An In-Depth Analysis of the Security of the Connected Repair Shop

Pierre Kleberger, Tomas Olovsson, and Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden
Email: {pierre.kleberger,tomas.olovsson,erland.jonsson}@chalmers.se

***Abstract*— In this paper, we present a security analysis of delivering diagnostics services to the connected car in future connected repair shops. The repair shop will mainly provide two services; vehicle diagnostics and software download. We analyse the security within the repair shop by applying a reduced version of the threat, vulnerability, and risk analysis (TVRA) method defined by ETSI. First, a system description of the repair shop is given. Security objectives and assets are then identified, followed by the threat and vulnerability analysis. Possible countermeasures are derived and we outline and discuss one possible approach for addressing the security in the repair shop. We find that many of the identified vulnerabilities can directly be mitigated by countermeasures and, to our surprise, we find that the handling of authentication keys is critical and may affect vehicles outside the repair shop as well. Furthermore, we conclude that the TVRA method was not easy to follow, but still useful in this analysis. Finally, we suggest that repair shop security should mainly be addressed at the link layer. Such an approach may integrate network authentication mechanisms during address allocation and also support encryption of data for all upper layer protocols with minimal modifications.**

Keywords-security analysis; vehicle diagnostics; connected car.

I. Introduction

The ongoing trend with equipping vehicles with wireless access will bring many new services into the vehicle. Mainly, these services are used when the vehicle is on the road, but there are also other cases when a wireless connection to the vehicle is useful. One is the usage of WiFi-technology to connect the vehicle to a repair shop. A wireless connection between the vehicle and the repair shop has many benefits [1]; no cables are needed, which shorten the time for connecting the vehicle to the repair shop, and also makes it possible to connect more vehicles at the same time, e.g., to update the firmware in several vehicles at the same time. However, using WiFi-technology, where many vehicles can connect to the same wireless Access Point (AP), also raises security related questions; how does the mechanic know that she is working with the right vehicle, and what support is implemented in the network to protect the vehicle against malicious network behaviour? For example, Checkoway et al. [2] have already demonstrated some security issues with the PassThru-device used for connecting the in-vehicle network to the WiFi-network. When the PassThru-device was compromised, malicious software was installed in the device, which attacked the connected vehicle. As the vehicle is safety critical, it is crucial that such attacks are prevented in the repair shop.

Two services are mainly requested in the repair shop, vehicle diagnostics and software download. In this paper, we assess the security within the repair shop when vehicles are connected to the repair shop using wireless connections. The analysis is performed by applying a reduced version of the Threat, Vulnerability, and Risk Analysis (TVRA) method proposed by ETSI [3] as it has been used for evaluating the emerging Intelligent Transportation Systems (ITS) architecture [4]. Originally, ETSI defined this method for use by their standards developers to analyse telecommunication systems [3]. Even though this is a rather limited setting, we believe that results from such an analysis, not only will derive security mechanisms for this environment, but also can be used for secure vehicle diagnostics, software download, and possibly other services in a larger more generalised environment.

The rest of this paper is outlined as follows. Section II presents the related research within the area. The analysis method, together with an overview of the repair shop and its services, are given in Section III. In Section IV, the model of the repair shop network is described followed by the security objectives in Section V. An inventory of assets is established in Section VI. Threats and vulnerabilities are then identified and the countermeasures are derived in Section VII and VIII, respectively. These countermeasures are then used in Section IX for discussing one possible approach for addressing the security. The paper closes with a discussion and proposal for future work in Section X and our conclusion in Section XI.

II. Related Work

Even though much effort has been spent on research in the vehicular communication (VC) domain [5], most of the work during the last decade has been directed towards systems for ensuring the safety of the vehicle and less towards security. However, the effort in addressing security of VC systems seems to have increased during the last few years. Both the SeVeCOM project [6] and the EVITA project [7] have been addressing security with focus on communication between vehicles and within the vehicle, respectively. In the SeVeCOM project, a security architecture for VC systems was developed, and one of the outcomes was the three security services of secure beaconing, secure neighbour discovery, and secure

ISBN: 978-1-61208-231-8

geocasting [8]. Methods for handling identification and privacy (by help of pseudonyms) using certificates and how to revoke these were also proposed.

Efforts in defining a standardized platform for ITS applications have also been spent [9, 10] and the security for such an ITS architecture has also been evaluated [4, 11]. Both software download and remote diagnostics are included as applications of this ITS platform [12]. However, in this paper, we look at the vehicle diagnostics as a stand alone service within the repair shop, outside the scope of the ITS platform. We extend the Local Area Network (LAN) in the repair shop with a wireless connection to the vehicles. Hence, we assess security within a local network without Vehicle-to-Vehicle (V2V) communication. Vehicles connect to and disconnect from the local network and local network devices are included in the assessment.

Specialised approaches for providing secure software download and firmware updates to vehicles have been proposed [13–15]. In these approaches, protocols for secure software download have been described, protocols that can cope with arbitrary distance between the vehicle and the software supplier. Furthermore, methods for ensuring that the firmware is flashed correctly have also been proposed [16, 17]. These approaches are specific to the delivery of ECU firmware and do not include remote diagnostics. In this paper, the delivery of ECU firmware is an integrated part of the vehicle diagnostics protocol.

Idrees et al. [18] give a detailed presentation of a remote software download procedure including some remote diagnostics, which utilises the hardware security module (HSM) designed within the EVITA project. Mechanisms for exchanging necessary keys between EVITA-enabled devices and for protection of transmitted data are described. However, we take a broader perspective by assessing the security of the whole repair shop network.

A risk assessment of the wireless communication infrastructure between the backend system, used for providing diagnostics service and firmware, and the vehicle was performed by Nilsson et al. [19]. In their analysis, they target end-to-end communication between the backend system and the vehicle, while we consider the whole repair shop network and the included devices.

Efforts are also made by ISO to create a standardized diagnostics protocol, Diagnostics over IP (DoIP) [20], and some initial tests have been performed by Johanson et al. [21]. However, appropriate security mechanisms are still missing in the DoIP-protocol.

III. Background

A. The Repair Shop

In our previous work [22], we proposed a model of the connected car infrastructure to clarify the possible communication paths with future connected vehicles. To derive a model of the repair shop for our analysis in this paper, this previously proposed model was used. An overview of the repair shop is shown in Figure 1.

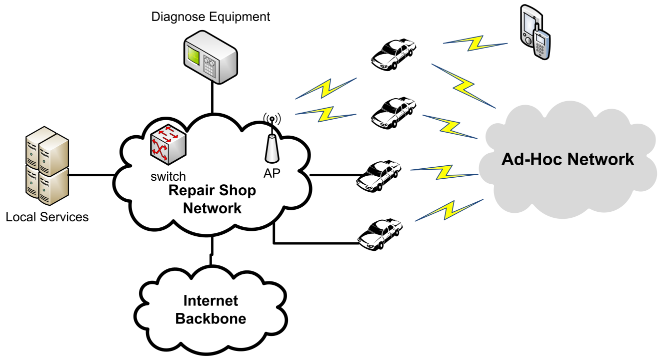
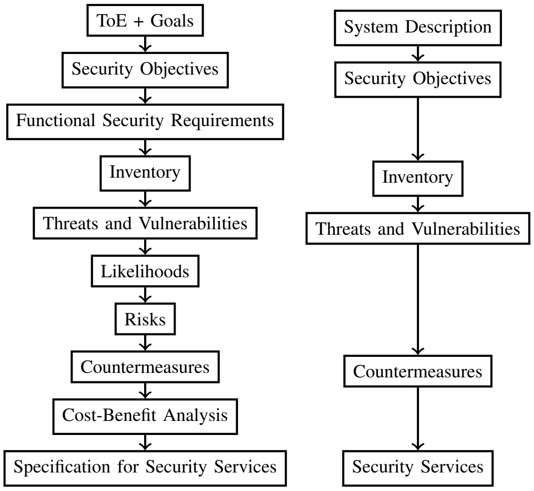


Figure 1. Overview of the repair shop



(a) TVRA method (b) Analysis method used

Figure 2. Overview of analysis methods

We consider the repair shop network to be trusted. Multiple vehicles are connected to this network, both with wired and wireless connections, as well as the diagnostics equipment and local servers providing necessary services to the LAN (e.g., DHCP [23]). The internal network at the repair shop contains wireless APs, Ethernet switches, and a connection to the Internet. Furthermore, the vehicles in the repair shop can communicate directly with other vehicles or devices through an ad-hoc network.

B. Analysis Method

For our analysis, we apply a subset of the TVRA method proposed by ETSI [3]. An overview of the method and our subset is shown in Figure 2. We will first summarise the complete method and then discuss the parts left out.

The TVRA method [3] can briefly be summarised as follows; The *target of evaluation (ToE)* is identified and the assets within are described together with the goals of the evaluation. *Security objectives* are then identified and classified based on the five security attributes: confidentiality, integrity, availability, authenticity, and accountability (CIAAA). These security objectives are then used to derive the *functional* *security requirements*. Then, an *inventory of assets* is done. Possible *vulnerabilities* are then identified and classified together with their *corresponding threats* and their unwanted outcome. These threats are classified based on the following four categories: interception, manipulation, denial of service, and repudiation. *Risks* are then calculated depending on the *likelihood* of these threats and their unwanted outcome. Finally, a set of *countermeasures* are derived and a *cost-benefit analysis* is performed to select the most suitable ones to *reduce the risks* of the identified threats. These results are then used to design the *security services*.

Four steps in the TVRA method are omitted in our analysis: deriving the *functional security requirements* and calculations related to *likelihoods*, *risks*, and *cost-benefit analysis*. The functional security requirements are a more detailed specification of the security objectives and include descriptions of how a certain security objective should be addressed in the implementation, e.g., that access control should be implemented by means of a username and password. Since we want to find general security mechanisms and not limit the analysis to a single security implementation, we leave this step out. Furthermore, we do not want to calculate any likelihoods, nor risks for the different threats and vulnerabilities and it will therefore be up to an implementor to make a trade-off and choose the best countermeasures and security services for their settings.

IV. System Description

A. Network Model and Assumptions

A more detailed model of the repair shop network is shown in Figure 3. We assume that a set of diagnostics equipment, $\{D_1, D_2, ...\}$, and vehicles, $\{V_1, V_2, ...\}$, are connected to the repair shop network, using wireless and/or wired connections. The diagnostics equipment can be either dedicated hardware or a general computer used to perform vehicle diagnostics. A local server, LS, is also available to provide necessary services and to maintain the LAN, e.g., DHCP for dynamic IP address allocation. Furthermore, we assume that other devices, which are needed to run the business and not to maintain cars, are connected to the network using wired connections. These devices, denoted office hosts, cannot be excluded from the model, since they need network connectivity in order for employees to, e.g., read emails and write documents. However, these computers may be potentially threatening to the communication with the vehicles if misused or being compromised. These office hosts are marked with the grey box in Figure 3.

B. Vehicle Diagnostics Scenario

The scenario of performing vehicle diagnostics can be divided into the following three steps. First, the vehicle arrives to the repair shop and *connects to the wireless AP*. If the vehicle lacks wireless access, the vehicle is connected to the wired network by a mechanic in the repair shop. Then, when the link is established, the vehicle needs to *announce its presence* in the network, so that the diagnostics equipment can find it [24]. Finally, the diagnostics equipment can initiate a *diagnostics session* with the vehicle and perform its tasks, e.g., diagnose an Electronic Control Unit (ECU) or update the firmware of an ECU.

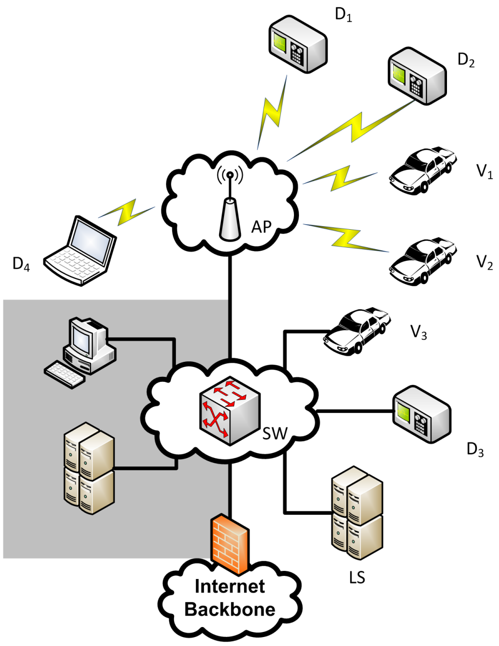


Figure 3. Model of the repair shop network

C. Definitions

The following definitions are used in this paper:

Diagnostics session. An established connection between diagnostics equipment and a vehicle.

Diagnostics data. Data, transmitted or stored, associated with a diagnostics session. Diagnostics data is classified as confidential or non-confidential, where *non-confidential is assumed* unless otherwise stated.

ECU firmware. Program code installed in non-volatile memory of ECUs.

Confidential data. Diagnostics data classified as confidential and ECU firmware.

Core network traffic. Network communication necessary to maintain the network infrastructure, i.e., ARP, DHCP, DNS, and ICMP.

Authorised device. A device is an authorised device if it fulfils one of the following requirements:

(1) a vehicle, which has been connected to the network by a mechanic, who thereby authorises the vehicle, using a cable or wireless connection, or
(2) a vehicle, which has been authorised by a trusted party to connect to the repair shop network, e.g., a service booking system giving the vehicle authorisation to connect to the network at a reserved service time, or
(3) diagnostics equipment, or
(4) any other device needed to diagnose a vehicle.

Note that office hosts are not included in the definition of an authorised device. A clear distinction between the devices in the repair shop is made, where authorised devices are those that take part in vehicle diagnostics.

D. Limitations

The following limitations are assumed in this paper:

1) Even though the in-vehicle network is not secure, we assume that the communication within the vehicle is correctly transmitted.
2) Denial of service (DoS) attacks against the network are not addressed. Other security systems, e.g., Intrusion Detection Systems (IDSs), are needed to identify such activities, which we believe would be too costly and too complicated to manage for a repair shop.
3) Theft of physical assets. The physical assets are not considered to be of great value, but logical assets are (see Table I).

V. Security Objectives

The following security objectives are identified:

O1: To ensure the availability of the repair shop network, only office hosts and authorised devices should be given access to the repair shop network.

O2: Authorised devices must properly verify and validate the source of diagnostics data.

O3: Logical assets and diagnostics data must be protected against unauthorised modification.

O4: Logical assets must not be revealed to unauthorised parties.

O5: Only the following communication scenarios should be allowed in the repair shop network:

(1) devices may process core network traffic in the repair shop;
(2) diagnostics sessions may only be established between vehicles and diagnostics equipment;
(3) diagnostics equipment may connect to any device in the repair shop and to backend servers at the automotive company via the Internet connection;
(4) office hosts may establish connections with office hosts and the Internet, and process traffic from diagnostics equipment.

These security objectives include some important scenarios. For example, it is important that only authorised vehicles are allowed to connect to the network (O1), so that vehicles, when they are passing the repair shop, cannot connect to the wireless AP. Another example is, that certain types of communication should be prevented (O5), such as car-to-car communication inside the repair shop network; if vehicles are allowed to communicate with each other, an attacker may utilise this possibility to try to infect other vehicles with malicious software. However, since we are only concerned with protecting authorised devices, office hosts may communicate with other office hosts and the Internet, and process traffic from diagnostics equipment, so that a mechanic can retrieve necessary data to the diagnostics equipment.

Table I
Assets to protect

(a) Physical assets

ID	Model Reference	Asset
A_{P1}	V_x	vehicle
A_{P2}	D_x	diagnostics equipment
A_{P3}	AP	wireless access point
A_{P4}	SW	Ethernet switch
A_{P5}	LS	local server

(b) Logical assets

ID	Asset	Physical Assets
A_{L1}	authentication data and cryptographic keys stored in physical assets	A_{P1}, A_{P2}, (A_{P3}), (A_{P4}), A_{P5}
A_{L2}	diagnostics data that is considered confidential	A_{P1}, A_{P2}, A_{P5}
A_{L3}	ECU firmware	A_{P1}, A_{P2}, A_{P5}

It is also important to note that O1 only states that the repair shop should identify and authorise devices to connect to the repair shop network, but says nothing about how and whether the connecting device will verify the network. Hence, from the perspective of the network, it is important to make sure that availability is ensured by not giving access to unauthorised devices. However, from the perspective of the device, it is not important if it connects to a repair shop network or not, as long as O2 is ensured. The device will still only accept communication from sources it can validate.

VI. Inventory of Assets

The assets to protect are divided into two categories, physical assets and logical assets. The identified physical assets are listed in Table Ia and the logical assets, together with the associated physical asset, are listed in Table Ib. As already mentioned, in this paper we only deal with threats against the logical assets.

VII. Threat and Vulnerability Analysis

An analysis of possible vulnerabilities in the repair shop has been conducted. We will summarise the vulnerabilities here and highlight some important issues. For details, we refer to Appendix A.

A. Identified Vulnerabilities

Fourteen (14) vulnerabilities were identified. These were classified based on the five threat categories defined by the TVRA method [3]: eavesdropping, unauthorised access, masquerading, forgery, and information corruption.

- *eavesdropping (1).* Since malicious devices may eavesdrop on network traffic, weak protection of confidential data may lead to data disclosure.
- *unauthorised access (6).* Among the six vulnerabilities identified, three were the results of weaknesses in authentication and two due to software bugs. The last vulnerability was the result of issues regarding traffic separation. Due to weak authentication mechanisms and

Table II
POSSIBLE COUNTERMEASURES

	Countermeasure	Threat Category	Weakness
1	encryption	interception	weak protection of confidential diagnostics data and ECU firmware
2	(1) PKI + certificates (2) Kerberos	unauthorised access	(a) weak authentication (b) lack of proper authentication for wireless connections
		masquerade	lack of proper device identification
3	(1) logical traffic separation (2) cryptographic traffic separation (3) firewalls	unauthorised access	(a) lack of traffic separation (b) software bugs
4	(1) digital signatures (2) message authentication codes	forgery	(a) lack of data authentication (b) weak integrity check of diagnostics data (c) weak integrity check in vehicle ID broadcast
		information corruption	weak integrity check of diagnostics data
5	timestamps	forgery	lack of freshness in diagnostics session

software bugs, an attacker may circumvent authentication mechanisms or install malware, leading to disclosure of confidential data and modification of stored data. Furthermore, by circumventing the protection mechanisms to establish a wireless connection, an attacker may also get unauthorised access to the repair shop network.

- *masquerading (2).* Due to lack of proper device identification, an attacker may impersonate as another device and manipulate data or acquire confidential data. Even worse, if an attacker is in possession of proper authentication keys, for example, by a previous theft, the attacker can act as an authorised device.
- *forgery (4).* Due to the lack of data authentication and integrity checks, an attacker may fabricate and inject malicious data into diagnostics sessions. This may lead to problems such as wrong vehicle IDs being presented to the diagnostics equipment. Furthermore, replay of earlier diagnostics sessions may be possible, which may lead to dangerous situations, e.g., an attacker replays commands of her choice from a recorded diagnostics session.
- *information corruption (1).* Malicious devices may modify the data that pass through them. Therefore, weak integrity checks of diagnostics data can lead to malicious data being processed or stored in the vehicle. To ensure the safety of the vehicle, it is of outmost importance that such modifications are prevented.

We find that the exploitation of some of the vulnerabilities results in that logical assets can be acquired or that data can be illicitly modified.

B. Consequences of Lost and Modified Logical Assets

The loss of logical assets can have a major security impact. For confidential diagnostics data and ECU firmware, these might get copied, and for authentication keys, the loss of these can cause great damage. For example, if authentication keys to the diagnostics equipment are copied, an attacker may be able to impersonate as diagnostics equipment and connect to vehicles anywhere outside the repair shop. If there are no other authorisation mechanisms which protect the vehicle from accepting seemingly valid diagnostics sessions, the attacker can initiate new diagnostics sessions to vehicles until these authentication keys expire or are invalidated. Considering the number of vehicles these keys may give access to, the possibility of large scale attacks should not be neglected.

Modification of data can be critical. For example, if the ECU firmware can be modified, an attacker may change the behaviour of the vehicle in any way she desires.

VIII. COUNTERMEASURES

From the vulnerabilities found and discussed in the previous section, possible countermeasures against these were identified and grouped together based on the threats and weaknesses they address. These are presented in Table II. The following countermeasures were identified:

1) Encryption can be used to protect confidential data against eavesdropping. Furthermore, to prevent access to this data in intermediate storage, it can also be stored encrypted.
2) Strong authentication is needed. Private/public keys, with or without certificates, and Kerberos-like authentication mechanisms [4] can be used. However, precaution needs to be taken in case of lost keys. Either the keys should have a short lifetime and procedures for updating these are needed, or the keys have a longer lifetime and procedures for revoking them are needed.
3) Several possible countermeasures can be used to handle the lack of traffic separation within the repair shop network and to deal with misbehaving software. Traffic separation can be achieved either by logical separation or cryptographic separation. Logical separation can be implemented using virtual LAN (VLAN)-technology together with network mechanisms that only allow communication between connected hosts and the uplink [25]. For cryptographic separation, communication can be split into groups of allowed devices, where each group shares a session key. Furthermore, network filters, i.e., firewalls, can be used to limit network access so that software only is accessible to those devices that need it. Thereby, the exposure of software bugs is also limited.

4) Digital signatures and message authentication codes (MACs) can be used to verify the source of and the integrity in the communication, so that forgery and corruption of data can be detected. Furthermore, the digital signature or MAC should be created by the ultimate source of the communication and verified at the final destination so that possible modification in intermediate storage can be detected, e.g., ECU firmware should be signed by the software supplier and verified in the target ECU.
5) Timestamps in transmitted data can be used to prevent the possibility of replay attacks.

IX. Security Services

Based on the identified countermeasures, different approaches in securing the repair shop network are possible. In this section, we will outline one approach and discuss how this approach fulfils the security objectives, as well as how all identified threats and vulnerabilities are addressed.

We note that security objective O5 limits the possible communication scenarios in the repair shop network and that there are different approaches to address this. Depending on which approach is chosen, it will affect the architecture and thereby the implementation of the security mechanisms. Traffic separation is therefore discussed first, so that the architecture for other security mechanisms is defined.

A. Traffic Separation

To address security objective O5, the use of logical traffic separation or cryptographic traffic separation are possible. Since logical traffic separation, using for example VLAN-technology, depends on the equipment and communication technology used, we believe that such an approach is limited; it may not work in all environments, it needs to be maintained by someone with knowledge about the technology, and it is easy to make mistakes. The use of cryptographic separation, on the other hand, can be independent of the underlying communication technology and limited knowledge of the underlying protocols is needed. We therefore suggest that the security mechanisms addressing O5 should be implemented using cryptographic traffic separation.

Cryptographic traffic separation can be implemented at different communication layers, e.g., the network layer or the link layer. We suggest that it should be deployed at the lowest common communication layer, which is the link layer. With this approach, malicious traffic will progress through as few communication layers as possible, limiting the possibility of utilising software bugs in the network stack. Furthermore, encryption at link layer also addresses security objective O4, protection of logical assets, and vulnerabilities VU1 and VU5, and to some extent VU2, VU3, VU6–VU12, and VU14.

The details of how such a link layer encryption protocol should be implemented, needs to be investigated further. However, one interesting approach of applying link layer encryption in LANs has been implemented and demonstrated in the Linux operating system [26].

B. Authentication

Both public key infrastructure (PKI) with certificates and centralised authentication schemes are possible authentication mechanisms to address security objective O1 and vulnerabilities VU2–VU4, VU8, and VU9. However, we note that PKI together with certificates have already been discussed for usage in Inter-Vehicle Communication (IVC) [27]. Although we leave the choice of authentication protocol open to the implementor, special attention is needed regarding loss of authentication keys, as discussed in Section VII-B.

Since loss of the authentication keys used by the diagnostics equipment may give an adversary full access to vehicles, additional security mechanisms are needed. Thus, the vehicle should only accept diagnostics sessions when such a session is expected. A possible approach could be to use an authorisation mechanism where the authorisation is initiated by the vehicle's owner and not by the network. Another approach would be to use temporary authentication keys for diagnostics equipment, which are issued for a certain diagnostics session by some trusted third party.

An interesting outcome of using cryptographic traffic separation at the link layer, is the possibility not to use authentication mechanisms in wireless APs. Instead, authentication is performed at the link layer, between the connecting device and the DHCP service at the local server, during the process of IP-address assignment. Approaches for DHCP authentication have been proposed as part of link layer security protocols [26, 28], but need to be adapted to our context. For example, key management needs to adapted with respect to the amount of vehicles that may connect to the repair shop and that these vehicles may use different repair shops over time. Also, the authorisation process to the repair shop network needs to be adapted. This approach would remove vulnerability VU4, since encryption keys in the wireless AP will not be needed any more.

C. Data Integrity

Both digital signatures and MACs are possible to use. However, we leave the choice to the implementor. What is important regarding the chosen algorithm and its implementation, is that it ensures end-to-end integrity protection, so that data cannot be modified in any intermediate storage. Security objectives O2 and O3 and vulnerabilities VU10–VU14 are addressed here.

D. Firewalls

Firewalls should be used in the Internet gateway, in front of office hosts or in each of them, and in authorised devices in order to further restrict access to and between devices in the repair shop network. This would partly addresses vulnerability VU5–VU7.

X. Discussion and Future Work

In our work, we have chosen to follow a reduced version of the TVRA method to analyse the security of the repair shop network. The main reason for this choice was that the

TVRA method is used by ETSI in their ITS architecture standardisation process. Even though the repair shop network can be considered to be a rather limited system, the TVRA method has not been easy to follow and apply. However, experience from an earlier analysis of the ITS architecture [4] helped us forward.

Of the 14 vulnerabilities identified, we found countermeasures that directly address twelve of them. The last two, VU6 and VU7, are related to software bugs. Firewalls and link layer encryption may to some extent address these two by removing traffic from unknown sources. However, malicious traffic from known sources might still be received.

Addressing security in the repair shop network by using link layer encryption comes with some possibilities, but also with some drawbacks. The introduction of encryption at the link layer offers a basic protection level that the rest of the security mechanisms can be built on. The encryption keys used at the link layer can be used for mutual authentication of the connecting device and the DHCP service. Only authenticated devices can thereby retrieve an IP-address together with necessary information about the network, e.g., information about routing and DNS. Furthermore, link layer encryption will provide protection against eavesdropping for all upper layer protocols. This approach may also be used in other places, where LANs are used, e.g., in homes or in suppliers' networks. Unfortunately, encryption is not part of the common link layer protocols of today and such protocols need to be developed. We know of at least one such approach that has already been demonstrated in the Linux operating system [26]; still it needs to be investigated how such an approach will work in our context and how key management for vehicles and repair shops should be addressed. The main advantage of such a protocol would be that network and data authentication, data confidentiality, and data integrity are combined at the link layer. The network and data authentication will not be based on a specific communication technology, and data confidentiality and data integrity will be provided for all upper layer protocols at the same time.

In this work, we have addressed vehicle diagnostics within the repair shop, i.e., within a LAN, but the identified countermeasures may also be used when performing remote diagnostics outside the LAN.

Regarding authentication keys, we found that the loss of those used by diagnostics equipment is a major security problem. Authentications keys should therefore not give access to vehicles unless some authorisation mechanism also approves the access. Such authorisation can be given by the vehicle's owner or by issuing short-lived authentication keys to the diagnostics equipment. How authentication keys should be handled, especially for diagnostics equipment, needs careful considerations and it is important that possible approaches are identified soon.

XI. Conclusion

The evolution of a connected car is still just beginning and there are many security problems that need to be solved. In this paper, we have analysed the security of diagnostics services in connected repair shops. This has been done by applying a reduced version of the TVRA method. Even though we did not find the TVRA method easy to follow, the method was still useful. We have identified several security threats against the repair shop and the vehicles during service, and also suggested mechanisms to address these problems. To our big surprise, the biggest security threat was not related to the repair shop or the vehicles therein, but to other vehicles. If the keys used to authenticate repair shops to vehicles are stolen or copied, an attacker with access to these keys can create faked repair shop networks and vehicles connecting to them will be unable to differentiate these faked networks from real repair shop networks. Furthermore, our analysis suggests that addressing security at the link layer is a promising approach. This approach may integrate network authentication mechanisms during address allocation and also support encryption of data for all upper layer protocols with minimal modifications.

Acknowledgements

This research was funded by the project Security Framework for Vehicle Communication (2011-04434), co-funded by VINNOVA, the Swedish Governmental Agency for Innovation Systems.

References

[1] M. Shavit, A. Gryc, and R. Miucic. “Firmware Update Over The Air (FOTA) for Automotive Industry”. In: *14th Asia Pacific Automotive Engineering Conference*. Hollywood, CA, USA, Aug. 2007. DOI: 10.4271/2007-01-3523.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. “Comprehensive Experimental Analyses of Automotive Attack Surfaces”. In: *Proc. of the 20th USENIX Security Symposium*. San Francisco, CA, USA, Aug. 2011, pp. 77–92.

[3] *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis*. Tech. Spec. TS 102 165-1, v4.2.3. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2011.

[4] *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*. Tech. Rep. TR 102 893, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2010.

[5] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil. “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions”. In: *IEEE Communications Surveys & Tutorials* 13.4 (2011), pp. 584–616. DOI: 10.1109/SURV.2011.061411.00019.

[6] *Secure Vehicle Communication (SeVeCOM)*. URL: http://www.sevecom.org/ (visited on 07/25/2012).

[7] *E-safety Vehicle Intrusion Protected Applications (EVITA)*. URL: http://www.evita-project.org/ (visited on 07/25/2012).

[8] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. “Secure Vehicular Communication Systems: Design and Architecture”. In: *IEEE Communications Magazine* 46.11 (Nov. 2008), pp. 100–109. DOI: 10.1109/MCOM.2008.4689252.

[9] B. Oehry, C. van Driel, L. Haas, M. Wedlock, K. Perret, and T. van de Ven. *ITS Action Plan; Final Report Action 4.1*. Final Report. DG MOVE, Unit B4, Rue De Mot 28, 4/73. B-1049 Brussels, Belgium: European Commission, Dec. 2010.

[10] *Intelligent Transport Systems (ITS); Communications Architecture*. European Standard EN 302 665, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Sept. 2010.

[11] *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*. Tech. Spec. TS 102 731, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Sept. 2010.

[12] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. Tech. Rep. TR 102 638, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, June 2009.

[13] S. M. Mahmud, S. Shanker, and I. Hossain. “Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links”. In: *Proc. of the IEEE Intelligent Vehicles Symposium*. 2005, pp. 588–593. DOI: 10.1109/IVS.2005.1505167.

[14] I. Hossain and S. M. Mahmud. “Secure Multicast Protocol for Remote Software Upload in Intelligent Vehicles”. In: *Proc. of the 5th Ann. Intel. Vehicle Systems Symp. of National Defense Industries Association (NDIA)*. National Automotive Center and Vectronics Technology. Traverse City, MI, June 2005, pp. 145–155.

[15] D. K. Nilsson and U. E. Larson. “Secure Firmware Updates over the Air in Intelligent Vehicles”. In: *Proc. IEEE International Conference on Communications Workshops (ICC Workshops ’08)*. May 2008, pp. 380–384. DOI: 10.1109/ICCW.2008.78.

[16] D. Nilsson, L. Sun, and T. Nakajima. “A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs”. In: *GLOBECOM Workshops*. IEEE. Nov. 2008, pp. 1–5. DOI: 10.1109/GLOCOMW.2008.ECP.56.

[17] A. Weimerskirch. “Secure Software Flashing”. In: *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* Vol. 2. 1. 2009, pp. 83–86.

[18] M. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger. “Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates”. In: *Communication Technologies for Vehicles*. Vol. 6596. LNCS. 2011, pp. 224–238. ISBN: 978-3-642-19785-7. DOI: 10.1007/978-3-642-19786-4_20.

[19] D. K. Nilsson, U. E. Larson, and E. Jonsson. “Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles”. In: *Proc. of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP ’08)*. Newcastle upon Tyne, UK, 2008, pp. 207–220. ISBN: 978-3-540-87697-7. DOI: 10.1007/978-3-540-87698-4_19.

[20] *ISO/DIS 13400-1: Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 1: General information and use case definition*. ISO.

[21] M. Johanson, P. Dahle, and A. Söderberg. “Remote Vehicle Diagnostics over the Internet using the DoIP Protocol”. In: *Proc. of the Sixth International Conference on Systems and Networks Communications (ICSNC 2011)*. IARIA. Barcelona, Spain, Oct. 2011, pp. 226–231.

[22] P. Kleberger, A. Javaheri, T. Olovsson, and E. Jonsson. “A Framework for Assessing the Security of the Connected Car Infrastructure”. In: *Proc. of the Sixth International Conference on Systems and Networks Communications (ICSNC 2011)*. IARIA. Barcelona, Spain, Oct. 2011, pp. 236–241.

[23] R. Droms. “RFC 2131: Dynamic Host Configuration Protocol”. Mar. 1997.

[24] *ISO/DIS 13400-2: Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 2: Network and transport layer requirements and services*. ISO.

[25] S. HomChaudhuri and M. Foschiano. “RFC 5517: Cisco Systems’ Private VLANs: Scalable Security in a Multi-Client Environment”. Feb. 2010.

[26] Y. Jerschow, C. Lochert, B. Scheuermann, and M. Mauve. “CLL: A Cryptographic Link Layer for Local Area Networks”. In: *Security and Cryptography for Networks*. Vol. 5229. LNCS. 2008, pp. 21–38. ISBN: 978-3-540-85854-6. DOI: 10.1007/978-3-540-85855-3_3.

[27] F. Dressler, F. Kargl, J. Ott, O. Tonguz, and L. Wischhof. “Research Challenges in Intervehicular Communication: Lessons of the 2010 Dagstuhl Seminar”. In: *IEEE Communications Magazine* 49.5 (May 2011), pp. 158–164. ISSN: 0163-6804. DOI: 10.1109/MCOM.2011.5762813.

[28] B. Issac. “Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks”. In: *International Journal of Network Security* 8.2 (2009), pp. 107–118.

Appendix A
Threat and Vulnerability Analysis

In this appendix, the detailed results of the threat and vulnerability analysis are presented.

A model of the network with devices and possible communication paths for the analysis is shown in Figure 4. We identified 14 vulnerabilities which were classified based on the five threat categories defined by the TVRA method [3]: eavesdropping, unauthorised access, masquerade, forgery, and information corruption. The results are presented in Table III and the format is based on those used in [3, 4].

A few columns in Table III need to be explained. The *attack interface* identifies the communication interface where the vulnerability exists. The *source* is from where the vulnerability can be utilised. The source can be one of the following three:

- *radio.* A device only within the radio range of the repair shop.
- *local.* A device that is connected to, or within the radio range of, the repair shop network.
- *all.* Any host in the Internet, or any of the other two sources, radio and local.

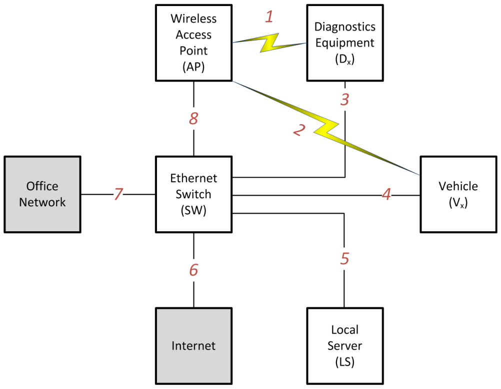


Figure 4. Assets in the repair shop. Physical assets are marked as white boxes.

Table III
VULNERABILITIES

ID	Threat Category	Weakness	Threat Agent	Unwanted Outcome	Violated Security Objective	Attack Interface	Source
VU1	eavesdropping	weak protection of confidential diagnostics data and ECU firmware	device eavesdrop on network traffic	disclosure of confidential data	O4	1–5	local
VU2	unauthorised access	weak authentication	someone tries to circumvent authentication mechanisms	disclosure of confidential data	O4, O5	1–8	all
VU3				manipulation of data	O3, O5		
VU4		lack of proper protection of wireless connections	someone tries to circumvent protection mechanisms to establish a wireless connection	unauthorised devices get access to the repair shop network	O1	1,2	radio
VU5		lack of traffic separation	device communicates with the wrong device in the network	communication scenarios are violated, facilitating other attacks	O5	1–8	all
VU6		software bugs	someone utilizes bugs to install malware	disclosure of confidential data	O4, O5	1–5	all
VU7				manipulation of data	O3, O5		
VU8	masquerade	lack of proper device identification	device identifies itself as another entity (impersonation)	disclosure of confidential data	O2, O4, O5	1–5	local
VU9				manipulation of data	O2, O3, O5		
VU10	forgery	lack of data authentication	someone injects fabricated diagnostics data into diagnostics session	final destination stores or processes malicious diagnostics data	O2, O3, O5	1–5	all
VU11		weak integrity check of diagnostics data			O3, O5		
VU12		lack of freshness in diagnostics session	someone replays a previously eavesdropped diagnostics session	a previous diagnostics session is executed	O3, O5	1–4	local
VU13		weak integrity check of vehicle ID broadcast	someone fabricates that a non-existing vehicle has arrived to the repair shop	diagnostics equipment establishes a diagnostics session to the wrong vehicle	O3	1, 3	local
VU14	information corruption	weak integrity check of diagnostics data	device modifies data during transmission	final destination stores or processes malicious diagnostics data, which could lead to other vulnerabilities, e.g., denial of service or buffer overflow.	O3, O5	1–5	local