Software Validation of Medical Instruments*

Davidson R. Boccardo, Raphael C. S. Machado, Sergio M. Camara, Charles B. do Prado, Wilson S. Melo Jr,
Leonardo C. Ribeiro, and Luiz F. R. da Costa Carmo
Brazilian National Institute of Metrology, Quality and Technology – Inmetro
Rio de Janeiro, Brazil
{drboccardo, rcmachado, smcamara, cbprado, wsjunior, lcribeiro, lfrust}@inmetro.gov.br

Abstract—**Software validation is a critical issue in several applications. For medical instruments, an ineffective validation may result in human injuries and death. We consider the problem of analyzing software embedded in these medical instruments, correlating with other instruments of the Legal Metrology and Conformity Assessment, such as smart meters or employee payroll recorders. In such cases, an effective way to guarantee an appropriate behavior of an instrument is to conduct a complete validation of its software and hardware – including the source-code and hardware topology details. In the present work, we describe an approach that reduces the amount of intellectual property released to the regulator, protecting the manufacturer's intellectual property, and at the same time it provides traceability and correctness of the measurements.**

Keywords—information system validation; traceability and correctness of medical records; cryptography *(key words)*

I. INTRODUCTION

Increasingly, medical measurement instruments make use of information systems with embedded software. These play a important role in finding errors in diagnosis and treatment, assisting in decisions and reducing health care costs. However, since these instruments contain software modules and perform data processing, they can have incorrect or misleading behaviour.

The incorrect behaviour occurs due to engineering failures afforded by programming errors or a not well-designed architecture. These behaviours can cause monetary losses, and human injuries and death. A historical example of malfunctioning is the Therac-25 medical system that resulted in people receiving overdose of radiation [1,2]. However, an inadequate behaviour can be also intentionally crafted to manipule the measures in order to lead to unnecessary medical procedures, to uncover medical errors or medical malpractice, to change the diagnosis for labor and retirement purposes.

For so, a careful information system validation is vital to guarantee the trust on measurements [3]. Such validation frequently demands a complete disclosure of the information system's implementation, including the software source code, as well as the hardware topology details. This disclosure can be undesirable for the regulatory authority and information system's manufacturer.

On the side of the regulatory authority, such validation may demand an intensive work because of the complexity of the information system and the amount of available time. In many cases, such validation can not be totally effective in the identification of software or hardware flaws. On the side of the manufacturer, the disclosure of information system implementation details could represent a risk for intellectual property – or, at least, most manufacturers feel unconfortable in releasing such details, even for renowned government agencies [4].

This complexity is increased when medical instruments are integrated on cyber physical systems, such as a Pervasive Health Monitoring System (PHMS). PHMS combines different measurement instruments collecting data from physiological and environmental sensors, analyzing and storing patient health information [5]. The effort required for validation of such system is practically an impossible task unless it is applied methods for reducing the critical software amount.

In the present work we describe a pathway to mitigate such inconveniences by reducing the amount of software (intellectual property) disclosured to the regulator by the manufacturer. This of course may appear to be a difficult task, considering that information systems become more and more complex each day. Such challenge, however, is feasible by recurring to cryptography techniques.

More specifically, the proposal consists in digitally signing the measurement information as close as possible of its consolidation in such a way that anyone can change such information in an unnoticed manner in the forward software pathways, i.e. paths in the software execution flows after the measurement signature. This digital signature provides traceability, i.e. integrity of the data and authenticity of the origin. Moreover, the architecture presented provides a way to verify the correctness of the measurements and ensures the legitimacy of the measurement by digitally signing means.

The paper is organized as follows. In Section II we describe the increasingly awareness about safety and measurement correctness of medical instruments in the world context, including the brazilian cases of the conducted evaluations in other instruments, such as smart meters and employee payroll recorder. In Section III we present the key ideas of our proposed approach, detailing how cryptographic techniques can aggregate trust on measurements, providing traceability and how it can be used to reduce the evaluation complexity. Section IV contains our final considerations.

II. Current Scenario Overview

Nowadays, all devices that are used in commercial transactions have gone through some level of software validation, depending on the type of device, to verify that the software embedded in certain device is reliable in terms of measurement correctness and safety.

For medical devices, the both software and hardware validation are stricter as a medical device can be in direct contact with patient or be placed inside a patient, as for instance a pacemaker. Obviously, according to type of device there are different regulations based on the level of control necessary to assure the safety of the device [6].

Within the United States (US), the governing agency for medical device is Food and Drug Administration (FDA). The FDA has created three regulatory classes, which are Class I, Class II and Class III, with the last one being for medical devices with the highest risk [7]. According to classification, the evaluation complexity increases.

In the European Union, the governing area responsible to regulation medical devices is the European Commission (EC). The EC releases directives which serves as the regulatory guide/framework, in the specific case of medical devices is simply called Medical Device Directive (MDD). Similarly to the FDA, the MDD divides medical devices into either Class I, Class IIa, Class IIb or Class III, with Class III being for medical devices with the highest risk [8]. In the Class I, for example, devices are low risk such as stethoscopes, hospital beds, wheelchairs. On the other hand, medical devices belong to Class III has the highest risk as for example balloon catheters and prosthetic heart valves.

In [9] is described the risk management for medical software and additional regulatory requirements are defined in [10]. FDA and EC regulations are based on both documents. The software reliability classification is listed below and the definitions are detailed in such regulations:

- Class A – No injury or damage to health is possible
- Class B – Non-serious injury is possible
- Class C – Death or serious injury is possible

A serious injury is defined as an injury or illness that directly or indirectly is life threatening, results in permanent impairment of a body function or permanent damage to a body structure, or necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.

In Brazil, the concern about software validation control is already performed in evaluations of the Legal Metrology and Compliance Assessment.

In the Legal Metrology, measurement instruments involved in commercial relations are subject to a certain control, by which a government agency – known as Legal Metrology Authority – analyses and certifies that the meter possess an appropriate behavior [11] . The process by which a meter is evaluated by the Legal Metrology Authority is known as type approval and comprises, among other providences, the complete evaluation and control of the legally relevant software, that is, every module of software that is involved or may interfere in the process of capture, processing, transmition and exhibition of measurement results to the end user [12,13].

In the Compliance Assessment, instruments that are used for supporting consumption, commercial and job relations or which the use can implicate safety or health risk issues shall have their compliance evaluated. This is conducted, in Brazil, by imposing a set of functional and non-functional requirements for these instruments. The compliance assessment is performed by independent accredited bodies, evaluating either a respective instrument fullfills all the specified requirements. In the software scope, Brazil has already defined requirements for PKI (Public Key Infrastructure) devices such as smartcards, security tokens, readers and HSMs (Hardware Security Modules), as also for employee payroll recorders.

On both cases, the evaluations require the disclosure of the information system's source code of the software and its hardware details. The main contributions of this work may be summarized as follows:

- It introduces an architecture to deal with the software validation complexity, reducing the amount of intellectual property that should be validated;
- It assures the traceability of the measurement, ensuring its integrity and authenticity;
- It introduces a way to perform a posteriori verification, in which the end user can check the measurement correctness.

III. Proposed Approach

A pathway to deal with the validation complexity and not disclosing the whole intellectual property is to reduce the "amount of software" that can influence on measurements. Our proposed approach consists in the following: a software module that processes the measurement information in advance of its signature should be evaluated – including its hardware topology. The remaining software modules cannot change such measurement in an unnoticed manner since it is traceable by its digital signature.

Our approach classifies the embedded software into two distinct types: the software modules that can interfere in the measurements that are exhibited to the user are said to be relevant; the software modules that process only digitally signed data – hence cannot change such data unnoticely – are not relevant.

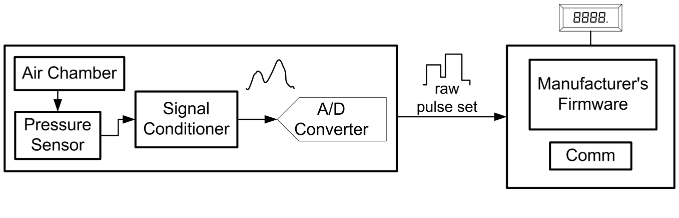

Fig. 1. An example of a sphygmomanometer architecture.

We describe how such approach can be implemented in medical instruments (case study: sphygmomanometer) by means of a trusted hardware device or by software separation inside the same microcontroller, allowing a reduction of the amount of software that is relevant – and, consequently, reducing the amount of software that must be fully analyzed by the regulator.

The key idea is to establish a root of trust (hardware or privileged software) in the early stages of data processing, and delegating to it the task of signing an amount of data that is sufficient to trace, at any time, the correctness of the measurement software. While our approach resembles Trusted Computing ideas and tools such as the Trusted Platform Module [14], the root of trust can be more properly seen as a Trusted Third Party [15] working inside the instrument and certifying the measurement correctness.

Following, we show our proposed architecture of reducing the amount of software to be evaluated applied for sphygmomanometer (blood pressure monitor), allowing hypertension diagnostics (high blood pressure) and helping their patients keep it under control. The proposal architecture is generic and can be easily extended for other medical instruments.

A. Case Study: Sphygmomanometer

A common design pattern that is present in these instruments contains a data raw acquisitor, a measurement function, and a measurement display. The data acquisitor provides raw data to be processed by the measurement software. The main components of the data acquisitor are sensors - which are in direct contact with the physical event under measurement -, transducers - which convert the sensed quantities to an analog voltage signal -, and analog-to-digital converters - which convert an analog signal to a digital one.

In such instrument, each time a given quantity is measured, there is the emission of one pulse by a set composed by pressure monitor, air chamber, analog-to-digital converter (ADC) and digital circuit. The pulses are forwarded to a measurement function, basically embedded in a microcontroller (MCU). The measurement function processes the data generated in the data acquisitor in order to obtain a final measurement. It typically receives raw data, processes it and consolidates a measurement. However, this measure is not immediately informed to the patient: it is further processed by other pieces of software before it is finally exhibited to the patient (as illustrated in Fig. 1).

In this case study, we add a microcontroller with cryptography-based authentication/ signature algorithms inside the architecture, between the component that delivers the pulses and the component that performs pulses processing. This microcontroller shall sample the sensor signals from the beginning to the end of the measurement and will be capable of signing the raw pulses set. This signature enables integrity/ authenticity verification of the measurement data in any subsequent stages of data processing, i.e. in any software components or software execution flows disposed after the signature. Also, it is needed a start/stop interface in order to establish the beginning and the end of the raw pulses that should be collected and signed. Figure 2 shows the proposed architecture.

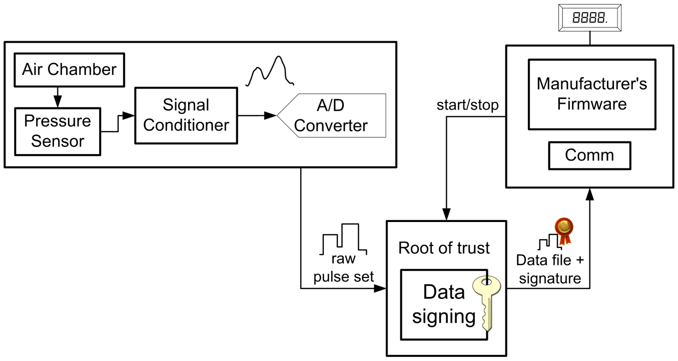

Fig. 2. Our proposed architecture with a root of trust, implementing cryptographic-based authentication/signature algorithms.

In our proposed model, the verification is based on a posteriori procedure, moved to the patient or regulator's website, so that no software code lines should need to be analyzed. In such a scheme, a patient or the regulator can check the traceability and the measurement correctness. In the case of the regulator, it can provide a site in which the patient enters the following data, as illustrated in Figure 3:

- Sphygmomanometer display output, which contains instrument identification, measurement identification, timestamp, and diastolic and systolic measures;
- Data file (available to the user via the communication port of the sphygmomanometer), containing the measurement identification, the raw pulses set, and the digital signature of the whole data file.

The regulator's website performs the verification in three steps. In the first step, it compares the cryptographic digest of the data file with the public-key, related to the instrument identification, applied to the digital signature. If the results are the same, we can trust that the data file was originated from the specified sphygmomanometer and it is authentic. Moreover, it infers that the regulator previously evaluated the instrument.

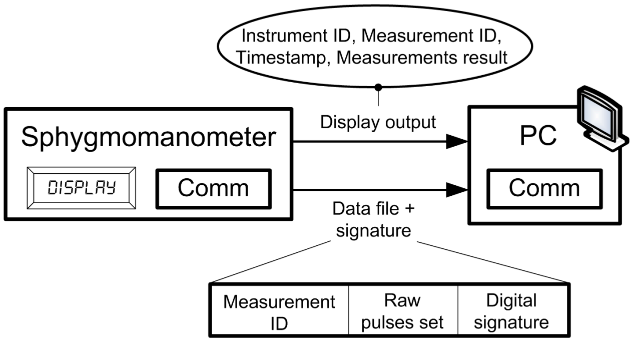

Fig. 3. Information contents of sphygmomanometer display and data file.

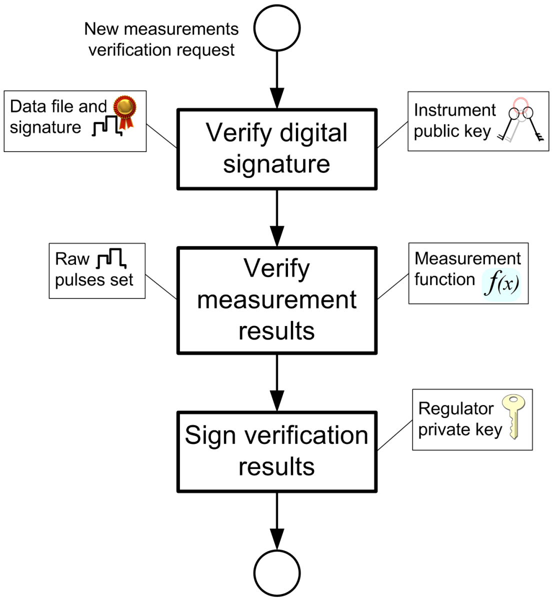
New measurements verification request
Data file and signature
Verify digital signature
Instrument public key
Raw pulses set
Verify measurement results
Measurement function $f(x)$
Sign verification results
Regulator private key

Fig. 4. Proccess by the regulator's website for new measurements verification request.

In the second step, it performs the verification of the measurement by manipulating the data file. The idea is that the patient can, at any time, insert the data file (raw pulses set) in the regulator's website and "reproduce" the measurement, comparing the result calculated by the site with the result provided by the sphygmomanometer. In this case, the regulator website implements all the measurement functions for each manufacturer.

This allows an a posteriori verification of the correctness of the measurement software, and any malfunction of the measurement software can be detected. The third step consists in digitally signing the output of the verification ensuring its legitimacy. The whole process is illustrated in Figure 4.

IV. Conclusions

In the present work we proposed the use of a root of trust module based on hardware or privileged software to improve the confidence on measurements produced by a measurement instrument. We claimed that such approach allows a simplification of the software validation process by the regulatory authority. Although the focus of the present paper is medical instruments, the ideas here proposed naturally extend to other areas of metrology and even to other critical software-based devices.

References

[1] Garfinkel, "History's worst software bugs", Byte Magazine, November 2005.

[2] N. G. Leveson, and C. S. Turner, "An investigation of the therac-25 accidents", IEEE Computer Society, 26, pp. 18–41, USA, 1993.

[3] N. G. Leveson, "Software safety in embedded computer systems", Commun. ACM, 34(2), pp 34–46, 1991.

[4] D. R. Boccardo, L. C. Gomes dos Santos, L. F. R. da Costa Carmo, M. H. Dezan, R. C. S. Machado, and S. de A. Portugal, "Software Evaluation of smart meters within a Legal Metrology Perspetive: A Brazilian Case," IEEE Innovative Smart Grid Technologies Conference Europe, pp. 1–7, October 2010.

[5] K. K. Fletcher, X. Liu, "Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber-Physical Systems", IEEE International Conference on Secure Software Integration and Reliability Improvement, pp 106—113, 2011.

[6] A. Magnusson, "Regulation for the Development of Medical Device Software", Master of Science Thesis. Department of Signal and Systems. Chalmers University od Technology. Gothenburg, Sweden, 2011.

[7] Premarket Notifications, "Food and Drug Administration" Available: http://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketnotification510k/default.htm.

[8] Europe Comission, "Guide to the implementation of directives based on the New Approach and Global Approach", 2000.

[9] ISO 14971, "Medical Devices – Application of risk management to medical devices".

[10] IEC 62304, "Medical Device software – Software life cycle processes".

[11] A. J. Dick. "Balancing legal metrology and market model requirements", IEEE International Conference on Metering and Tariffs for Energy Supply, pp 7–11, 1999.

[12] OIML - Organization Internacionale de Métrologie Légale, "General Requirements for Software Controlled Measurement Instruments", 2008.

[13] WELMEC - European Cooperation in Legal Metrology, "WELMEC 7.2, Issue 5, Software Guide ", March 2012.

[14] TCG - Trusted Computing Group, "TPM Main Specification Level 2 Version 1.2, Revision 116", March 2011.

[15] W. Stallings, "Cryptography and Network Security", Fourth Edition, 2005.