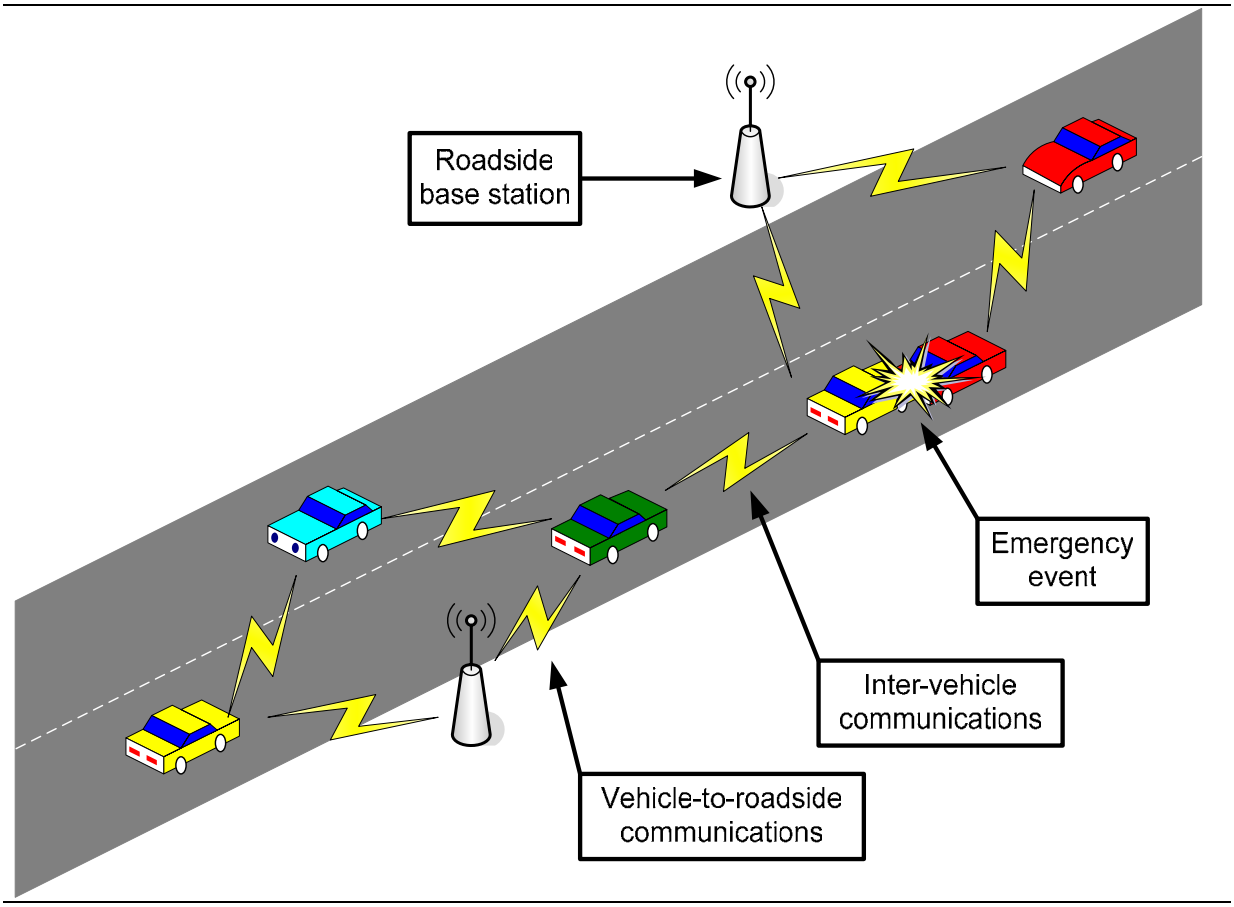


Security Aspects of Inter-Vehicle Communications

Maxim Raya, EPFL
Jean-Pierre Hubaux, EPFL

Conference paper STRC 2005

STRC | 5th Swiss Transport Research Conference
Monte Verità / Ascona, March 9-11, 2005

Security Aspects of Inter-Vehicle Communications

Maxim Raya
EPFL-IC-LCA
Lausanne

Phone: 021 693 2648
Fax: 021 693 6610
email: maxim.raya@epfl.ch

Jean-Pierre Hubaux
EPFL-IC-LCA
Lausanne

Phone: 021 693 2627
Fax: 021 693 6610
email: jean-pierre.hubaux@epfl.ch

March 2005

Abstract

Inter-Vehicular Communications (IVC) are a cornerstone of the future intelligent transportation systems. A crucial enabling component of IVC is its security and privacy. Indeed, as vehicular computing systems become interconnected, there will be new venues for attackers to exploit system vulnerabilities. In addition, proper security mechanisms can assist in law enforcement and automate payment operations, such as toll collection. Leveraging on experience gained from other networks like the Internet or wireless LANs, system security for vehicular networks has to be introduced in the design phase. In the following sections, we outline several security threats encountered in IVC, then we present the obstacles needed to overcome in order to cope with these threats. Finally, we describe several tools that will be helpful in building secure IVC networks.

Keywords

Inter-vehicle communication – vehicular networks – security

1. Introduction

Despite the big improvements in road safety in the last decade, fatalities in Switzerland caused by road traffic accidents still accounted for 546 persons in 2003 [8]. The quest for better safety is still ongoing, relying on technologies, such as electronic car safety systems, better road equipment, and radio traffic information. Recently, a new major player has joined the team, namely Inter-Vehicle Communications (IVC) and Roadside-to-Vehicle Communications (RVC) [3, 12, 16]. Using wireless radio technologies that mainly rely on the popular IEEE 802.11 [7] standard for wireless networks, IVC technology researchers and developers are set up for enabling vehicles to talk to each other, sometimes aided by roadside infrastructure. The benefits are multifold and the applications are numerous. The DSRC[1] tutorial [1] lists around forty applications, including cooperative driving, collision avoidance, traffic information, vehicle diagnostics, toll collection, and entertainment. And although the dream of fully autonomous cars is still futuristic, self-organized networks of vehicles will be a reality soon.

Yet, by introducing more intelligence and complexity in vehicles, major responsibilities will arise, not only from the safety point-of-view but also the security aspect. In fact, wireless communications have always been prone to higher security threats than their wired counterparts. And given the high reliability required of IVC and the large amount of potential financial transactions (e.g., toll collection), IVC will soon be the target of malicious users. Hence comes the need for a high level of security that can cope will all kinds of existing and future attacks on wireless networks.

Despite these important stakes, the security of vehicular networks has not been sufficiently addressed in any related ongoing projects. It seems that there is a risk of the common and flawed practice of introducing security only after deployment slowly taking place in IVC. To address this problem, in this paper we highlight the main security issues in IVC by describing the related challenges and the imposing threats. In addition, we provide a set of security tools and services that can be the bricks for building robust security architecture for IVC.

The paper is organized as follows. Section 2 presents the related work; Section 3 describes several security attacks on IVC; Section 4 lists the challenges to be overcome in order to provide IVC security; Section 5 introduces the security toolbox that can be used to counter the some of the previously described attacks; and Section 6 concludes the paper.

[1] DSRC stands for “Dedicated Short Range Communications” and is the draft standard for vehicular communications.

2. Related work

The work on IVC has started several years ago in both academic institutions and industrial reasearch labs. Yet security has been almost left out of these efforts so far, especially by industrial projects, following the common practice of introducing it only after the initial products become subjected to security threats. Recently, some academic research teams have started addressing this subject, although existing work is still highly theoretical and does not specify concrete solutions.

The most prominent articles on this subject are [9], [15], and [22]. In [9], the authors describe a security architecture for vehicular communications intended mainly to counter the so-called "intelligent collisions" (meaning that they are intentionally caused) by using an infrastructure of digital signatures[2]. But this is only one type of attacks and building the security architecture requires awareness of as many potential threats as possible. The authors of [15] take a different perspective of IVC security and focus on privacy and secure positioning issues. They point the importance of the tradeoff between liability and anonymity and also introduce Electronic License Plates (ELP), unique electronic identities for vehicles. The work in [22] describes an infrastructure for vehicular communications and briefly mentions some related security issues and possible solutions. None of these works provides a global view of IVC security that includes the threat model, the constraints, and the available solutions.

Other works tackle very specific subjects in IVC such as the use of digital signatures for vehicular communications [13], or the detection of erroneous data [14]. A software framework for mobile commerce security in IVC is proposed in [10].

In parallel with the academic efforts, industry has also contributed to the definition and fulfillment of security needs in vehicular communications. The most important work is carried out by the industrial consortium that launched DSRC in the context of the IEEE P1556 Working Group (Security and Privacy of Vehicle and Roadside Communications including Smart Card Communications). Yet the results of this working group are not publicly available.

[2] In communication security, digital signatures, the cryptographic equivalent of hand-written signatures, are used to verify the identity of the message signer.

3. Threats

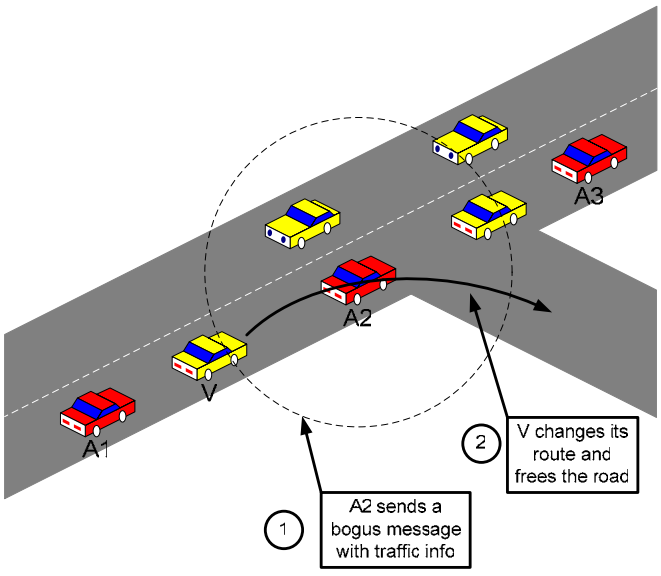
Before proposing security solutions for IVC, it is important to construct a threat model able to encompass all possible attacks on vehicular networks. In addition, describing specific attacks on these networks would enable security designers to choose the right minimum set of tools in order to counter these attacks. We categorize security threats into three groups according to the application type that they target:

1. **Attacks on safety-related applications:** safety-related applications [20, 21] are the major incentive behind the development of IVC. As they are required to provide a high level of liability, their security should be no less important. The results of an attack on these applications can be not only annoying (e.g., causing traffic congestion) but also disastrous leading to accidents and losses of lives.

2. **Attacks on payment-based applications:** a considerable number of IVC applications will involve financial transactions, e.g., for toll collection, payment for location-based services, and insurance. This will inevitably create a set of corresponding financial frauds that leverage on the open nature of wireless communications.

3. **Attacks on privacy:** one of the major concerns in future vehicular networks is the question of privacy. In fact, enabling vehicles to communicate with each other will allow tracking their drivers. This would create a Big Brother phenomenon over a large scale.

Figure 1: Bogus information attack

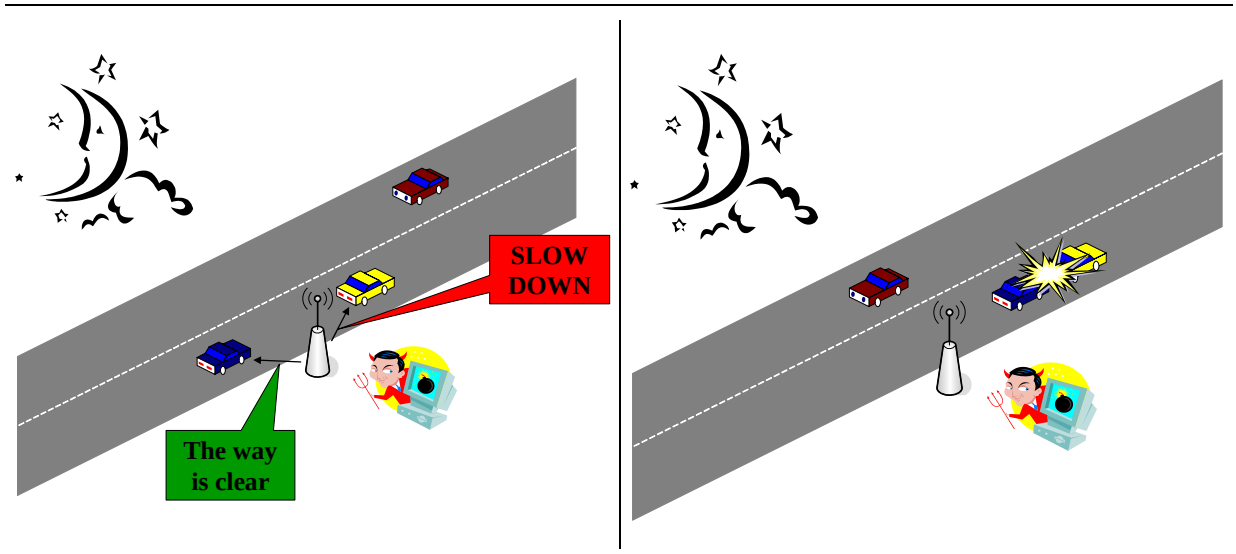


3.1 Specific attacks

In this section we describe several example attacks on vehicular networks.

1. **Bogus information attack:** In this case, the attacker disseminates false information in the vehicular network in order to affect the decisions of other drivers. For example, as Figure 1 shows, several drivers may collude in order to help each other arrive to their destinations faster. Vehicle A2 sends messages indicating to all following vehicles that the road they are taking is congested after a short distance. As a result, the drivers of these vehicles may change their routes in order to avoid congestion by following different roads. The result is that the road is freed in front of vehicle A1 that can go faster. Although this example attack is rational, the same mechanism can be used to create congestions on specific roads for malicious reasons. This attack belongs to the first category of threats.

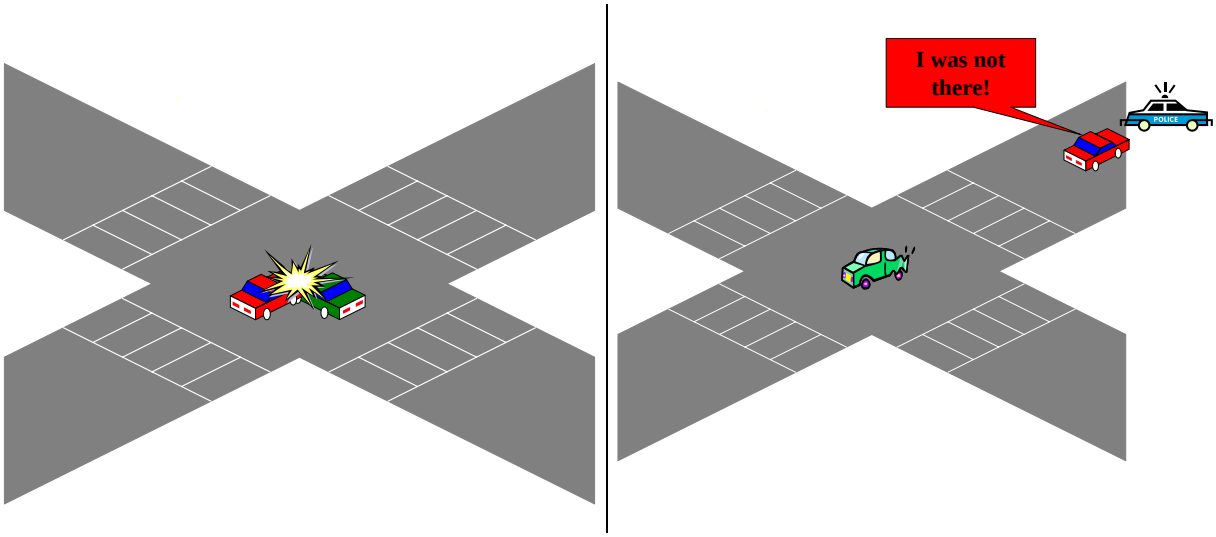
Figure 2: Disruption of network operation attack



2. **Disruption of network operation:** the aim of this attack is to prevent the network from carrying out safety-related functions. There are many ways to perform this attack, either by sending messages that would lead to improper results or by jamming the wireless channel (this is called a Denial of Service, or DoS, attack) so that vehicles cannot exchange safety messages. The example in Figure 2 illustrates the first case: a malicious attacker sends contradictory messages to two vehicles, one behind the other, during a night drive. As one vehicle receives a message warning it of congestion ahead and slows down, the following vehicle receives a message saying that the road ahead is clear and hence it speeds up. The worst-case scenario is when an accident results because of this manipulation. The DoS attack consists in jamming the wireless channel thus interrupting all communications. It can be used against both

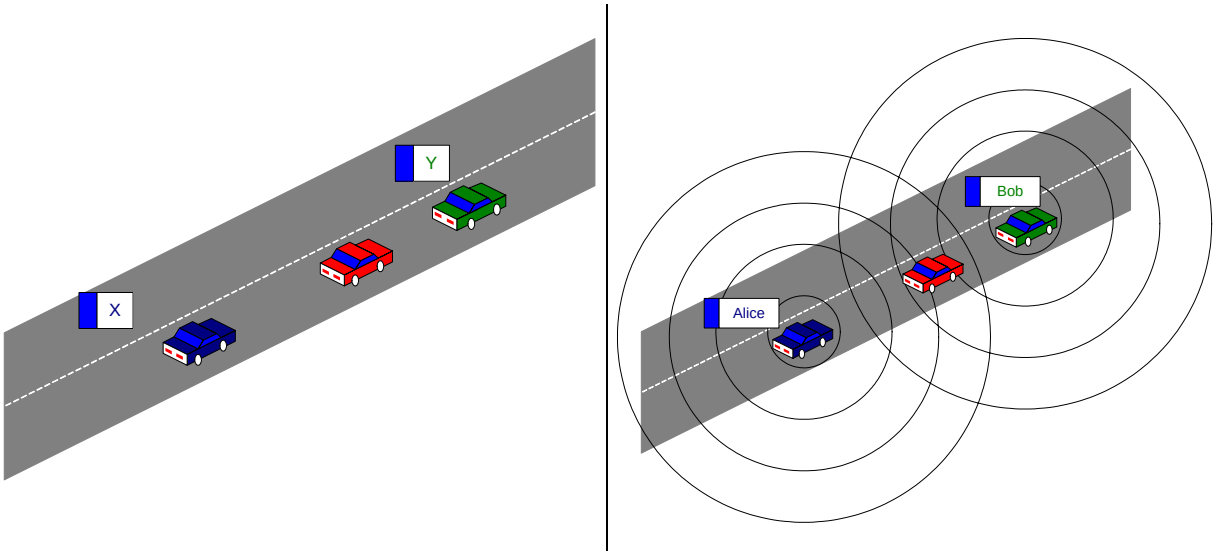
safety-related and payment-based applications and is one of the hardest security problems in IVC.

Figure 3: Cheating attack



3. **Cheating with identity, speed, or positioning information:** in cases where liability is involved, drivers may be tempted to cheat with some information that can determine the location of their car at a given time. For example, as Figure 3 illustrates, a vehicle may be involved in an accident and then claim that it was not on the spot when the accident happened. This can be done by tweaking the reported speed or location information. Although this example applied to safety-related applications, cheating with identity by *impersonation* can also be very useful in attacks on payment-based applications.

Figure 4: Identity disclosure attack



4. **Identity disclosure attack:** this is the Big Brother scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way freight companies track their trucks). To monitor, the global observer can leverage on the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbors of the target and collects the required data!). The attacker can be only passive in this case (listening to the wireless transmissions of surrounding vehicles as Figure 4 shows), thus making the attack impossible to detect. We assume that the attacker does not make use of cameras, physical pursuit, or onboard tracking devices to track his target; otherwise, the tracking problem becomes simpler but also more expensive and tied to few specific targets, and it can be done anyhow based on existing license plates. This attack exemplifies the last category of threats.

4. Challenges

The provision of robust security for vehicular networks must overcome a set of technical, economic, and social challenges, which we overview in this section.

4.1 Network scale and dynamics

Vehicular networks will be the largest real-life instance of self-organized ad hoc networks. Its size will be in millions of nodes, distributed among different authorities and services providers. Problems of scalability and seamless interoperability should be solved in a way transparent to the driver, especially that most operations are performed on-the-fly while the vehicles are moving at high speeds. This brings the challenge of mobility into the picture, as vehicles will not be able to participate in long-term security protocols because of the high dynamicity of the network (e.g., two cars crossing each other on the highway have only few seconds to exchange, mainly safety-related, information).

4.2 Privacy

One of the major consumer concerns about the IVC technology is its potential influence on privacy. Attack 4 shows how privacy can be hijacked without the victim even knowing that. Although there are solutions that can provide vehicle and driver anonymity, this may negatively affect the liability of the network. In fact, if vehicles are totally anonymous, those involved in an accident and fleeing the scene may not be easily identified. Hence, a balance should be kept between the privacy and liability of drivers. One way to do that is to allow law enforcement authorities to uncover the identities of some vehicles only after getting the permission of a court.

4.3 Trust

A key element in a security system is trust. This is particularly emphasized in vehicular networks because of the high liability required from safety applications and consequently the vehicles running these applications. Due to the large number of independent network members (i.e., they do not belong to the same organization) and the presence of the human factor, it is highly probable that misbehavior will arise. In addition, consumers are becoming increasingly concerned about their privacy. Drivers do not make an exception, especially because the lack of privacy and the related potential of tracking may result in high financial charges on the drivers (e.g., due to occasional over speeding). As a result, the level of trust in vehicles as well as service provider base stations will be low. Beside drivers and service providers, there will be a considerable presence of governmental authorities in IVC. But due

to the reasons stated above, trust in these authorities will only be partial (e.g., a given police officer may abuse his authority if given full trust).

4.4 Cost

Cost is another inhibitive factor in the deployment of IVC solutions. In fact, the introduction of new communication standards, such as DSRC, for vehicular communications will require manufacturers to install new hardware modules on all vehicles, thus increasing the unit cost for consumers. Another costly addition will be the infrastructure that will allow vehicles, e.g., to access online authorities as part of security services, such as authentication. These costs should be minimized keeping sufficient support for vehicular networks applications.

4.5 Gradual deployment

The time span of IVC deployment until it reaches considerable penetration is around a decade [18]. This means that only a small proportion of vehicles will contain the enhanced features of IVC over the next couple of years. Yet, this functionality should still be supported despite the low penetration rate. This also applied to security services where, for example, protocols should be performed without the widespread existence of roadside infrastructure. This means that vehicles should be able to carry out most of the security functions autonomously.

5. Security toolbox

We have selected a set of existing and new security tools that can potentially cope with the threats described in Section 3 and overcome the challenges presented in Section 4. Hereafter are the major elements of this toolbox.

5.1 Electronic License Plates

Electronic License Plates (ELPs) [15] are unique cryptographically verifiable numbers that will be used as equivalents of traditional license plates. The advantage of ELPs is that they will automate the paper-based document checkup of vehicles. It will also allow the detection of stolen cars. ELPs will be used to identify vehicles, for example, when crossing country borders or during the annual technical checkup. ELPs may be issued by governmental transportation authorities, although an ELP should be also valid outside its country of issuance. Typically, an ELP will be accompanied by a digital signature of the issuing authority that certifies its validity. Hence, authorities should have cross-certification agreements that will allow them to verify the ELPs issued by the other authorities.

5.2 Vehicular PKI

A PKI (Public Key Infrastructure) is the typical security architecture used for networks where the presence of online authorities is not always guaranteed. Given the properties of large scale and initially low penetration of vehicular communications infrastructure, a Vehicular PKI is a good choice for enabling IVC security. In a VPKI, each vehicle will be equipped with one or more private/public key pairs certified by a Certification Authority (CA), whereby a message sender will use the private key is used mainly to generate digital signatures on messages that need to be certified and the message receiver will use the corresponding public key to verify the validity of the message. Although this architecture seems very convenient for vehicular networks, some problems still exist. One of them is key distribution, which allows message receivers to obtain the public keys of message senders. Another problem is certificate revocation, by which a CA invalidates some private/public key pairs due, for example, to their discovery by an attacker. A third problem of PKI is increased overhead, especially in terms of digital signature sizes and the accompanying signature generation, verification and transmission delays, although this is alleviated by the fact that onboard computers and communication facilities in vehicles will be powerful enough to handle this overhead. The comparison of several existing digital signature algorithms (RSA Sign [6], ECDSA [2], and NTRUSign [5]) in [17] shows that some of them are promising (ECDSA due to its small signature size and NTRUSign due to its fast signature generation and verification) for use in vehicular networks.

5.3 Event Data Recording

Similar to the black boxes on airplanes, Event Data Recorders (EDRs) will be used in vehicles to register all important parameters, especially during abnormal situations, such as accidents. This data can be later used for crash reconstruction and the distribution of responsibility on the involved drivers. Recently, some insurance companies have equipped their customer vehicles with such EDRs to collect information related to driving habits, such as average speed and number of driving hours, and consequently compute the insurance costs [4].

5.4 Tamper-proof hardware

Vehicles will store cryptographic material such as ELPs and VPKI private/public keys in tamper-proof hardware that will keep this material safe from attackers, thus decreasing the possibility of information leakage. This is further motivated by the fact that car electronics are inevitably vulnerable to attacks, especially the data buses responsible for transferring information and control commands between the different electronic components of a vehicle. The tamper-proof box will take care of signing and verifying messages so that they cannot be altered even if the data buses are hacked.

5.5 Data correlation

Contrary to some attacks that can be detected, like the DoS attacks, the bogus information attack cannot be easily discovered as it relies on sending false but seemingly valid messages. The solution to this problem can be in using data correlation techniques that will collect data received from different sources and thus allowing the vehicle to make a decision on the level of credibility, consistency, and relevance of the received information. Such technique have been recently explored in the context of a data reputation system [14].

5.6 Secure positioning

As described in Attack 3, a vehicle can cheat with its position to escape liability in an accident that it caused. Hence there is a need for secure position verification . In addition, vehicles or base stations may want to verify the position of other vehicles or base stations on-the-fly to ensure they are communicating with the claimed party. Although GPS [11] is a common positioning tool in automotive, it has security weaknesses [19]. An alternative may be “verifiable multilateration” [15] that works by measuring the distances from three points (vehicles) to a claimant (the vehicle whose position is being verified) and verifying that the claimed position is consistent with the measured one.

6. Conclusion

The security of vehicular communications is an important component of the successful launch of this technology. In fact, as with other networking and especially wireless technologies, IVC will be the subject of many kinds of attacks with potentially fatal consequences. In this we have highlighted the issue by describing the various security aspects of IVC. We have categorized the attacker and the security threats and substantiated the different categories with specific attacks. We have also discussed the main challenges facing IVC security. Finally, we proposed a toolbox that would enable security architecture designers to choose the most suitable solutions to counter the previously described threats.

7. References

1. 5.9 GHz DSRC. http://grouper.ieee.org/groups/scc32/dsrc/index.html.

2. Digital Signature Standard (DSS). http://csrc.nist.gov/cryptval/dss.htm.

3. http://ivc.epfl.ch.

4. http://www.norwichunion.com/pay-as-you-drive/.

5. http://www.ntru.com.

6. http://www.rsasecurity.com.

7. IEEE 802.11a, Wireless LAN Medium Access Control and Physical Layer Specifications High-Speed Physical Layer in the 5 GHz Band, 1999.

8. Road traffic accidents, 1965–2003, Swiss Council for Accident Prevention bfu, 2004.

9. Blum, J. and Eskandarian, A. The threat of intelligent collisions. *IT Professional*, *6* (1). 24–29.

10. Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M. and Tang, J.-M., Framework for security and privacy in automotive telematics. in *Proceedings of the 2nd international workshop on Mobile commerce*, (2002), ACM Press, 25–32.

11. Enge, P. Retooling the Global Positioning System. *Scientific American*.

12. Enkelmann, W., FleetNet - applications for inter-vehicle communication. in *IEEE Intelligent Vehicles Symposium*, (2003), 162–167.

13. Gollan, L. and Meinel, C., Digital signatures for automobiles. in *Systemics, Cybernetics and Informatics (SCI)*, (2002).

14. Golle, P., Greene, D. and Staddon, J., Detecting and correcting malicious data in VANETs. in *Proceedings of the first ACM workshop on Vehicular ad hoc networks*, (2004), ACM Press, 29–37.

15. Hubaux, J.-P., Capkun, S. and Luo, J. The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine*, *2* (3). 49–55.

16. Luo, J. and Hubaux, J.-P. A survey of Inter-Vehicle Communication *Technical Report*, EPFL, 2004.

17. Raya, M. and Hubaux, J.-P. The security of vehicular networks *Technical report*, EPFL, 2005.

18. Samuel, P. Of sticker tags and 5.9GHz. *ITS International*.

19. Warner, J.S. and Johnston, R.G. Think GPS Cargo Tracking = High Security? Think Again *Technical report*, Los Alamos National Laboratory, 2003.

20. Xu, Q., Mak, T., Ko, J. and Sengupta, R., Vehicle-to-vehicle safety messaging in DSRC. in *Proceedings of the first ACM workshop on Vehicular ad hoc networks*, (2004), ACM Press, 19–28.

21. Yang, X., Liu, J., Zhao, F. and Vaidya, N., A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning. in *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004)*, (2004).

22. Zarki, M.E., Mehrotra, S., Tsudik, G. and Venkatasubramanian, N., Security Issues in a Future Vehicular Network. in *European Wireless*, (2002).