Fortschritt-Berichte VDI

VDI

Reihe 10

Informatik/
Kommunikation

Dipl.-Met. Christoph Maget, M.Sc.,
München

Nr. 872

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Der
FernUniversität in Hagen
Fakultät für Mathematik und Informatik
vorgelegte

DISSERTATION

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

von
CHRISTOPH FRANZ MAGET
aus München

Hagen, 2020

Gutachter:
Prof. Dr. Dr. Wolfgang A. Halang, Hagen
Prof. Dr.-Ing. Linus Schleupner, Köln
Prof. Dr.-Ing. Kyandoghere Kyamakya, Klagenfurt

Tag der mündlichen Prüfung: 11.12.2020

Fortschritt-Berichte VDI

Reihe 10

Informatik/
Kommunikation

Dipl.-Met. Christoph Maget, M.Sc.,
München

Nr. 872

Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Maget, Christoph
Auf sichere Mobilfunkkommunikation gestütztes Fahrzeugleitsystem
Fortschr.-Ber. VDI Reihe 10 Nr. 872. Düsseldorf: VDI Verlag 2021.
148 Seiten, 25 Bilder, 23 Tabellen.
ISBN 978-3-18-387210-7, ISSN 0178-9627,
€ 57,00/VDI-Mitgliederpreis € 51,30.

Keywords: Fahrzeugleitsystem – Mobilfunk – Kryptologie – Perfekte Sicherheit – Car2X

Die vorliegende Arbeit richtet sich an Ingenieure und Wissenschaftler in den Bereichen Kryptografie und Mobilkommunikation. Sie stellt ein Fahrzeugleitsystem vor, das mit seiner Kommunikationsarchitektur post-quanten-sichere Kryptografie und Nachrichtenübertragung bei harten Echtzeitbedingungen ermöglicht. Grundlage ist eine genaue Analyse bestehender Standards und die Schlussfolgerung, dass existierende Ansätze diese nicht erfüllen. Die Kommunikationsarchitektur macht sich das Prinzip der perfekt sicheren Einmalverschlüsselung zu Nutze und löst den Schlüsselaustausch durch eine an den Anwendungsfall angepasste Organisationsstruktur. Eine detaillierte Berechnung des benötigten Schlüsselbedarfs beweist die grundsätzliche Eignung der perfekt sicheren Einmalverschlüsselung für die Automatisierungstechnik. Das Fahrzeugleitsystem erfüllt weitestgehend die von der Europäischen Kommission aktuell erarbeiteten Anforderungen an das ethische Verhalten vernetzter und autonomer Systeme.

Bibliographische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter www.dnb.de abrufbar.

Bibliographic information published by the Deutsche Bibliothek
(German National Library)
The Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie (German National Bibliography); detailed bibliographic data is available via Internet at www.dnb.de.

Schriften zur Informations- und Kommunikationstechnik
Herausgeber:
Wolfgang A. Halang, Lehrstuhl für Informationstechnik
Herwig Unger, Lehrstuhl für Kommunikationstechnik
FernUniversität in Hagen

ISSN 0178-9627

ISBN 978-3-18-387210-7

Danksagung

Die vorliegende Arbeit entstand parallel zu meiner beruflichen Tätigkeit in den Jahren 2016 bis 2020 und wäre ohne zahlreiche Unterstützer nicht möglich gewesen.

Herrn Prof. Dr. Dr. Wolfgang A. Halang danke ich für die wissenschaftliche Betreuung und Befürwortung der vorliegenden Arbeit. Seine langjährige konstruktive und strukturierende Begleitung hat einen unschätzbaren Beitrag zu meinem akademischen Werdegang geleistet.

Gleichermaßen danke ich Herrn Prof. Dr.-Ing. Linus Schleupner für die Übernahme des zweiten Gutachtens, für die fachlichen Diskussionen und Anregungen und nicht zuletzt für Ermutigung und Zuspruch aus seinem persönlichen Erfahrungsschatz.

Herrn Prof. Dr.-Ing. Kyandoghere Kyamakya danke ich für die Übernahme des dritten Gutachtens und freue mich auf einen weiteren Austausch.

Den Kollegen an der FernUniversität in Hagen danke ich für wertvolle Ideen und Gespräche.

Schließlich danke ich meiner Familie sowie meinen Kollegen und Freunden für Verständnis und Rückhalt.

Christoph Maget, 2020

Die Gefahr, dass der Computer so wird wie der Mensch, ist nicht so groß wie die Gefahr, dass der Mensch so wird wie der Computer.

– Konrad Zuse

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
ASIL	Automotive Safety Integrity Level
B	Byte
BSI	Bundesamt für Sicherheit in der Informationstechnik
C-V2X	Cellular Vehicle to everything
CAM	Cooperative Awareness Message
CAP	Consistency, Availability and Partition Tolerance
CPOC	Cooperative ITS Point of Contact
CPS	cyberphysisches System
DENM	Decentralized Environment Notification Message
DES	Data Encryption Standard
dID	digitale Identifikation
DIN	Deutsches Institut für Normung
DoS	Denial of Service
EMV	elektromagnetische Verträglichkeit
EN	Europäische Norm
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUID	Globally Unique Identifier
HMI	Human-Machine Interface
HSM	Hardware-Sicherheitsmodul
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ID	Identifikator
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnik
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol

ISM	Industrial, Scientific and Medical
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
IVS	Intelligente Verkehrssysteme
JSON	JavaScript Object Notation
KDC	Key Distribution Center
M2M	Machine to Machine
MAC	Media Access Control
MITM	Man in the Middle
OBU	On Board Unit
OSI	Open Systems Interconnection
OTP	One Time Pad
P2P	Peer to Peer
PKI	Public Key Infrastructure
RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
RDS-TMC	Radio Data System – Traffic Message Channel
RFC	Request for Comments
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SE	Secure Element
SGAM	Smart Grid Architecture Model
SIKAF	Sichere Kommunikationsarchitektur für Fahrzeugleitsysteme
SIL	Safety Integrity Level
SIM	Subscriber Identity Module
SPOF	Single Point of Failure
SSP	Smart Secure Platform
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UML	Unified Modeling Language
UUID	Universally Unique Identifier
V2X	Vehicle to everything
VANet	Vehicular Ad hoc Network
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VDI	Verein Deutscher Ingenieure
WLAN	Wireless Local Area Network
WWW	World Wide Web

Nomenklatur

Alphabet Ein Alphabet ist eine Menge von Zeichen, aus denen durch Verkettung Klartext, Schlüssel, Maske und Schlüsseltext zusammengesetzt werden.

Chiffriermaske Eine Chiffriermaske (kurz Maske) ist ein Parameter des eingesetzten kryptografischen Verfahrens. Durch *XOR*-Verknüpfung von Klartext und Maske entsteht der Schlüsseltext. Durch *XOR*-Verknüpfung von Schlüsseltext und Maske entsteht der Klartext. Zur Maskierung wird jedes Zeichen des Klartextes mit genau einem Zeichen der Maske verknüpft. Die Maske hat daher dieselbe Länge wie der Klar- bzw. Schlüsseltext und wird aus dem gleichen Alphabet wie der zu verschlüsselnde Klartext gebildet. Um unautorisierte Entschlüsselung zu verhindern, darf die Maske nur berechtigten Nutzern bekannt gemacht werden.

Codebuch In einem Codebuch können häufig übermittelte Informationen tabelliert und mit einem Code verbunden werden. Zur Übermittlung der Information muss dann nicht die vollständige Zeichenkette zur Darstellung der Information übertragen werden, sondern es genügt die Übertragung des Codes. Die Datenmenge kann dadurch reduziert werden.

Maske Kurzform von Chiffriermaske

Maskengröße siehe Schlüsselgröße

Maskenlänge siehe Schlüssellänge

Maskenvorrat siehe Schlüsselvorrat

Maskierung Maskierung ist eine besondere Art der Verschlüsselung. Sie zeichnet sich dadurch aus, dass jedes Zeichen des Klartextes mit genau einem Zeichen der Maske verknüpft wird, um den Schlüsseltext zu erzeugen. Durch Demaskierung wird aus dem Schlüsseltext der Klartext zurückgewonnen. Maskierung ist das Verschlüsselungsverfahren bei der Einmalverschlüsselung (engl. *One Time Pad*).

Nachricht Eine Nachricht ist eine sinnhafte Verkettung von Zeichen, sodass alle zur Übermittlung einer Information notwendigen Angaben vorhanden sind. Die Nachricht kann teilweise verschlüsselt oder maskiert sein.

Nachrichtenlänge Die Nachrichtenlänge ist die Anzahl der Zeichen einer Nachricht. Handelt es sich bei der Nachricht um Binärcode, so kann die Nachrichtenlänge anstatt in Zeichen auch direkt in Bytes angegeben werden.

Prüfsumme Eine Prüfsumme ist eine Zeichenkette fester Länge, die durch einen Algorithmus aus einer Nachricht beliebiger Länge erzeugt wird. Eine

Veränderung der Nachricht oder ihrer Bestandteile führt mit hinreichender Wahrscheinlichkeit zu einer veränderten Prüfsumme. Es wird zwischen technischer und kryptografischer Prüfsumme unterschieden. Eine technische Prüfsumme dient der Entdeckung von Übertragungsfehlern. Eine kryptografische Prüfsumme dient der Entdeckung unautorisierter Änderungen an einer Nachricht und damit der Integritätsprüfung.

Relais Ein Relais ist eine Vermittlungsstelle zwischen zwei Kommunikationsteilnehmern. Alle Nachrichten werden vom Sender zum Relais geschickt und von dort zum Empfänger weitergeleitet.

Schlüssel Ein Schlüssel ist ein Parameter des eingesetzten kryptografischen Verfahrens. Er bestimmt die Zeichenfolge des Schlüsseltextes und ermöglicht die Rückgewinnung des Klartextes aus dem Schlüsseltext. Der Schlüssel wird aus dem gleichen Zeichenvorrat wie der zu verschlüsselnde Klartext gebildet. Um unautorisierte Entschlüsselung zu verhindern, darf der jeweils eingesetzte Schlüssel nur berechtigten Nutzern bekannt gemacht werden. Im Gegensatz zur Maske ist der Schlüssel von geringerer Länge als der zu verschlüsselnde Klartext. Die Menge aller möglichen Schlüssel wird Schlüsselraum genannt.

Schlüsselgröße Die Schlüsselgröße ist die Summe aller Schlüssellängen der Elemente (Schlüssel) eines Schlüsselvorrats. Die Schlüsselgröße ist damit die Anzahl der Zeichen, die bei einem Nutzer vorgehalten wird. Sie kann in Zeichen oder Bytes angegeben werden.

Schlüssellänge Die Schlüssellänge ist die Anzahl der Zeichen eines einzelnen Schlüssels.

Schlüsseltext Ein Schlüsseltext ist die durch Verschlüsselung oder Maskierung eines Klartextes entstandene Zeichenkette. Weitere Bezeichnungen sind Geheimtext, Kryptogramm oder Chiffrat.

Schlüsselvorrat Jedem Nutzer steht eine Teilmenge des Schlüsselraums als Schlüsselvorrat zur Verwendung bei der Ver- und Entschlüsselung zur Verfügung. Die Mächtigkeit dieser Teilmenge wird als Schlüsselvorratsmächtigkeit bezeichnet.

Verschlüsselung Eine Verschlüsselung (auch Chiffrierung genannt) ist eine Funktion (auch Verschlüsselungsverfahren oder Chiffre genannt), die aus Klartext und Schlüssel als Eingangsdaten den Schlüsseltext als Ausgangsdatum erstellt. Aus dem Schlüsseltext kann der Klartext ohne Kenntnis des Schlüssels nicht zurückgewonnen werden. Die in der Nachricht enthaltenen Informationen werden dadurch vor unberechtigten Empfängern verborgen. Die Umkehrung der Verschlüsselung ist die Entschlüsselung.

Zusammenfassung

Automatisierungssysteme spielen in modernen Industriegesellschaften eine zentrale Rolle und durchdringen nahezu alle Lebensbereiche. Der Trend zu verteilten und mobilen Systemen stellt hohe Anforderungen an Sicherheit, Zuverlässigkeit und Echtzeitfähigkeit der Kommunikation zwischen den beteiligten Komponenten. Etablierte Verschlüsselungsverfahren haben sich entweder als unsicher oder als nicht echtzeitfähig beim Einsatz in verteilten Automatisierungssystemen erwiesen. Das einzige, nachweislich sichere Konzept der perfekt sicheren Verschlüsselung wird aufgrund praktischer Hürden bislang kaum in der Automatisierungstechnik eingesetzt. Eine sehr heterogene Systemlandschaft erschwert zudem den übergreifenden Datenaustausch zwischen Systemen unterschiedlicher Hersteller.

In der vorliegenden Arbeit wird eine Kommunikationsarchitektur für Automatisierungssysteme entwickelt und evaluiert, die für drahtlos kommunizierende Komponenten perfekt sichere Verschlüsselung bereitstellt und Echtzeitanforderungen erfüllt. Wesentliche Bestandteile sind eine zentrale Instanz zur Authentifizierung der Teilnehmer, Erzeugung und Verteilung der benötigten Schlüssel sowie eine auf Relaisstationen gestützte Übertragungsinfrastruktur. Die vorgestellte Kommunikationsarchitektur fokussiert auf Automatisierungssysteme im Verkehrsbereich. Die Kommunikationsarchitektur dient dabei dem Datenaustausch in einem Fahrzeugleitsystem, das eine effizientere Ausnutzung vorhandener Verkehrsinfrastruktur ermöglichen soll. In diesem Anwendungsbereich bestehen besonders hohe Anforderungen an Sicherheit und Echtzeitfähigkeit der Datenübertragungen, da der Nachrichtenaustausch zur Abstandsregelung zwischen Fahrzeugen und zur Kollisionsvermeidung dient. Für Konzeption und Evaluierung der Kommunikationsarchitektur werden aus Normen wie der ISO 26262 spezifische Anforderungen an die funktionale sowie an die informations- und kommunikationstechnische Sicherheit abgeleitet. Sicherheitsrelevanten Funktionen wird ein ASIL zugeordnet, um Sicherheitslücken systematisch zu identifizieren und zu schließen.

Es wird nachgewiesen, dass die entwickelte Kommunikationsarchitektur diese spezifischen Anforderungen im Gegensatz zu bestehenden Übertragungssystemen erfüllen kann. Entscheidend dabei ist die Umsetzung als zentralisierte Lösung, da nur so perfekte Datensicherheit möglich ist und gleichzeitig die Komplexität der Gesamtarchitektur auf ein kontrollierbares Maß beschränkt bleibt. Die vorgestellte Kommunikationsarchitektur wird prototypisch auf Basis frei verfügbarer Softwarebibliotheken und Hardwareplattformen implementiert. Dies ermöglicht zum einen die Übertragung der Konzepte auf weite Bereiche der Automatisierungstechnik und zum anderen Geschäftsmodelle, die keine Lizenzierung proprietärer Komponenten voraussetzen.

Abstract

Automation systems are of crucial importance for modern industrial societies and permeate almost any sphere of life. The trend towards distributed and mobile systems imposes high demands on the security, reliability and real-time performance of communication among the components involved. Established encryption methods have proven to be either insecure or to lack real-time capability when used in distributed automation systems. The only provably secure concept – perfectly secure encryption – is rarely used in automation technology due to practical impediments. Different paradigms of system integration impede data exchange between systems from different manufacturers.

In this work a communication architecture for automation systems is developed and evaluated, which features perfectly secure encryption and meets real-time requirements for wireless communication. Essential elements are a central authority to authenticate the participants, and to provide them with the necessary keys as well as a dedicated transmission infrastructure based on relay stations. The main applications of the presented communication architecture are automation systems in the transportation sector. The communication architecture is used to exchange data in a vehicle control system, which is intended to improve safety and capacity of existing transportation infrastructure. Since the message exchange in this application aims at distance control and collision avoidance, all data transmissions impose particularly high demands on security and real-time capability. For conception and evaluation of the communication architecture, specific requirements concerning functional safety as well as information and communication security are derived from standards such as ISO 26262. Consequently, an ASIL is assigned to safety-relevant functions of the communication architecture. No existing concept can meet the identified requirements so far.

It is shown that the developed communication architecture can meet the requirements derived. Implementation with a centralised topology is the only way to allow the use of perfectly secure encryption and, at the same time, to limit the complexity of the overall architecture. The presented communication architecture is implemented as a prototype based on freely available software libraries and hardware platforms. This enables, on one hand, transfer of the concepts to wide areas of automation technology and, on the other, business models that do not require the licensing of proprietary components.