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 Funktionsweise der C2C-Kommunikation

Im folgenden Abschnitt wird die Funktionsweise der C2C-Kommunikation und die dafür benötigte Infrastruktur näher beschrieben. Der Nachrichtenaustausch zwischen Fahrzeugen beruht auf Public-Key Kryptografie, somit werden die Nachrichten mit einer Signatur und einem Zertifikat versehen, die von einer zentralen Stelle ausgegeben werden. Weiterhin wird auf die Nachrichtenformate der C2C-Kommunikation eingegangen, sowie auf

die darin gespeicherten Daten, die möglicherweise für die Identifikation des Fahrzeugs benutzt werden können. Des Weiteren werden mögliche Angriffe auf die Pseudonymität der Nachrichten aufgeführt, aufgrund deren Bewegungsprofile von Fahrzeugen erstellt werden können.

3.1 Public-Key Infrastruktur

Um den oben genannten Nachrichtenaustausch zu ermöglichen, braucht man eine entsprechende Public-Key Infrastruktur (PKI), die aus einer oder mehreren Certification Authorities (CAs) besteht. Die CAs sind in der Lage, digitale Zertifikate zu erstellen, diese Zertifikate der End-Entitäten zu erteilen und zu verifizieren. Als End-Entitäten fungieren ITS-Stationen (u.a. Fahrzeuge), die die erstellten Zertifikate für die Kommunikation untereinander verwenden und somit die Authentizität von einer Nachricht beweisen und überprüfen können [12].

Die PKI wird aus drei Stufen zusammengesetzt [10]:

- Root-CAs (erstellen Zertifikate für untergeordnete CAs)
- Mindestens zwei Sub-CAs
- End-Entitäten (EEs)

Darüber hinaus gibt es zwei Arten von Sub-CAs: Enrolment Authorities (EA) und Authorization Authorities (AA). Die EAs erstellen langlebige Zertifikate für EEs, die für die Authentifizierung innerhalb der PKI verwendet werden. Die AAs hingegen stellen kurzzeitige Zertifikate zur Verfügung, mit denen die EEs (z.B. Fahrzeuge) untereinander kommunizieren können ohne die Pseudonymität von einzelnen Entitäten zu verletzen.

Bevor jegliche Kommunikation stattgefunden hat, muss sich die End-Entität zunächst bei der zugehörigen EA registrieren und ein Enrolment Credential erhalten, das mehrere Jahre gültig ist. Die EA bekommt dabei die Registrierungsinformationen von der EE, zum Beispiel ihre Fahrzeugidentifizierungsnummer und ihren öffentlichen Schlüssel. Die EE signiert den initialen Zertifikatsrequest mit ihrem eingebauten privaten Schlüssel und übermittelt ihn an die EA. Falls die Daten übereinstimmen, erhält die EE einen Enrolment Credential (EC).

Mit einem gültigen EC kann die EE weiterhin sogenannte Authorization Tickets (AT) bei der AA beantragen. ATs sind kurzzeitgültige Zertifikate für C2X Kommunikation, die oft gewechselt werden und somit der Senderpseudonymität dienen. Die Nachrichten sollten keinen eindeutigen Identifikator erhalten, damit kein Personenbezug hergestellt werden kann. Daher werden CAMs und DENMs mit ATs signiert und nicht mit den langlebigen ETs, die für eine EE über mehrere Jahre gültig ist.

Ein AT wird von einer Entität bei der AA beantragt. Die Anfrage an die AA enthält unter anderem verschlüsselte Daten, die nur von der entsprechenden EA ausgelesen

werden können [5], darunter die EC von der Entität. Die EA bestätigt die Authentizität der Daten mit dem angehängten EC und schickt eine Statusmeldung an die AA, ohne diese zusätzliche Information preiszugeben. Es ist wichtig, die EA und AA organisatorisch getrennt zu halten, da sonst bei der AT-Anfrage eine Zuordnung zu der End-Entität bzw. ihrem EC möglich wäre.

Nachdem die mit dem AT signierte Nachricht erfolgreich an die empfangende EE übermittelt wurde, nutzt sie den AT um die Nachricht zu verifizieren. Dies erfolgt mittels einer Kettenprüfung durch die AA und das entsprechende Root-Zertifikat, wodurch die Authentizität der Nachricht festgestellt wird.

In Europa ist zusätzlich zu der oben beschriebenen PKI eine globale Vertrauensliste vorgesehen, die innerhalb der europäischen Grenzen alle vertrauenswürdige Root-CA-Zertifikate beinhaltet. Diese wird von einem zentralen Trust List Manager (TLM) erstellt und elektronisch signiert. Somit wird die Interoperabilität von europäischen PKIs über Grenzen sichergestellt. Darüber hinaus ist es wichtig, die nicht mehr vertrauenswürdigen Zertifikate zurückziehen zu können - dies wird durch sogenannte Certificate Revocation Lists (CRL) sichergestellt. Diese werden allen PKI-Teilnehmern von der jeweiligen Root-CA zur Verfügung gestellt und enthalten die Liste mit allen revozierten Zertifikaten.

3.2 Nachrichtenformate

Die Nachrichtenformate, die für die oben beschriebene PKI nötig sind, wurden von dem Europäischen Institut für Telekommunikationsnormen (ETSI) definiert. Im Weiteren wird auf [5] verwiesen, in dem die Paketstruktur für gesicherte C2X-Nachrichten und deren Zertifikatsformat festgelegt wurde.

Der grobe Aufbau einer gesicherten C2X-Nachricht wird in der Abbildung ... dargestellt. Sie enthält unter anderem die ECDSA-Signatur ([1]), den Verifikationsschlüssel des Senders und die eigentliche Nachricht, die im Payload gespeichert ist. Für die Car-2-Car Kommunikation sind zurzeit zwei Nachrichtenformate vorgesehen:

- die Cooperative Awareness Message (CAM) und die
- Decentralized Environmental Notification Message (DENM) [13].

Im Weiteren wird nur die CAM betrachtet, da die DENM keine personenbezogenen Daten beinhaltet und im datenschutzrechtlichem Sinne kein Problem darstellt [7]. Der Aufbau einer CAM wird in der Abbildung ... dargestellt. Sie besteht aus vier Elementen: Header, CAM Information, Signature und Certificate. Die tatsächliche Information über das Fahrzeug wird im Block CAM Information gespeichert. Er beinhaltet sowohl dynamische Daten (z.B. Last Geographic Position, Speed) als auch statische Daten über das Fahrzeug, die trotz ständigem Pseudonymwechsel identisch bleiben (z.B. Length, Weights). Eine CAM erhält keinen primären Identifikator, aufgrund dessen eine eindeutige Zuordnung zum Fahrzeug möglich wäre.

3.3 Angriffsmöglichkeiten

Auch wenn CAMs keine primären Identifikationsmerkmale erhalten, existieren es mehrere Möglichkeiten, um mithilfe von CAMs Bewegungsprofile von Fahrzeugen zu erstellen. Dies kann zu diversen Risiken für die Privatsphäre führen, falls der Personenbezug von Fahrdaten hergestellt werden kann. Im folgenden Abschnitt werden einige Angriffsarten auf die Pseudonymität von CAMs näher beschrieben und analysiert.

Als erstes Beispiel sei ein sogenannter 'Big Brother Angreifer' angeführt, der eine Infrastruktur von Empfangseinrichtungen in einer geografischen Region betreibt und in der Lage ist, in dieser Gegend CAMs von Fahrzeugen zu erfassen und auszuwerten. Das wäre möglich, indem der Angreifer zum Beispiel eine Fahrzeug-Flotte aufstellt, die eingehende CAMs an einen zentralen Server übermittelt. Auch wenn vorbeifahrende Fahrzeuge ihr Pseudonym jede 10 Sekunden ändern würden, könnten sie mit solch einer Infrastruktur verfolgt werden [16]. Da diese Art von Überwachung alle Fahrzeugdaten in der Gegend erfassen würde, könnte sie für breitere Verkehrsanalysen genutzt werden.

Darüber hinaus gibt es einige Möglichkeiten, die Bewegungen von einzelnen Fahrzeugen detailliert aufzuzeichnen. Zum Beispiel kann man mithilfe eines an das Fahrzeug befestigtes Überwachungstools sogenannte CAM-Traces erstellen, d.h. die gefahrene Strecke eines Fahrzeugs und alle von ihm auf dieser Strecke erstellten CAMs. Auch wenn das Fahrzeug regelmäßig seinen Signaturschlüssel wechselt, würde es reichen, nur eine CAM aus der CAM-Trace dem Fahrzeug eindeutig zuzuordnen, um die gesamte CAM-Trace diesem Fahrzeug zuzuordnen [7].

Es existiert eine Reihe von Methoden, um diese Zuordnung durchzuführen. In [14] wurde dargelegt, dass sie aufgrund der sog. Secondary Vehicle Identifier erfolgen kann. Diese wird von diversen drahtlosen Schnittstellen im Auto zur Verfügung gestellt (z.B. eine Headunit, die eine öffentliche Bluetooth-Schnittstelle mit einem nutzerfreundlichen Namen besitzt). Die Secondary Vehicle Identifiers sind einfach zu erfassen und können einer eindeutigen Zuordnung der empfangenen CAM-Trace zum Fahrzeug dienen.

4 Vereinbarkeit mit datenschutzrechtlichen Prinzipien

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

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

4.1 Anwendbarkeit der DSGVO

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

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

Herstellbarkeit des Personenbezugs [7]

[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 Datenschutzmaßnahmen

[11] - alle o.g. Datenschutzmaßnahmen + öbligation to report a data breach, to conduct a data protection impact assessment". änalytical 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 Wieschebrink. „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 Wieschebrink. *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.