A formal passive testing approach to control the integrity of private information in eHealth systems*

Azahara Camacho, Mercedes G. Merayo and Manuel Núñez

Departamento de Sistemas Informáticos y Computación
Universidad Complutense de Madrid, Madrid, Spain
mariaazc@ucm.es, mgmerayo@fdi.ucm.es, mn@sip.ucm.es

Abstract. Intelligent Information is generated with each click that we do. The systems that are responsible of this tend to have a log where they record all the accesses to them. Unfortunately, the integrity and anonymity of this vast amount of information is not always ensured. There exist many threats that can change or even delete part of these logs. One of the purposes of the Internet of Things (IoT) is to generate Intelligent Information from different sources. Therefore, if there are some irregularities, then the generated information is not useful. In this paper we present a proposal to take into account some of these threats and prevent their consequences in some eHealth systems. In order to increase the applicability of our approach, we have implemented a tool that allow us to manage communications and check whether they are performed as intended.

1 Introduction

The appropriate control of data integrity is one of the open issues where more research areas involves. Different reasons, mainly security and privacy, have provoked this trend. In fact, this is currently a matter of public and professional areas because huge amounts of data are generated by the countless systems used in our daily routine. There are many hazards that surround us and turn these devices on vulnerable systems. With the aim of preventing these risks, it is necessary to apply techniques to ensure the safety of our privacy. If the used technique has a formal basis then it will be possible to prove that they behave as expected. According to different features, we can find different testing methods, but a classical distinction is between *active* and *passive* [CHN15]. In *active testing*, the tester needs to interact with the system under test (SUT). Therefore, it is necessary to stop the usual activities of the SUT in order to carry out testing activities. In addition, the tester needs to introduce some data (inputs) to decide whether the observed behaviour (outputs) is the expected one. These *fictitious*

* Research partially supported by the Spanish MEC projects ESTuDIo and DArDOS (TIN2012-36812-C02-01 and TIN2015-65845-C3-1-R) and the Comunidad de Madrid project SICOMORo-CM (S2013/ICE-3006).

inputs can modify the data in the system (for example, the tester may require to modify the balance of a current account in order to test some features). Taking into account that systems in use are required to run 24/7 and that sensible data should not be modified in the real system, active testing, even though more powerful to find errors in a system, cannot be used in many situations. In *passive testing* the tester only observes the behaviour of the SUT, without influencing its performance by providing inputs. Thus, in order to perform the testing process, it is not necessary to change, stop or modify either the system or its associated data. Unfortunately, we lose the ability to *guide* the system through situations where it is more likely to find an error (this can be done in active testing by providing specific inputs targeting certain components of the SUT). In any case, although less powerful, passive testing techniques are being used more frequently and there are many proposals with a formal basis [BCNZ05,AMN12].

In this paper, we adapt a formal approach to perform passive testing in systems where communications are asynchronous[HMN13] to the control of the elements involved in the exchanging of information between two remote systems. We focus on eHealth computerized remote systems, more specifically, we are interested in checking the integrity of the transmitted data and the privacy of the process. In order to show a concrete case study, we consider the communication between a pacemaker and its monitor. The rest of the paper is structured as follows. In Section 2 we introduce the basic concepts of the Internet of Things (IoT) that are related to this paper. Section 3 explains the concept of eHealth and how it is related to IoT issues. Section 4 explains the scenario for the application of our approach and in Section 5 we present our proposal. Finally, in Section 6 we present our conclusions and provide some lines for future work.

2 The Internet of Things (IoT)

Technology makes life easier with original improvements. These could be in the form of better materials, new devices or healthier products. In this line, the Internet of Things is able to ease the management of information from different sources. Domotics, health-care, smart buildings and surveillance are only a few of them where IoT can be applied. According to the National Intelligence Council, "*by 2025 Internet nodes may reside in everyday things - food packages, furniture, paper documents, and more*" [Nat08]. That is, each element of our daily routine will have a sensor able to send information about weather conditions, environment, its user, etc. Therefore, the evolution of IoT is an inevitable consequence and its ubiquitous application is only a matter of time. In this section we review the main characteristics of IoT, some open issues, and the main application areas.

2.1 Characteristics

In order to have a clearer idea about IoT, a possible definition is: "*Internet of Things is the combination of supporting resources to interconnect smart objects*

by means of extended Internet technologies, obtaining as a result the ensemble of applications and services leveraging them to open new business and market opportunities" [MSPC12]. These *smart objects* are the *things* of the Internet of Things and for being one of them, there are some requirements that should be fulfilled [RNL11]. In a nutshell, an IoT element has the following characteristics:

- *Existence*: It could be in the physical world such as computers, cars or houses, but it can be also the virtual data provided by the physical ones.
- *Sense of self*: Due to the huge number of elements to interconnect, it is essential to have an identification that let the other elements to find it in the network.
- *Connectivity*: Using the previous identification, the entity should be able to communicate with its surroundings and locate it.
- *Interactivity*: If the communication is established, then the element has to manage the sending and reception of information with other elements. Provoking a wide range of services as a result.
- *Dynamicity*: All the elements have to be available at any time, any place and in any way.

2.2 Open issues

The previously mentioned characteristics generate new issues to support. The network where all the elements are connected is bigger everyday and this causes a greater difficulty for their performance [AIM10]. The current issues to control are:

- *Authentication*: Objects need to be uniquely identified with an ID. The most used technique is IP addresses. The problem is the number of IPs in IPv4 are not enough to identify all the elements. Therefore, it will be necessary to use IPv6 to control all the elements [CJ09].
- *Heterogeneity*: IoT has to be able to manage many different types of devices, without difficulty and being only aware of the IP for the identification. The management of such a high number of differences between systems provokes the necessity of better protocol levels.
- *Scalability*: One of the unavoidable problems in a global information structure, such as IoT, is scalability. Due to the continuous growth of the network, it is essential that all the elements are able to adapt themselves to the new architecture.
- *Energy-optimization*: The dynamicity of IoT elements is the main reason why the optimization of energy is an open research issue. The devices depend on batteries and the minimization of the consumption is a trend that developers should adopt.
- *Localization and tracking*: The continuous tracking of IoT elements confronts the problem of the current state of the availability of wireless networks. Some applications such as health-care control or weather management could be affected by the lack of wireless resources in some areas.

- *Data management*: IoT generates massive amounts of data and its storage and exchanging require a proper architecture. Besides this, the design of the architecture should be the most efficient in order to manage data at the same time that other systems.
- *Security and privacy*: In this case, there are three key sub-issues which require some solutions. These are data confidentiality, privacy and trust. The guarantee that only authorized entities can access and modify the generated data is quite weak. Therefore, it is necessary to use control techniques to avoid the leakage of information.

2.3 Applications

Although the number of issues to resolve is large, there are a big amount of fields where IoT is starting to be successfully applied. Its potentialities offer the possibility of developing many applications and services that were unthinkable a few years ago. They could be divided in four domains:

1. *Transportation and logistics*: Thanks to the use of sensors and actuators, the application of IoT in roads and vehicles is gaining momentum. Some of the benefits in this area could be: transportation information, assisted driving and monitoring of transportation of hazardous materials.
2. *Smart environment*: This field is oriented to make easier and more comfortable our surroundings such as the house, the office or the supermarket. The appropriate distribution of sensors can facilitate the automatic regulation of room lighting, heating or energy consumption. In addition, a security option can be used to detecting natural phenomena. In the later case, real and current information can be provided and a rapid response can save human lives, mitigate the damage and reduce the level of disaster.
3. *Personal and social domain*: People tend to look for the faster and better social network in order to receive updates about news, friends and events. With the compilation of historical queries about websites and devices data, social networks can improve the information to show to users, according to their searches and preferences. In terms of security, this area can be benefited in case of losses or thefts.
4. *eHealth*: This is a sensitive area where any benefit can have an important impact and increase the number of lives saved. Considering the previous characteristics of IoT elements, there are many applications that can improve the current state of healthcare. Some of them are the automatic data collection from Implantable Medical Devices (IMD), patient identification and alarm actuators. This can be helpful for controlling its problems and either react in a faster way or inform about a critical situation of the patient.

We focus on eHealth and IMD. Therefore, in order to put our research in context, we need to explain some of the threats and open issues in the IMD area and what is our proposal to improve the current situation.

3 eHealth: Implantable Medical Devices

The healthcare industry has been affected by numerous (software) errors during the last years [SOMM10]. Since 2001, with the emerging of the *eHealth* concept [Eys01], some approaches seem to be the improvement that this field needs. Around 3.337 recalls, out of 8.320 manufactured IMD, were reported to the US Food and Drug Administration (FDA) between 2010 and 2012, a 40% from the total of elements [U.S14]. In this case, the enhancements are been motivated by the errors related to software, hardware, data management and energy supplies. Some of them have been identified by the consequences of the open issues with IoT elements previously enumerated. Thanks to eHealth research, they might be farther reduced by implementing some of the following proposals:

- *Heterogeneity*: IMD need to be connected with different elements such as PCs and monitors. For the problem of connecting to all these types of heterogeneous devices, it is necessary to apply specific protocols managing all the necessary layers [Cha07].
- *Scalability*: IMD developers need to be consistent with the continuous evolution of materials and software. A clear solution is the application of fault tolerance techniques, with the aim of diminishing the impact of this situation [AIKR13].
- *Localization and tracking*: Some IMD are provided with sensors that inform about the state, position and patient situation. In the case of insulin pumps, pacemakers and defibrillators, this technology allows physicians to check their data in case of emergency [BCRF12].
- *Data management*: The continuous service of these devices generates massive amounts of data, being some databases systems available for their management. We can mention the Electronic Health Records (EHR), a collection composed by the healthcare information of patients, and the Picture Archiving & Communication Systems (PACS), registering digital images in order to post-process and collect them for future medical cases [BCP+11].
- *Security and privacy*: In order to control the actors who access a device, it is necessary the implantation of an authorization system. In relation to the previously mentioned heterogeneity problem, specific medical protocols could include this feature with the aim of fulfilling two issues with one solution [HKHB+08].

4 Scenario

There exists a wide range of vulnerable IMD and each of them has their own hazards. In this paper, we focus on pacemakers due to the fact that, alongside infusion pumps, they are the most implanted devices which require a software for the storing of data and the interaction with external elements [All11]. For this group of IMD the main threats are related to data access, device identification and configurability [HKHB+08]. Although their software is private, this is not

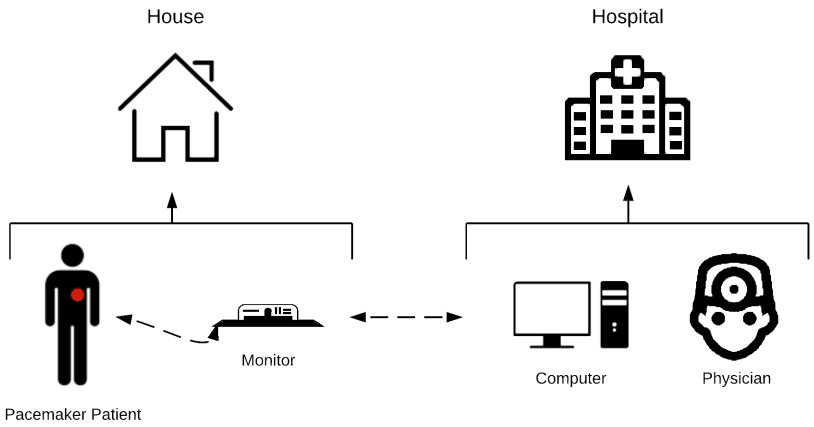

Fig. 1. Sending information from the pacemaker.

a problem for hackers when they try to violate their security. Unfortunately, and difficult to understand because human lives are at risk, these devices tend to have an extremely low level of security measures. Developers do not pay too much attention to the possibility that an external element tries to capture data or alter its configuration. In order to prevent some of these situations, we present a scenario where our proposal can be applied in order to avoid the capture of private data by unauthorized actors.

The scenario is a patient whose pacemaker tries to send to the monitor, located in his house, the data captured during a certain period of time. This monitor, at the end of the transmission, sends this information to the computer of the physician, placed in the hospital. With this sequence of actions, the patient is completely tracked in terms of how the pacemaker works with the heart. A graphical representation of this scenario appears in Figure 1.

Since the communication between these elements is by wireless connections, the level of danger is quite high. The risk that we seek to prevent is the intrusion of third parties inside this connection with the aim of capturing, modifying or deleting information from the pacemaker. As a solution, we propose controlling this threat by always checking the origin and destiny of messages. Monitoring this exchange of information can ensure that only the authorized actors are involved in the transmission. In order to achieve this goal, it is necessary the management of a list including all the users and devices that are authorized, so that during the communication, it should be possible to review the active actors. This identification will be possible thanks to the IP address of each source of the message.

5 Our proposal

We propose a software tool to control the actors previously mentioned. The underlying methodology is based on a formal approach to perform passive testing with asynchronous communications [HMN13]. The main reason why we decided to use a passive testing methodology is, as we explained in the introduction of the paper, is because we do not need to stop the system to check its correctness. In our case, due to the fact that we are working with the scenario of an implanted pacemaker, this kind of techniques are the most suitable. In addition, although this complicates the framework, we need to take into account that the communication between devices will be asynchronous.

The proposed software will be based on a graphical user interface (GUI) which is designed to connect it to the network where the pacemaker and the monitor communicate between them. The user is in charge of defining the elements conforming the list of authorized actors. This list is also made from the definition of properties where the user specify how messages should be transmitted and what actors will be allowed to participate in the exchange of information. The tool will be divided into different layers, each of them focusing on the specific feature for what it has been designed. Next we explain the main components of the tool.

5.1 Administration of actors

This will be the most active part of the tool and it will allow the users to define the behaviour of the communications by using a certain set of properties. These properties will include the actors participating in the conversation and the messages that will be transmitted. The appropriate use of this layer of the GUI is essential in order to ensure correct communications. In Figure 2 we show an example of this layer. Its main parts are:

- *Group*: This is the set of properties where the new one will be grouped.
- *Property*: This is the (unique) name of the property.
- *Sequence of actions*: This is the set of actions taking part in the property. Each of them includes information about the actor which performs it.
- *List of actors*: This is the group of authorized actors that can appear during the communication. It is not necessary to include the actors that defined in the property. This list is updated with the content of the sequence of actions.

Next we describe a typical property that we should ensure when a pacemaker is programmed to send its data to the monitor located in the house of the patient. In the property, actions prefixed by *?* denote inputs while properties prefixed by *!* denote outputs.

- Group: Communication.
- Property: Sending records.
- Sequence of actions: (*?send*,pacemaker) (*!ready*,monitor) (*?ip*,pacemaker) (*!info*,monitor), where:

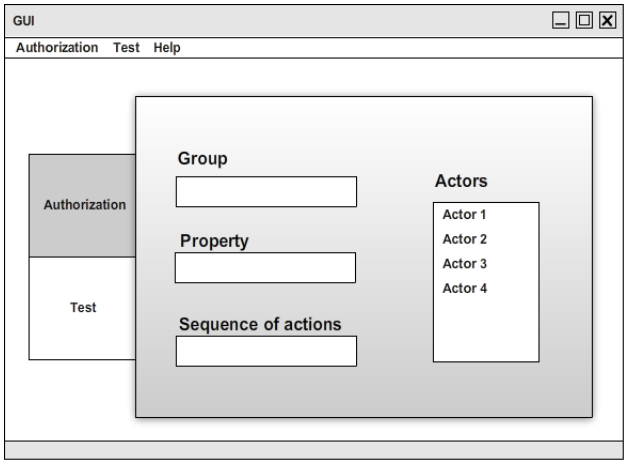

Fig. 2. Layer for the definition of the actions and actors of a property.

- *?send* is the request of the pacemaker to send the data.
- *!ready* is the confirmation of availability from the monitor to receive the records.
- *?ip* is the request of the IP of the monitor to check against the list of actors that it is an authorized device.
- *!info* is the IP of the monitor.

– List of actors: pacemaker and monitor.

5.2 Authorization control

This will be the *passive* component of the tool. In order to verify the correctness of the transmission of information between the pacemaker and the monitor, an online checker tests the current transmission against the previously defined messages and actors. In Figure 3 there is an example of this layer.

This component is the core of the GUI because it is in charge of checking the actors involved in the communication. This process will consist in the analysis of every message sent between the actors. However, this examination will concentrate on their features, not in their content, that is, the origin and destiny of the message, the type of the message and the order of the sequence. The result of checking the property against the observed trace will appear on the list of the right side of the GUI, showing the actors and their actions. If one of these sequences is invalid, then the process will stop and inform the user of the problem found in the transmission of the data.

6 Conclusions and future work

In this paper we have presented the main features of a tool which would be able to check the actors involved in the transmission of data from a pacemaker. By using

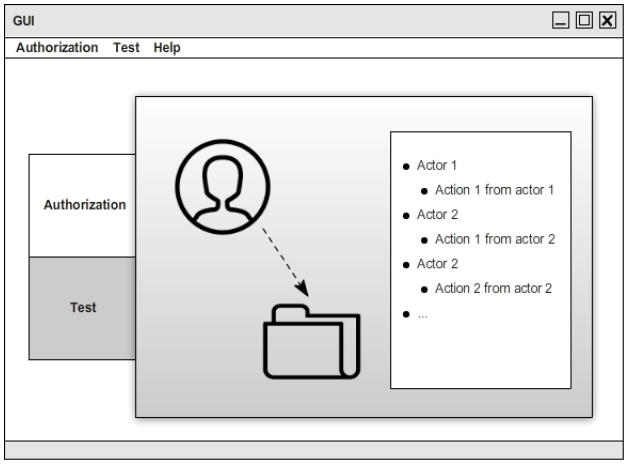

Fig. 3. Layer for the test of the current communication.

passive techniques, it is possible to perform online checking of the performance against the properties previously defined without stopping the involved systems. If an irregularity is detected, then the user can apply the appropriate measures in order to avoid the alteration of private information.

As future work, we plan to analyse and study the complete medical protocol used in this type of communications. This will allow us to reflect its behaviour in our application and we will be able to ensure that the transmission of information is correct. In addition, we will study the impact of explicitly considering probabilities and time [GN99,HM09,HMN09,AMN12].

References

[AIKR13] H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk, and J. Raman. Analysis of safety-critical computer failures in medical devices. *IEEE Security Privacy*, 11(4):14–26, 2013.

[AIM10] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[All11] B. Allen. The Eleven Most Implanted Medical Devices In America. http://247wallst.com/healthcare-economy/2011/07/18/the-eleven-most-implanted-medical-devices-in-america/, 2011.

[AMN12] C. Andrés, M. G. Merayo, and M. Núñez. Formal passive testing of timed systems: Theory and tools. *Software Testing, Verification and Reliability*, 22(6):365–405, 2012.

[BCNZ05] E. Bayse, A. Cavalli, M. Núñez, and F. Zaïdi. A passive testing approach based on invariants: Application to the WAP. *Computer Networks*, 48(2):247–266, 2005.

[BCP+11] A. D. Black, J. Car, C. Pagliari, C. Anandan, K. Cresswell, T. Bokun, B. McKinstry, R. Procter, A. Majeed, and A. Sheikh. The Impact of

eHealth on the Quality and Safety of Health Care: A Systematic Overview. *PLoS Medicine*, 8(1), 2011.

[BCRF12] W. Burleson, S.S. Clark, B. Ransford, and K. Fu. Design challenges for secure Implantable Medical Devices. In *ACM/EDAC/IEEE 49th Design Automation Conference, DAC'12*, pages 12–17. IEEE Computer Society, 2012.

[Cha07] P. E. Chadwick. Regulations and standards for wireless applications in eHealth. In *29th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society, EMBC'07*, pages 6170–6173. IEEE Computer Society, 2007.

[CHN15] A. R. Cavalli, T. Higashino, and M. Núñez. A survey on formal active and passive testing with applications to the cloud. *Annales of Telecommunications*, 70(3-4):85–93, 2015.

[CJ09] J. Cooper and A. James. Challenges for database management in the Internet of Things. *IETE Technical Review*, 26(5):320–329, 2009.

[Eys01] G. Eysenbach. What is e-Health? *Journal of Medical Internet Research*, 3(2):e20, 2001.

[GN99] C. Gregorio and M. Núñez. Denotational semantics for probabilistic refusal testing. In *Workshop on Probabilistic Methods in Verification, PROBMIV'98, ENTCS 22*. Elsevier, 1999.

[HKHB+08] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel. Security and privacy for Implantable Medical Devices. *Pervasive Computing*, 7(1):30–39, 2008.

[HM09] R. M. Hierons and M. G. Merayo. Mutation testing from probabilistic and stochastic finite state machines. *Journal of Systems and Software*, 82(11):1804–1818, 2009.

[HMN09] R. M. Hierons, M. G. Merayo, and M. Núñez. Testing from a stochastic timed system with a fault model. *Journal of Logic and Algebraic Programming*, 78(2):98–115, 2009.

[HMN13] R. M. Hierons, M. G. Merayo, and M. Núñez. Passive testing with asynchronous communications. In *IFIP 33rd Int. Conf. on Formal Techniques for Distributed Systems, FMOODS/FORTE'13, LNCS 7892*, pages 99–113. Springer, 2013.

[MSPC12] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[Nat08] National Intelligence Council. Six Technologies with Potential Impacts on US Interests Out to 2025. http://fas.org/irp/nic/disruptive.pdf, 2008.

[RNL11] R. Roman, P. Najera, and J. Lopez. Securing the Internet of Things. *Computer*, 44(9):51–58, 2011.

[SOMM10] K. Sandler, L. Ohrstrom, L. Moy, and R. McVay. Killed by code: Software transparency in implantable medical devices. Software Freedom Law Center, 2010.

[U.S14] U.S. Food and Drug Administration. Medical Device Recall Report - FY2003 to FY2012, 2014.