

eSecurity WG - A4: Security Requirements -DRAFT-

Frank Kargl
Ulm University
frank.kargl@uni-ulm.de

October 15, 2007

1 Introduction and Definitions

This document aims at analyzing the security requirements for eSafety applications. It is based on several earlier documents that have been provided by research projects or individual research groups and tries to compile and integrate their views.

As the author of this document is also involved in the EU IST project SeVeCom¹, the work done there heavily influences the thoughts expressed here. To get an overview on the security requirements analysis done in SeVeCom, have a look at Deliverable 1.1 [RKAKFK06] and [KMS06]

Futhermore, some significant work on security requirements for vehicular communication systems has been done in the frame of the Network on Wheels project², described especially in [AABBFD⁺06] and at the work analyzing security in vehicular networks done at EPFL [RH07]. Finally also [BPAP05] addresses security requirements in VANETs.

The overall goal of our work is to create dependable eSafety system. IFIP defines dependability as

The property of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) which interacts with the former.

Dependability has two aspects: Safety and Security. Safety is used with a slightly different meaning here than in the traffic domain. In traffic, safety describes the fact that driving is safe, so e.g. no accidents occur. In the context of dependability, safety might be defined as

¹Secure Vehicle Communication; see <http://www.sevecom.org/>

²see <http://www.network-on-wheels.de/>

The condition of being safe from unwelcomed consequences of unintentional failure caused by exceptions in the operating environment, e.g. power/hardware failures, random/wrong input, disk full, etc.

Whereas safety assumes rather random or at least unintentional failures, security addresses dependability problems created on purpose. Wikipedia describes information security like this:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.[1] The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.³

As mentioned there, confidentiality, integrity, and availability are the predominant security goals – or security requirements – in any IT system. Also the necessity to have one or the other might depend on the application, when discussing security requirements it is a reasonable approach to start the discussion with these three items and analyze how important they are in the specific domain and what they actually mean. Next, there are also some related or secondary security goals/requirements that also play a role in eSafety system. In this document we also address authentication, access control, non-repudiation, and privacy.

Table 1 shortly summarizes the primary security requirements and gives a preliminary estimation on how important the individual security requirements might be in the context of eSafety applications. Table 2 does the same with secondary security requirements. As one can see, primary security requirements often mandate secondary requirements, e.g. in order to ensure confidentiality in a communication system, the communicating parties first need to authenticate each other. Next, we will discuss the individual requirements and their relationship with eSafety.

2 Integrity

2.1 In-vehicle aspects

Integrity aspects inside the vehicle IT system include the prevention of modifications of in-vehicle communication on internal communication busses by external entities, i.e. it should be impossible to tamper with internal communication via external communication interfaces.

Even more critical, the integrity of on-board software needs to be protected from attackers, i.e. no unauthorized party with access to the external communication link or the car should be able to modify the on-board software.

³see http://en.wikipedia.org/w/index.php?title=Information_security&oldid=163453646

Name	(Short) Definition	Esteemed Importance
Authentication	Ensure the claimed identity	Integrity of data plays a major role in eSafety applications, as maliciously modified data can cause a lot of damage
Confidentiality	Prevent unauthorized disclosure of data	Confidentiality is not required for most eSafety applications, as the data to be transferred is mostly public data (e.g. warnings) that should be made public in contrast to being kept confidential
Availability	Prevent unauthorized reduction of data/system availability	The importance of system availability depends heavily on the actual scope of applications and the reliance which people put on these systems. Whereas the failure of an optional warning application will be easily compensated by a careful driver, the failure of an automated driving system will be disastrous.

Table 1: Primary Security Requirements

Another aspect is the integrity of sensor readings, e.g. positioning information or radar information. The data path of this information from the sensor, through on-board systems, to the communication link should also be integrity protected.

2.2 Inter-vehicle aspects

Integrity also plays a vital role in inter-vehicle communication. Messages and the information contained need to be protected from modification while being in transit or forwarded by another node.

Whereas this is comparatively easy in simple beaconing or flooding schemes, it gets by far more demanding as the forwarding schemes become more complex and involve e.g. aggregation of information in relaying nodes.

2.3 More aspects

Integrity is usually ensured using some kind of signatures or message authentication codes. This then creates the demand for key distribution centers or PKI like structures to ensure key authenticity and/or integrity. However, the additional effort to establish these structures needs to be considered as well as the fact that these classical methods will not be sufficient once the data dissemination strategies become more complex. So methods that check the consistency of data by some other means (e.g. using heuristics, cooperative checks, reputation systems) need to be considered.

Another important observation is that in-vehicle security is mandatory for establishing

Name	(Short) Definition	Esteemed Importance
Authentication	Ensure the claimed identity	For most eSafety applications, knowing the identity of communication partners is of secondary importance. Other aspects like attribute authentication are more relevant
Access Control	Decide on access to services/data; Access Control = Authentication + Authorization	Most eSafety services/data will be public, therefore authorization/access control will be relevant only to a small number of closed (paid) applications
Non-repudiation	Prove originator of message/information; provides Accountability	Depends on the kind of liability properties that stakeholders want to have
Privacy	Prevent privacy infringements, i.e. leakage of private data to unauthorized parties	Privacy is a major concern esp. in Europe and a distinguishing feature compared to non-European activities

Table 2: Secondary Security Requirements

inter-vehicle security. Because as e.g. on-board sensors are tampered with or the software a large number of vehicles might be modified, it becomes very hard to ensure the integrity of the communication system.

DRAFT: in this subsection we should reference specific attacks that target integrity from the other documents.

3 Confidentiality

3.1 In-vehicle aspects

Inside the vehicle, confidentiality is mostly about preventing unauthorized access to data inside the control units or the data communicated over internal busses. A motivation for this could e.g. be to protect competitors of car manufacturers from analyzing the internal software or communication protocols of another brand's cars. Another aspect could be the unauthorized cloning of certain software and copying it from one car to another, e.g. to enable certain features which the second car owner has not paid for.

3.2 Inter-vehicle aspects

If thinking of software updates in the field, the motivation for protecting some data while communicated over the air becomes obvious. Another aspect where confidentiality is required is when e.g. people communicate personal information (music playlists, inter-vehicle messages, ...).

3.3 More aspects

One should note that the confidentiality requirements do not really address typical eSafety applications, but are more concerned with personal privacy of comfort applications or protection of intellectual property of car manufacturers.

In order to ensure confidentiality, standard mechanisms include encryption can be used, but again the situation becomes more complex when the communication mechanisms do so.

DRAFT: in this subsection we should reference specific attacks that target confidentiality from the other documents.

4 Availability

The need for availability in eSafety systems – no matter if in-vehicle or inter-vehicle – depends very much on the way applications are designed. If the applications are mere warning applications, the absence of the warnings primarily mean that the driver is back to the state without the eSafety system. Depending on how much the driver relies on getting the warning, this might however still lead to accidents. He might e.g. neglect the necessary precaution and drive too fast in curves where there is no curve speed warning.

If the eSafety applications interfere with the actual driving process, non-availability might have even more devastating effects. One general conclusion is to design the eSafety systems failsafe, i.e. if availability for whatever reason is degraded, the driving safety should be not less than today.

This is however beyond the scope of pure security, as also safety and the overall application design is involved. The part of security is to design the systems in a way that intentional Denial of Service attacks become harder.

4.1 In-vehicle aspects

In in-vehicle security, availability needs to be ensured for driving-critical systems. As these systems rely more and more on IT systems, one way to secure them from attacks is to prevent access/modifications to the car-internal systems by means of tamper-proof hardware and software design.

4.2 Inter-vehicle aspects

Guaranteeing availability in the inter-vehicle communication system is very hard, as certain kinds of attacks (jamming, overloading, ...) are difficult to prevent.

4.3 More aspects

DRAFT: in this subsection we should reference specific attacks that target availability from the other documents

5 Authentication

5.1 In-vehicle aspects

Authentication of car-internal components may help preventing all kind of replacement and spoofing attacks, ensure that only genuine parts are used, and only authorized repair personell changes the car configuration.

5.2 Inter-vehicle aspects

There are different forms of authentication that are relevant in this context. Entity authentication, i.e. the precise identification of individual cars, is often not so relevant in vehicular communication, as the cars surrounding yourself are usually unknown to you anyway. It is more important to reliably distinguish different cars, i.e. to prevent so called Sibyl attacks where one node spoofs the existence of multiple others cars.

The other relevant form of authentication is so called attribute authentication where vehicles are ensured of certain attributes of the communication partner, e.g. the type of object (car, truck, RSU), its dimensions, maximum speed, the location of RSU etc. These kind of information can then be used for data consistency checks to ensure integrity or availability of the communication system.

5.3 More aspects

Authentication can be ensured by various authentication protocols, using cryptographic mechanisms like Message Authentication Codes or asymmetric Digital Signatures. As eSafety communication has often a broadcast addressing, interactive protocols are difficult to use and unidirectional protocols are to be preferred.

Authentication is very often a mandatory step to later ensure e.g. confidentiality, integrity, or access control. One open question is how authentication should be performed in case of complex message dissemination strategies that include aggregation, etc.. Finally, there is a natural contradiction of (entity) authentication on the one hand and privacy requirements on the other hand.

DRAFT: in this subsection we should reference specific attacks that target availability from the other documents

6 Access Control

6.1 In-vehicle aspects

Access to different in-vehicle communication systems (like control busses, etc.) is to be strictly controlled to avoid tampering of external entities with in-car components. This can be done e.g. by means of either a complete separation of car-control and communication systems or by having firewalls in place that strictly govern the kind of communication possible between internal and external systems.

Communication relationships between different in-vehicle components might need access control mechanisms, too. Then e.g. certain sensors may only be read by authorized components but not by others and certain actuators (e.g. the braking system) might only be influenced by in-vehicle controllers (but e.g. not by the on-board communication unit).

6.2 Inter-vehicle aspects

The role of access control in inter-vehicle communication is rather limited. As usually all nodes – or at least all valid vehicles – should participate in the vehicle communication system, participation should be free. Only non-vehicles claiming to be a vehicle (e.g. attackers with laptops) should be denied access to eSafety applications.

For other kinds of applications (like software downloads, messaging, internet access) individual access control decisions have to be implemented based on the relevant business models, but this is beyond the scope of eSafety and will usually be implemented with specific access control mechanisms on the application layer.

6.3 More aspects

DRAFT: in this subsection we should reference specific attacks that target availability from the other documents

7 Non-Repudiation

In general, non-repudiation requires a combination of authentication and tamper-proof data recording.

The requirements for non-repudiation in inter-vehicular communication depend heavily on what you want to do with this information later. If you want to use communication information in court, a very stringent form of non-repudiation is required. This might include the need to prevent/impede cloning of identifiers, e.g. by embedding key materials in tamper-resistant hardware.

7.1 In-vehicle aspects

It is unclear what role non-repudiation plays in in-vehicle security. It might be useful to prove responsibility in case of accidents to decide on liability of suppliers or OEMs in case of technical failures. An on-board electronic data recorder (EDR) could also record the actions of the driver and the vehicle to later prove responsibility of a driver for an accident.

7.2 Inter-vehicle aspects

Non-repudiation requirements in inter-vehicle communication also depend on the legal framework in which the information is to be used. This might need e.g. tamper-proof devices to prevent copying of identifiers to other cars. Otherwise, vehicles might impersonate as other vehicles and non-repudiation of communicated messages is not given.

7.3 More aspects

Some stakeholders have strong objections against this use of eSafety systems, because data from the communication/in-vehicle systems might be used to prove the guilt of car owners, suppliers, OEMs, etc. Overall, the role of non-repudiation is not clear at the moment.

DRAFT: in this subsection we should reference specific attacks that target availability from the other documents

8 Privacy

8.1 In-vehicle aspects

As in-vehicle data of eSafety systems is to remain inside the car, privacy protection is no primary goal of in-vehicle security. The EDRs discussed in the last section might be an exemption from this. If EDRs are to be installed, this should be controlled by binding regulations when and how to use this data to prevent privacy infringements.

8.2 Inter-vehicle aspects

Vehicular communication can be used to track drivers and create location profiles which needs to be prevented. Some argue that tracking is already possible by today's technologies like GSM. SeVeCom has created a document that discusses these arguments and shows that the situation in vehicular communication is significantly different. Ensuring location privacy can either be done by hiding the position or the identity of cars. As precise position information is mandatory for many eSafety applications, the preferred solution should be to hide identities of other cars/drivers.

8.3 More aspects

The approach to inter-vehicular communication privacy discussed most often today is the use pseudonyms that will not reveal the identities of cars/drivers. However, research has shown that there are a lot of potential problems in simple pseudonym system that need to be addressed.

DRAFT: in this subsection we should reference specific attacks that target availability from the other documents

References

- [AABBFD⁺06] Amer Aijaz, Bernd Bochow, Florian Dötzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmüller. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Int'l Workshop on Intelligent Transportation (WIT)*, March 2006.
- [BPAP05] Bryan Parno and Adrian Perrig. Challenges in Securing Vehicular Networks. In *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, November 2005.
- [KMS06] Frank Kargl, Zhendong Ma, and Elmar Schoch. Security engineering for vanets. In *4th Workshop on Embedded Security in Cars, escar 2006*, Berlin, Germany, November 2006.
- [RH07] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.
- [RKAKFK06] Rainer Kroh, Antonio Kung, and Frank Kargl. Threats and requirements analysis. Deliverable 1.1, SeVeCom Project, 2006.