"[16]

Überwachungstool - CAM-Trace

Secondary Vehicle Identifier - [14]

z.B: nervöse Fahrer können von ruhigen unterschieden werden - [4]

Andere Papers und andere möglichen Datenschutzverletzungen finden.

4 Vereinbarkeit mit datenschutzrechtlichen Prinzipien

Warum stellen IVS ein datenschutzrechtliches Problem dar? Ist DSGVO anwendbar?

(Beispiel von rechtlicher Problematik und Richtlinien zu deren Lösung - [3]) - wird wahrscheinlich nicht behandelt oder kurz erwähnt, da wir uns auf DSGVO konzentrieren

4.1 Anwendbarkeit der DSGVO

Art.6 Abs.1c DSGVO - Personenbezug Fahrdaten. Sind Fahrdaten personenbezogen, bzw. können sie für eine eindeutige Identifizierung der Person benutzt werden?

[15] - Datenschutzrechtliche Analyse der Car-2-Car-Communication, guter Ausgangspunkt.

4.2 Grundsatz der Datenminimierung

Art.5 Abs.1c DSGVO - "Datenminimierung".

Geeignete Pseudonymisierung

4.3 Recht auf Datenübertragbarkeit

Art.20 DSGVO - "Recht auf Datenübertragbarkeit"

[8] - Analyse der Datenübertragbarkeit, Begründung der DSGVO-Anwendbarkeit

4.4 Andere Datenschutzmaßnahmen

[11] - alle o.g. Datenschutzmaßnahmen + obligation to report a data breach, to conduct a data protection impact assessment". analytical progress of AI". Guter Ausgangspunkt für Kapitel 4.1

Die in [7] aufgeführten Empfehlungen untersuchen und analysieren.

5 Zusammenfassung und Ausblick

...

Literatur

- [1] Elaine Barker u. a. „NIST Special Publication 800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography“. In: (2013). DOI: 10.6028/NIST.SP.800-56Ar3. URL: <https://doi.org/10.6028/NIST.SP.800-56Ar3>.
- [2] CAR 2 CAR Communication Consortium. URL: <https://www.car-2-car.org>.
- [3] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019SC0096#_Ref521658883.
- [4] Frank Dettki. *Methoden zur objektiven Bewertung des Geradeauslaufs von Personenkraftwagen*. 2005. URL: <https://elib.uni-stuttgart.de/handle/11682/4059> (besucht am 24. 11. 2020).
- [5] ETSI (European Telecommunications Standards Institute). *TS 102 941 - V1.2.1 - ITS; Security; Trust and Privacy Management*. Techn. Ber. 2018, S. 1–30.
- [6] Jochum. „Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung“. In: *ZD 2020*, 497 (2020).
- [7] Michael Kiometzis und Markus Ullmann. „Fahrdaten für alle?“ German. In: *Datenschutz und Datensicherheit - DuD 41.4* (März 2017), S. 227–232. DOI: 10.1007/s11623-017-0763-6.
- [8] Klink-Straub/Straub. „Vernetzte Fahrzeuge – portable Daten“. In: *ZD 2018*, 459 (2018).
- [9] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN *Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme - ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität*. Techn. Ber. 2016.
- [10] *Result of C-ITS Platform Phase II Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1*. Techn. Ber. 2017. URL: https://ec.europa.eu/transport/sites/transport/files/c-its%7B%5C_%7Dsecurity%7B%5C_%7Dpolicy%7B%5C_%7Drelease%7B%5C_%7D1.pdf.
- [11] Olga Seewald. „Regulation of data privacy and cybersecurity in connected and automated vehicles in the U . S . and the EU – Part 1 ***“. In: (2018), S. 124–132.

- [12] Thomas Strubbe, Nicolas Thenée und Christian Wiesebrink. „IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen“. German. In: *Datenschutz und Datensicherheit - DuD* 41.4 (März 2017), S. 223–226. DOI: 10.1007/s11623-017-0762-7.
- [13] *TS 103 097 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. Techn. Ber. 2013, S. 1–33.
- [14] Markus Ullmann, Thomas Strubbe und Christian Wiesebrink. *Technical Limitations and Privacy Shortcomings of the Vehicle-to-Vehicle Communication*. c. 2016, S. 22–27. ISBN: 9781612085159.
- [15] Thilo Weichert. „Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung“. In: *Svr* (2016), S. 361.
- [16] B. Wiedersheim u. a. „Privacy in inter-vehicular networks: Why simple pseudonym change is not enough“. In: *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*. 2010, S. 176–183. DOI: 10.1109/WONS.2010.5437115.