Security in Automotive Bus Systems

Marko Wolf, André Weimerskirch, and Christof Paar

escrypt GmbH, Bochum, Germany
{mwolf, aweimerskirch, cpaar}@escrypt.com

Abstract: This work presents a study of current and future 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, attacks, encryption, authentication, LIN, CAN, FlexRay, MOST, Bluetooth

1 Introduction

The progress in automotive electronics proceeds still unabatedly (Table 1). Today modern cars already 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 the engine control. Cars that are moreover equipped with driving aid systems like ESP (Electronic Stability Program) 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 current 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.

We begin in Section 2 by introducing well-known established automotive communication systems with respective one representative for each basic group of vehicular

Electronic fuel injection	Electronic gear box	Airbag	Drive-by-Wire
Electronic control panel	Antilock break system	Electronic Navigation	Internet
Centralized door locking	Automatic climate regulation	Electronic driving assistance	Telematics
Cruise control	Automatic mirror	Electronic traffic guidance	Ad-hoc networks
	Car phone	Voice control	Personalization
1970s	**1980s**	**1990s**	**2000s**

Table 1: *Development of automotive electronics based on [We02]*

communication systems. We briefly describe technical properties of every representative (Section 2.1) and introduce two methods for vehicular bus interconnections (Section 2.2). Section 3 presents various exposures to automotive bus systems. We indicate possible attackers and present feasible attacks for each representative bus system. In the final Section 4, we offer elementary approaches to improve automotive bus communication security along with a practical example implementation.

2 Automotive Bus Systems

Today, a wide variety of vehicle communication systems is already used in the automotive area. Possible applications range from electronic engine control, several driving assistants and safety mechanisms up 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.

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

Table 2: *Grouping of selected automotive bus systems*

Local sub networks such as LIN (Local Interconnect 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, TT-CAN (Time-Triggered CAN) or TTP (Time-Triggered Protocol) guarantee determined transmission times for controller communication and therefore can be applied in highly safety relevant 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 more and more expand also into the automotive area. They enable the internal vehicle network to communicate with external devices surrounding the car as well as the reception of various broadcast stations (Location Based Services).

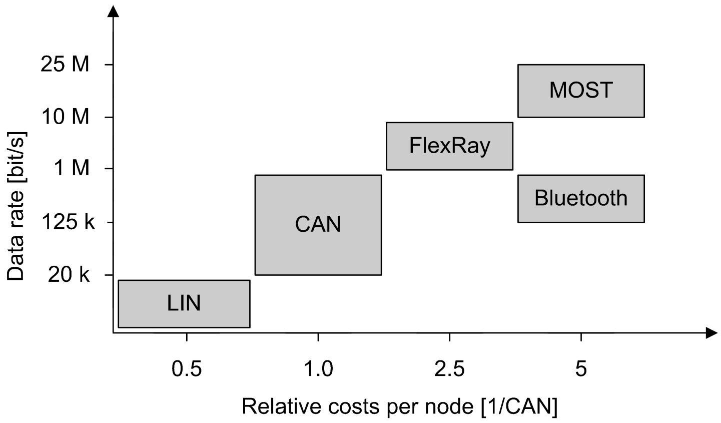

Figure 1: *Data rates and relative costs of automotive bus systems*

2.1 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 readings can be found in [Do02, He02, Kr02, Ra02, RT03].

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 defect. CAN messages do not have a recipient address, but are classified over their respective identifier. Therefore, CAN controller broadcast their messages to all connected nodes and all receiving nodes 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 every time the transmission of the top priority message always first. In order to employ CAN also 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.

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 on everywhere in a car, where the bandwidth and versatility of a CAN network is not required. A single master controls the hence collision-free communication with up to 16 slaves, optionally including time synchronization for nodes without a stabilized time base. LIN is similarly to CAN a receiver-selective bus system. Incorrect transferred LIN messages are detected and discarded by the means of parity bits and a checksum. Beside the normal operation mode, LIN nodes provide also a sleep mode with lower power consumption, controlled by special sleep respectively wake-up message.

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, point-to-point or over a classical bus structure connected, nodes. As 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 the priority-driven control of asynchronous and synchronous transmission of non-time-critical respectively 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 include always 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 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, so-called Piconets, single Bluetooth devices can maintain up to seven point-to-point or point-to-multipoint connections, optionally also encrypted.

Following Table 3 gives an overview of the characteristics of the five representative automotive bus systems.

Bus	**LIN**	**CAN**	**FlexRay**	**MOST**	**Bluetooth**
Adapted For	Low-level Subnets	Soft Real-Time	Hard Real-Time	Multimedia Telematics	External Communication
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	Entertainment Navigation Information services Mobile Office	Telematics Electronic toll Internet Telediagnosis
Architecture	Single-Master	Multi-Master	Multi-Master	Multi-Master	Multi-Master
Access Control	Polling	CSMA/CA	TDMA FTDMA	TDM CSMA/CA	TDMA TDD
Transfer Mode	Synchronous	Asynchronous	Synchronous Asynchronous	Synchronous Asynchronous	Synchronous Asynchronous
Data Rate	20 kBit/s	1 MBit/s	10 MBit/s	24 MBit/s	720 kBit/s
Redundancy	None	None	2 Channels	None	79 Frequencies
Error Protection	Checksum Parity bits	CRC Parity bits	CRC Bus Guardian	CRC System Service	CRC FEC
Physical Layer	Single-Wire	Dual-Wire	Optical Fiber Dual-Wire	Optical Fiber	Air

Table 3: *Properties of selected automotive bus systems*

2.2 Bus Interconnections

For network spanning communication, automotive bus systems require appropriate bridges or gateways processors to transfer messages among each other despite their different physical and logical operating properties. Gateways processors read and write all the different physical interfaces and have to 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 interconnect centralized all existing bus systems, local gateways are linking only two different 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 are installed into cars, they were also always a feasible target for malicious attacks or manipulations. Mileage counter manipulation [Mos04], unauthorized chip tuning or tachometer spoofing [An98] are already common, whether still more harmless practiced examples. Further possible electronic automotive applications like digital tachograph, electronic toll and electronic license plate or paid information services (Location Based Services) 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 accordingly instructed garage employees and third parties such as competing manufactures or other unauthorized persons and institutions may have reasonable attacking intents. Moreover, in contrast to most common computer networks, the car owner and the garage personnel have full physical access to all transmission media and respective 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 in 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, technical sophisticated garage employees, acting on the owners instructions, are the most dangerous attacker group.

Attacker	Capabilities	Physical Access
Car owner	Varied (generally low)	Full
Garage personnel	High	Full
Third party	Varied (maybe high)	Limited or None

Table 4: *Attackers in the automotive area based on [Pa03]*

While current analyses [Pl02, Po01] can verify the safety and reliability of vehicle networks against random failures, most existing automotive communication systems are virtually unsecured against malicious encroachments. Several reasons make it difficult to implement security in the vehicular area. So far, safety was the most crucial factor and therefore security was 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 proceeds unimpaired and the lack of security becomes more and more a 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 the most vehicle buses. 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, allows potentially access to any vehicular bus out of 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 contactless, 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 be a possible promising way to break into an expensive car today already. Next generation future image-processing assistances for autonomous driving systems such as lane tracking or far field radars access high safety-relevant vehicular driving systems based on information from external data bases received via known quite insecure wireless links. Besides this, interconnections of multimedia buses like MOST, D2B with the control network of the vehicle, enables software programs such as viruses or worms, received over inserted CD/DVDs, email messages or possibly attached computers, to penetrate also highly safety-relevant vehicular systems. Even if today modern gateways already include simple firewall mechanism, 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 restraints up to the risk of an accident. Therefore, the probability of an attack and the level of security required in a given bus system depends 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 of the driving safety. A succeeded systematic malfunction on real-time buses like FlexRay, which handle elementary driving commands like steering or breaking, can lead in acute hazards for the affected passengers and other surrounding road drivers. Nonetheless, also just a simple malicious car locking may have serious consequences for passengers [BaP03].

Group	Subbus	Event-triggered	Time-triggered	Multimedia	Wireless
Representative	LIN	CAN	FlexRay	MOST	Bluetooth
Exposure	Little	Big	Acute	Little	Varied
Possible Harms	Lessened functionality	Lessened driving safety	Risk of accident	Data theft, Lack of comfort	Unauthorized data access

Table 5: *Endangerment of selected automotive bus systems*

In the following, we describe some feasible attacks on the protocol layer of the representative car bus systems described in Section 2, assuming that we have physical or logical access to the corresponding vehicle network.

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 wakeup 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.

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 be forwarded always first (even though they will immediately discarded by the receiving controllers) and prevent permanently 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.

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.

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 buses. Manipulated false bandwidth statements for the synchronous and asynchronous area within the boundary 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.

Bluetooth: Wireless interconnections imply a distinct security disadvantage over wired communications in that all information is broadcasted over an open, easily tapping-capable air link. Although, Bluetooth transmissions are at least simple encrypted, there exist various feasible attacks [Ast03, BSI03, JS01]. Actually, even first worms and viruses begin infecting Bluetooth devices wirelessly [Cab04, Spg04].

4 Approaches to Security

Most future vehicular applications require high end-to-end communication security as enabling environment. It is generally important that all transferred information

[1] $f \geq n/3$, where n is the number of existing FlexRay nodes. Further reading in [WL88]

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 secrecy, manipulation prevention and authentication based on cryptographic algorithms and protocols, to solve most of the car security problems. The uncontrolled interference of the vehicle communications networks can be prevented by a series of measurements. 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 processed separately or 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 Manufacturer) 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.

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

Table 6: *Controller authentication*

4.2 Encrypted Communication

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

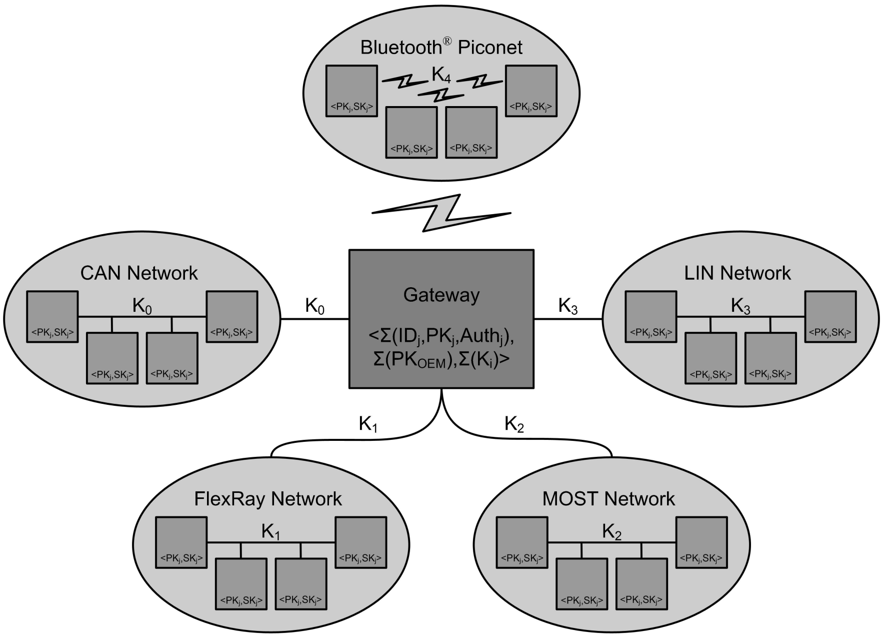

Figure 2: *Secure vehicular communication*

In our example implementation shown in Figure 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 store securely (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 (TPM) 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 and of every 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 posses a valid K_i are able to decrypt and read all local broadcasted 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 include a digital signature S_M, to provide message integrity and sender authentication. On the other hand, it is also possible to provide message integrity utilizing an asymmetric message authentication code (MAC) [Ca99].

Table 8 shows the receipt of encrypted message C by a controller or the gateway processor. Whereas network internal controllers decrypt only the symmetric part C_1 of C, gateways have to verify also the optionally enclosed signature S_M. Only if the sender verification succeeds and the sending controller has appropriate authorizations, the gateway forwards the message encrypted again into the targeted subnet.

Sending	
1.$C_1 = Encrypt(M, K_i)$	Encrypt message M with symmetric key K_i
2.$S_M = Sign(C_1, SK_j)$	Sign C_1 with secret key SK_j (optional)
3.$C = C_1 \| \| S_M$	Send C composed of C_1 and S_M (optional)

Table 7: *Secured message sending*

Receiving	
1.$M = Decrypt(C_1, K_i)$	Decrypt C_1 to message M with symmetric key K_i
2.$Verify(S_M, PK_j)$	Verify S_M with public key PK_j (gateway only)
3.$Target \in Auth_j$	Forward M into target subnet if $Auth_j$ allow (gateway only)

Table 8: *Secured message receiving*

To enhance the security additionally, the gateway may initiate periodic bus group key updates. This prevents installing unauthorized controllers using a compromised K_i. To inform all controllers of a bus system, the gateway broadcasts for each controller on its 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 key.

4.3 Gateway Firewalls

For completing vehicular bus communication security, gateways have to implement capable firewalls. If the vehicular controllers are capable to implement digital signatures or MACs, 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 digital signatures or MACs, 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 completely be disabled by the firewall, during normal driving operation.

5 Summary and Outlook

In this work, we briefly presented current and future vehicular communication systems and pointed out several bus communication security problems. We described an approach that uses modern communication security mechanisms to solve most of the local vehicular communication security problems. We expect that multimedia buses and wireless communication interfaces will be soon available in the most modern automobiles. As already happens now in the internet, malicious attackers are a not to be underestimated and most notably a real existing threat, the more so as already a single successful attack with even only minor hazards for passengers may seriously jeopardize the public confidence in a brand [Ro03]. Since future automotive systems and business models particularly depend on comprehensive and efficient measurements that provide vehicular communication security, adequate technical, organizational and finical expenditures have to be arranged today already.

References

[An98] R.J. Anderson. On the Security of Digital Tachographs. In *Lecture Notes in Computer Science, Vol. 1485, 1998, pp. 111+.*

[BSI03] Bundesamt für Sicherheit in der Informationstechnik. Bluetooth - Gefährdungen und Sicherheitsmaßnahmen. In `www.bsi.de/literat/doc/bluetooth/bluetooth.pdf`, *2003.*

[Ca99] R. Canetti, J. Garay, G. Itkis, D. Miccianicio, M. Naor, B. Pinkas. Multicast Security: A Taxonomie and Some Efficient Constructions. In *Proceedings of IEEE INFOCOM '99, New York, USA , March 1999.*

[Do02] T. Dohmke. Bussysteme im Automobil CAN, FlexRay und MOST. In *Entwicklung verteilter eingebetteter Systeme, TU Berlin, March 2002.*

[He02] H. Heinecke, A. Schedl, J. Berwanger, M. Peller, V. Nieten, R. Belschner, B. Hedenetz, P. Lohrmann und C. Bracklo. FlexRay - ein Kommunikationssystem für das Automobil der Zukunft. In *Elektronik Automotive 09/2002.*

[JS01] M. Jakobsson, S. Wetzel. Security Weaknesses in Bluetooth. In *Lecture Notes in Computer Science, Vol. 220, 2001, pp. 176+.*

[Kr02] R. Kraus. Ein Bus für alle Fälle. In *Elektronik Automotive 01/2002.*

[Pa03] C. Paar. Eingebettete Sicherheit im Automobil. In *Konferenz „Embedded Security in Cars (ESCAR)“, Köln, November 2003.*

[Pl02] M. Plankensteiner. Sicherheit beim Bremsen und Lenken. In *Elektronik Automotive 09/2002.*

[Po01] S. Poledna, G. Stöger, R. Schlatterbeck, M. Niedersüß. Sicherheit auf vier Rädern. In *Elektronik Automotive 10/2001.*

[Ra02] M. Randt. Bussysteme im Automobil. In *ECT Workshop Augsburg, 2002.*

[Ro03] A. Rother. Krisenkommunikation in der Automobilindustrie - Eine inhaltsanalytische Studie am Beispiel der Mercedes-Benz A-Klasse. In *Dissertation an der Neuphilologischen Fakultät der Universität Tübingen, Tübingen, November 2003.*

[RT03] B. Rucha, G. Teepe. LIN - Local Interconnect Network. In *Elektronik Automotive 01/2003.*

[We02] U. Weinmann. Anforderungen und Chancen automobilgerechter Softwareentwicklung. In *3. EUROFORUM-Fachkonferenz, Stuttgart, July 2002.*

[WL88] J.L. Welch, N. Lynch. A new fault-tolerant algorithm for clock synchronization. In *Information and Computation, Vol. 77, No. 1, April 1988. pp. 1 - 36.*

[Ast03] stake Security Consulting Inc. Webpage, 2003. `www.atstake.com/events_news/press_mentions/press_mentions_2003.html`.

[BaP03] Computer traps Thailand's Finance Minister Suchart. Webpage, May 19, 2003. `www.bangkokpost.com`.

[Cab04] F-Secure Virus Description: Bluetooth worm Cabir. Webpage, 2004. `www.f-secure.com/v-descs/cabir.shtml`.

[LIN04] LIN Consortium. Webpage, 2004. www.lin-subbus.de.

[BC04] BOSCH CAN. Webpage, 2004. www.can.bosch.com.

[CIA04] CAN in Automation. Webpage, 2004. www.can-cia.org.

[FL04] FlexRay Group. Webpage, 2004. www.flexray.com.

[MO04] MOST Cooperation. Webpage, 2004. www.mostnet.org.

[Mos04] Mosen Automobilelektronik Webpage, 2004. www.tachoteam.de.

[Spg04] Handyviren: Der Ernstfall wird wahrscheinlicher. Webpage, 2004. www.spiegel.de/netzwelt/technologie/0,1518,310953,00.html.

[VI04] Vector Informatik. Webpage, 2004. www.vector-informatik.de.