Journal of Information Assurance and Security 4 (2009) 226-235

Applying Intrusion Detection to Automotive IT – Early Insights and Remaining Challenges

Tobias Hoppe[1], Stefan Kiltz[1] and Jana Dittmann[1]

[1] Otto-von-Guericke University of Magdeburg,
Department of Computer Science
{tobias.hoppe, stefan.kiltz, jana.dittmann}@iti.cs.uni-magdeburg.de

***Abstract*:** Holistic concepts for IT security are an increasing aspect of research also in the automotive domain. In this paper we motivate the application of Intrusion Detection approaches as a promising supplemental measure for future automotive IT security concepts. First, we define basic requirements for automotive Intrusion Detection meeting the specific demands in the automotive context. We also discuss concrete concepts for both the detection and decision phase. With respect to the detection phase, an automotive Intrusion Detection component has prototypically been implemented and tested on recent automotive IT hardware to demonstrate the potential of the approach. For the decision phase we present a conceptual model to determine the optimum way of communication of IT-security related events to the car occupants. An adaptive dynamic concept is proposed to address the frequently changing environmental conditions in the automotive domain and discussed using three exemplarily selected scenarios.

Keywords: Automotive, IT-security, Intrusion Detection, Security Application on Critical Environments, Multimedia, Human Computer Interaction.

1 Introduction / Motivation

An upcoming topic in the automotive domain, which is becoming a focus point of research, is the (IT) security of automotive IT systems [1]. Current automobiles already contain up to 70 Electronic Control Units (ECUs), which are communicating with each other over automotive bus systems. With Car-to-Car (C2C) and Car-to-Infrastructure (C2I) communication, a much more global interconnection of automotive systems is already in development[1]. The protection of automotive systems, their communication and stored data/information against intended attacks like manipulation and eavesdropping [2] is therefore of increasing importance. In [3] and [4] we showed that targeted attacks on recent automotive IT systems nowadays are often possible without much effort and knowledge required, so the threat potential has already been demonstrated practically. When developing holistic security concepts for automotive systems (e.g. hardware supported as proposed in [5]), strong resource and cost constraints exist. However, since security violations in the automotive context are assumed to have implications on the safety of the entire system and its users, this is nevertheless a very important area of research.

IT security measures, concerning both conventional and automotive IT systems, can be divided into *reactive* and *proactive* measures (see also the following Figure 1 and examples from research as provided by [6]). *Proactive measures* are provided to help prepare, protect and secure systems from attacks or events, usually taken by the manufacturer or administrator of an IT system. According to [7], *reactive measures* are triggered by a sudden occurrence or an event, for example malicious code attack, virus attack or serious vulnerability. Common examples for such measures are the mechanisms of intrusion detection and/or prevention. This may also include the conduct of a forensic investigation (see also [8]). Often, reactive measures are based on proactively installed components. This obviously holds true for IDS components (which need to be installed first), but is increasingly also important for forensic measures. For example, to maximise the quality of (reactive) forensic investigations, a strategic preparation (i.e. the establishment of reliable data sources and mechanisms) forms a part of the proactive measures. The investigation could result in the knowledge about attack patterns which, in turn, could be used as rules for an intrusion detection system (see section 3).

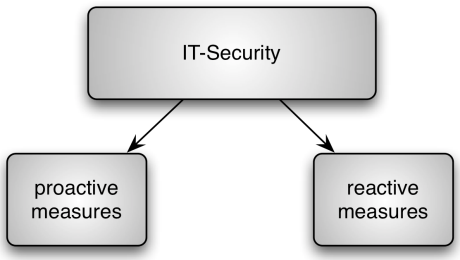

Figure 1. Measures to establish and maintain IT-Security

Especially with regards to automotive systems, the proactive part includes all the measures taken by the car manufacturer as well as the owner/driver of a car in anticipation of IT security related incidents. Some proactive measures currently discussed in automotive IT security research are introduced in section 2.2.

Reactive IT security measures for automotive systems are less common, even in current research. Based on the experiences of Intrusion Detection System already established in the desktop IT environment, in this paper we motivate the application of Intrusion Detection approaches as a supplemental measure for future automotive IT security. Due to the specific properties and requirements in the automotive domain, some aspects of this transition are a

[1] Car-2-Car Communication Consortium, http://www.car-2-car.org/

Received June 10, 2009

challenging task.

After discussing the main requirements of an automotive application of Intrusion Detection approaches, in this paper we investigate two general aspects in more detail. The first covers technical aspects of detecting attacks in automotive IT infrastructures (which are different to those known from desktop IT). With reference to a practically demonstrated attack on recent automotive IT, we present a prototypically implemented anomaly-based Intrusion Detection component and its technical concept. In the second part we cover the reaction to attacks once they have been detected. Here we concentrate on the fact, how a warning could be communicated to the driver in an optimal way. We propose to utilise the increasingly powerful multimedia environment which is provided to the driver and the other occupants. Based on these already existing possibilities for their use as Computer-Human-Interface via a variety of visual, acoustic and haptic actuators we propose their additional application to communicate system security related information to the driver in the case of detected incidents. Utilising a wide range of a modern car's sensory input, the optimal means of communication between the car and its occupants with respect to the current environmental conditions is determined by applying an adaptive dynamic mechanism (see section 4).

The application of IDS technology to automotive systems is expected to be of future importance, especially to react on potential security threats posed by the emerging interconnection of local automotive communication with global networks like the Internet and to decrease their potential safety implications.

The paper is structured as follows: In section 2 we provide basic reflections about Intrusion Detection and automotive IT security in general and discuss the main challenges of their combination. In section 3 we present a deeper view onto technical concepts for the detection of attacks on automotive IT. Section 4 focuses on possible ways of reacting to detected incidents. This is done on the example of the communication of security related warnings using a conceptual model which is illustrated using exemplarily chosen scenarios. After pointing out remaining challenges of automotive Intrusion Detection in section 5, section 6 summarises and closes the paper.

2 Intrusion Detection and its application to the automotive domain

Currently, Intrusion Detection is nearly exclusively developed for and operated in the desktop IT domain. However, the application of these approaches might also be reasonable for other, upcoming domains. In this paper we discuss their applicability to automotive IT as an additional security module, facing the special requirements and challenges evident for this specific domain. The section starts with a short introduction to Intrusion Detection in general (as operated in desktop IT) in subsection 2.1. Subsequently we focus on current and oncoming security threats in automotive IT in subsection 2.2 to demonstrate the need for effective countermeasures in future, presenting some approaches from current research. In the final subsection 2.3, we identify general requirements and challenges of the proposed application of Intrusion Detection approaches for automotive IT by discussing main requirements which are individual for its application in this specific domain.

2.1 Intrusion Detection as Known from Desktop-IT – a Short Introduction

In the desktop IT domain (especially in larger networks) Intrusion Detection Systems are already an established part of IT security infrastructures. As defined by [9], IDS implement a *variety of techniques for detecting attacks in the form of malicious and unauthorized activity*. To achieve this, these systems observe activity within networks or directly on the end systems. Network based Intrusion Detection Systems (also called NIDS [10]) analyse the traffic including information from the header and the content of each message/packet in order to identify characteristics for known attacks. The activity inspected by Host based Intrusion Detection Systems (also called HIDS [10]) includes events like process and thread activity like system calls or resource access. This means that IDS usually perform passive monitoring of network or system activity and do not actively filter any events like e.g. Firewalls do (also see [11]). Figure 2 shows a broad overview of an IDS' structure.

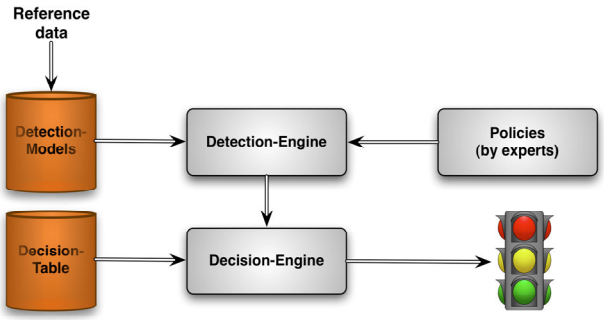

Figure 2. Schematic of an Intrusion Detection System (IDS)

As illustrated by the *Detection Models* component in Figure 2, the *Detection Engine* relies on some reference data. The appearance of these models depends on the respective detection method. Different general detection strategies can be distinguished, depending on the way how incidents are detected within the observed activities.

Signature/rule based detection: One common approach (e.g. implemented by the commonly known, network-based IDS Snort[2]) is signature based (or: rule based) detection. Certain combinations or sequences of events known to be characteristic for a specific attack are managed in form of a signature database and checked by the detection engine.

Anomaly based detection: Another strategy is based on anomaly detection. Certain events or situations deviating from the normal behaviour are considered anomalous by the

[2] For more information on Snort see http://www.snort.org/

IDS and can be used as detection basis. Existing work on anomaly based approaches can e.g. be found in [12] or [13].

In case of a match, the decision engine is triggered to handle the incident according to a decision table. For dedicated Intrusion Detection Systems, the generated warnings are logged to a file and the responsible administrator is notified, if necessary.

In desktop IT, the functionality of Intrusion Detection systems is often extended by so-called Intrusion Response techniques. With reference to [9], *in the event that intrusive behavior is detected*, the purpose of such systems is *to take (evasive and/or corrective) actions to thwart attacks and ensure safety of the computing environment*, which also covers its security. Such systems, providing autonomous response once first indications of active attacks are detected, are often called Intrusion Prevention Systems (IPS), as well.

2.2 Current and Oncoming Threats and Counter-measures: Examples from Automotive IT Security

Especially when applied to automotive systems, attacks on IT systems might not only violate the IT security, but also have implications on the safety of the system affected.

In past publications, we practically demonstrated the conceivability of respective attacks on current automotive IT:

Starting with very basic attacking techniques like the replay attack strategy we demonstrated attacks on components like the electric window lift [3]. A sudden opening of the driver's window enforced by an IT security attack at high speed could affright the driver and notably also affect the safety of the car's occupants. Also similar attacks on the warning light system ([3], [14]) have been conceived which are referred to in section 3 in more detail.

More sophisticated/complex attacking techniques we demonstrated in further publications. In [15] we identified an attack that might allow thieves of airbag components (which are very common in practice) to mask all electronic symptoms of this incident by inserting malicious logic. Although the airbag system is effectively disabled, this malicious logic communicates the faultless status of the removed devices to all other internal components and even to the infrastructure, i.e. actively interacts during diagnostics sessions (e.g. in the car service station at the regular service inspection). In [4] we located and exploited an implementation flaw in the gateway ECU of an international manufacturer's recent car series. This attack allows an attacker to read out arbitrary, potentially privacy-relevant internal communication from the open diagnostics port bypassing the software-based filtering of the gateway ECU.

Since all of these demonstrated attacks on automotive IT can be conceived very easily (even from a black box perspective without any internal specifications from the manufacturers), this strongly motivates the need for holistic automotive IT security measures.

A promising concept currently under discussion among automotive IT security researchers is the migration of Trusted Computing (TC) technology to the automotive domain. Being already on the market for desktop IT systems, an application in automotive environments would have to be adapted according to several special requirements which are individual to this domain. This includes the reduction of resource demands, e.g. by reducing the wide range of functionality offered by common Trusted Platform Modules (TPMs) to a minimal set (which is sufficient for the automotive context) and by utilising efficient cryptographic algorithms like Elliptic Curve Cryptography (ECC). Also a more intensive protection against hardware based attacks would have been implemented, which is less important in the desktop IT's practice (e.g., instead of separate TPM modules attached using unprotected buses, integrated On-Chip solutions have recently been discussed [16]). Other open questions are the implementation of key management issues and how an efficient maintenance of the implemented cryptographic algorithms can be realised facing a common life cycle of modern automobiles of between 15 and 20 years (since the life cycles in cryptography are notably shorter).

If TC will someday be available also in automotive IT systems this would mean a clear increase to the IT security of automotive IT compared to the status quo. However, as already known from the desktop IT domain, TC as single measure can not provide a complete protection against the various kinds of attacks (even completely software based ones. This underlines the need for also discussing further, supplementary security measures, including approaches beyond the scope of the proactive level (see Figure 1). This remaining gap might be addressed by motivated Intrusion Detection approaches discussed before.

2.3 Special Requirements of Intrusion Detection Approaches Specific to the Automotive Application

Some typical properties of Intrusion Detection Systems (as known from desktop IT) can be mapped to the automotive domain in a very direct way. For example, this includes the discrimination into host and network based IDS components: In analogy to desktop IT Intrusion Detection, host based Intrusion Detection components could be placed on sensitive ECUs to have a direct view onto the internal activities. This way they would be able to detect malicious code that has been injected during runtime, e.g. exploiting implementation flaws of running code (which even might have been checked for integrity at its start-up by the TPM). Also network-based IDS components (attached to an entire bus system in form of a separate ECU or as part of a central component like the gateway) could scan the on-board communication for indications of active attacks. These might be run by infected ECUs not equipped with a host-based IDS component or by custom devices additionally attached by the attacker.

However, a migration of IDS technology to the automotive domain raises many new questions as discussed exemplarily in the following subsections.

2.3.1 Technical challenges

The architecture of modern automotive IT systems differs from the structure of common desktop IT systems in several aspects. Compared to PC systems, a typical ECU does only have very limited resources in terms of CPU power and available storage (with respect to both, persistent and volatile memory). They also do not have fully-fledged operating systems (although first standardisation approaches exist[3]) and very limited multi tasking ability. The internal networking is implemented by field bus systems[4] like CAN, LIN, MOST or FlexRay using the respective communication protocols. Consequently, even modern cars are not based on a TCP/IP stack in their internal communication[5], which disables a straightforward migration of existing desktop IT IDS implementations. Additional technical challenges are the real-time requirements in the automotive domain. On the one hand, an automotive IDS would not be allowed to delay central functions of the car, once a potentially suspicious event has been observed. On the other hand, the car can be expected to cover a notable distance during the calculation of an appropriate decision, intensifying potential safety risks.

2.3.2 A System Administrator vs. the Common Driver

In the desktop IT, each IDS usually has a dedicated administrator who maintains the system (e.g. keeps the detection signatures up-to-date) and is notified in case of important alerts. When migrating the Intrusion Detection concept to the automotive domain, it is obvious that not each automotive IDS can be maintained continuously by a qualified administrator. In many cases, the driver of the car is the only person in question. However, the typical user of a car cannot be expected to be an IT expert. Consequently, operational tasks like maintenance and alert handling can be delegated to him in only a very limited way.

2.3.3 Intrusion Detection vs. Intrusion Response

The previous point might motivate to design an automotive IDS as self-contained as possible, e.g. integrating autonomous Intrusion Response measures. However, the high safety requirements in the automotive domain render this to another important challenge. In general, automotive systems shall never take safety relevant decisions autonomously but may only support the driver in his reaction (final decisions regarding control or safety of the vehicle are only to be made by the driver). This is written in laws of many countries (e.g. §18 StVG in Germany [17]). Consequently, autonomous response of automotive IDS/IPS components would have to be designed very carefully and should invoke the driver into decisions which are potentially safety-relevant.

2.3.4 Signature based vs. anomaly based detection

As a matter of principle, also in the automotive domain Intrusion detection approaches could be signature or anomaly based (as introduced in section 2.1). For an actual migration, both have individual advantages and disadvantages.

One issue is the *demand for maintenance*. While anomaly based approaches generally require less maintenance, the set of detection signatures would have to be maintained continuously in order to cover novel attacks. Today, typical cars have no regular connection to the internet and the service intervals are too long for this purpose to update detection signatures in the car service station. Future C2X technology could provide a solution to this issue.

Another issue is *dependability of the detection*: Since signatures are used to detect known attacks, their detection is quite accurate in general. Anomaly based approaches can even detect novel attacks, for which no signatures are available, yet. However, a detected anomaly does not necessarily indicate a real security incident and false alarms in the automotive domain are to be avoided to an even higher degree (see below).

Selected approaches for addressing some of these challenges are presented in the following sections. First, in section 3 we discuss exemplary technical approaches for the detection phase to identify IT security relevant incidents in automotive IT environments and we present a first practically implemented prototype tested on real automotive hardware. Subsequently, section 4 will cover the decision phase by presenting a conceptual model of integrating the communication of detected incidents in an adaptive way meeting the requirements of the current environmental conditions.

3 Detection Phase: Recognising automotive attacks

As its very basic fundament, an automotive Intrusion Detection System would need mechanisms to detect the occurrence of IT security relevant incidents. This phase is mainly represented by the components from the top row depicted in Figure 2.

As discussed in section 2.3.4, both signature and anomaly based detection approaches would be possible for automotive intrusion detection. For the practical demonstration presented in this section we chose an anomaly-based strategy, which is a promising approach especially in this early stage of automotive Intrusion Detection research. Unlike in the desktop IT domain, only a very limited number of attacks on automotive IT systems has been publicly documented, yet – most as proof of concept by scientific researchers. While this does not necessarily mean that these are harder to implement (in fact, large parts of automotive IT systems are essentially unprotected) it would

[3] For example, OSEK (http://www.osek-vdx.org/) or AUTOSAR (http://www.autosar.org/)

[4] See http://www.can.bosch.com/, http://www.lin-subbus.org/, http://www.mostcooperation.com/ and http://www.flexray.com/ for more information about the listed bus systems

[5] However, this was already considered by the industry and tested in research studies using prototypical implementations, e.g. as reported by D. Roth in *AutoBlog* entry from Dec 1st, 2007, titled "iDrive via IP? - BMW uses Internet Protocol underhood" http://www.autoblog.com/2007/12/01/ idrive-via-ip-bmw-uses-internet-protocol-underhood/

be difficult to specify detection signatures for a sufficient number of probable attacks in order to provide a reasonable detection quality. Consequently, we expect an anomaly detection to cover many basic automotive attack strategies.

3.1 The exemplarily chosen attacking technique

We demonstrate the basic potential of IDS approaches for the detection of IT-based attacks in the automotive domain using a practical example. With reference to a practically conceived attack on current automotive IT, we developed a prototypical implementation of an anomaly-based IDS component which is able to detect the attack once it occurs and to generate a warning.

As test environment we use a large part of the ECUs from a recent CAN-bus based car series of an international manufacturer (build since 2005) connected by the original wiring harness. Using CAN bus equipment we can read and create arbitrary bus communication.

The attacked component is the warning light system. As Table 2 shows, devices like the anti theft system usually trigger the warning lights by periodically sending a sequence of CAN messages of a certain message type (0x395) containing a flag to set or unset the indicator lights.

Time stamp (sec)	ID (hex)	Data	Comment
120.218	395	08	Signal off
120.268	395	08	Signal off
120.279	395	88	Signal on
120.329	395	88	Signal on
120.378	395	88	Signal on
120.428	395	88	Signal on
120.478	395	88	Signal on
120.528	395	88	Signal on
120.579	395	88	Signal on
120.629	395	88	Signal on
120.679	395	88	Signal on
120.688	395	08	Signal off
120.738	395	08	Signal off

Table 2. Message excerpt recorded during normal operation

The attack aims at suppressing the warning lights (e.g. during a break-in attempt) and can be implemented by any malicious component with access to the target bus network, e.g. an infected existing device within the network or an additionally attached device.

Whenever the malicious component observes a respective command message on the bus sent by any component to set the warning lights, it instantly reacts by generating an own copy of the message telling the responsible ECU to unset them again (deleting and modifying existing messages is not possible in this scenario due to the broadcast character of CAN). Since the original messages are immediately followed by the opposite commands, in our tests the connected indicator lights stay completely dark (or occasionally slightly flicker for a short moment due to side effects caused by timing and bus-load related issues). This attack illustrated in Table 3 is also possible due to the broadcast character of CAN without any sender authentication (or even identification).

Time stamp (sec)	ID (hex)	Data	Comment
121.038	395	08	Signal off (real)
121.088	395	08	Signal off (real)
121.098	395	88	Signal on (real)
121.100	395	08	Signal off (spoofed)
121.149	395	88	Signal on (real)
121.152	395	08	Signal off (spoofed)
121.198	395	88	Signal on (real)
121.201	395	08	Signal off (spoofed)
121.249	395	88	Signal on (real)
121.252	395	08	Signal off (spoofed)
121.298	395	88	Signal on (real)
121.300	395	08	Signal off (spoofed)
121.349	395	88	Signal on (real)
121.352	395	08	Signal off (spoofed)
121.398	395	88	Signal on (real)
121.401	395	08	Signal off (spoofed)
121.449	395	88	Signal on (real)
121.452	395	08	Signal off (spoofed)
121.498	395	88	Signal on (real)
121.500	395	08	Signal off (spoofed)
121.508	395	08	Signal off (real)
121.558	395	08	Signal off (real)

Table 3. Message excerpt recorded during the attack

3.2 The implemented, anomaly-based IDS approach

Looking at the attack representation in Table 3, this attack strategy can even be detected by a network based automotive IDS without insights to the internal activities of any ECU.

We implemented a prototype of an anomaly-based Intrusion Detection component on the network level. It keeps track of all CAN messages having the target message type 0x395 and evaluates two different characteristics:

- The current frequency of these messages, which is either 0 or 22 (±1) occurrences per second during normal operation. During the attack, up to 36 messages per second are observed.
- The semantical meaning of the previous 8 messages observed (“on” and “off”). In normal operation, this value only changes 0-1 times during this interval. When the attack is active, up to 7 inversions can be noticed.

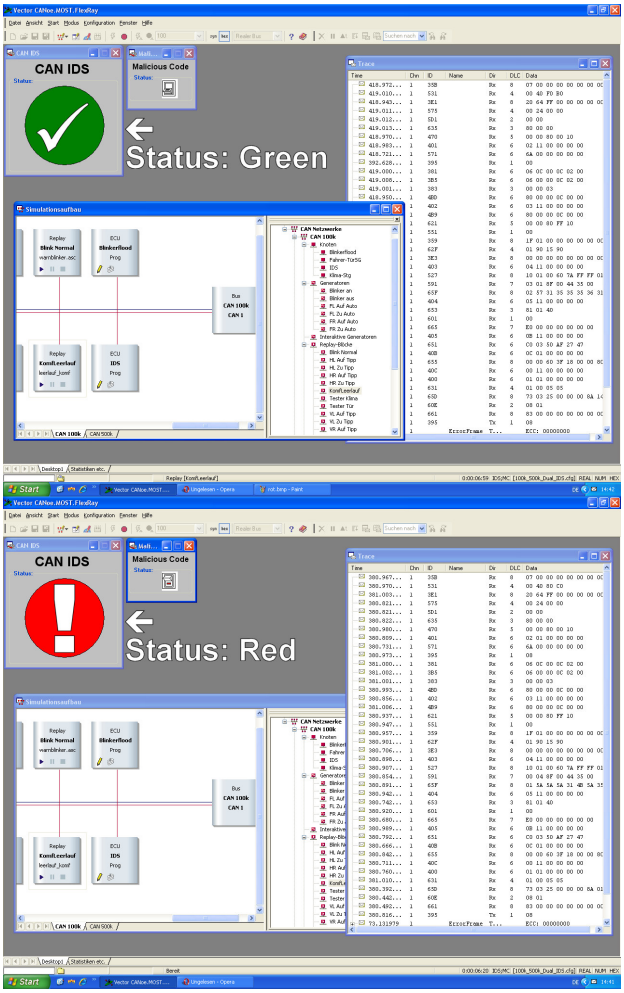

Figure 3. Prototypical automotive IDS component

Within our tests, the anomaly-based prototype treats the overstepping of 26 messages per second as well as 4 semantical inversions among 8 messages as anomaly. In this prototype, we simply visualised the detection using a green and red light, respectively (see Figure 3). More elaborate concepts for the decision phase are discussed in the following section 4.

4 Decision Phase

While the previous section discussed basic concepts for *detecting* IT security relevant incidents during operation, in this section we rather concentrate on the question how an appropriate *decision* could be determined once an incident has been detected. This phase is represented by the bottom row within Figure 2.

As the basic requirements identified in section 2.3.3 state, autonomous intrusion response would have to be applied very carefully, so for now we focus on the communication of information and advice. As stated in section 2.3.2, the typical driver has little knowledge about technical activity inside his car. Therefore such a system requires a sound design[6] that respects what information is to be communicated to the users in which way. We identified four aspects:

Use a modern way of communication: The system should tap the full potential of modern car's multimedia environment.

Communicate a sense of peace of mind: In order to provide a sense of security to be experienced, we propose also an active communication of a healthy system status (e.g. a green light).

Avoid a high frequency of indicated incidents: This might lead the driver to feel nagged by these warnings and reduce his attention to them. If reactions are required from him, he might lapse into routine. So the system should be conceived to be as self-contained as possible and to avoid repeating procedures in the interaction with the driver.

Support the driver: If a reaction by the driver is required, the system should propose possible choices and (if available) already pre-select the most suiting/safe one.

For this purpose we propose an integration of the IDS communication to the driver into the multimedia environment already present in current cars.

Having started with simple radio systems and later the integration of mobile telephones and CD players, today complete multimedia environments have become available. These are usually managed by a central on-board computer, which integrates a variety of audio based systems like radio, telephone and CD/MP3 players with audiovisual systems like navigation systems, DVD/BluRay players and television or head-up displays. In the automotive domain there is a large amount of information provided by the multimedia systems to the car occupants, which also requires much interaction with the system, especially by the driver (e.g. the interaction with the navigation system). While also the potential for an application as Human Computer Interface (HCI) is growing, in this paper we concentrate on already existing possibilities for their use as Computer-Human-Interface (CHI) to communicate system security related information to the driver.

The concept presented in the following is intended as a first discussion of how modern automotive multimedia environments could be employed to support a future automotive IDS technology in its interaction with the car's occupants, especially the driver. This is especially necessary because in a car, unlike in desktop IT, autonomous responses (like e.g. service reboots or disconnects) might have severe safety implications and would be to consider very carefully.

Besides using the potential of modern multimedia environments for informing the driver, its features might also be used as platform for subsequent input from the driver. For this purpose, automotive multimedia devices could also serve as HCI to capture and evaluate the driver's reaction interactively, similar to approaches examined by [18] and [19].

However, the conditions around and within the car as well as their perception by the driver are subject to heavy change. Depending on the current driving and environment

[6] For example, the RNIB Scientific Research Unit maintains general *„Guidelines for the design of accessible information and communication technology systems"* accessible at www.tiresias.org/research/guidelines/

conditions, factors like acoustic influences, lighting conditions or the recent shape of the road and traffic density influence the perception of these systems. Therefore we propose a concept that we call *adaptive dynamic reaction* to also consider such factors when communicating detected IT security related incidents, which might again require decisions from the driver. After a short introduction of relevant automotive devices for the communication and *adaptive dynamic reaction* in subsection 4.1, this concept is introduced in subsection 4.2 and illustrated by some exemplary scenarios in subsection 4.3.

4.1 Exemplary automotive components for adaptive dynamic reaction and communication

When looking at the components required for the proposed system, two major groups can be identified: the devices, which are used directly for the communication of the system to the driver (CHI) and those who support the system during the *adaptive dynamic decisions*.

Beneath classic displays e.g. within the dashboard, other important components of modern car's multimedia environment are especially audio/video systems (like radio, phone, media-players, TV, head-up displays) that are supplied by modern infotainment systems like navigation or on-board computer.

For the consideration of the current environment situation (to support the *adaptive dynamic decisions*), mostly input from sensors can get utilised. Useful information about the interior situation can be obtained from sensors like interior lighting sensor, microphones, seat usage sensors or cameras. For information about the outside conditions sensors like rain and sunlight sensors can be used. Additionally, by combining this information with additional data like current car and engine speed (from the powertrain network), current position (from the GPS) or map data from the navigation system, an even more clear view on the current situation (about current road shape, noise level etc.) can be obtained.

Where applicable, for the communication via the multimedia devices, known multimedia techniques could be utilised. For example, the current video/audio output could be dimmed / faded and the information to be communicated could be blended in. Depending on the detected situation, we choose the appropriate way of communication to the driver using a specific subset of the multimedia environment supported by a conceptual model introduced in the following subsection.

4.2 Three stages model for adaptive dynamic reaction

Looking at the variety of devices found in a modern car's multimedia environment, many ways are possible as to how a warning message could be communicated to the driver. We expect a fixed configuration not to be a good choice for two major reasons. As already mentioned, the first one is the varying perception of specific entertainment systems due to changing driving conditions (noise/light levels, stress etc.). Secondly, more severe warnings have to be communicated more urgently while less severe warnings could possibly be communicated in a more silent way.

To address this, we propose a conceptual model consisting of three stages (see Figure 4) as described in the following. It directly depends on the severity of a detected security incident while the perceptibility aspects are dominating in the phase of the model's application.

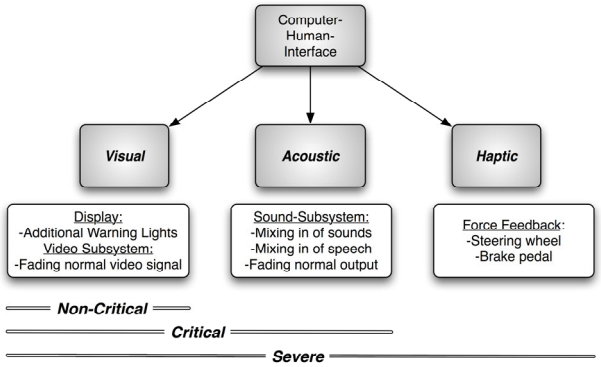

Figure 4. Three stages model for adaptive dynamic reaction

Being part of the CHI, we classify the various components of automotive multimedia environment into three groups. Determined by the perception by the user, we distinguish *visual* interfaces in the first, *acoustic* interfaces in the second and *haptic* interfaces in the third group. Visual interfaces contain common dashboard lights or simple led displays together with modern equipment like video screens of on-board computer, navigation, media or TV systems. Acoustic interfaces mainly consist of the sound subsystems (used by radio, phone, media players etc.). An example of available haptic systems is the force feedback ability of components like the mechanism employed in today's ABS break systems; in future also the steering wheel could be equipped with a similar feature.

Left to right: Increasing severity. In the order chosen, these three ways of communication implicate an increasing severity of the communicated message. A message only communicated visually does usually not get the driver's attention unless he looks in the direction of the respective display. An audible signal (we consider both warning sounds as well as spoken messages) usually gets his attention instantly. Haptic warning output like the steering wheel vibration should only be chosen in very severe situations since a sudden activation could affright the driver unnecessarily.

Right to left: Increasing information capacity. However, the capability of these communication models with respect to their message capacity is decreasing from left to right. A force feedback signal mainly transports binary (something happened) or intensity information. Moreover, a user often registers visual information on a screen faster than a message being spoken through a sound system. Consequently, we propose that a choice for one of the communication models should always include all the blocks left to it in Figure 4. After being alarmed by a force feedback signal, the warning could be explained acoustically while the driver can have a quick look over the entire message already displayed on screen.

Adaptive dynamic choice of the communication model. As mentioned, once an incident has been detected by the automotive IDS, the choice of the appropriate

communication model depends on two factors.

First the severity of the incident is determined. Depending on its severity, the first, second or third stage is selected. We propose a choice of visual-only communication for non-critical warnings, audio-visual information for critical warnings and additionally haptic signals for severe incidents (see Figure 4).

After this initial classification, the environmental conditions are determined. If the preliminary choice of communication is not appropriate due to the current conditions, the assignment might be taken to the next stage. For example, if the light sensors (e.g. sun or interior light sensors) detect a high light level, the warning might not be perceptible by the driver. An increase of the assignment to the second stage, i.e. the support by an audible signal, would be an appropriate *adaptive dynamic reaction*.

4.3 Illustration by exemplarily chosen scenarios

In this section we introduce three exemplary scenarios that demonstrate a potential application of the model proposed for the *adaptive dynamic reaction* to IT security incidents.

We assume the following preconditions: An attacker, who wants to spy on sensitive data or even endanger the safety of the car's occupants, has infected an ECU of the car with malicious code. This incident might not be detected instantly, e.g. because of cost reasons there is no (host based) IDS component on every device. Once the infected device interacts with others in an abnormal way a (comparatively cheaper) network based IDS might detect symptoms for the incident and need to communicate it.

Scenario 1: Theft of information. Future automotive malicious code might gather sensitive information and transmit this to the outside using Car-to-Car (C2C) or Car-to-Infrastructure (C2I) communication. If the IDS detects such communication to be generated without a plausible reason, it might generate a hint advising the driver to check his car at a service station soon. The leakage of information does not directly endanger the safety of the car and its occupants. Consequently, this incident is classified as *non-critical* and stage 1 is the initial choice for the communication to the driver. In this scenario, the lighting conditions (as registered by the interior lighting sensors) are well so the driver notices the warning next time he takes a look at the displays.

Scenario 2: DoS-Attack under regular conditions. The malicious code might attack other ECUs via the car's bus networks. In this scenario, it uses a spoofing technique to perform a Denial-of-Service (DoS) attack on the Electronic Stability Control (ESC, also ESP) device in order to disable it. Since the ESP only activates in exceptional cases, an immediate impact of the attack is usually not to expect but it holds obvious safety threats anyway. Once detected, this incident has to be classified as *critical*. If no technical means are present or applicable to thwart this attack autonomously (e.g. as part of future autonomous intrusion response techniques), a warning of at least stage 2 is required in order to inform the driver and advise him to bring the car in a safe position at the next opportunity (and eventually call a service car). Since he might not take a look at the displays timely, an acoustic warning signal or text is also required. In this scenario, the sound level within the car (as registered by the compartment microphones) is appropriate so the driver can hear the warning and then look at the description displayed.

Scenario 3: DoS-Attack under difficult conditions. For this scenario, we consider the same *critical* attack as described in scenario 2. But this time the driver is currently moving with open windows alongside an industry plant with an extreme noise level. The microphones inside the compartment register this disturbance and report it to the communication system. When generating the warning, it can respect these conditions by increasing the required way of communication to stage 3. A force-feedback signal put onto the steering wheel will lead the driver to look at the warning message at the display and allow him to react instantly.

5 Open Challenges and Outlook

In section 2.3 we introduced and discussed main challenges of the migration of Intrusion Detection technology to the automotive domain. We subsequently addressed some of these challenges with respect to both the detection and decision phase in more detail in section 3 and 4. However, several of these challenges still need to be subject of closer research in future.

Especially the extension to Intrusion Response approaches has special potential for the automotive application. If safety implications can be ruled out or at least reduced to a minimum, this might help to bridge the gap between the technical IDS components and the typically car occupants, which are not technically experienced in general.

However, since the users of the car are directly affected by violations of IT security (and their potential implications to safety), the focus on the communication of security-relevant information to the human users is an important challenge of automotive Intrusion Detection. Consequently, sophisticated concepts are needed for the future to provide a balanced basis between autonomous detection and maintenance on the one hand and appropriate user-interaction on the other hand.

Open questions like the maintenance of the IDS' reference data (especially updates for signature based components) might be solved in future by the planned C2X technology that might become an appropriate infrastructure for central maintenance of automotive Intrusion Detection platforms.

Beyond the *proactive* IT-security measures introduced in section 1 and 2.2, further *reactive* approaches (additional to automotive IDS strategies) might supplement a comprehensive IT security basis for future cars. In analogy to desktop IT, novel incidents that pass the proactive measures and are not blocked (if even detected) by reactive

measures (e.g. IDS components) might be covered by the IT forensics discipline in a further step: A transition of existing experiences in IT-forensics to the automotive domain could be used to investigate incidents in automotive environments [8]. The authors see a field for its application in accident research and in warranty cases. It can be used to reconstruct events not yet handled by upstream mechanisms. Knowledge gained from IT forensics can also be used to create signatures and rules for attack patterns to be used in the intrusion detection system.

6 Summary and Future Work

Since the complexity and networking of automotive IT systems is constantly increasing, the IT security is an emerging topic in this domain. Especially because IT security related attacks are assumed to have strong safety implications in automotive environments, IT security mechanisms are expected to be of great importance in future automotive development concepts. As an addition to proactive IT security measures, in this paper we focused on reactive approaches. Looking at Intrusion Detection Systems already established in the desktop IT domain, we motivated the application of this concept also for the automotive domain.

After discussing general challenges to be addressed in this special, safety sensitive domain, we provided some practical insights into the detection of incidents on the example of current automotive IT and presented a conceptual model for the decision phase. Within this phase we focused on the communication of security warnings to the driver by using the multimedia environment of modern cars. By applying a concept that we call *adaptive dynamic reaction*, the choice from the components available for communication is determined by the severity of the detected incident as well as the current driving and environmental conditions.

Being a first basis for future automotive IT security systems, our demonstrated detection techniques and the proposed communication concept exemplify the importance of meeting the special requirements in the automotive application when transferring established IT security measures to the automotive domain.

In future, we plan to extend the existing implementation of the detection phase by a first implementation of the discussed communication concept to analyse the intended perception properties in more detail. As further steps, the research about automotive IDS components might also be extended towards intrusion response abilities as well as for covering non-security but safety or comfort related incidents: In future, the existing concept of monitoring the driver's condition could be integrated into the IDS to tap the full potential of its adaptive communication model (e.g. in case of detected fatigue, the generated audio warnings might be supplemented by force feedback this way if the noise conditions are difficult). Yet another possibility would be monitoring outside conditions (e.g. by outside video cameras and radar systems of Active Break Assists [20]) or inclusion of information communicated via C2C/C2I.

Acknowledgment

The work described in this paper has been supported in part by the European Commission through the EFRE Programme *COmpetence in MObility* (COMO) under Contract No. C(2007)5254. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

European Commission
European Regional Development Fund
INVESTING IN YOUR FUTURE

References

[1] M. Wolf. *Security Engineering for Vehicular IT Systems - Improving the Trustworthiness and Dependability of Automotive IT Applications*, Vieweg + Teubner Research, Wiesbaden, Germany, 2009.

[2] A. Lang, J. Dittmann, S. Kiltz, T. Hoppe. "Future Perspectives: The Car and its IP-Address - A Potential Safety and Security Risk Assessment". In *Computer Safety, Reliability, and Security, Proceedings of the 26th International Conference SAFECOMP 2007*, pp. 40-53, Nuremberg, Germany, 2007.

[3] T. Hoppe, S. Kiltz, A. Lang, J. Dittmann. "Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system". In *Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security*, pp. 165-183, Wolfsburg, Germany, 2007.

[4] T. Hoppe, S. Kiltz, J. Dittmann. "Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats". To appear in *SAFECOMP 2009: 28th International Conference on Computer Safety, Reliability and Security*, Hamburg, Germany, 2009.

[5] M. Wolf, A. Weimerskirch, T. Wollinger. "State of the Art: Embedding Security in Vehicles", In *EURASIP Journal on Embedded Systems*, Volume 2007, Article ID 74706, 16 pages, 2007.

[6] A. Sardana, R.C. Joshi. "An Integrated Honeypot Framework for Proactive Detection, Characterization and Redirection of DDoS Attacks at ISP level", *Journal of Information Assurance and Security*, Volume 3, Issue 1, pp. 1-15, 2008.

[7] A. Kumar. "CIRT – Framework and Models", http://www.securitydocs.com/pdf/2964.PDF, 2005.

[8] S. Kiltz, M. Hildebrandt, J. Dittmann. "Forensische Datenarten und Analysen in automotiven Systemen". In *DACH Security 2009*, pp. 141-152, Berlin, Germany, 2009.

[9] N. Stakhanova, S. Basu, and J. Wong. "A Taxonomy of Intrusion Response Systems", *International Journal*

of Information and Computer Security Vol. 1(1), pp. 169–184, 2007.

[10] J. Molina, M. Cukier. "Evaluating Attack Resiliency for Host Intrusion Detection Systems", *Journal of Information Assurance and Security*, Volume 4, Issue 1, pp. 1-9, 2009.

[11] W. Lee, W. Fan, M. Millerand, S. Stolfo, E. Zadok. "Toward cost-sensitive modeling for intrusion detection and response", *Journal of Computer Security*, Volume 10, pp. 5–22, 2002.

[12] G. Florez-Larrahondo, Z. Liu, Y. Dandass, S. Bridges, R. Vaughn. "Integrating Intelligent Anomaly Detection Agents into Distributed Monitoring Systems", *Journal of Information Assurance and Security*, Volume 1, Issue 1, pp. 59-77, 2006.

[13] E. Nikolova, V. Jecheva. "Anomaly Based Intrusion Detection Based on the Junction Tree Algorithm", *Journal of Information Assurance and Security*, Volume 2, Issue 3, pp. 184-188, 2007.

[14] T. Hoppe, S. Kiltz, J. Dittmann. "IDS als zukünftige Ergänzung automotiver IT-Sicherheit". In *DACH Security 2008,* pp. 196–207, Berlin, Germany, 2008.

[15] T. Hoppe, J. Dittmann. "Vortäuschen von Komponentenfunktionalität im Automobil: Safety- und Komfort-Implikationen durch Security-Verletzungen am Beispiel des Airbags". In *Sicherheit 2008,* pp. 341-354, Saarbrücken, Germany, 2008.

[16] J. Pelzl. "Secure Hardware in Automotive Applications. In *escar - Embedded Security in Cars, 5th Conference*, München, Germany, 2007.

[17] A. Seeck, T. M. Gasser. "Klassifizierung und Würdigung der deutschen und völkerrechtlichen Rahmenbedingungen im Zusammenhang mit der Einführung moderner FAS". In *2. Tagung Aktive Sicherheit durch Fahrerassistenz*, 6 pages, München, Germany, 2006.

[18] O. Vybornova, M. Gemo, R. Moncarey, B. Macq. "Ontology-Based Multimodal High Level Fusion Involving Natural Language Analysis for Aged People Home Care Application", In *Interspeech 2007*, pp. 2577-2580, Antwerp, Belgium, 2007.

[19] M. Ablaßmeier, T. Poitschke, S. Reifinger, G. Rigoll. "Context-Aware Information Agents for the Automotive Domain Using Bayesian Networks". In - *Human Interface and the Management of Information. Symposium on Human Interface 2007*, Part of HCI Intern. 2007, Proc. Part I. pp. 561-570, Bejing, China, 2007.

[20] R. Heilmann. "Entwicklung von Algorithmen zur Sensordatenfusion für Sicherheitsanwendungen im Automobilbereich", Diploma Thesis, University of Magdeburg, Germany, 2006.

Author Biographies

Tobias Hoppe With a focus on topics of IT security, Tobias Hoppe is currently working as a research assistant in the Research Group Multimedia and Security at the University of Magdeburg, Germany. In the context of the project COmpetence in MObility (COMO) his current research activities cover oncoming IT security challenges in the automotive domain. This covers the identification and analysis of several threats to current automotive IT and their potential safety implications (featured by substantial automotive laboratory equipment) as well as general concepts for appropriate IT security solutions.

Stefan Kiltz The co-author currently works as a research assistant in the Research Group Multimedia and Security at the University of Magdeburg, Germany. Among other, general topics regarding IT security, he has a special focus on research about IT-forensics. Within the project COmpetence in MObility (COMO), his current research activities cover aspects of IT security in the automotive domain, including the application of IT-forensics to current automotive IT components .

Jana Dittmann Jana Dittmann studied Computer Science and Economy at the Technical University in Darmstadt. In 1999, she received her PhD from the Technical University of Darmstadt. She has been a Professor in the field of multimedia and security at the University of Otto-von-Guericke University Magdeburg since September 2002. Jana Dittmann specializes in the field of Multimedia and Security. She has many national and international publications, is a member of several IEEE and ACM conference PCs, and organizes workshops and conferences in the field of multimedia and security issues. For example she was involved in all last ten ACM Multimedia and Security Workshops. In 2001 and 2005, she was a co-chair of the Communication and Multimedia and Security conference (CMS'02 in Darmstadt, Germany and CMS'05 in Salzburg, Austria). In 2006 she organized the second conference GI Sicherheit 2006 in Magdeburg, Germany. She is an Associated Editor for the ACM Multimedia Systems Journal and for SPIE Journal on Electronic Imaging. Dr. Dittmann is a member of the IEEE, ACM and the German Society of Computer Science (GI Informatik).