

Improving Automotive Security by Evaluation

From Security Health Check to Common Criteria

Overview

Automotive manufacturers recognize that sensitive functions like car immobilizer, software download or engine control must be designed securely. But even if a security concept exists, often no security measures are defined which really ensure that the design and the implementation of the correspondent system is secure. Managers often suppose that the engineer has chosen adequate security mechanisms, that the software developer has well implemented the security functions and that potential errors are detected during functional tests. From an IT security point of view this approach can lead to insecure systems. Automotive engineers and developers are frequently not able to detect some kind of security bugs since they neither have expertise nor time to evaluate the security of their systems. Security evaluation of the system performed by independent evaluation facilities is an adequate and cost-effective measure to improve IT security ensuring a secure realization.

1 Introduction

There are several methods to evaluate IT security. The methods mainly differentiate in the evaluation depth and in the documentation need. If the evaluation depth is low, then e.g. only a fast vulnerability analysis is done. If the evaluation depth is high, then in advance of the detailed vulnerability analysis the complete design documentation including source code are evaluated, security tests are performed by the security evaluator, the development and production environment are part of the security evaluation and so on. Documentation need means that the developer must document the design, the usage, the production, ... of the device and that the security evaluator must document its evaluation work in order to make the evaluation reproducible.

Evaluation depth and documentation need depend on the value to be protected. The main device of an electronic immobilizer or the engine electronic control unit may need a higher evaluation depth and a higher documentation need than a device to control a comfort function. But evaluation depth and documentation need affects also the costs of the security evaluation. Therefore a suitable evaluation method has to be chosen depending on the values to be protected. In the following the different evaluation methods are presented and advantages and disadvantages of their usage in the automotive environment are explained.

2 Security Health Check

A cost-effective security evaluation is the so-called "Security Health Check". During the Security Health Check potential vulnerabilities are not searched systematically. Attacks are performed in a way a hacker would do, but the security evaluator uses furthermore the existing

documentation of the device or system in order to identify the design weaknesses which can lead to vulnerabilities. Which specific kind of method is used by the security evaluator, depends on the device or system to be analysed. In the network environment (e.g. interface to Internet, CAN) penetration tests - with tools used by the developer, tester or security evaluator - may be the fastest way to find vulnerabilities. If the security of a basic automotive device shall be checked, a short study of the device design together with an inspection of selected parts of the source code may be the better method.

So during the Security Health Check the security evaluator concentrates on the essential. In short time - usually one to three weeks - potential vulnerabilities are tested without any formal process. The low evaluation depth leads to low costs and low documentation need.

3 Security Analysis

Costs, evaluation depth and the documentation need increase if a security analysis is chosen. This kind of security evaluation may be used to evaluate e.g. a security concept. During this informal security analysis the evaluator searches systematically potential vulnerabilities of the system. In order to reach an effective analysis at the beginning the evaluator identifies threats. Based on the found threats, security objectives are defined which must be realised to countermeasure the threats. In a next step security requirements are defined. These requirements must be met by the security mechanisms implemented in the security devices of the system. Afterwards the effectiveness of the security functions is verified. The results of the security analysis are documented in a security evaluation report. Depending on the system to be analysed the costs of a concept security analysis are twice as much as a "Security Health Check".

A security analysis is also a suitable method to analyse the design and implementation of a device. The same method as described above may be used. Additionally the evaluator analyses the source code or the hardware layout. The security analysis can also be reduced to the source code/ hardware layout analysis if suitable security requirements are defined in the design phase. This kind of method is used by the banking industry in Germany since it reduces the costs to an acceptable level.

4 Using Common Criteria in the Automotive Environment

Common Criteria (CC) is a standard (ISO 15408) which defines a process to achieve international comparable security evaluations of products and systems. A successful CC evaluation leads to a certificate of a certification body (in Germany usually the Bundesamt für Sicherheit in der Informationstechnik (BSI)). A CC certificate is recognised in nearly all industrial countries, among them Canada, USA, Japan and nearly the complete European Union. Especially public organisations require CC evaluations for security components.

CC allows different evaluation assurance levels (EAL). The higher the level, the deeper the product or system is analysed, starting with EAL 1, where only minimal documentation is examined and ending with EAL 7, where the security of the product must be proven formally. During a CC evaluation not only the design documentation is evaluated, but CC consists also of the examination of documents regarding delivery and operation, configuration management, guidance, life cycle support and tests. The main part of a CC evaluation, the vulnerability analysis, is performed, when the evaluator has examined the complete product.

CC has already entered the automotive field: the European Commission Regulation No 1360/2002 on recording equipment in road transport and the related Annex 1B (Requirements for Construction, Testing, Installation and Inspection) specifies a Tachograph System which requires a CC evaluation of EAL 4. Each device of the Tachograph System needs a CC evaluation: Vehicle Unit, Motion Sensor and Tachograph Card.

The price for an EAL 4 CC evaluation is significantly higher than for a security analysis. Since also developer documentation must be created, internal costs must be added. Evaluation facilities offer the service to create this CC conform developer documents based on the already existing design documentation. Even if millions of automotive devices are produced, the cost for a EAL 4 CC evaluation seems to be high. But it has to be noted that a lower assurance level will also reduce the cost.

5 How to disable Arguments against Automotive Security Evaluation

As shown above Security Evaluation is an adequate measure to improve IT security. Nonetheless there are arguments against automotive security evaluation. This chapter shows how such arguments can be disabled.

Keyword "Cost": Manager responsible for costs might argue that the benefit of a security evaluation does not justify the cost. As shown above the costs depend on the kind of security evaluation method chosen. Due to mass production in the automotive environment a five-digit amount for the security analysis of a device is not much, since the cost must be divided through the number of devices. An immobilizer evaluated marks down the premiums of theft insurance. Sensitive devices evaluated protect the automotive brand (protection of image against "demonstration effect"). Both measures justify the expenses for the security evaluation. Conclusion: If an adequate security evaluation method is chosen, the benefit of the security evaluation justifies the cost.

Keyword "Insecure Hardware": The hardware of automotive devices must be cheap resulting in insecure hardware protection. Technical Manager might argue that security evaluations are not reasonable since hardware attacks are always possible. But if the attack potential is classified according to elapsed time, expertise of the attacker, knowledge of the device design or access to the device, attack scenarios are identified which can still be prevented by a security evaluation. So a security evaluation can detect vulnerabilities which can be exploited via the interfaces of the devices without having access to the hardware. Interface attacks,

especially if they are published, endanger the image of the automotive brand more than hardware attacks. Conclusion: a security evaluation is a suitable measure, even if the hardware is insecure.

Keyword "Internal Resources": Manager might argue that a security evaluation needs resources within the development department of the manufacturer and that these resources are not available. Even if a contact person is necessary for the security evaluator, the evaluation methods "Security Health Check" and "Security Analysis" only need low support. Usually the quality of the already existing documentation is good enough to perform a security evaluation and the communication with the development department can be reduced to a few meetings and e-mail exchange. Even in the field of Common Criteria the internal resources can be minimised, since already existing documentation can be used within the security evaluation and the evaluation facility can be charged with the creation of Common Criteria conform developer documents. Conclusion: The security evaluation needs only low support by the development department.

Keyword "Intellectual Property": Compared with a "black-box-test" the probability to find vulnerabilities is higher, if a "white-box-test" is used. In a "white-box-test" the security evaluator has access to hardware and software design documentation, to source code and hardware layouts. The device manufacturer might argue that a "white-box-test" leads to a misuse of his intellectual property. He might decline therefore the security evaluation to protect his intellectual property. This argument can be disabled as following. Beside the non-disclosure-agreement between device manufacturer and evaluation facility, it has to be noted that the evaluation facilities are highly trustworthy: Evaluation facilities are usually accredited by certification bodies like public departments or other institutions (e.g. banking association). Additionally the evaluation method could be chosen in such a way, that documentation, source code or hardware layouts do not leave the manufacturer environment. This kind of restriction could be necessary if security functions shall be checked in the electronic control unit of the engine. Conclusion: Even a "white-box-test" does not jeopardize the intellectual property of the device manufacturer.

6 Conclusion

Security evaluation is a suitable security measure to ensure the secure design and implementation of a device or system. Security evaluation is not only used in the banking or public sector, but also in the automotive environment as the Tachograph System and other examples show. The costs can be optimized regarding the value to be protected by choosing the adequate evaluation method. Internal resources are conserved during a security evaluation, the intellectual property is not jeopardized. Even if the hardware is not secure, the security evaluation is an adequate method to identify attacks via the interfaces of the system. Additionally the documentation of the security evaluation may help the manufacturer to meet quality assurance requirements.