Secure In-Vehicle Communication

Marko Wolf[1], André Weimerskirch[2], and Christof Paar[1,2]

[1] Horst Görtz Institute (HGI) for IT Security,
Ruhr University of Bochum, Germany
{mwolf,cpaar}@crypto.rub.de

[2] escrypt GmbH, Bochum, Germany
{aweimerskirch,cpaar}@escrypt.com

Summary. This work presents a study of state of the art bus systems with respect to their security against various malicious attacks. After a brief description of the most well-known and established vehicular communication systems, we present feasible attacks and potential exposures for these automotive networks. We also provide an approach for secured automotive communication based on modern cryptographic mechanisms that provide secrecy, manipulation prevention and authentication to solve most of the vehicular bus security issues.

Keywords: automotive communication security, vehicular bus systems, LIN, CAN, FlexRay, MOST, Bluetooth

1 Introduction

Progress in automotive electronics proceeds unabated (Table 1). Today modern cars contain a multiplicity of controllers that are increasingly networked together by various bus communication systems with very different properties. Automotive communication networks have access to several crucial components of the vehicle, like breaks, airbags, and engine control. Moreover, cars that are equipped with driving aid systems like ESC (electronic stability control) or ACC (adaptive cruise control) allow deep interventions in the driving behavior of the vehicle. Further electronic drive-by-wire vehicle control systems will fully depend on the underlying automotive data networks. Although car communication networks assure safety against several technical interferences, they are mostly unprotected against malicious attacks. The increasing coupling of unsecured automotive control networks with new car multimedia networks like MOST (Media Oriented System Transport) or GigaStar as well as the integration of wireless interfaces such as GSM (Global System for Mobile Communications) or Bluetooth causes various additional security risks [32].

Table 1. Development of automotive electronics based on [30]

1970s	1980s	1990s	2000s
Electronic fuel injection	Electronic gearbox	Airbag	Drive-by-wire
Electronic control panel	Anti-lock brakes	Electronic navigation	Internet
Centralized door locking	Climate control	Electronic driving assistants	Telematics
Cruise control	Automatic mirror	Electronic traffic guidance	Ad-hoc networks
	Car phone	Voice control	Personalization

We begin in Section 2 by introducing respectively one well-known representative for each particular group of vehicular communication systems. We briefly describe technical properties of every representative (Section 2.3) and introduce two methods for vehicular bus interconnections (Section 2.4). Section 3 presents various exposures to automotive bus systems. We indicate possible attackers and present feasible attacks for each representative bus system. In the Section 4, we offer elementary approaches to improve automotive bus communication security along with a practical example implementation.

2 Automotive Bus Systems

2.1 Bus Communication

Unlike a point-to-point connection a bus is a communication system that can logically connect several peripherals, i.e. bus controllers over the same set of wires. The consequential potential savings of cost and weight encourage the increasing application of bus systems as communication systems within the automotive area. Moreover busses are easy to implement and to extend, and the failure of one node should not affect others. However, since in a bus system all nodes share the same communication line, they need schemes for collision handling or collision avoidance, or require a bus master which controls access to the shared bus resource. Furthermore, bus systems have a limited cable length and a limited number of nodes. The performance of a bus communication degrades the more nodes are connected, whereas a cable break can disable the entire vehicular bus network.

2.2 Vehicle Communication Systems

Today, a wide variety of vehicle communication systems are used in the automotive area. Possible applications range from electronic engine control, several driving assistants and safety mechanisms to the broad variety of infotainment applications. As shown in Table 2, we distinguish the following five different vehicle communication groups according to their essential technical properties and application areas. Local sub networks such as LIN (Local Interconnect

Table 2. Grouping of selected automotive bus systems

Subbus	Event-triggered	Time-triggered	Multimedia	Wireless
LIN	CAN	FlexRay	MOST	Bluetooth
K-Line	VAN	TTP	D2B	GSM
I^2C	PLC	TTCAN	GigaStar	Wi-Fi

Network) control small autonomous networks used for automatic door locking mechanisms, power-windows and mirrors as well as for communication with miscellaneous smart sensors to detect, for instance, rain or darkness. Event-triggered bus systems like CAN (Controller Area Network) are used for soft real-time in-car communication between controllers, networking for example the antilock breaking system (ABS) or the engine management system. Time-triggered hard real-time capable bus systems such as FlexRay, TTCAN (Time-Triggered CAN) or TTP (Time-Triggered Protocol) guarantee determined transmission times for controller communication and therefore can be applied in highly safety-relevant areas such as in most drive-by-wire systems. The group of multimedia bus systems like MOST, D2B (Domestic Digital Bus) and GigaStar arise from the new automotive demands for in-car entertainment that needs high-performance, wide-band communication channels to transmit high-quality audio, voice and video data streams within the vehicle. The wireless communication group contains modern wireless data transmission technologies that are increasingly expanding into the automotive area. They enable the internal vehicle network to communicate with other cars nearby, external base stations as well as the utilization of various location-based services. Figure 1 completes the overview with a short comparison of

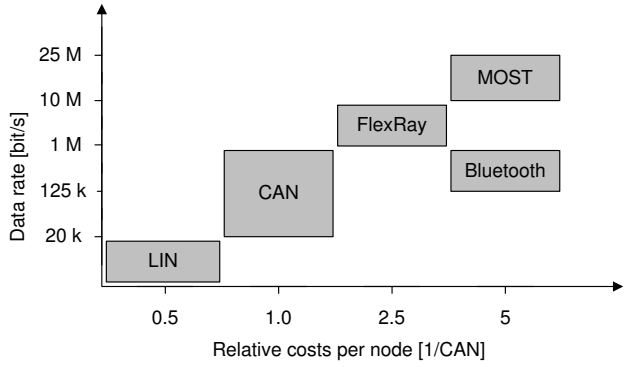

Fig. 1. Data rates and relative costs of automotive bus systems

typical data rate and relative cost per node for each vehicular communication group mentioned.

2.3 Bus Representatives

In the following, we give a short technical description of one appropriate representative from each identified vehicular communication network group (see Section 2). Further information can be found in [6, 10, 12, 22, 26].

LIN: The UART (Universal Asynchronous Receiver Transmitter) based LIN (Local Interconnect Network) is a single-wire sub network for low-cost, serial communication between smart sensors and actuators with typical data rates up to 20 kbit/s. It is intended to be used from the year 2001 everywhere in a car where the bandwidth and versatility of a CAN network are not required. A single master controls the collision-free communication with up to 16 slaves, optionally including time synchronization for nodes without a stabilized time base. LIN (similarly to CAN) is a receiver-selective bus system. Incorrectly transferred LIN messages are detected and discarded by the means of parity bits and a checksum. Besides the normal operation mode, LIN nodes also provide a sleep mode with lower power consumption, controlled by special sleep (or wake-up) message.

CAN: The all-round Controller Area Network, developed in the early 1980s, is an event-triggered controller network for serial communication with data rates up to one Mbit/s. Its multi-master architecture allows redundant networks, which are able to operate even if some of their nodes are defective. CAN messages do not have a recipient address, but are classified over their respective identifier. Therefore, CAN controllers broadcast their messages to all connected nodes and all receiving nodes and decide independently if they process the message. CAN uses the decentralized, reliable, priority-driven CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access control method to guarantee the transmission of the top-priority message first. In order to employ CAN in the environment of strong electromagnetic fields, CAN offers an error mechanism that detects transfer errors, interrupts and indicates the erroneous transmissions with an error flag and initiates the retransmission of the affected message. Furthermore, it contains mechanisms for automatic fault localization including disconnection of the faulty controller.

FlexRay: FlexRay is a deterministic and error-tolerant high-speed bus, which meets the demands for future safety-relevant high-speed automotive networks. With its data rate of up to 10 Mbit/s (redundant single channel mode) FlexRay is targeting applications such as drive-by-wire and Powertrain. The flexible, expandable FlexRay network consists of up to 64 nodes connected point-to-point or over a classical bus structure. For physical transmission medium both optical fibers and copper lines are suitable. FlexRay is (similarly to CAN) a receiver-selective bus system and uses the cyclic TDMA (Time Division Multiple Access) method for data transmission control. Therefore, it

uses synchronous transmission for time-critical data and priority-driven asynchronous transmission for non-time-critical data via freely configurable, static and dynamic time segments. Its error tolerance is achieved by channel redundancy, a protocol checksum and an independent instance (bus guardian) that detects and handles logical errors.

MOST: The ISO/OSI standardized MOST (Media Oriented System Transport) serial high-speed bus became the basis for present and future automotive multimedia networks for transmitting audio, video, voice, and control data via fiber optic cables. The peer-to-peer network connects via plug-and-play up to 64 nodes in ring, star or bus topology. MOST offers, similarly to FlexRay, two freely configurable, static and dynamic time segments for the synchronous (up to 24 Mbit/s) and asynchronous (up to 14 Mbit/s) data transmission, as well as a small control channel. The control channel allows MOST devices to request and release one of the configurable 60 data channels. Unlike most automotive bus systems, MOST messages always include a clear sender and receiver address. Access control during synchronous and asynchronous transmission is realized via TDM (Time Division Multiplex) respectively CSMA/CA. The error management is handled by an internal MOST system service, which detects errors over parity bits, status flags and checksums and disconnects erroneous nodes if necessary.

Bluetooth: Originally developed to unify different technologies like computers and mobile phones, Bluetooth is a wireless radio data transmission standard in the license-free industrial, scientific, and medical (ISM) band at 2.45 GHz. It enables wireless ad-hoc networking of various devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, and digital cameras for transmitting voice and data over short distances up to 100 meters. Primarily designed as a low-cost transceiver microchip with low power consumption, it reaches data rates of up to 0.7 Mbit/s. Within the limited multi-master capable architecture, so-called Piconets, single Bluetooth devices can maintain up to seven point-to-point or point-to-multipoint connections. Bluetooth includes optional security mechanisms for authentication and confidentiality of messages at the link layer. Table 3 gives an overview of the characteristics of the five representative automotive bus systems.

2.4 Bus Interconnections

For network spanning communication, automotive bus systems require appropriate bridges or gateways to transfer messages among each other despite their different physical and logical operating properties. Gateways read and write all the different physical interfaces and manage the protocol conversion, error protection and message verification. Depending on their application area, gateways include sending, receiving and/or translation capabilities as well as some appropriate filter mechanisms. While so-called super gateways centrally interconnect all existing bus systems, local gateways link only two different

Table 3. Properties of selected automotive bus systems [14, 24, 5, 9, 17]

Bus	**LIN**	**CAN**	**FlexRay**
Adapted for	Low-level subnets	Soft real-time	Hard real-time
Target application examples	Door locking Climate regulation Power windows Light, rain sensor	Antilock break system Driving assistants Engine control Electronic gear box	Break-by-wire Steer-by-wire Shift-by-wire Emergency systems
Architecture	Single-master	Multi-master	Multi-master
Access control	Polling	CSMA/CA	TDMA FTDMA
Transfer mode	Synchronous	Asynchronous	Synchronous Asynchronous
Data rate	20 kbit/s	1 Mbit/s	10 Mbit/s
Redundancy	None	None	2 Channels
Error protection	Checksum Parity bits	CRC Parity bits	CRC Bus Guardian
Physical layer	Single-wire	Dual-wire	Dual-wire, Optical fiber
Security	None	None	None

	MOST	**Bluetooth**
Adapted for	Multimedia	External communication
Target application examples	Entertainment Navigation Information services Mobile Office	Telematics Electronic toll Internet Telediagnosis
Architecture	Multi-master	Multi-master
Access control	TDM CSMA/CA	TDMA TDD
Transfer mode	Synchronous Asynchronous	Synchronous Asynchronous
Data rate	24 Mbit/s	720 kbit/s
Redundancy	None	79 Frequencies
Error protection	CRC System Service	CRC FEC
Physical layer	Optical fiber	Air
Security	None	WEP

bus systems together. Therefore, super gateways require some kind of sophisticated software and plenty of computing power in order to accomplish all necessary protocol conversions, whereas local gateways realize only the hard- and software conversion between two different bus backbones.

3 Exposures of Automotive Bus Systems

Ever since electronic devices were installed into cars, they have been a feasible target for malicious attacks or manipulations. Mileage counter manipulation [15, 16], unauthorized chip tuning or tachometer spoofing [1] are already common. Further possible electronic automotive applications like digital tachograph, electronic toll and electronic license plate or paid content and information services such as *Digital Rights Management* (DRM) or *Location Based Services* (LBS) increase the incentive for manipulating automobile electronics. Above all, unauthorized vehicle modifications can compromise particularly the driving safety of the respective car and of all surrounding road users. Besides

the most obvious attacker, the car owner, also garage employees (mostly on behalf of the car owner) and third parties such as competing manufacturers or other unauthorized persons and institutions may have incentives for attacks. Moreover, in contrast to most common computer networks, the car owner and the garage personnel have full physical access to all transmission media and affected devices of the automotive network. As the car owner normally has only low theoretical and technical capabilities, garage personnel and some external third parties may have both adequate background knowledge and the appropriate technical equipment, for feasible intrusions. This allows deep and above all permanent manipulation of the automobile electronics. Possible motivations of third parties for breaking into automotive networks may be attacks on the passenger's privacy (phone tapping, data theft) or well-directed attacks on particular vehicle components in the case of a theft or even a potential assault. Table 4 briefly represents the three groups of potential attackers and their respective capabilities. Apparently, technically sophisticated garage employees, acting on the owners instructions, are the most dangerous attacker group. Many analyses [2, 20, 21, 7] can verify the safety and reliability of ve-

Table 4. Attackers in the automotive area based on [18]

Attacker	Capabilities	Physical access
Car owner	Varied (generally low)	Full
Garage personnel	High	Full
Third party	Varied (may be high)	Feasible

hicle networks against random failures. Analyses that consider also intended malicious manipulations, i.e. discuss vehicular communication security, are still very rare [13, 23]. Thus, most existing automotive communication systems are virtually unsecured against malicious encroachments. Several factors make it difficult to implement security in the vehicular area. So far, safety has been the most crucial factor and therefore security has been only an afterthought. Automotive resource constraints, the multitude of involved parties and insufficient cryptographic knowledge cause additional difficulties when implementing appropriate precautions. Moreover, security may need additional hardware and infrastructures, may cause considerable processing delays and particularly generates extra costs, without apparent benefits. Nonetheless, vehicle electrification and in-car networking proceed unimpaired and the lack of security becomes an increasingly serious risk, so the emerging challenge in automotive communication is to provide security, safety and performance in a cost-effective manner.

Many typical characteristics of current automotive bus systems enable unauthorized access relatively easy. All communication between controllers is done completely unencrypted in plain text. Possible bus messages, their respective structures and communication procedures are specified in freely

available documents for most vehicle busses. Furthermore, controllers are not able to verify if an incoming message comes from an authorized sender at all. Nevertheless, the major hazard originates from the interconnection of all the car bus systems with each other. The net-spanning data exchange via various gateway devices, potentially allows access to any vehicular bus from every other existing bus system. In principle, each LIN, CAN or MOST controller is able to send messages to any other existing car controller. Hence, without particular preventive measures, a single comprised bus system endangers the whole vehicle communication network. In combination with the increasing integration of miscellaneous wireless interfaces, future attacks on automotive communication systems can be accomplished without contact, just by passing a car or via cellular phone from almost anywhere in the world. Breaking away the electronic mirror and connecting to the underlying LIN network with a mobile computer could already be a possible promising way to break into an expensive car today. In the next generation image-processing assistance for autonomous driving systems such as lane tracking or far field radar will access high safety-relevant vehicular driving systems based on information from external databases received via known, but quite insecure wireless links. Besides this, interconnections of multimedia busses like MOST and D2B, with the control network of the vehicle, enable software programs such as viruses or worms, received over inserted CD/DVDs, email messages or possibly attached computers, also to penetrate highly safety-relevant vehicular systems. Even if today modern gateways already include simple firewall mechanisms, most of them offer unprotected powerful diagnostic functions and interfaces that allow access to the whole car network without any restrictions. The consequences of successful attacks range from minor comfort problems to the the risk of an accident. Therefore, the probability of an attack and the level of security required in a given bus system depend on the potential consequences of loss or manipulation. As shown in Table 5, whereas attacks on LIN or multimedia networks may result in the failure of power windows or navigation software, successful attacks on CAN networks may result in malfunction of some important driving assistants that leads to serious impairments in driving safety. A successful systematic malfunction on real-time busses like FlexRay, which handle elementary driving commands like steering or breaking, can lead to acute hazards for the affected passengers and other surrounding road users. Nonetheless, also just a simple malicious car locking may have serious consequences for passengers [3]. In the following, we describe some feasible attacks on the protocol layer of the representative car bus systems described in Section 2. In doing so we assume we have either direct physical or logical access to the corresponding vehicle network. Physical access means a direct interconnection with the respective communication wires, whereas logical access means exploiting another (existing or deployed) controller or misusing the diagnosis or even a wireless interface [19].

Table 5. Endangerment of selected automotive bus systems

Group	*Subbus*	*Event-triggered*	*Time-triggered*	*Multimedia*	*Wireless*
Exemplar	LIN	CAN	FlexRay	MOST	Bluetooth
Exposure	Low	High	Acute	Low	Varied
Possible harms	Lessened functionality	Lessened driving safety	Risk of accident	Data theft, Lack of comfort	Unauthorized external access

LIN: Utilizing the dependency of the LIN slaves on their corresponding LIN master, attacking this single point of failure, will be a most promising approach. Introducing well-directed malicious sleep frames deactivates completely the corresponding subnet until a wake-up frame posted by the higher-level CAN bus restores the correct state again. The LIN synchronization mechanism can be another point of attack. Sending frames with bogus synchronization bytes within the SYNCH field makes the local LIN network inoperative or causes at least serious malfunctions. LIN is unprotected against forged messages.

CAN: The priority-driven CSMA/CD access control method of CAN network enables attacks that jam the communication channel. Constantly introduced topmost priority nonsense messages will always be forwarded first (even though they will be immediately discarded by the receiving controllers) and permanently prevent the transmission of all other CAN messages. Moreover, utilizing the CAN mechanisms for automatic fault localization, malicious CAN frames allow the disconnection of every single controller by posting several well-directed error flags. Furthermore, CAN is vulnerable to forged messages.

FlexRay: Similar to the CAN automatic fault localization, FlexRay's so-called bus guardian can be utilized for the well-directed deactivation of any controllers by appropriate faked error messages. Attacks on the common time base, which would make the FlexRay network completely inoperative, are also feasible, if within one static communication cycle more than f [1] malicious SYNC messages are posted into a FlexRay bus. Moreover, introducing well-directed bogus sleep frames deactivates corresponding power-saving capable FlexRay controllers. FlexRay is also vulnerable to forged messages.

MOST: Since in a MOST network one MOST device handles the role of the timing master, which continuously sends timing frames that allow the timing slaves to synchronize, malicious timing frames are suitable for disturbing or interrupting the MOST synchronization mechanism. Moreover, continuous bogus channel requests, which reduce the remaining bandwidth to a minimum, are a feasible jamming attack on MOST busses. Manipulated false bandwidth statements for the synchronous and asynchronous area within the boundary

[1] $f \geq n/3$, where n is the number of existing FlexRay nodes. Further reading in [31]

descriptor of a MOST frame can also make the network completely inoperative. Due to the utilized CSMA/CD access control method used within the asynchronous and the control channel, both are vulnerable to jamming attacks similar to CAN. MOST is also vulnerable to forged messages.

Bluetooth: Wireless interconnections imply a distinct security disadvantage over wired communications in that all information is broadcast over an open, easily tapping-capable air link. Although Bluetooth transmissions can be configured to be encrypted, there exist various feasible attacks [27, 4, 11]. Actually, even first worms and viruses begin infecting Bluetooth devices wirelessly [8, 29].

4 Approaches to Security

Many future vehicular applications will require high end-to-end communication security as enabling environment. It is then important that all transferred information can be seen and received in clear only by the desired parties, that potential modifications are impossible to conceal and that unauthorized parties are not able to participate in vehicular communication. Modern communication security mechanisms provide confidentiality, integrity and authentication based on cryptographic algorithms and protocols, to solve most of the car security problems. The uncontrolled interference of the vehicle communication networks can be prevented by a bundle of measures. In the following, we show three elementary practices to achieve vehicular bus communication security.

4.1 Controller Authentication

Authentication of all senders is needed to ensure that only valid controllers are able to communicate within automotive bus systems. All unauthorized messages may then be processed separately or are just immediately discarded. Therefore, every controller needs a certificate to authenticate itself against the gateway as a valid sender. A certificate consists of the controller identifier ID, the public key PK and the authorizations $Auth$ of the respective controller. The gateway in turn securely holds a list of public keys PK_{OEM} of all accredited OEMs (Original Equipment Manufacturers) of the respective vehicle. Each controller certificate is digitally signed by the OEM with its respective secret key SK_{OEM}. As shown in Table 6, the gateway again uses the corresponding public key of the OEM to verify the validity of the controller certificate. If the authentication process succeeds, the respective controller is added to the gateway's list of valid controllers.

4.2 Encrypted Communication

A fundamental step to improve the security of automotive bus communication is the encryption of all vehicular data transmission. Due to the particular

Table 6. Controller authentication

Authentication	
1.$Verify(Sig, PK_{OEM})$	`Verify` Sig `with corresponding OEM public key` PK_{OEM}
2.$ID, Auth$	`Save controller properties, if verification succeeds`
2.$C = E_{PK}(K_i)$	`Send corresponding symmetric bus group key` K_i

constraints of automotive bus communication systems (computing power, capacity, timing, ...), a combination of symmetric and asymmetric encryption meets the requirements on adequate security and high performance. Whereas fast and efficient symmetric encryption secures the bus-internal broadcast communication, asymmetric encryption is used to handle the necessary secure key distribution. In that case, all controllers of a local bus system share the same, periodically updated, symmetric key to encrypt their bus-internal communication. Asymmetric encryption provides the acquisition of the symmetric key for newly added authorized controllers and carries out the periodic symmetric key update, as well as the required authentication process. In our

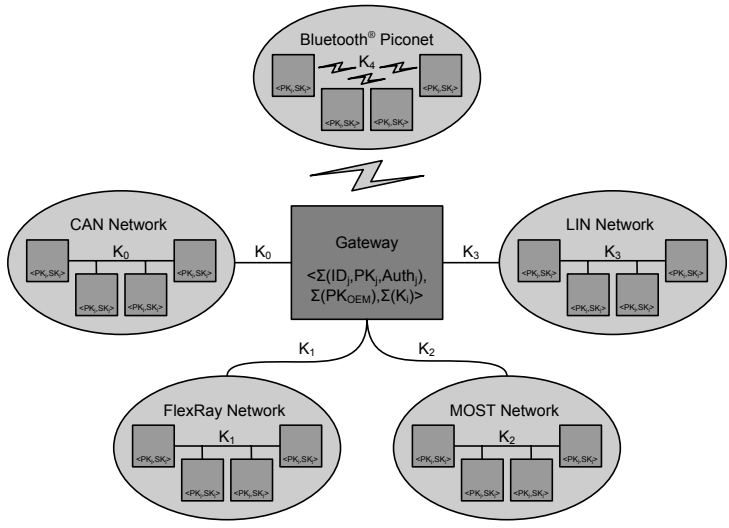

Fig. 2. Secure vehicular communication

example implementation shown in Fig. 2, a centralized super gateway processor connects all existing bus systems with each other. Therefore, all inter-bus communication is done exclusively only over the gateway processor. Moreover, the gateway has a protected memory area to securely store (tamper-resistant) the secret keys and the list of valid controllers together with their respective

authorizations $Auth$. The application of so-called trusted computing modules [28] can provide such particular secured memory portions. In our example, every successful verified bus controller holds the symmetric bus group key K_i as well as its own public and secret key pair PK_j, SK_j and the public key of the gateway PK_G. The gateway itself stores the certificates of each valid controller node as well as each bus-internal group key K_i for fast inter-bus communication. As all internal bus data is encrypted by K_i, only controllers that possess a valid K_i are able to decrypt and read all local broadcast bus messages. Since the centralized gateway holds the symmetric keys of every connected bus system, fast and secure inter-bus communication between valid controller nodes is provided. As shown in Table 7, every controller may optionally also receive a symmetric authentication key K_j from the gateway, to provide message integrity and sender authentication. If so, each controller could append a message authentication code (MAC) to every message, i.e. the respective hash value $H(M)$ encrypted with its personal authentication key K_j. Even though an asymmetric digital signature scheme could accomplish this task as well without additional authentication keys, it would probably exceed the timing requirements and the computing power of most automotive controllers. Table 8 shows the receipt of encrypted message C by a controller or

Table 7. Secured message sending with MAC authentication

Sending	
1. $C_1 = Enc(M, K_i)$	Encrypt message M with group key K_i
2. $MAC = Enc(H(M), K_j)$	Encrypt hash value of M with authentication key K_j
3. $C = C_1 \| \| MAC$	Send C composed of C_1 and MAC

the gateway processor. Whereas network internal controllers decrypt only the symmetric part C_1 of C, gateways have to verify also the optionally enclosed message authentication code MAC. Only if the sender verification succeeds and the sending controller has appropriate authorization does the gateway re-encrypt and forward the message into the targeted subnet. To enhance the

Table 8. Secured message receiving with MAC authentication

Receiving	
1. $M = Dec(C_1, K_i)$	Decrypt C_1 to message M with group key K_i
2. $H(M) \stackrel{?}{=} Dec(MAC, K_j)$	Verify integrity and sender of M with MAC (gateway only)
3. $Target \in Auth_j$	Forward M into target subnet if $Auth_j$ allow (gateway only)

security additionally, the gateway may initiate periodic bus group key updates. This prevents installing unauthorized controllers using a compromised

K_i or SK_j. To inform all controllers of a bus system, the gateway broadcasts for each controller on its current list of valid controllers a message encrypted with the respective public key PK_j of each controller. When every controller has decrypted its key update message with its secret private key SK_j, a final broadcast of the gateway may activate the new symmetric bus group keys.

4.3 Gateway Firewalls

For completing vehicular bus communication security, gateways should implement capable firewalls. If the vehicular controllers are capable of implementing MACs or digital signatures, the rules of the firewall are based on the authorizations given in the certificates of every controller. Therefore, only authorized controllers are able to send valid messages into (high safety-relevant) car bus systems. If the vehicular controllers do not have the abilities to use MACs or digital signatures, the rules of the firewall can be established only on the authorizations of each subnet. However, controllers of lower restricted networks such as LIN or MOST should generally be prevented from sending messages into high safety-relevant bus systems as CAN or FlexRay. Moreover, diagnostic functions and messages as well as all diagnostic interfaces, normally used only for analyses in garages or during manufacturing, should be disabled completely by authorized garage personnel to be inaccessible during normal driving operation.

5 Summary and Outlook

In this work, we have briefly presented current and future vehicular communication systems and pointed out several bus communication security problems. We presented an approach that uses modern communication security mechanisms to solve most of the local vehicular communication security problems. We expect that multimedia busses and wireless communication interfaces will soon be available in most modern automobiles. As already occurs now on the Internet, malicious attackers should not be underestimated and are most definitely a real existing threat. Even if a single successful attack causes only minor hazards for passengers it may seriously jeopardize public confidence in a brand [25]. Since future automotive systems and business models particularly depend on comprehensive and efficient measures that provide vehicular communication security, adequate technical, organizational and financial expenditures have to be arranged today.

References

1. Ross J. Anderson. On the security of digital tachographs. In *ESORICS '98: Proceedings of the 5th European Symposium on Research in Computer Security*, pages 111–125, London, UK, 1998. Springer-Verlag.
2. M. Baleani, A. Ferrari, L. Mangeruca, A. Sangiovanni-Vincentelli, M. Peri, and S. Pezzini. Fault-tolerant platforms for automotive safety-critical applications, 2003.
3. Bangkok Post. Computer traps thailand's finance minister Suchart. *Bangkok Post*, May 19 2003.
4. Bundesamt für Sicherheit in der Informationstechnik. Bluetooth – Gefährdungen und Sicherheitsmaßnahmen, 2003.
5. CAN in Automation. Website. `www.can-cia.org`, 2005.
6. T. Dohmke. Bussysteme im Automobil CAN, FlexRay und MOST. Master's thesis, TU Berlin, March 2002.
7. Richard Evans and Jonathan D. Moffett. Derivation of safety targets for the random failure of programmable vehicle based systems. In *SAFECOMP*, pages 240–249, 2000.
8. F-Secure. Bluetooth worm Cabir. `www.f-secure.com/v-descs/cabir.shtml`, 2004.
9. FlexRay Group. FlexRay main specifications. `www.flexray.com`, 2005.
10. H. Heinecke, A. Schedl, J. Berwanger, M. Peller, V. Nieten, R. Belschner, B. Hedenetz, P. Lohrmann, and C. Bracklo. FlexRay – ein Kommunikationssystem für das Automobil der Zukunft. *Elektronik Automotive*, September 2002.
11. Markus Jakobsson and Susanne Wetzel. Security weaknesses in bluetooth. In *CT-RSA 2001: Proceedings of the 2001 Conference on Topics in Cryptology*, pages 176–191, London, UK, 2001. Springer-Verlag.
12. R. Kraus. Ein Bus für alle Fälle. *Elektronik Automotive*, January 2002.
13. Andreas Lang and Jana Dittmann. Steigende Informationstechnologie: Sicherheitsrisiko im Fahrzeugbau. In Erhard Plödereder, Hubert Keller, Hans von Sommerfeld, Peter Dencker, Michael Tonndorf, and Francesca Saglietti, editors, *Automotive – Safety & Security 2004 -Ű Sicherheit und Zuverlässigkeit für automobile Informationstechnik*, LNI, pages 21–33, Aachen, September 2004. GI, Shaker Verlag.
14. LIN Consortium. LIN main specifications. `www.lin-subbus.de`, 2005.
15. Maximilian Maurer. Tachomanipulation – Jungbrunnen aus dem Laptop. *ADAC Presseservice*, March 2005.
16. Mosen Automobilelektronik. Company website. `www.tachoteam.de`, 2005.
17. MOST Cooperation. MOST main specifications. `www.mostnet.org`, 2005.
18. Christof Paar. Eingebettete Sicherheit im Automobil. In *Embedded Security in Cars Conference*, Cologne, Germany, November 2003. GITS AG.
19. Jan Pelzl and Thomas Wollinger. Security Aspects of Mobile Communication Systems. In *this book*.
20. M. Plankensteiner. Sicherheit beim Bremsen und Lenken. *Elektronik Automotive*, September 2002.
21. S. Poledna, G. Stöger, R. Schlatterbeck, and M. Niedersüß. Sicherheit auf vier Rädern. *Elektronik Automotive*, October 2001.
22. M. Randt. Bussysteme im Automobil. ECT Workshop Augsburg, 2002.

23. Maxim Raya and Jean-Pierre Hubaux. The security of vehicular networks. Technical report, Laboratory for Computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland, March 2005.
24. Robert Bosch GmbH. CAN main specifications. `www.can.bosch.com`, 2005.
25. A. Rother. *Krisenkommunikation in der Automobilindustrie - Eine inhaltsanalytische Studie am Beispiel der Mercedes-Benz A-Klasse.* PhD thesis, Neuphilologische Fakultät, Universität Tübingen, November 2003.
26. B. Rucha and G. Teepe. LIN - local interconnect network. *Elektronik Automotive*, January 2003.
27. Yaniv Shaked and Avishai Wool. Cracking the bluetooth PIN. `www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html`, 2005.
28. Trusted Computing Group. TPM main specifications. `www.trustedcomputinggroup.org`, 2005.
29. Unknown. Handyviren - Der Ernstfall wird wahrscheinlicher. *Spiegel Online*, 2004.
30. U. Weinmann. Anforderungen und Chancen automobilgerechter Softwareentwicklung. In *3. EUROFORUM-Fachkonferenz*, Stuttgart, Germany, July 2002.
31. J.L. Welch and N. Lynch. A new fault-tolerant algorithm for clock synchronization. In *Information and Computation*, volume 77 of *Information and Computation*, pages 1–36, April 1988.
32. T. Zeller and N. Meyersohn. Can a virus hitch a ride in your car? *New York Times*, March 13 2005.

http://www.springer.com/978-3-540-28384-3

Embedded Security in Cars
Securing Current and Future Automotive IT Applications
Lemke, K.; Paar, C.; Wolf, M. (Eds.)
2006, X, 273 p., Hardcover
ISBN: 978-3-540-28384-3