Attacks on Inter Vehicle Communication Systems - an Analysis

Amer Aijaz[1], Bernd Bochow[2], Florian Dötzer[3], Andreas Festag[4],
Matthias Gerlach[2], Rainer Kroh[5] and Tim Leinmüller[5]
[1]Volkswagen AG, Konzernforschung Elektroniksysteme, Amer.Aijaz@volkswagen.de
[2]Fraunhofer Institute for Open Communication Systems (FOKUS), {Bernd.Bochow|Matthias.Gerlach}@fokus.fraunhofer.de,
[3] BMW Group Research and Technology, Florian.Doetzer@bmw.de,
[4]NEC Europe, Andreas.Festag@netlab.nec.de,
[5]DaimlerChrysler AG, Research Vehicle IT and Services, {Rainer.Kroh|Tim.Leinmueller}@DaimlerChrysler.com.

***Abstract*— Inter-vehicle communication systems are a new paradigm of networking. Largely related to mobile ad hoc networks and their distributed, self-organizing structure, they also introduce new threats. In order to assess these threats we introduce a model of attacks on an inter-vehicle communication system in this paper. This model is used to refine the system model of the NoW communication system and to find potential weaknesses during the specification phase of the NoW communication system.**

Our work shows that there are several interesting new challenges requiring novel solutions, some of which are outlined at the end of this paper. Although this is still work in progress, it is the foundation for analysis and assessment of future work.

As one of the main results of this paper, we identified several difficult to detect attacks on the hard- and software, and on the sensor input. We further point out system requirements to thwart such attacks.

I. Introduction

Inter-vehicle communication (IVC) and vehicle to infrastructure communication are amongst the most promising applications of mobile ad hoc networks. Therefore these mobile ad hoc networks, sometimes also referred to as vehicular ad hoc networks (VANETs), are studied in several research projects. Many applications are discussed in this context, but road traffic related messaging and local danger warning remain the most prominent ones for car-to-car communications, while car-to-home and car-to-infrastructure are the scenarios that will support the deployment of such systems.

Especially safety related applications require a secure and reliable system. Therefore, in this work we present an overview on the various possible attacks and countermeasures that have to be studied intensively. This work is considered as base for future development and analysis of security related functionalities within the NoW system model.

The remainder of this paper is organized as follows. In the next section, we discuss related work, followed by the introduction of the generic NoW system model. Then we apply the technique of attack trees in the context of vehicular ad hoc networks and the NoW system (Section III) in particular. In Section IV we discuss the results of the previous section and the resulting impact on the security system that has to be developed. Finally, Section V concludes the paper and provides an outline of future work.

A description of attack trees, the system model used in the attack analysis, and more attack trees for further applications can be found in [1]

II. Related Work

Security issues have not been a major issue in past inter-vehicle communication research projects. Among past projects, significant work has been done in VSC [2], while currently there are security working groups within the EU's 6 Framework Programme's Research Project Willwarn [3] and the German national research project NoW – Network on Wheels [4].

But inter-vehicle communications' (IVC) topics have seen rising research efforts in the past years. Contributions to security in this field have been general analyses, such as [5], [6], and [7].

Others presented approaches to solve specific problems or security objectives. Golle et al. introduced a scheme to detect malicious data in IVC [8]. Dötzer discussed privacy issues for vehicle communications in [9]. Gerlach presents a holistic approach

to VANET security in [10]. Leinmueller et al. [11] analyzed the impact of falsified position information on geographic routing.

Many papers have been written about trust establishment and decentralized key management, such as [12], [13], [14] and [15], while Kargl wrote his Dissertation about general security in mobile ad hoc networks (MANETs) [16].

III. Attack Modeling for the NoW System

In [1] we classified applications and introduced general attacks that can be found in VANET environments.

A. Attacker Model

Our threat model is based on a generic attacker model with four groups of attackers:

1) Attackers with a programmable radio transmitter/receiver.
2) Attackers with access to an un-modified NoW unit who can therefore control the inputs, sensors, etc.
3) Attackers who have access to a modified NoW unit and who have obtained the keying material.
4) "Inside" attackers who have access to records and equipment operated by the vehicle manufacturer or the NoW unit manufacturer.

B. Reusable Attack Subtrees

During attack tree construction on the current high level of attacks it seemed necessary to create reusable ("general") attack trees in order to avoid redundancy in the attack trees for each application. As the attack trees become more detailed, these general attack subtrees may turn out to be distinct as different applications introduce different kinds of vulnerabilities. In the current status of the work we stick to the general attack trees for the sake of compactness of the presentation of attacks. There are three major general subtrees:

- *Become Part of the Network* (Figure 1): once a malicious node is legitimate part of the network, it is easier for an attacker to insert malicious content or affect the network, this may be the basis for many attacks.
- *Manipulate OBU Input* (Figure 2). Manipulating this input has impact on the proper functioning of the NoW system, as many warnings are based on sensor input.
- *Violate Privacy* (Figure 3). The subtree on violating privacy summarizes the general attacks on privacy based on the NoW communication system.

1) Get Identifier
   a) Copy (NoW protocols/OBU/RSU)
   b) Steal (NoW protocols/OBU/RSU)
   c) Create (NoW protocols/OBU/RSU)
2) Have Identifier

Fig. 1
General Subtree B: Become Part of the Network.

1) Become Part of the Network: A node is part of the network once it obtained and is able use an identifier (cf. Figure 1). The principle is similar to that in DHCP[1] networks, where a node can only take part in the networking, once it obtains a (valid) IP address from the DHCP server. In this attack tree, getting or having an identifier implies that only possession of this identifier authorizes a node to take part in the communciation. Usually, this requires some sort of certification for the nodes, an aspect which has not been included in the tree for the sake of simplicity.

Stealing an identifier is like copying it and making it unusable for the victim at the same time. Assuming some sort of binding of identifiers to nodes by using public key cryptography (e.g. using certificates or identity based cryptography) copying this identifier implies either breaking the respective cryptographic primitive on the basis of overheard messages or being able to access the private information on the victims platform itself. Stealing the identifier may be harder to do using the wireless interface, but possibly be done by stealing the physical device (e.g. SIM card) attached to the NoW unit. Creating an identifier implies either knowing secret information to actually create valid key pairs and valid bindings to a certain (malicious) node. To achieve this, an attacker must be able to intrude the security infrastructure, an attack we consider hard to carry out, if this infrastructure is well protected and thought out.

2) Manipulate OBU Input: As the on board units of the NoW system will probably be installed in a place that is not easy to access, altering the sensor readings is a straightforward way to attack a system.

[1] Dynamic Host Configuration Protocol

Like this, the attacker has an OBU with a valid identifier (and credentials) and can therefore attack the network from the inside.

Manipulations of the car – in other words, tuning it – is not uncommon. It will, however, require some skills to tamper with the car electronics directly, as these systems are becoming more and more complex, and will even include cryptography-based in-vehicle network protections (cf. [17]). One of the more probable attacks of this subtree would be stressing the components, as this probably goes undetected and rather leads to a faulty car.
Changing the sensor readings can be more effective, due to the following reasons. First, the in-vehicle system will probably not detect this kind of attack since no components are touched, when for example only the temperature sensor is put into ice water. Second, a receiving vehicle would still receive authorized, valid messages, only that their content is wrong.

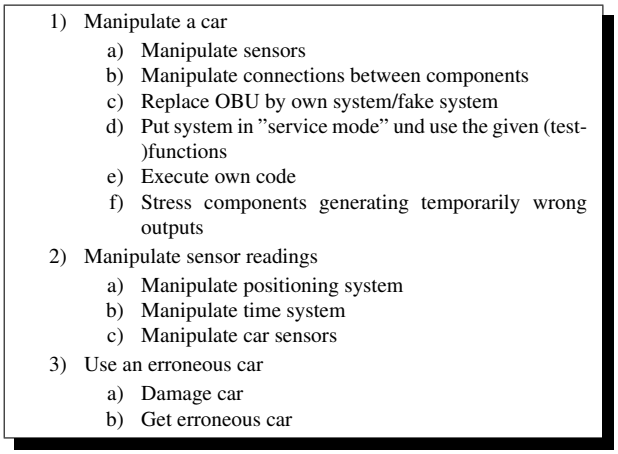

Fig. 2
GENERAL SUBTREE A: MANIPULATE OBU INPUT.

3) Violate Privacy: In Figure 3, the attacks on the privacy of the users are listed. This subtree is a general view of attacks on privacy, and will be reused for the applications in this document. Some applications in themselves be a threat to the privacy of users, such as credit card payments; we will focus on privacy violations inherent to the communication system on NoW.

Linking the identity of a user by observing his behavior is intuitively the easier and therefore more probable attack in subtree 1 in Figure 3. Observing somebody mounting his car and observing newly popping up nodes while the car is started is very easy in comparison to hacking a trusted third party (TTP) where security precautions will be high. Being that trusted third party is a completely different matter. Therefore note that a trusted third party should not be understood as a single entity, but a network of authorities.

A similar attack on privacy, i.e. revealing and tracking the location of a user requires either physical presence (at least in the radio propagation area) of the attacker or a networked grid of receivers and a database in the background. The first is an attack is feasible already by just observing a car (chasing a car by its color or number plate, or the like). The second-mentioned attack, however, would require a significant amount of money and organization to be implemented but should not be ignored. The VII (Vehicle Infrastructure Integration) project [18], currently underway in the United States could actually provide the infrastructure to deploy such a surveillance system even though its benefit for the deployment of vehicular communication is undisputed [19].

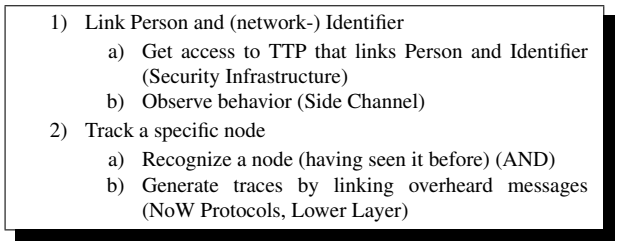

Fig. 3
GENERAL SUBTREE C: PRIVACY VIOLATIONS.

C. Attacks on Car to Car Traffic Applications

The attack trees shown in Figures 4 and 5 correspond to the specifics of car to car traffic applications. These applications exchange mainly traffic related information such as warnings of obstacles behind a curve, low visibility, etc. In addition to the general attack trees in Section III-B it can be thought of two attack subtrees: disseminate false messages and disturb system.

1) Disseminate False Messages: Figure 4 depicts the subtree for dissemination of false messages. A car to car traffic messaging system is relying on messages that are distributed by cars that experience a traffic relevant event. It is therefore critical that the messages about events are correct. An attacker can either try to generate new valid messages, replay existing messages or modify existing messages. One approach that could help to achieve either one of those

1) Generate new message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Become part of the Network (Subtree D) (AND)
   c) Inject directly
2) Replay message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Capture message (AND)
   c) Send out
3) Modify message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Capture message (AND)
   c) Break message integrity protection

Fig. 4
CAR TO CAR SUBTREE A: DISSEMINATE FALSE MESSAGES.

goals is the to attack the cryptographic system by breaking cryptographic algorithms, attacking cryptographic protocols or force the system to use less secure algorithms or protocols. We placed it in every subtree, since the specific targets are different.

Another way of generating new messages than attacking the cryptographic system would be to become part of the network by manipulating the OBU input or use manipulated / dismantled hardware AND inject false messages directly.

In order to replay a message, an attacker must capture a message and send it out without getting caught by timing protocols.

A message modification would again require to capture a message and then finding a way to break the message integrity protection.

1) Remote Incapacitation of NOW components (OBU, RSU)
   a) Generate EMP
   b) Stimulate System Malfunction
2) Suppress Communication
   a) 802.11p jamming
   b) GPS jamming (OBU Input)
   c) Inhibiting physical environment (Lower Layer)
   d) 802.11p weaknesses and flaws abuse (lower layer)
3) NoW network misbehavior
   a) Overload nodes (NoW Protocols, OBU)
   b) Disturb routing (Now Protocols)
   c) Don't participate in message forwarding / routing (NoW Protocols)
4) Application layer misbehavior
   a) Generate many false messages (NoW Protocols, OBU)
   b) Generate corrupt messages (OBU)

Fig. 5
CAR TO CAR SUBTREE B: DISTURB SYSTEM.

2) Disturb system: Figure 5 shows the attacks that lead to a crippled system. There are a couple of ways to disturb the system. Either an attackers tries to disable nodes remotely, suppresses wireless communications, exploits network vulnerabilities or abuses application level functionalities. The ultimate goal is to deny services, but even weaker forms that reduce the overall system performance may have significant effects.

Two approaches lead to the incapacitation of a node from a remote place. One is to overload the electronics by generating a electromagnetic pulse. While this seems to be a military scenario in the times of frequent terrorist attacks this may cause additional trouble in case of a critical situation. Apart from this, we have to assume that attackers may find a way to shut down systems remotely exploiting vulnerabilites.

Wireless communication is more susceptible to suppression than wired communication. In this Section by communication we mean all in- and outgoing wireless signals to and from a car that transport data packets of some kind. The most obvious way to achieve this is to jam the wireless channels, in our case either the 802.11p or the GPS system. Another variant is to set up a physical environment that hinders communication. Finally, some special weaknesses of the 802.11p protocols may be used to deny their operation.

The network's operation can be abused to overload nodes in such a way that they cannot respond as they should. Alternatively, the routing or message distribution protocols may be disturbed so that messages are not relayed properly. Some nodes may also deny to forward packets and behave in a selfish way. In a worst case this could be done in a coordinated way.

On application layer, many false messages can be produced in order to overload nodes that are busy checking these messages authenticity and integrity. Or corrupt messages may be generated that can be authenticated properly but whose content does not meet the actual situation.

IV. EVALUATION AND LESSONS LEARNED

In Section III, different attacks on different applications and components of the NoW system have been outlined. From these attacks, important characteristics of and requirements on the NoW system can be derived. A summary of those requirements is given in Table I. A more detailed discussion can be found in the following sections.

a) Plausibility Checks: As discussed in the attacks for Manipulating OBU (and RSU) input depicted in Figure 2, altering the physical environment

Applications	*Components*	*Requirement*
All	OBU, RSU	Trusted platform
All	OBU, RSU, HomePC	Firewall
All	Security infrastructure	Trust establishment and control for applications
Car to car, Car to infrastructure	OBU, RSU, NoW Protocols	Plausibility checks
Car to home	OBU, HomePC, NoW Protocols	Secure wakeup of the OBU
Car to infrastructure, Car to car	RSU	Tamper evidence mechanisms
Routing	OBU, RSU, NoW protocols	Trust establishment for NoW protocols

TABLE I
SECURITY REQUIREMENTS, COMPONENTS AND APPLICATIONS.

around the sensor for just that sensor may be hard to detect while easy to do. It may therefore be a quite probable attack to such kinds of systems. Note that in the case of manipulated sensor input malicious nodes are hard to distinguish from faulty ones. It would therefore be a good idea to introduce some sort of plausibility checks for sensor readings into the system. For instance, receiving an icy road warning while the own external temperature sensor indicates temperatures sufficiently above 0 deg C, would be a good indication that the message might have been send by a malicious or malfunctioning node.

b) Trusted Platform: From the short analysis of the attack tree in Figure 1, it becomes clear that choosing a platform that protects private information is among the prominent design issues of NoW system implementations in addition to choosing strong cryptographic primitives.

c) Trust Establishment for Communication: Trust establishment for the communication system, in particular for the routing in the NoW system is important. Even though there already are existing solutions on intrusion detection systems and distributed trust establishment techniques, there are currently few solutions tailored to IVC networks. Trust establishment will probably both rely on some trusted infrastructure (e.g. for initial identity management) but also on completely distributed mechanisms when the ad hoc network has no connection to the fixed security infrastructure. Note that there may be different providers of trust, i.e. those who provide for trust in the communication interface and those - and possibly many different ones thereof - who provide trust in the different application instances.

d) Secure Wakeup: Battery draining attacks against parked vehicles should be prevented as they may become a serious threat to vehicle functionality and hence to deployment of the application. Users would probably not buy an application which can be used to make their car be dead after two days of parking. As the OBU must not run all the time the vehicle is parked, a wake-up mechanism is sought. This mechanism could be subject to attack if too simple or insecure. In [20] an approach to secure the wake-up mechanism based on hash chains or WiFi Protected Access of car to home applications is discussed which deals with such attacks.

e) Privacy Protection: Privacy has been identified as one major security goal in Section III. The attack trees, in particular the attack tree in Figure 3 stress that to detect the user's privacy, a holistic approach is necessary. This includes that first the communication system can provide for anonymous communications. Second, it will not be sufficient to only have one identifier which is detached from the user's identity, because a system will then be recognizable and therefore easier to trace; in addition the act of mapping a system identifier to a real world identity is easy for a men with a transceiver, as has been pointed out above. Therefore, pseudonyms are a promising solutions to be used in the communication system even though their extensive use will be detrimental to system functionality and performance. In a nutshell, the system must provide for the untraceability of its users. Finally, infrastructure, both communication wise and traffic related should be designed or integrated into such systems carefully considering the possibility of privacy violations due to centralized collection of massive amounts of user data.

f) Tamper Evidence Mechanisms: Based on the attacks on RSUs, it becomes clear that an RSU connected to some communication infrastructure can quickly detect attacks on its functionality. Protection of RSUs may consist of, e.g., a UMTS[2] transceiver, which can issue either alive-messages every now and then, or issue some sort of attack notification to a traffic center. Further, the RSU must detect tampering, vandalism or its unauthorized relocation and notify the responsible traffic information center. Referring to OBUs, it shall be possible to detect malicious changes to hard or software at least when the car is being inspected. For tamper evidence, again plausibility checks in connection with additional communication capabilities can be thought of.

[2]Universal Mobile Telecommunication Standard

V. Conclusions and Future Work

During our work we found that attack trees provide a useful tool to assess the security of a system gradually. The top-down approach allows us to influence the system design at an early development phase regarding security considerations, while on the other hand being able to generate a more detailed analysis as soon as the system's specifications become more specific.

Looking at the attacks, we found that two procedures would enhance overall security essentially, doing local plausibility checks in cars and regular system checks on the nodes, most notably RSUs. Plausibility checks could include comparison of received information to internal sensor data, evaluating messages from different information sources about a single event and scenario building, where single traffic events are related using statistics. Simulations have shown that this greatly increases the effort of an attacker, but it requires proper models for every application. Regular system checks would verify the proper function of a unit and therefore reduce the number of malfunctioning units. This could also include the option to update the software.

VI. Acknowledgements

This work has been carried out in the project "NoW: Network-on-Wheels" project supported by the German Ministry for Education and Research (BMB+F) under Contract No. 01AK064F.
We would like to thank Michael Schäfer, Elmar Schoch (both DaimlerChrysler), and Benedikt Ostermaier (BMW) for their valuable contributions and comments to this paper.

References

[1] Amer Aijaz, Bernd Bochow, Florian Dötzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmüller, "Attacks on inter vehicle communication systems - an analysis," Tech. Rep., The Network on Wheels Project, 2005, `http://www.network-on-wheels.de/documents.html`.

[2] "US Vehicle Safety Communication Consortium," `http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm`.

[3] The Willwarn Project, "The Willwarn project website," 2005, `http://www.prevent-ip.org/willwarn`.

[4] The Network on Wheels (NOW) Project, "NOW website," 2004, `http://www.network-on-wheels.de`.

[5] Albert Held and Rainer Kroh, "It-security and privacy for telematics services," in *Workshop on Requirements for Mobile Privacy & Security*, University of London, UK, September 2002.

[6] Jean-Pierre Hubaux, Srdjan Čapkun, and Jun Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004.

[7] Magda El Zarki, Sharad Mehrotra, Gene Tsudik, and Nalini Venkatasubramanian, "Security issues in a future vehicular network," in *Proceedings of EuroWireless 2002*, February 2002.

[8] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and correcting malicious data in vanets," in *VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks*. 2004, pp. 29–37, ACM Press.

[9] Florian Dötzer, "Privacy issues in vehicular ad hoc networks," in *Workshop on Privacy Enhancing Technologies*, Cavtat, Croatia, May 2005.

[10] Matthias Gerlach, "VaneSe - An approach to VANET security," in *Proceedings of V2VCOM 2005*, 2005.

[11] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer, "Influence of falsified position data on geographic ad-hoc routing," in *ESAS 2005: Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, jul 2005.

[12] Matt Blaze, Joan Feigenbaum, and Jack Lacy, "Decentralized trust management," in *Proceedings of IEEE Symposium on Security and Privacy*, 1996, number 96-17, pp. 164–173.

[13] Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, 1999.

[14] Laurent Eschenauer, Virgil Gligor, and John Baras, "On trust establishment in mobile ad-hoc networks," in *Proceedings of the Security Protocols Workshop*, April 2002.

[15] Christian Schwingenschlögl and Marc-Philipp Horn, "Building blocks for secure communication in ad-hoc networks," in *Proceedings European Wireless*, 2002.

[16] Frank Kargl, *Sicherheit in Mobilen Ad hoc Netzwerken*, Ph.D. thesis, Universität Ulm, 2003.

[17] Marko Wolf, André Weimerskirch, and Christof Paar, "Security in automotive bus systems," in *Proceedings of ESCAR 04*, 2004.

[18] U.S. Department of Transportation, "Vehicle infrastructure integration (vii)," `http://www.its.dot.gov/vii/`.

[19] Jerry Werner, "Details of the vii initiative's 'work in progress' provided at public meeting," `http://www.ntoctalks.com/icdn/vii_pubmtg_v1.php`.

[20] Matthias Gerlach, Jens Hünerberg, Bernd Bochow, Christian Maihöfer, and Carsten Tittel, "Secure wakeup on WLAN for car to home applications - MagicPackets for wireless," in *Proceedings of V2VCOM 2005*, 2005.