Reliable data acquisition for inspection systems

V P Silva, D S Silva, D R Boccardo, R C S Machado and L F R C Carmo

Inmetro — National Institute of Metrology, Quality and Technology, Rio de Janeiro, Brazil

E-mail: {vpraia-prometro, dssilva, drboccardo, rcmachado, lfrust}@inmetro.gov.br

Abstract. In Brazil, the road transportation of dangerous goods is subject to regulatory control, which is conducted by Inmetro, the National Institute of Metrology, Quality and Technology. Currently, the process of monitoring such inspections is done manually, leaving the possibility of some inconsistencies: inspections held outside the authorized local inspection, incorrectly, incompletely, or even be held. Thus, in order to increase the reliability of such inspections, it is needed a closer monitoring by the regulatory agency. One approach towards that, is the implementation of an automated process in which evidences are collected in a reliable way during the inspections, enabling further analyses. This work employs security mechanisms on a portable device to ensure the confidence of the evidences collected during an inspection, paving the way for later more robust analyzes.

1. Introduction

In Brazil, the National Institute of Metrology, Quality and Technology (Inmetro) is responsible for the conformity assessment program for inspection of vehicles and equipments that transports dangerous goods road [1]. Until very recently, the inspection in such vehicles and equipments where was made in carriers or shippers of dangerous goods, which made it difficult to trace inspections records, and consequently, with little or no monitoring by the government authorities. Recently, via Regulation 91 of 2009 [2], Inmetro began a new phase in this program. This regulation dictates, among other things, that the entire inspection should be conducted on an accredited inspection site.

This regulation represented a vast improvement in the dangerous good transportation. However, there are evidences that a large number of inspections is still conducted in improperly ways: such inspections are held outside the authorized local inspection, incorrectly, incompletely, or even are not held. In addition, one cannot be confident on the correctness of the data generated in such inspections. Such scenario suggest that it may be necessary a closer monitoring by regulatory agency to monitor and verify the reliability of inspections. In the present paper, we describe a model developed at Inmetro that aims at monitoring inspections on vehicles and equipment that transport dangerous goods [3]. Our model is strongly based on an *a posteriori* analysis of the information generated by the inspection equipments. Any inconsistency in the analysis leads to suspension or even cancellation of accreditation of an inspection body.

In this model, the main idea is the acquisition of reliable evidences indicating the proper execution of the inspection by accredited inspection bodies. These evidences are composed by data and images recorded at key points of the inspection process. Each evidence is linked to time information — instant record generation — and space — the geographical location where the record was generated. Finally, the record time and its spatial position are digitally signed in order to trace the equipment origin, including the time and coordinates of the records. This work presents the implementation of a mobile device that will be used to collect records of a inspection in a reliable way. More specifically, this work focuses on mechanisms employed to ensure security properties of the records, so guarantying the reliability of a inspection.

This work is structured as follows. Section 2 discusses the inspection system to perform an automated and reliable inspection for dangerous good transportation. It also specifies some requirements for the evidences collection in such systems. Section 3 presents our implementation in a mobile device responsible for the data acquisition and how we addressed reliable issues. Section 4 presents our concluding remarks.

2. Proposed Model for Enhancing the Reliability of Inspection Systems

Historically, in Brazil, all inspections were done on checklist paper and the checking analysis conducted by sampling. However, this kind of checking is highly prone to be forged, leading to inaccurate records, then misleading checking analysis.

The following model overcomes such a problem and it is based on a post checking analysis. The core idea is a trustful generation, by the inspection body, of some evidences of the inspection, with the subsequent analysis of those by Inmetro. The evidences generated consist of a set of records and images, and their respective geographic and temporal information, all digitally signed, guaranteeing the authenticity and integrity of them. Inmetro is responsible for reviewing all the evidences of each inspection, searching for any inconsistencies that may compromise its reliability to ensure that it was performed correctly. Any deviations committed by inspection bodies will lead to punishments such as suspension or cancellation of the accreditation of the inspection body.

The main advantage of this model is that it offers very low impact to current inspection processes conducted in accredited inspection bodies. The only differences are the following tasks:

- evidences generation (photographic and records) at key points of the inspection process;
- evidences submission to Inmetro — along with additional information.

Hence, the inspection process will suffer little change. The proposed model for enhancing the reliability of inspection systems, represented in Figure 1, consist of three main parts: evidence acquisition subsystem, communication subsystem, and post analysis checking subsystem.

Evidence Acquisition Subsystem. The evidences of conducting an inspection will be a set of images and records associated with geographic and temporal information. The records represent the data inserted throughout the inspection process. These evidences will be generated by GPS-equipped devices with photo capability. Moreover, all evidences will be digitally signed by the equipment, ensuring the authenticity and integrity of such evidences. Such evidences are said traceable, because the moment and place of its execution can be identified.

Communication System. Once completed an inspection (or set of inspections) and produced the necessary data related to this inspection, it becomes necessary to consolidate such data in the form of a structured file and forward it to Inmetro for later analysis.

Post Checking Subsystem. Every inspection conducted by an inspection body shall be communicated to Inmetro, along with its set of evidences. The Inmetro will receive data from an inspection and review them, seeking for inconsistencies by making use of the records and images, and their associated spatial and temporal information.

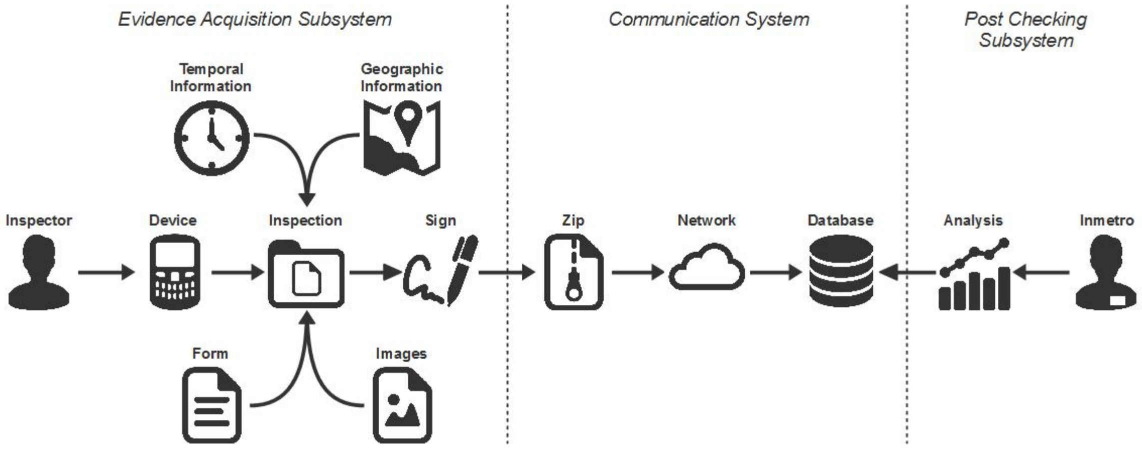

Figure 1. Proposed model for Inspection Systems.

3. Evidence Acquisition Subsystem

In this work, we focus on the evidence acquisition subsystem since it is the core of the model and it is prone to Man-At-The-End attacks. It is the core of the model since it provides the evidences in their origin; and it is prone to Man-At-The-End attacks because an adversary with physical access to the device is capable of compromising it, by inspecting or tampering with the hardware or software it contains.

The evidence acquisition subsystem, in our model, will be embedded in a mobile device that will be used by accredited inspection bodies for each vehicle or equipment inspection performed. The embedded software contains forms for each kind of inspection to be filled by the inspector, and security mechanisms to guarantee authenticity and integrity of the evidences, and to deter Man-At-The-End attacks. The security requirements for this equipment are discussed in the following:

- Authenticity of the evidence. The device must provide a means to verify the origin of the inspection evidence, ensuring that they were generated by a trusted device.
- Integrity of the evidence. The device should provide assurance that the inspection evidence remained the same (intact) from its generation. This aspect concerns the preservation of the evidence generated during an inspection, making it difficult to change without the consent of the responsible body.
- Tamperproofing of the embedded software. The device should contain mechanisms to keep always in the expected state even before tampering or surveillance. This aspect aims to provide device defenses against modification or monitoring functions of the embedded software.
- Confidentiality of secret information. The device must have mechanisms to protect the confidentiality of secret information, for example, cryptographic keys used in the device. An attacker on the possession of such keys could compromise the information security aspects of giving legitimacy to a given inspection that, in fact, is untrue.

3.1. Prototype Implementation

A prototype was developed in the Android platform since it provides greater ease of implementation, as well as greater popularity, which ensure greater portability in the case of prototype approval. During development and testing were collected results which endorsed the feasibility of this inspection system model, however some problems occur in the use of the

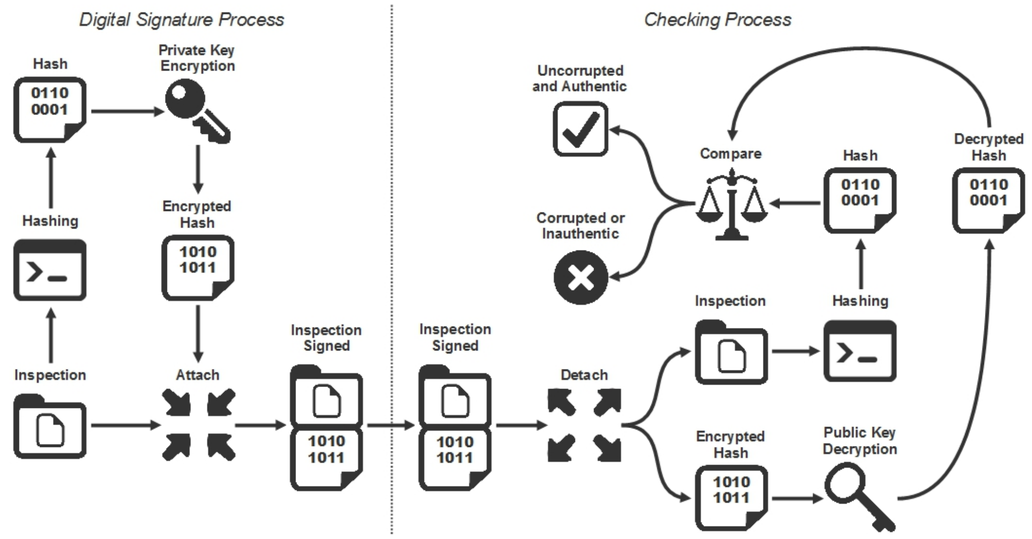

Figure 2. Digital signature process carried by the handheld device, and checking process to validate the digital signature.

Android platform. The favorable results to the inspection system were the various inconsistencies that could be observed by analyzing the inspection records generated during the test, which confirmed the effectiveness of our model. The unfavorable results were related to aspects of usability and security. The Android platform besides presenting vulnerability to various forms of attacks, did not allow the development of effective security mechanisms as planned. Other problems were the fragility and difficulty of using devices equipped with Android, such as smartphones and tablets, in the environment of an inspection body.

3.2. Final version

In order to overcome the prototype issues, we adopted a mobile device with the Windows Mobile Operating System. This device presents robustness and ease of use more suitable to the environment where they are carried out the inspections, and provides a more effective implementation of security mechanisms. An important aspect refers to the environment in which the device is operated, where there is no form of control over who or how it is operating. So, then we detail the techniques that were applied aiming to guarantee aspects of information security.

Digital signature. This technique deals with the integrity and authenticity of the evidences of an inspection. The implementation of this technique is performed by calculating the cryptographic digest (MD5) of the inspection with its correlated time and spatial information. After, it encrypts using asymmetric encryption (RSA). The result of this operation is the digital signature. More details about digital signatures can be found on [4].

In order to verify the authenticity and integrity of the inspection, the cryptographic summary is calculated and compared with the digital signature decryption. If the comparison result is equal it is checked the authenticity and integrity of such inspection. Otherwise, it means that the data was corrupted or is not authentic. Figure 2 illustrates the technique: the digital signature performed in the mobile device, and the checking procedure carried by Inmetro.

Obfuscation of secret information. The implementation of this technique is to make changes in the code of a software, preserving the same functionality, so that it shows greater difficulty

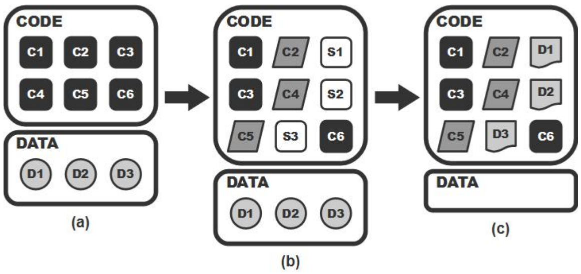

Figure 3. Code obfuscation technique: (a) non-ofuscated code, (b) obfuscated code after applying control obfuscations techniques and (c) after camouflaging the data.

on reverse engineering.

A software is commonly divided into two segments: (i) code segment, containing the instructions to be executed, and (ii) data segment, where data used by the software (constants and variables) are stored. However, this provision facilitates reverse engineering.

So, we used the obfuscation of secret information technique, described in details in [5], which camouflages the data of the data segment in the code segment, leading to incorrect interpretation of these data by reverse engineering tools. Such a technique uses obfuscation control techniques (call, return and return false) [6] in order to create sections in the code segment, capable of storing data. Using this technique to camouflage secret information, such as cryptographic keys, is critical to ensure authenticity and integrity security aspects. Figure 3 illustrates this technique and its steps: (a) non-ofuscated code, (b) obfuscated code after applying control obfuscations techniques and (c) after camouflaging the data. Observe that, in (a) the secret information is clearly visible to an reverse engineer attacker in the data segment, (b) we apply control obfuscation techniques to create sections in the code segment, capable of storing data, and in (c) the secret information is interleaved with other instructions, making it harder to reverse engineering.

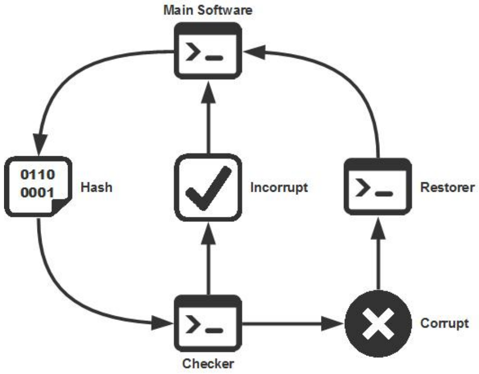

Figure 4. Tamperproofing technique: Self-repairing corrupted software.

Tamperproofing. This technique deals with the tamperproofing of the embedded software. It works in two steps: first by looking up some corruption in the software running in memory and, in the second, taking a response action, for example, self-repairing the corrupted software[7]. This technique was implemented in software, and it runs concurrently, always looking for some corruption of the software. It performs the comparison by calculating the cryptographic digest (hash) of an authentic (unmodified) embedded software and the current embedded software. If the comparison result is equal the embedded software is not corrupted and the device keeps running. Otherwise, the modified embedded software is replaced with the unmodified one and the device is restarted. Figure 4 illustrates this technique.

To give greater robustness to the confidentiality of the secret data and the integrity of the embedded software running on the device, some physical restrictions were applied in the device to enhance the security. For example, the USB communication ports were disabled by hard locks and the shortcut keys of the operating system were disabled by register manipulation.

4. Conclusions

Our proposed model for the evidence acquisition subsystem is critical to aggregate trust of an inspection system since it provides reliable acquisition of evidences in their origin. Such reliable acquisition is obtained by the employment of security mechanisms. Once the evidences are acquired, they are used for a more effective and efficient post checking analyses by Inmetro, looking for clues that indicate inconsistencies in the inspections.

References

[1] Decree n. 96.044 , May 18 1988

[2] Regulation INMETRO n. 91, March 31 2009

[3] Machado R C, Boccardo D R, Carmo L F R C, Prado C B, Nascimento T M, Ribeiro L C and Oliveira T D 2011 Sistema de acompanhamento de inspeções de produtos perigosos *VI Congresso Brasileiro de Metrologia, Natal. Anais do VI Congresso Brasileiro de Metrologia*

[4] Stallings W 2005 *Cryptography and Network Security: Principles and Practice* (Prentice Hall) ed 4

[5] Costa R O, Pirmez L, Boccardo D R, Carmo L F R C and Machado R C S 2012 TinyObf: Code Obfuscation Framework for Wireless Sensor Networks *Int. Conf. on Wireless Networks (ICWN), 2012, Las Vegas. Proc. of the 2012 Int. Conf. on Wireless Networks. Las Vegas: CSREA, 2012. v. 1. p. 68-74*

[6] Lakhotia A, Boccardo D R, Singh A and Manacero Jr A 2011 Context-sensitive analysis without calling-context *Higher-Order and Symbolic Computation, v. 23, p. 275-313*

[7] Collberg C and J Nagra 2010 *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection* (Addison Wesley)