Multimedia Systems as Immune System to Improve Automotive Security?

Jana Dittmann, Tobias Hoppe, Claus Vielhauer

Multimedia Systems as Immune System to Improve Automotive Security?

Jana Dittmann[1], Tobias Hoppe[1]
[1] Otto von Guericke University Magdeburg
Germany

Claus Vielhauer[1, 2]
[2]Brandenburg University of Applied Sciences
Germany

***Abstract*—Our motivation is driven by the fact, that security mechanisms often cause additional efforts and costs, and need to be aligned with safety goals - protecting human and environment. Especially in the field of automotive security, producers are seeking cost efficient, environmental-condition-adaptive (robust) and fast approaches, if possible combined with existing concepts reusing resources. Initially, working in automotive security, it was easy to see that a wide variety of attacks is possible, e.g. using knowledge from classical computer and network security incidents. It became clear, that malicious activities on car IT systems might also lead to safety relevant issues such as accidents with threats to life or physical condition of the driver herself, occupants and people in the environment. We are inspired by the basic law of robotics established by I. Asimov[1] and apply it to automotive design: "1. A vehicle may not injure a human being, or, through inaction, allow a human being to come to harm. 2. A vehicle must obey orders given it by human beings except where such orders would conflict with the First Law. 3. A vehicle must protect its own existence as long as such protection does not conflict with the First or Second Law.". This entire bunch of requirements would cause "heavy" technology and expensive solutions. Coming from multimedia security, it became stepwise clearer that we cannot neglect known security mechanisms, but it is worth to combine them with knowledge about multimedia systems (MM systems). For example MM sensory, data streams, protocols, quality etc. enable the car to perceive the occupants and environment more precisely and can help to detect in-car and outside-car anomalies caused by security incidents with an estimation/prediction of harm. Existing automotive components designed for safety, entertainment and comfort services should be able to help in achieving secure and safe car behavior. In the article we discuss the opportunity to understand vehicles as single and cooperative MM systems with the ability to become an enabler for future automobile security detection, warning and reaction strategies – as a kind of vehicular immune system building Multimedia-enabled Asimovian Secure Automobiles (MASA).**

I. Multimedia Automobiles and Automobile Security challenges

IT has arrived in the automotive world since years. Comfort and safety goals guided and still guide the developments and car IT becomes increasingly complex; autonomous and self-interacting cars offer a wide variety of sensory and complex analysis logic for interaction and presentation.

The bad thing - Due to complex functional and structural component dependencies, vulnerabilities in design, implementation or configuration are very likely and may be exploited maliciously to cause security incidents. Motivations are manifold ranging from tuning, stealing, manipulations or unlocking of functions/restrictions up to infecting cars with malware disturbing or harming driver and occupants. Managing automotive security incidents has to face the challenge, that incidents should not cause any threat to life or physical conditions by ensuring fundamental Asimov laws, which is very seldom explicitly considered yet. Therefore several constraints arise, e.g. existing security mechanisms which stop and reconfigure or update hard- or software should not be applied whilst driving to avoid difficult handling by the driver. When vulnerabilities, e.g. as reported in [1], [2] and [3], get exploited in complex scenarios like downhill driving on a winding road, the car needs to recognize this as difficult situation and well-selected reactions are needed to keep the car well on the road. Using the findings from [4], we can summarize: the car needs complete and correct information of the initial state of the world, the car is the sole cause of change, and action execution is atomic, indivisible, and results in effects which are deterministic and completely predictable. Of course, the automotive world is not static or has complete information to derive and determine a perfect security mechanisms avoiding harm. The awareness of security as relevant business factor is raising, but producers need to balance their costs and resources by reusing existing components and implementations and try to reduce restrictions coming along with the introduction of security mechanisms.

II. The future: Multimedia enabled Security Incident Detection and Reaction

The good thing - automotive systems are mobile MM systems offering a wide variety of sensor and media technology enabling cars to perceive humans, other subjects and objects behavior or its environment and context more precisely. For example, car sensors determine inside climate, outside weather, road conditions, know vehicle speed even those from other objects, windows and doors states, distance to surrounding subjects and objects, can determine seat occupations, number of persons in the car, profile drivers and occupants (persons gender, age, weight, height) etc. This involves indeed a lot of MM acquisition aspects. Sensory data is communicated to electronic control units for analysis and appropriate adjustment, to driver – car-to-human – or, in future, to other cars (car-to-car) and infrastructure (car-to-infrastructure), e.g. to enable autonomous driving. Based on individual car sensors and available MM capabilities it should be possible to design and build a model about what a car can "see" and which information can be used and communicated for incident detection, warning and reaction. Based on safety functions in case of an incidents, the in-

[1] I. Asimov. 1942. Runaround. Astounding Science Fiction.

volved MM system should be able to determine the current driving situation and environment and which potential harm needs to be avoided. Further, it should be capable of a wide variety of driver support for handling incidents in a safe manner. Knowledge from MM systems can help to **better understand** car behavior, identify anomalies and implausible states. Of course car MM systems are not yet designed as security measure and there is still uncertainty about interplay of individual technical system states to the global system behavior on roads (e.g. imperfect data propagation). Conditions of individual drivers and occupants (health etc.), environment, other cars and car occupants etc. are very dynamic and not yet considered in a global manner and transferred into a context model to determine secure and safe states. E.g., [5] motivates complex multi-agent environment solutions as *adjustable autonomy* considering different humans' interaction with varying preferences, inaccuracies and uncertainties. In [6] vehicles behavior is understood as team context actions with uncertainty and mutual information mismatch. **How may MM systems become a use case for automotive security?** Some examples:

MM systems can support security incident handling to **make an informed decision by providing a detailed cross media analysis** of available data from car sensory and connected systems. Existing cross media analysis can help to further investigate fast algorithms in high speed drives and on highly dynamic media – with sensory data of different spatial/temporal resolution and quality, or with varying amounts of surrounding activities – e.g. activity level during low/high traffic.

Drivers and occupants interact with modern cars, environment and with infrastructure (other cars, their drivers etc.) causing complex interplay, further uncertainty, error or loss of information. **MM data needs to be interpreted in its context to determine secure and insecure states, potential error and loss within its dynamic environment**. A car context model might help to interpret cross media analysis results, considering different drives such as high/low speed or parking, to be able to predict harm and to achieve a more efficient reaction. **Enhancing context-based cross media analysis with consistency and plausibility checks** on signal, data, feature and application level are further examples. After malicious actions (such as handbrake activation requests at high driving speed), implausible behavior detected early in the particular context (analyzing all sensor data and fusing into driving context) can help to stop hazards already before they occur.

"*First aid*" *guidelines* can be defined and applied, controlling how the car should behave avoiding blackout situations before full recovery is performed in a secure and safe manner – e.g. in the next service station. Similar strategies are already applied today on failures of safety-critical components: default / fallback strategies like "limp home mode" for engine control units, override functions for automatic steering or emergency modes in the ESP system. For security incidents, a more fine granular analysis of component behavior and context seems possible to define sensor-dependent command variables enforcing normal behavior. Approaches might use **re-injection of all kind of available plausible data** known from context models to components/networks. Resources of other nodes could be shared via the network to take over functionality from a failing node, or considering **organic computing principles within MM context for self-healing**.

How to solve conflicts? To avoid harm, cross media analysis and car MM context can check consistency and plausibility to find anomalies and define reactions for the current driving context. Further questions arise: how to react when not all multilateral security and safety interests of the affected car(s) and human(s) can be satisfied? Is the safety of the infected car's driver more important than the safety of other humans – or how can the MM system help to understand cross-party content/context and communicate risks to others?

How can MM user interfaces be used to communicate security incidents and safety risks to drivers, occupants or even the environment? **Security warnings might be designed MM based and context-adaptive** (e.g. regarding speed and traffic), as already discussed e.g. for incident reactions [1]. Also the resilience behavior of individual drivers and occupants to technical incidents could be investigated and how MM systems can address this. Which MM elements (visual, acoustic, haptic …) should be selected, what advice should be given? After accidents, systems could evaluate context criteria to select first aiders and derive/communicate appropriate instructions [7].

In summary, it is worth to extensively study and enhance MM technology means as vehicular immune system to enhance security incident detection, reaction and warning to prevent harm. We see a great potential to understand vehicles as single and cooperative MM systems, also for future autonomous cars. Whilst a large number of MM acquisition, processing, analysis and understanding techniques have been developed specifically for investigating comfort and safety applications, relatively few attention has been paid to the understanding of automobile-related MM content for security incident handling. MM systems can be a substantial enabler of immune systems for future automotive security to avoid/reduce harm by building *Multimedia-enabled Asimovian Secure Automobiles (MASA)*.

Acknowledgements: This work was partly supported by German Research Foundation, project ORCHideas (DFG GZ: 863/4-1). Thanks to A. Lang, S. Kuhlmann, S. Kiltz, M. Hildebrandt and J. Fruth for our joint work during the last six years.

REFERENCES

[1] T.Hoppe, S.Kiltz, J.Dittmann. 2009. Applying intrusion detection to automotive IT - early insights and remaining challenges. Journal of information assurance and security, Vol. 4. 2009, 3, ISSN: 1554-1010.

[2] T.Hoppe, S.Kiltz, J.Dittmann. 2011. Security threats to automotive CAN networks: practical examples and selected short-term countermeasures, In: Reliability engineering & system safety, Elsevier, Vol. 96.2011, 1.

[3] K.Koscher et al.., 2010. Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, 2010.

[4] D.Weld, O.Etzioni. 1994. The first law of robotics (a call to arms). Proceedings of the twelfth national conference on Artificial intelligence (vol.2), AAAI'94, ACM, USA, ISBN 0-262-61102-3.

[5] D.V.Pynadath, M.Tambe. 2002. Revisiting Asimov's First Law: A Response to the Call to Arms. ATAL '01, Springer, ISBN 3-540-43858-0.

[6] N.Schurr et al.. 2007. Asimovian multiagents: applying laws of robotics to teams of humans and agents. 4th international conference on Programming multi-agent systems, ISBN: 978-3-540-71955-7.

[7] S.Tuchscheerer, T.Hoppe, C.Krätzer, J.Dittmann. 2011. FirstAidAssistanceSystem (FAAS). Intelligent robots and computer vision XXVIII, Proceedings of SPIE; 7878.