Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Grundseminar

Milena Hippler

Automotive Security

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Milena Hippler

Automotive Security

Grundseminar eingereicht im Rahmen der Veranstaltung Grundseminar

im Studiengang Master of Science Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Kai von Luck, Prof. Dr. Tim Tiedemann

Eingereicht am: 31. August 2017

Milena Hippler

Thema der Arbeit
Automotive Security

Stichworte
Automobile Sicherheit, fahrzeug-internes Netzwerk, vernetzte Fahrzeuge, Penetrationtests

Kurzzusammenfassung
Diese Ausarbeitung handelt über die Sicherheit von modernen vernetzten Fahrzeugen. Sie weist die Schwachstellen von automobilen Systemen auf und erörtert Ansätze möglicher Schutzmechanismen. Des Weiteren werden Penetrationstest vorgestellt mit denen etwaige Schwachstellen identifiziert werden können.
Milena Hippler

Title of the paper
Automotive Security

Keywords
automotive security, in-vehicle network, connected vehicles, penetration tests

Abstract
This seminar paper is about the security of modern connected vehicles. It introduces to vulnerabilities of modern automotive systems and discusses current protection approaches. Moreover penetration test will be presented which help to identify possible vulnerabilities.

Contents

1 Introduction

1.1 Significance of Automotive Security

According to a survey from April 2017 the car is the most used means of transport in everyday life in Germany [Brandt]. In reference to this, the security of vehicles has to be assured and vehicles shall not offer attack surfaces for attackers. A common vehicle has a life cycle of approximately five years, therefore the security should be increased as soon as possible to prevent too many attackable vehicles in the traffic for a long time. Moreover an amount of new technologies were implemented in vehicles or infrastructure which as an example increased the comfort, appeal and facilitate the driving. For instance traffic warning system were even developed to advance the traffic safety. But these technologies also open new possibilities for attackers to harm its safety and security. The security standard ISO 26262 does not fulfil all modern requirements of security aspects of modern vehicles.
In the past vehicles were a closed network and accessible by the environment without physical access, therefore the focus was not on protection mechanisms since it seemed secure enough. Nowadays modern vehicles have interfaces that allow wired or wireless communication with the environment. Therefore the embedded computing systems in a modern car are no longer a closed network and security becomes a high prioritised issue.
This paper is an introduction of how many security risks and weak points of a vehicle exist and will exist while the technology of connected vehicles increases. Moreover it discusses possible resulting attacks which can be executed remotely. It also introduces to approaches of security mechanisms and how penetration tests shall identify more weak points.

1.2 Classification and Structure of this Seminar Paper

The chapter attack surfaces (see 2) is parted into the in-vehicle network (see 2.1) and the network of connected vehicles (see 2.2). Each of these sections is divided into three subsections. Each first subsection is about the structure of the most used or important networks and about which network protocols are used and how they function. Each second subsection relates to possible security risks and attack scenarios which can exploit these risks. Each third subsection

informs about current protection mechanisms which were developed or are in development to fix some identified weak points. Moreover it introduces to constraints by which an automotive system is affected and discusses the implementability of protection approaches.
The chapter penetration tests (see 3) refers to the process of a penetration test. It introduces a guideline which can be used to identify weak points in automotive systems.
The last chapter (see 4) concludes the paper and gives a perspective of my future scientific work.

2 Attack Surfaces

Evaluating attack surfaces is about to find weaknesses in the security of a vehicle. All the ways data access the vehicle, therefore the communication with the environment, must be considered. It is recommendable to split these communication interfaces into exterior and interior of a vehicle. This division is visible in the level 0 of a threat model (see [Smith]) in the figure 2.1.
The interior interface is represented by the in-vehicle network (see next section 2.1) and refers to interfaces for audio input and diagnostic ports. Those are visible below the dotted line with the denotation "internal" are those considered internal interface threats.
The exterior is represented by the gateway which is used by a connected vehicle to operate with its environment (see section 2.2). It concentrates on which signals are received and how they can threaten the security these are listed above the dotted line with the denotation "external".
The circle denoted by "vehicle" represents the whole vehicle and its system. In a next threat modelling step this system would be broke down further.
Despite this division note that attacking successfully one surface does not exclude the capture of the other part. This chapter does not cover the interest of an attacker, it covers how good those interfaces are designed and how they can be misused as well as how the security is or might be increased.

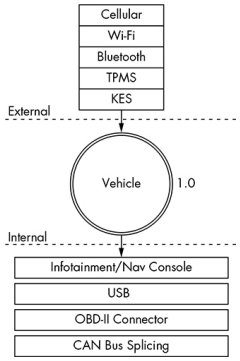

Figure 2.1: Defined inputs of the level 0 of the threat model

2.1 In-Vehicle Network

This section includes the structure of the in-vehicle network or also named on-board network. Moreover potential weaknesses of interfaces and network protocols as well as scenarios of possible attacks focussing on this network will be discussed.

2.1.1 Structure of the In-Vehicle Network

The in-vehicle network has multiple electronic control units (ECUs). Each ECU is an embedded system which controls one or more functionalities of a vehicle such as engine control, braking system and even comfort functionalities like seat control [4]. The amount and complexity of this embedded software is still growing nowadays [Charette]. The ECUs are connected by a bus system to communicate with other ECUs. Depending on the requirements, the ECU can be connected to more than one bus system. Therefore a vehicle consists of multiple sub-networks connected by gateway ECUs as shown as an example in figure 2.2. Due to the amount of ECUs, the data exchange cannot be performed by a point-to-point connection since that would lead to a high consumption of cable. For that reason ECUs are sending their messages via broadcast to all other connected nodes.

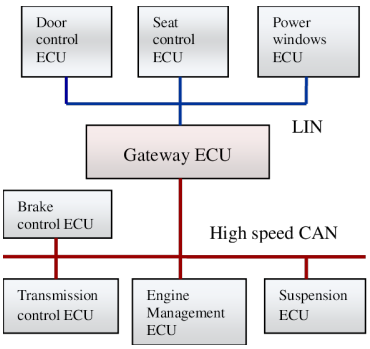

Figure 2.2: Example of the in-vehicle network [Mishra u. a. (2012)]

Bus protocols govern the transport of packages through the network of the vehicle. The used protocols vary by manufacturers since some are more applicable for their vehicles than other. One protocol, the CAN (controller area network) bus, exists in standard location on all vehicles [Smith]. Its data rate reaches up to 1Mbps and therefore used for midrange systems. CAN uses a multi-master concept for the transmission of messages. Each node can transmit its message immediately. In case more than one node wants to send a message, the frame identifier will be compared and the one with the highest MSB has the highest priority for transmission. The structure of the CAN Frame is visible in figure 2.3.

SOF	Identifier	Control	Data	CRC	ACK	EOF
1 bit	12/30 bits	6 bits	0 - 64 bits	16 bits	2 bits	7 bits

Figure 2.3: CAN Frame [Ivan Studnia]

Another communication protocol is LIN (local interconnect network). It is the cheapest of the vehicle protocols [Smith] since the data rate is about 20kbps maximum. It was developed to complement the CAN protocol and is used for the control of comfort systems since those are not time critical.
The MOST (media oriented systems transport) protocol is designed for multimedia devices and has a data rate up to 24Mbps.
FlexRay is a high-speed bus that communicates at speeds of up to 10Mbps. It is geared for time-sensitive communication, such as drive-by-wire, steer-by-wire or brake-by-wire [Smith].

2.1.2 Potential Vulnerabilities and Attack Scenarios

The goals of an attack range from the most obvious motivation of theft, which is possible by unlocking the vehicle and deactivating engine immobilizer as well as the alarm system, over electronic tuning, like resetting the mileage or installing unauthorised programs in the board computer, to theft of intellectual property. More about attack goals can be extracted from [Ivan Studnia] and information about the profile of attacker can be read in [Lotfi ben Othmane].
One of the main vulnerabilities of a vehicle is the security of the network protocols. As an example CAN will be discussed since it is the most used protocol. By reference to some security characteristics which CAN cannot ensure will be shown how insecure the in-vehicle network can be.
Due to the message sending via broadcast the security aspect of confidentiality is not ensured since it is possible for a malicious ECU (see 2.4) to eavesdrop on the bus and to read confidential messages. Not only eavesdropping is possible, but also sending messages. The CAN frame does not contain an array to authenticate the transmitter (CAN frame 2.3), therefore authenticity is not guaranteed and a malicious ECU can send messages which shall only be send by some specific ECUs. Moreover this can impair the availability, because the arbitration can be easily manipulated by such a malicious ECU. This ECU can transmit high prioritised frames and jam the bus for other ECUs. This leads to the security issue of verifiability since a correct ECU is not able to check whether it transmitted or received a message.
In 2.4 a malicious ECU is shown. The original program was replaced by a malicious one. From this point on the attacker is able to gain the control of other ECUs of the vehicle by the lack

of security of the bus protocol. It is perceptible that the CAN protocol is not secure, which was no direct problem in the past when physical access to the target vehicle was required, but since the connected vehicles allow wireless communication with the environment it became a high security risk.

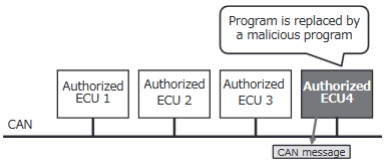

Figure 2.4: Malicious ECU [Hiroshi UEDA und HORIHATA]

Other security risks are the indirect access by the OBD-II port [Smith], CD-Player or USB-port. All these can inject malicious messages on the bus, for example a downloaded WMA file is corrupted and transmits messages on the bus while playing the audio file or through the USB-port a connection to an external device is possible such as a mobile phone which can perform attacks on the ECUs.

2.1.3 Protection Mechanism

Automotive security is not comparable to typical computing security concepts and methods, because there exist important differences in the design and context. Automotive security mechanism are constrained by the hardware since the ECUs are embedded systems which do not have great storage capacities and limited computational power which is designed for its certain functionalities. Therefore the implementation of expensive cryptographic functions on the ECUs is in most cases not possible. Attackers are not bound to those limitations and because of that a simple encryption algorithm is easy to attack.
Another constraint is the requirement of the capability of real-time. The more complex the instruction is the longer is the required runtime and that decreases the observance of real-time. If the real-time is not ensured for some critical embedded applications it could affect the safety of the vehicle and its passengers.
Other constraints are physical constraints, compatibility and the autonomy, security mechanism shall be as autonomic as possible since the driver shall concentrate on the driving [Ivan Studnia].
Solution approaches to decrease the security risks of the CAN bus, which were introduced in section 2.1.2, are categorised into three categories: cryptography, anomaly detection and ECU software integrity. Note that most of these approaches are in the early stages of development and not fully designed yet.

Cryptographic solutions can prevent eavesdropping since the ECUs which do not own the decryption key for an encrypted message cannot read them. This also increases the aforementioned security aspects of authenticity and integrity. Of course de- and encryption costs resources (hardware constraints) and time (real-time constraints), for this reason hardware modules were designed which relieves the ECU by executing the cryptographic operations. Such a module is called HSM (Hardware Security Module) and each ECU is connected to its own HSM, for further information about the HSM designed by EVITA see [EVITA].
Anomaly detection concentrates on observing the legitimacy of the transmitted data. This is for example implemented by a delay detection, if the delay between two transmitted frames of an observed ECU is too short the corrupt ECU will be muted. Another example would be that in each bus the frame identifier will be associated with one certain ECU. Such frames can only be send by this ECU and will be detected if another (malicious) ECU will send it. This detection proceeds in the following way: As soon as a message is send onto the bus, each ECU checks whether it is their frame identifier, if true and the ECU did not send this frame it will send immediately a high-prioritised alarm to override the illegal message. There are also other approaches like an anomaly database which defines all normal behaviours of an observed system and anomalies will be detected if the current state of the system differs. Of course this approach is very complex and difficult to design.
Last but not least the ECU software integrity, which is the validation of the security of the embedded code of the ECU and is about assuring that especially the critical software will not be affected by an attack.

2.2 Connected Vehicles

A vehicle which uses an external network in addition to the internal on board network is called connected vehicle [Lotfi ben Othmane]. The structure of the in-vehicle network, which is also visible in 2.5 was already explained in section 2.1.1. This section focusses on the off-board network, therefore the communication with the environment (V2X communication) as well as consequent possible attack.

2.2.1 Structure of Connected Vehicles

Connected vehicles (see 2.5) are not a closed network, they communicate with their environment by using different networks. In the following, the most important communication networks will be introduced.
The internal communication between the vehicles ECUs, therefore the in-vehicle network was

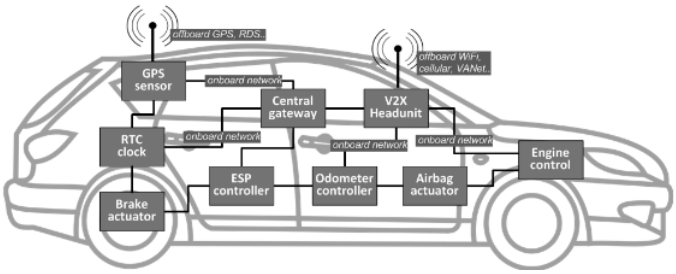

Figure 2.5: Connected Vehicle and its Interfaces [Lotfi ben Othmane]

already discussed in section 2.1).
The external communication can be the communication with other vehicles which is also called V2V (vehicle-to-vehicle) communication. The other type is called V2I (vehicle-to-infrastructure) communication. Infrastructure is mainly the information exchange with RSUs (Road Side Units) (for more informtaion about RSU see [Andreas Festag] and [ITWissen (a)]. V2V and V2I form the VANet (vehicular ad hoc network). Members of the VANet increase the safety by information sharing. Vehicles can exchange information like speed, destination and position. In reference to those data traffic situations can be estimated and alert messages can be send in case of traffic congestion or accidents [ITWissen (b)][Andreas Festag].
Another network is the WPAN (wireless personal are network) and it consists of personal devices, which communicate wireless in a short range with each other by using technologies like bluetooth, NFC (near field communication) and infrared. A vehicle owner is able to control the lights or windscreen wiper or the heating of his vehicle by a bluetooth activated headset or unlocks the doors with his mobile phone.
The cellular network consists of service provider and service center and is dedicated for the long range communication.

2.2.2 Potential Vulnerabilities and Attack Scenarios

Important security aspects of a connected vehicle are: security of the communication, data validity and security of devices. [Lotfi ben Othmane]
Attack scenarios and security risks for the aspect of the communication can be that an attacker is eavesdropping the communication of two parties. Moreover it is possible that an attacker creates incorrect messages. For example he could transmit an alarm message that his vehicle is an emergency vehicle to his neighbours thus he is able to speed up his drive. A connected vehicle in a connected traffic forwards a received message to other connected vehicles or infrastructures. An attack scenario would be that the attacker does not forward this message.

For example he discards a warning of a traffic congestion therefore his neighbour might not get the information and get stuck in the congestion while the bypass streets are less busy for the attacker. Another risk of the security of the communication is a replay attack. An attacker receives a message, changes the timestamps and transmits it multiple time via broadcast to other traffic participants. This attack causes that the communication channels are blocked by this message and no further communication is possible.
The aspect of data validity is also about broadcasting corrupt messages since smart mobility applications trust in the correctness and accuracy of their used data. This enables attacks like a wormhole attack to the VANet. As an example: Two communicating vehicles are controlled by an attacker. Now the attacker is able to nutmeg traffic information of a crowded location to another location. This misleads the traffic management system application, which collects traffic information and transmits it to other participants. This leads to a very fast dissemination of false information.
The aspect of the risk of security of devices enables in connected vehicle a simple denial of service (DoS) attack. For instance an attacker could provoke an accident and execute a DoS attack (for information about DoS see [McDowell]) which thwart a deceleration warning for approaching vehicles. Therefore a cascading crash could be created.

2.2.3 Protection Mechanism

Protection mechanism for connected vehicles are mostly focussing on the used communication protocols (see 2.2.1) which have to increase their security. In reference to this are also cryptographic anomaly detection approaches in development which are similar to the introduced mechanism in section 2.1.3. However the approaches are less developed than the ones in the in-vehicle network, since the networks are more complex and the constraints interfere solutions.
Therefore another development is the designing of secure architectures to protect the in-vehicle network in general from the connected environment since it is possible to attack the in-vehicle network by remote access through the interface to the environment. In theory the attack scenarios (see 2.2.2) could have been avoided by good security oriented programming of software and communication protocols, however it is not possible to check whether the policy is complied since the systems are too complex nowadays. In reference to that additional security are indispensable to secure the communication. Manufacturers are now aware of that and support industrial and academic projects to design communication architecture for in-vehicle inter-vehicle communication [Ivan Studnia]. For instance some European projects are SEVECOM [F. Kargl], PRESERVE [14] and EVITA [O. Henniger und Wollinger].

3 Penetration Tests

Penetration tests are an approved and suitable proceed to evaluate the security and attack potential of an IT infrastructure by safely trying to exploit vulnerabilities [Security]. Penetration tests examine the security of an IT-system as well as the efficiency of implemented security mechanism and therefore derive necessary additional security measures from those insights [BSI]. The following section 3.1 will introduce a guideline for the process of a penetration test. This guideline focusses only on the automotive systems and on the view of the penetration tester.

3.1 Process of Penetration Tests

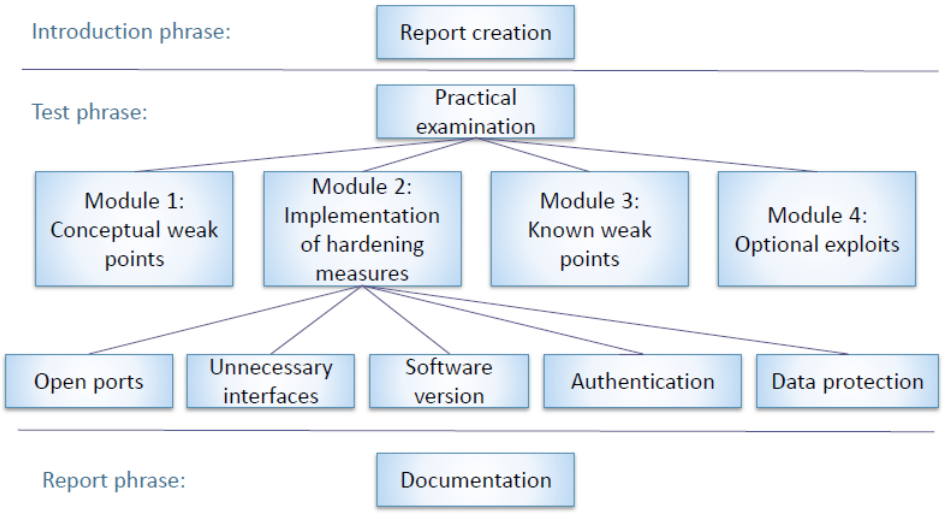

Figure 3.1: Procedure of a Penetration Test (modified on base of [BSI])

The possible process of an automotive penetration test is visible in figure 3.1. It is partitioned in three phases. The first phase is the introduction phase in which a report will be created which includes all the given information about the target system.
The second phase is the main phase, this is where the system is tested. The test is divided

in four modules. The first module includes all questions and points which were already conspicuous in the introduction phase and which give evidence of possible conceptual weak points. The module two is the implementation of hardening measures. This module contains the analysis and testing of different typical security risks. Those risk are for example open ports, unnecessary or redundant interfaces, old software versions, therefore no important security updates, authentication and data protection. Each suspicious risk will be notated. The third module is notating the known weak points, for example for the in-vehicle network that would be the mentioned security risks of the CAN protocol (see 2.1.2). The fourth and last module is the module where exploits can be deployed. The usage of this module is optional since exploits are exploiting the identified weak points and gain access to the system which is not in all cases necessary to exhibit its security weak points.
The last phase is the report phase. This is the moment in which all the collected identified security risks and weak points get documented by the penetration tester. The documentation often includes a recommendation how those weak points can be fixed.

4 Conclusion and Prospect

Existing security mechanisms in automotive networks are deficient. In the past the security was sufficient since a physical access to the target vehicle was a precondition of attacking its in-vehicle network and therefore its functionalities. Since connected vehicles conquer a bigger part of the traffic the condition changed and attackers are able to use the weak points of used network protocols remotely without accessing the target vehicle.
This paper introduced to some weak points and attack scenarios and shows how important it is to develop security mechanisms in vehicles to ensure a safe traffic. It also introduced some approaches of protection mechanisms and discussed how suitable those are and where the difficulties for the implementation are.
As a prospective to my further scientific work I will concentrate on the process of penetration testing and therefore the detection of weak points (mentioned in 3.1). Moreover it is a goal to find approaches for solutions to increase the automotive security to be a part of this development and to help vehicles become secure.

Bibliography

[14] About PRESERVE, URL http://www.preserve-project.eu/

[4] ECU (electronic control unit), URL http://www.itwissen.info/ECU-electronic-control-unit-Elektronisches-Steuergeraet.html. – Zugriffsdatum: 2017-22-05

[Andreas Festag] Andreas Festag, Roberto Baldessari Long Le Wenhui Zhang Dirk W.: VEHICLE-TO-VEHICLE AND ROAD-SIDE SENSOR COMMUNICATION FOR ENHANCED ROAD SAFETY, URL http://www.festag-net.de/doc/ITS2008_VANET-WSN_w.pdf. – Zugriffsdatum: 2017-22-05

[Brandt] Brandt, Mathias: Auto ist in Deutschland immer noch die Nummer 1, URL https://de.statista.com/infografik/9162/nutzung-von-verkehrsmitteln-in-deutschland/. – Zugriffsdatum: 2017-22-05

[BSI] BSI: Ein Praxis-Leitfaden für IS-Penetrationstests, URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=10. – Zugriffsdatum: 2017-22-05

[Charette] Charette, R. N.: This car runs on code, URL https://hal.archives-ouvertes.fr/hal-01176042/document. – Zugriffsdatum: 2017-22-05

[EVITA] EVITA: EVITA Project, HSM, URL evita-project.org. – Zugriffsdatum: 2017-22-05

[F. Kargl] F. Kargl, L. Buttyan M. Muter E. Schoch B. Wiedersheim T.V. Thong G. Calandriello A. Held A. K.: Secure vehicular communication systems: implementation, performance, and research challenges

[Hiroshi UEDA und HORIHATA] Hiroshi UEDA, Hiroaki TAKADA Tomohiro MIZUTANI Masayuki I. ; HORIHATA, Satoshi: Security Authentication System for In-Vehicle Network, URL http://global-sei.com/technology/tr/bn81/pdf/81-01.pdf. – Zugriffsdatum: 2017-22-05

[ITWissen a] ITWissen: RSU (roadside unit), URL http://www.itwissen.info/RSU-roadside-unit.html. – Zugriffsdatum: 2017-22-05

[ITWissen b] ITWissen: VANET (vehicular ad-hoc network), URL http://www.itwissen.info/VANET-vehicular-ad-hoc-network.html. – Zugriffsdatum: 2017-22-05

[Ivan Studnia] Ivan Studnia, Eric Alata Yves Deswarte Mohamed Kaniche Youssef L.: Survey on security threats and protection mechanisms in embedded automotive networks, URL https://hal.archives-ouvertes.fr/hal-01176042/document. – Zugriffsdatum: 2017-22-05

[McDowell] McDowell, Mindi: Security Tip (ST04-015) Understanding Denial-of-Service Attacks, URL https://www.us-cert.gov/ncas/tips/ST04-015. – Zugriffsdatum: 2017-22-05

[Mishra u. a. 2012] Mishra, Geetishree ; Hegde, Rajeshwari ; Kargal, Gurumurthy: Deploying Health Monitoring ECU Towards Enhancing the Performance of In-Vehicle Network. 2 (2012), 08

[O. Henniger und Wollinger] O. Henniger, H. Seudié B. Weyl M. W. ; Wollinger, T.: Securing vehicular on-board it systems: The evita project, URL http://www.preserve-project.eu/

[Lotfi ben Othmane] Othmane, Mohd Murtadha Mohamad Marko W. Lotfi ben: A Survey of Security and Privacy in Connected Vehicles

[Security] Security, CORE: Penetration Testing Overview, URL https://www.coresecurity.com/content/penetration-testing. – Zugriffsdatum: 2017-22-05

[Smith] Smith, Craig: *The Car Hacker's Handbook, A Guide for Penetration Tester.* – ISBN 1-59327-703-2