Security Evaluation of Mobile Device Integration with V2X Communication

Tim Leinmüller [1*], Boris Atanassow [1], Stefan Diewald [2], Lutz-Peter Breyer [1] and Matthias Kranz [3]

[1] DENSO AUTOMOTIVE Deutschland GmbH, Info & Safety Engineering Department, Germany,
[t.leinmueller|b.atanassow|l.breyer]@denso-auto.de

[2] Technische Universität München, Distributed Multimodal Information Processing Group,
Munich, Germany,
stefan.diewald@tum.de

[3] Universität Passau, Lehrstuhl für Informatik mit Schwerpunkt Eingebettete Systeme, Passau, Germany,
matthias.kranz@uni-passau.de

ABSTRACT

In previous work, we investigated possibilities of an architecture for the functional distribution of a vehicle-to-x (V2X) system on two devices with different capabilities. One of the devices is an in-vehicle onboard unit (OBU), the other a personal portable device (PPD), such as a smartphone or tablet PC. We developed three different concepts to split workload between the devices, and investigated them regarding overall performance and flexibility.

This work complements previous work with an in-depth security analysis. Security of V2X systems is challenging, especially in case parts of the system are not part of the physically reasonably well protected in-vehicle network domain. The security analysis unveils advantages and disadvantages of the three concepts. Based on the analysis, this work discusses how V2X security can be realized in the two-device setup, providing maximum security with minimum impact on the system performance. The conclusions summarize which level of security can be reached with each of the three approaches.

Keywords: Vehicular ad-hoc networks (VANETs), vehicle-to-x (V2X), security, smartphone.

1. INTRODUCTION

In light of current trends to use personal portable devices (PPDs) such as smartphones and tablets in vehicular environments, we have investigated a corresponding setup for vehicle-to-x (V2X) communication [1].

Usually, PPDs are used for non-safety related applications, such as navigation and infotainment. At first, PPDs were used rather independently from the vehicles' integrated systems, only recently, vehicle manufacturers started offering options for closer integration [2]. For example, Mercedes offers a solution that allows accessing the content from iPhones through the in-vehicle infotainment system (IVIS) [3]. Another example is MirrorLink (previously known as Terminal Mode) [4, 5]. These integrations have in common that they enable the vehicle systems to access capabilities and control functions of the PPD, but not vice versa.

Accessing in-vehicle data from PPDs is possible via OBD-II (On-board diagnostics II), e.g. using an OBD-II Bluetooth adapter. However, OBD-II does not allow the PPD to control vehicle functions, but only to receive data. Concepts for a secure, limited control of vehicle functions (e.g. convenience features such as auxiliary heating, windows) via telematics gateways are discussed in literature, e.g. by Bouard et al. [6]. These concepts will be summarized in the related work section.

In previous work [1], we developed a prototype that elaborates on the integration of vehicles and PPDs. It allows a PPD to access information and to control functions of a V2X system, i.e. a vehicle's safety-related system. With 'V2X system', we refer to systems that allow for the periodic exchange of vehicle data (e.g. position and speed) and the event driven notification of selected situations (e.g. hazardous locations, emergency braking, or traffic light phases). These scenarios can be determined either by the ego vehicle or by cooperative approaches [7]. V2X systems are currently under specification and development worldwide. These efforts are strongly supported by vehicle industry in the US (Crash Avoidance Metrics Partnership, CAMP), in EU (Car-2-Car Communication Consortium, C2C-CC [8]), and in Japan (several organizations and ministries).

In this work, we conduct a security analysis for the three previously developed integration concepts. The analysis unveils advantages and disadvantages of the studied concepts. Based on the analysis, we discuss how V2X security can be realized for a V2X system that splits functionality between a dedicated V2X onboard unit (OBU) and a PPD. The three concepts are briefly summarized in Section 3.

The remainder of this paper is organized as follows. The next section (Section 2) discusses related work. Section 3 introduces our previously investigated integration concepts and Section 4 conducts the corresponding risk analysis. Countermeasures are discussed in Section 5. Finally, Section 6 concludes the paper.

2. RELATED WORK

Terminal Mode [4] realizes security through a combination of network security, device attestation, application attestation, and content attestation. Network security requires either link layer authentication for wireless connections, or the use of wired connections (e.g. USB). The three attestation mechanisms ensure that only approved PPDs, running approved software, are allowed to show approved information on the IVIS at certain points in time. In addition to the attestation mechanism, the IVIS can use a challenge response mechanism to verify that the information from the PPD is authentic, at any point in time.

Bouard et al. [6] propose the concept of an (in-vehicle) security proxy that manages security and decouples communication between in-vehicle systems and PPDs (referred to as Consumer Equipment CE). The concept enables secure controlled connectivity between uncontrollable/insecure PPDs and in-vehicle systems, while limiting threats to the in-vehicle systems. The proxy provides functionality for secure network access, PPD authentication, policy enforcement and protocol/message filtering. It translates and filters messages/protocols between PPDs and in-vehicle systems.

The approach of Joy et al. [9] relies on the combination of a gateway in the vehicle and a proxy application on the PPD. The gateway restricts connectivity to authorized PPDs, the proxy establishes authorized connections with the gateway, and ensures that only authenticated applications are allowed to exchange information with the vehicle systems. Given that the proxy runs on an uncontrollable/insecure PPD, this approach carries the risk of the proxy being modified to allow arbitrary applications to communicate with the in-vehicle systems.

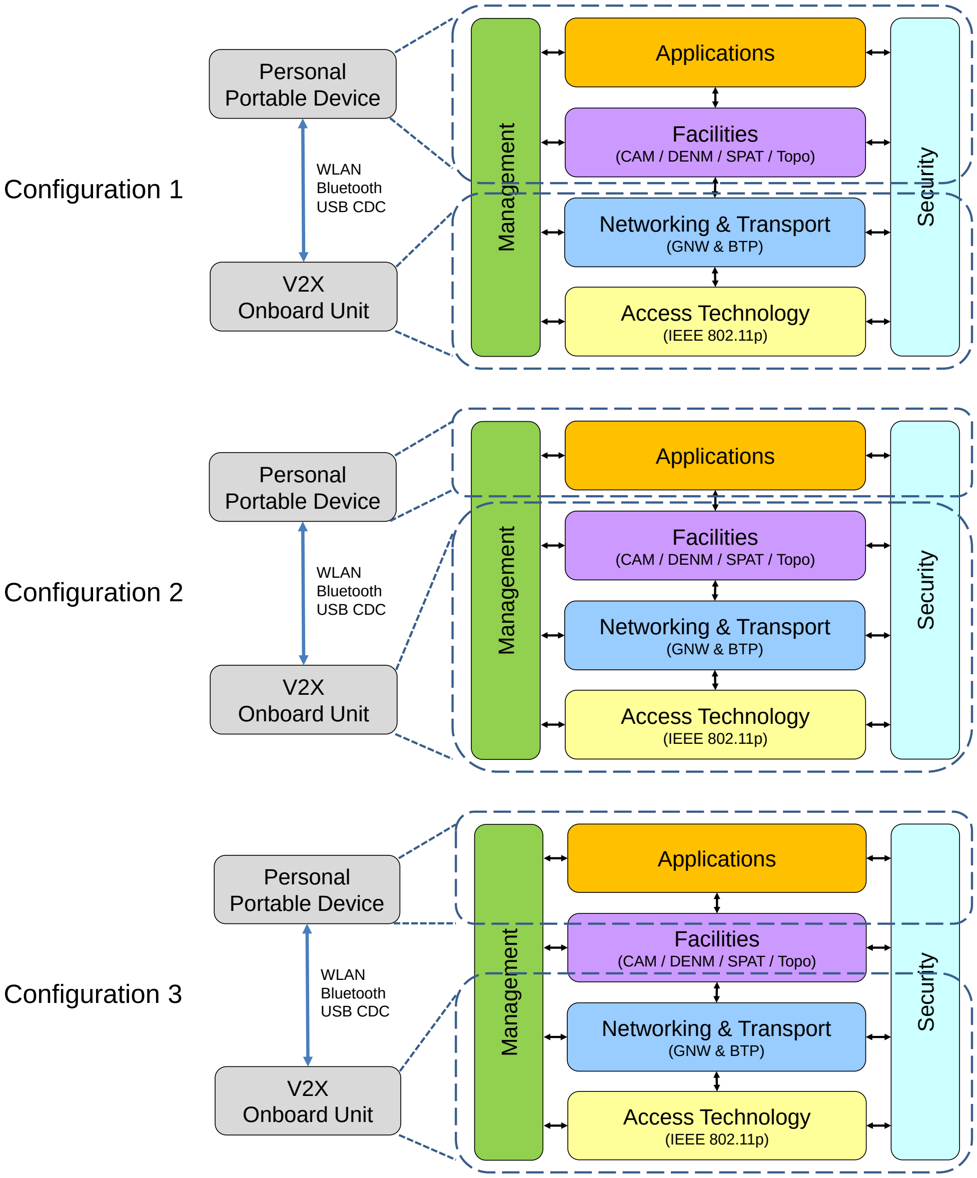

Fig. 1. Overview of the three previously investigated integration concepts.

In summary, related work emphasizes that connecting PPDs to in-vehicle systems poses considerable risk since PPDs are potentially insecure and might be under full control of the user or even malicious third parties. The presented security concepts rely on tight control of applications and/or information that is allowed to be exchange with in-vehicle systems. Especially control of information requires detailed knowledge about what kind of information is exchanged. Another important aspect is that the concepts are tailored to secure information from, or control of functions of the own vehicle. We consider these aspects in our risk analysis and the following discussion of countermeasures.

3. INTEGRATION CONCEPTS

The three previously introduced integration concepts are show in Figure 1.

In Configuration 1, the PPD serves as HMI and V2X Message Processing Unit. The V2X OBU acts as V2X message gateway. Incoming data is directly passed to the PPD, outgoing data is created and sent by the PPD.

In Configuration 2, the PPD is only responsible for running applications and for providing the HMI. The facilities, such as CAM (Cooperative Awareness Message) [10] service and DENM (Decentralized Environmental Notification Message) [11] service, run on the V2X OBU.

Configuration 3 is a combination of the two previous configurations. Facility functionality is split between the V2X OBU and the PPD. The message en-/decoding functionality remains on the V2X OBU, with the difference that the PPD can also request and send messages on any BTP (Basic Transport Protocol) [12] port in raw format.

4. RISK ANALYSIS

Similar to our previous work [13], this work conducts a risk analysis for the three V2X OBU-PPD integration concepts. It identifies assets, threats, vulnerabilities, attackers, and determines resulting risks. This work uses qualitative risk analysis because the investigated system concepts are not (widely) deployed or used, i.e. there is no statistical data regarding attacks or abused vulnerabilities.

4.1 Assets

The identified assets are listed below, sorted according to their importance (descending). They are

1) *(Safety) messages:* information submitted to and received from the V2X network
2) *Information displayed to driver:* information shown to driver on PPD display
3) *Privacy:* privacy impact of information sent over V2X network
4) *Communication system:* communication protocols, resources and hardware

(Safety) messages is ranked highest because it influences all V2X system participants. Information displayed to driver and privacy are limited to the individual participant. Communication system is ranked lowest because non-availability does not cause additional harm, i.e. the system does not trigger any actions.

4.2 Threats

Threats to the previously identified assets are

- Distribution of wrong or forged messages
- Display of wrong or forged information to driver
- Tracking and profiling of vehicles or vehicle drivers
- Disturbance or unavailability of communication system

4.3 Vulnerabilities

The vulnerabilities depend on the selected integration concept. The following vulnerabilities are common to all three integration concepts

- *PPD-V2X OBU interface*: Communication between PPD and V2X OBU is not secured (apart from e.g. using WPA2 for the WLAN connection). PPD and V2X OBU are not authenticated/authorized against each other.
- *Insecure/uncontrolled PPD*: Software on the PPD and the (system of the) PPD itself is subject to modification (especially if the PPD is rooted or jailbroken).

For configuration 2, there are not additional vulnerabilities. Specific vulnerabilities for configuration 1 and configuration 3 are

- *Message creation on PPD*: Messages are created by the PPD, the V2X OBU is just forwarding. This means that the V2X OBU has no control/information about what it is sending. This vulnerability is limited in configuration 3 since a subset of messages is created and decoded on the V2X OBU. This includes basic messages like CAM and DENM.

Note, as a general assumption, this work considers in-vehicle systems as being secure, although being aware of work that shows successful attacks, e.g. from Koscher et al. [14].

4.4 Attackers

Based on the system setup and generally known attacks to V2X systems, this analysis considers the following attackers.

- *PPD user:* PPD owner modifies V2X software on his PPD, e.g. to send / trigger messages as he likes, for instance forged messages.
- *PPD hacker:* PPD runs software (malware) that enables third person to (remotely) trigger actions/messages
- *Foreign PPD:* Vehicle passenger or a person in neighboring car connects his PPD to V2X OBU (instead of or in addition to the vehicle driver).

4.5 Risks

The risks of the system are summarized in risk statements in Table I. They are determined based on the identified asset value, the extent of the threat, and the likelihood of the threat exploiting an existing vulnerability. The classification uses commonly used metric triples for likelihood of attempt (Likely, Conceivable, Improbable), given the difficulty to exploit (Easy, Moderate and Difficult), and determination of overall risk (High, Medium, Low).

The risk statement values are attributed in a process that is based on discussions, common sense, and well educated guess, as usual for a qualitative risk analysis.

The risk analysis shows that the highest risk occurs if wrong or forged safety messages are distributed, if wrong or forged information is displayed to the driver, or if tracking or profiling is possible. The vulnerabilities used for mounting corresponding attacks are

- Insecure/uncontrolled PPD
- Message creation on PPD
- PPD-V2X OBU interface

Especially the first two vulnerabilities are used for most of the high-risk attacks, that is why the discussion of countermeasures will focus on these two aspects in more detail.

Attacker	Vulnerability	Threat	Exposed Asset	Likelihood		Risk
				Attempt	Exploit	
PPD user	Insecure/uncontrolled PPD & Message creation on PPD	Distribution of wrong or forged messages	(Safety) messages	Likely	Easy	High
PPD user	Insecure/uncontrolled PPD & Message creation on PPD	Disturbance or unavailability of communication system	Communication system	Conceivable	Easy	Low
PPD hacker	Insecure/uncontrolled PPD & Message creation on PPD	Distribution of wrong or forged messages	(Safety) messages	Conceivable	Moderate	High
PPD hacker	Insecure/uncontrolled PPD & Message creation on PPD	Disturbance or unavailability of communication system	Communication system	Improbable	Moderate	Low
PPD hacker	Insecure/uncontrolled PPD	Display of wrong or forged information to driver	Information displayed to driver	Conceivable	Moderate	High
PPD hacker	Insecure/uncontrolled PPD	Tracking and profiling of vehicles or vehicle drivers	Privacy	Conceivable	Moderate	Medium
Foreign PPD	PPD-V2X OBU interface & Message creation on PPD	Distribution of wrong or forged messages	(Safety) messages	Likely	Moderate	High
Foreign PPD	PPD-V2X OBU interface	Display of wrong or forged information to driver	Information displayed to driver	Conceivable	Difficult	Medium
Foreign PPD	PPD-V2X OBU interface & Message creation on PPD	Disturbance or unavailability of communication system	Communication system	Conceivable	Moderate	Low

TABLE I
RISK STATEMENTS

5. COUNTERMEASURES

This section identifies and discusses countermeasures, including the impact on overall system performance.

Several solutions to mitigate the *PPD-V2X OBU interface* vulnerability have been discussed in Section 2, e.g. link layer encryption or requiring wired links, or applying encryption and authentication on transport layer. Main challenge with these approaches is secure link setup, which can be addressed by well-known mechanisms like Wi-Fi Protected Setup (WPS), or proximity-based communication like Near Field Communication (NFC). With respect to performance, the impact is limited, especially in case link layer security is used because corresponding functionality is usually integrated in communication chipsets.

Message creation on PPD is a vulnerability that only applies to configurations 1 and 3. Potential solutions are

- *Tight application control:* only certified, authenticated and authorized applications are allowed to send messages to the V2X OBU. The V2X OBU periodically verifies the integrity of the applications.
- *Restricted message creation on PPD:* Configuration 3 implements parts of a simple countermeasure that can limit risk. By limiting for instance the BTP ports or message types an application on the PPD is allowed to use, the vulnerability can be limited to e.g. non-safety critical applications.
- *Plausibility checks:* V2X OBU performs plausibility checks on forwarded messages.

Drawbacks of all solutions are that they introduce some computational overhead and that they require updates on the V2X OBU if the Android application or the protocols are changed. To some extent, this contradicts the advantages of configuration 1 and 3. On the other hand, for non-safety critical extensions, *Restricted message creation on PPD* with configuration 3 looks like a viable compromise.

Insecure/uncontrolled PPD can be mitigated with some of the mechanisms that also helped with previous vulnerability. These are *Restricted message creation on PPD* and *Plausibility checks*. Note that *Tight application control* does not help as there could be some kind of software running on the PPD that provides the right answers to the control mechanism. Additional mechanisms against this vulnerability include usage of security frameworks on PPDs like the ones briefly mentioned by Bouard et al. [6].

6. CONCLUSIONS

Due to the increased presence and computing power of PPDs, they are more and more considered to become an integral part of in-vehicle system solutions. Such combined systems can offer higher flexibility but also help to overcome the problem of different lifecycles of automotive and consumer electronics alike.

Security is a challenging task when integrating consumer electronics and automotive systems, especially when PPDs have an influence on or are connected with safety critical systems, like in the usage for V2X communication. Specifically in this case, the more functionality is located in the V2X OBU, the simpler the control of the security impact. All three integration options have in common that they should employ an authorization of the application on the PPD in case the PPD is sending or triggering sending messages over the V2X link. In such case, the V2X OBU should also employ basic plausibility checks to prevent sending of false warning messages. For example, the V2X OBU should monitor vehicle movement through its own GPS receiver and prevent sending of ‘stationary vehicle warning’ messages while the vehicle is still moving. Consequently, the V2X-OBU may even refuse sending unknown messages, when accepting the inherent limitation of flexibility to the PPD integration concept.

The most secure solution can be achieved with configuration 2 because V2X messages are created by the V2X OBU. The most suitable compromise between flexibility/extensibility and security can be achieved with configuration 3. Basic safety services run on the V2X OBU, DENMs created on the PPD can be verified with plausibility checks. New message formats can either be allowed, blocked, or allowed after update of the corresponding plausibility check function on the V2X OBU.

In future work, we will investigate how the identified countermeasure can be integrated in our V2X communication-based Android driver assistance system *DriveAssist* [15].

REFERENCES

[1] S. Diewald, T. Leinmüller, B. Atanassow, L.-P. Breyer, and M. Kranz, “Mobile Device Integration and Interaction with V2X Communication,” in *Proceedings of 19th World Congress on Intelligent Transport Systems (ITS)*, Oct. 2012.

[2] S. Diewald, A. Möller, L. Roalter, and M. Kranz, “Mobile Device Integration and Interaction in the Automotive Domain,” in *AutoNUI: Automotive Natural User Interfaces Workshop at the 3rd International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, ser. AutomotiveUI ’11, Nov.–Dec. 2011.

[3] “The new Mercedes-Benz A-Class is ‘always on’: Mercedes-Benz puts the iPhone on wheels,” http://www.daimler.com, Feb. 2012.

[4] R. Bose, J. Brakensiek, and K.-Y. Park, “Terminal Mode: Transforming Mobile Devices into Automotive Application Platforms,” in *Proceedings of the 2nd International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, ser. AutomotiveUI ’10, Nov. 2010, pp. 148–155.

[5] Car Connectivity Consortium, “MirrorLink,” http://www.mirrorlink.com/, last accessed Jan. 2013.

[6] A. Bouard, J. Schanda, D. Herrscher, and C. Eckert, “Automotive Proxy-based Security Architecture for CE Device Integration,” in *Mobile Wireless Middleware, Operating Systems, and Applications*, C. Borcea, P. Bellavista, C. Giannelli, T. Magedanz, and F. Schreiner, Eds., vol. 65. Springer Berlin Heidelberg, 2013, pp. 62–76.

[7] M. Röckl, J. Gacnik, J. Schomerus, T. Strang, and M. Kranz, “Sensing the Environment for Future Driver Assistance Combining Autonomous and Cooperative Appliances,” in *Proceedings of the 4th International Workshop on Vehicle-to-Vehicle Communications*, ser. V2VCOM ’08, Jun. 2008, pp. 45–56.

[8] C2C-CC, “Car2Car Communication Consortium,” http://www.car-to-car.org/, last accessed Jan. 2013.

[9] J. Joy, A. Raghu, and J. Joy, “Architecture for Secure Tablet Integration in Automotive Network,” in *Proceedings of the FISITA 2012 World Automotive Congress*, ser. Lecture Notes in Electrical Engineering, vol. 194. Springer Berlin/Heidelberg, Nov. 2012, pp. 683–692.

[10] ETSI TS 102 637-2, “Intelligent Transport Systems (ITS); Vehicular Communications;

Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Technical Specification V1.2.1, March 2011.

[11] ETSI TS 102 637-3, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," Technical Specification V1.1.1, September 2010.

[12] ETSI TS102 636-5-1, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol," Technical Specification V1.1.1, February 2011.

[13] T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, "Modeling Roadside Attacker Behavior in VANETs," in *Proceedings of 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008)*, Nov.–Dec. 2008.

[14] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, ser. SP '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 447–462.

[15] S. Diewald, A. Möller, L. Roalter, and M. Kranz, "DriveAssist - A V2X-Based Driver Assistance System for Android," in *Mensch & Computer Workshopband*. Oldenbourg Verlag, Sep. 2012, pp. 373–380.