OPEN ACCESS

International Electronic Conference on Sensors and Applications
1 - 16 June 2014

www.mdpi.com/journal/sensors

Conference Proceedings Paper – Sensors and Applications

Automatic system for providing security services in the Internet of Things applications over Wireless Sensor Networks

J.A. Sánchez Alcón [1,*], Lourdes López [1] , José-Fernán Martínez [1] and Pedro Castillejo [1]

[1] Centro de Investigación en Tecnologías Software y Sistemas Multimedia para la Sostenibilidad (CITSEM). Universidad Politécnica de Madrid (UPM), Edificio La arboleda, Campus Sur UPM. Ctra. Valencia, Km 7, 28031 Madrid, Spain; E-Mails: jose.asanchez-alcon@upm.es; lourdes.lopez@upm.es; jf.martinez@upm.es; pedro.castillejo@upm.es

***** Author to whom correspondence should be addressed; E-Mail: jose.asanchez-alcon@upm.es; Tel.: +34-914-524-900 Ext. 20791.

Published: 1 June 2014

Abstract: This paper describes an automatically determination process of the security services for products and services on the Internet of Things. This process has as inputs the service context, the legislative diversity and the information involved among others. Considering the resources limitations in a Wireless Sensor Networks and the already mentioned inputs, it is possible to find the best solution to apply in each specific case. We will introduce the "Utility Matrix" as a main concept to link all interests of stakeholders regarding their security needs and the legal imperatives. The final solution has been implemented with an expert system. The process outputs are composed by several products as a security policy for the service; a protected data certification, and an effective tool to simulate and evaluate impacts over new services or when service conditions or laws change. Challenges to research over new technical solutions needs can also be obtained.

This proposal will connect the Industrial, Judicial and Technological areas working together to obtain trustworthy certifications for all stakeholders. The results have been evaluated in a real scenario made up of a Wireless Sensor Network, over middleware service oriented platform in the framework of "AWARE project" and the expert system are connected to the platform in order to configure the security services.

Keywords: Internet of Things; Wireless Sensor Network; automated security service determination; security service; data privacy; security of data; personal data protection; utility matrix concept; expert system;

---

1. Introduction

Personal data protection for product and services on the Internet of Things (IoT) should be considered from design stage [1-2], and should be adequate to countries legislation also. Otherwise user could have the perception that the new technologies may threaten their privacy. That user perception could be a barrier to IoT growth.

The N. 108 Convention of the European Union Council establishes common criteria for the same data protection levels in all members of the EC, changes of different laws of nations over data protection, are coordinated by Directive 95/46/EC. Some action lines are established in the EC Commission Communication (2009) 278 also.

When talking about "privacy" on public domain, the main concern is risk identification and consumer profiling, since it involves secured information exchange related to people privacy. Nevertheless, privacy for enterprise domains refers to confidential business information.

The European Union acknowledged the legislative heterogeneity in the report on the implementation of the Data Protection Directive of 24th February 2004, and emphasizes the need for States and European institutions to adopt an equivalent level of protection for fundamental rights and for individuals in the implementation of the Directive, noting that uneven national legislation on data protection hinders the development of the internal European market.

For now coexisting with this heterogeneity globally maybe must be needed. The main objective of this work is to automatically select the security services and mechanisms that should be implemented to a certain product or service IoT based on the usefulness of the service, the environment involved and the purpose of service, etc.. These results provide information to choose the most appropriate technologies and the security mechanisms for implementing them without compromising service quality. They can usually be multiple valid solutions, which will enable choosing the most efficient choice both from a technological viewpoint as from business viewpoint.

This article describes an Expert System involving areas that cover the needed knowledge and the confidence enough to provide quality solutions; these are companies, legal and technological areas. This will provide trust certificates for both users and businesses. It is a support system for companies while designing new products and services; they could perform virtual simulations before making decisions on the authentic market. Furthermore legal and political sectors could conduct impact assessments in the society and market about possible changes and new data protection laws as well as know what extent would affect existing products and services and future developments. Finally, it can be a useful tool for the technology sector as they could observe and evaluate critical issues that need research and innovation on new problems that require new technological solutions.

Integrating the expert system in a NOC (Network Operations Centre) the intelligence could be centralized and the security policies could be handle in a large IoT environment to be communicated with a service platform (as the one proposed in AWARE project[3]) to reconfigure security using appropriate middleware.

2. Experimental Section

The scenario we are using to develop our proposal is composed by one Wireless Sensor Network (WSN), one service-oriented middleware platform under the "Project AWARE" is a platform for access to wearable devices in smart environments [4], and an Expert System that connects to the AWARE platform to configure security policy in the WSN.

2.1. AWARE Project

The testing platform is a system that monitors the health status for users in different environments, and makes it possible to take emergency actions in case to health problems. Data collected are blood pressure, pulse, and body temperature. Data are collected by wearable devices [4] and are periodically sent to the medical assistants, for knowing the effectiveness of a particular medical treatment for example. The system can also be used for monitoring persons in critical activities, as firemen actuations, and others. These monitoring system may perform a processing of personal data therefore is necessary to consider security services, including privacy protected by the laws of the countries in the protection of personal data.

Our proposal is to select and implement the required security services by the stakeholders about the products and services of the IoT regarding data treatment, data storage and data movement that must be protected according to the legal framework and business criteria. Security services will be integrated as a new AWARE environment service (using the same procedure described in the project for the proposed services). The overall topology for the used scenario consists of several body area networks (BANs) in a WSN structure. Health information is collected and processed at the base station in order to launch one alert event when one problem appears, in order to launch the necessary actions to face it. In this proposal, SunSpot [5] nodes are used to deploy the WSN.

2.2. Description of the proposal

The expert system we have developed is divided into three engines: Business Expert System (BES), Legal Expert System (LES) and Technological Selection Expert System (TSES).

The BES system has the relevant information of the service specifications as input, such as service type, target people, personal data involved in the service and others. However BES system gives the relevant information to the LES system as output, included in a structure named "Utility Matrix".

The LES system obtains the "Utility Matrix" as input, it came from BES output, based on that information LES gives the legal imperatives over information that must be legally protected. When the "Utility Matrix" is processed, the legislative and regulatory framework for the specific application is obtained. Based on this framework, we obtain the security imperatives regarding legally protected information. This LES output is the TSES input used as imperatives and data to protect. With the security imperatives obtained to apply over dataset to be legally protected, the system can select the most appropriate security mechanisms.

Table 1 includes the basic model of the process, the information used for security services selection, the information flow between blocks and the information processing. This process is based on the

cooperation of several functional blocks BES, LES and TSES which are part of a complete system that interacts by transferring intermediate results between those blocks.

Several knowledge bases are used along the system for the information processing. Each knowledge area owns and manages its own knowledge base and contributes with its knowledge to the expert system final results. All of these areas are working together to achieve a high-grade people protection. Each part has its own evolution, but its inputs and outputs are standardized in format and content for files interchange purposes. This idea has been inspired by deployed applications for expert systems in the legal environments [6].

Table 1. Automatic system for providing security services process.

Automatic system for providing security services process stages				
Stage	**Functional Blocks**	**INPUT**	**KNOWLEDGE DATABASE**	**OUTPUT**
1º	**Business (BES)**	Services Requirements	Business Knowledge structure	Utility matrix Personal data involved
2º	**Legal (LES)**	Utility matrix + personal data involved	Laws, standards	Legal Imperatives sensitive information
3º	**Technological (TES)**	Legal Imperatives over sensitive information	Attacks, security services, mechanisms, …	Security services & mechanisms over information pieces.
4º	**Business (BES)**	Security services & mechanisms over information pieces.	Business Knowledge structure	Final decision over security strategy to apply over network elements
5º	**Legal (LES)**	Final decision	Validity check	Legal certification is emitted to BES. One message is sent to TES for register.

The name used for the dataset “Utility Matrix" has been selected because the legislative framework not always depends only on the devices, products or services, it also depends on the use case, that is, how it is used. That is because, for example, one service can be used either to monitor human or animal health. For each use case laws involved can be different. In other words if terms of use are changed, the regulatory framework may change too.

3. Results and Discussion

In [7] several examples are studied over the same technical equipment, but applied to different use cases with a very different social impact, and legal data protection frameworks very different also. These are the case of health monitoring applied to a soccer team, racing horses, a farm for cow's milk and a team of firemen working in a dangerous action.

Technically we are talking about a pectoral belt with sensors to monitor and record the health status for each monitored entity, managing its historical record, evaluating health status and generate alerts.

In these referenced examples above, some results are given about the election of the security services, the next step would be select the appropriate security mechanisms among the solutions provided as valid by the Expert System. Usually mechanisms enable the establishment of an intelligent synergy between them and can be possible to cover legal requirements with minimal computational cost and optimizing resources.

From the service definition for a specific use case, "Utility Matrix is made considering personal data involved in the service. This information is received and processed by the legislative expert system where legal imperatives are obtained to be applied to data which should be protected. Once that information is received by Technological Expert System, the task of this entity is to transform legal imperatives over dataset that should be protected in a set of security services and mechanisms. Finally, security policies are deployed, and sent to AWARE platform using JSON formatted messages in order to configure or re-configure the necessary network elements.

The selection criteria for security mechanisms are based on the idea that one specific security mechanism can be applied in several ways, and each mechanism can act as a countermeasure for one or more attacks. Each of these attacks may affect to one or more security services. All this along with the information about the network type used (resources, connectivity, topology, etc.), provides a great wealth of interesting options and with a high probability of reaching with a few mechanisms, coverage of protection requested by the legal and regulatory requirements.

When the security policy as a set of mechanisms has already been obtained to be applied to a service in a particular case, the AWARE platform, act as a mediator toward WSN and the nodes.

4. Conclusions /Outlook

We propose a support tool for collaboration between business, legal and technological areas who are working together to offer confidence to users about the security and of personal data protection in products and services on the Internet of Things.

The WSN resources are limited (battery, memory, processing power, etc..). A custom security for each use case may be a good idea to avoid risks for quality of service provided, especially in the cases where continuity service is an important requirement. This suggests that an intelligent combination of available security mechanisms could dramatically increase the efficiency. In other words, making an efficient security policy, personal data will be protected and will avoid risk for proper functioning of services. In a more general environment where coexist several different technologies of WSN, the intelligence and decision-making on security policies and their application to services could be centralized in one Network Operations Centre (NOC) officially recognized and certified by several entities (legal, social, business and technical). Decisions taken in NOC supported with an Expert System like this would configure or reconfigure the WSN for several technologies.

Another added value is the great management skills and change control to maintain and update a custom security for each use case in several dimensions, including legal diversity in various administrations and technological diversity.

Perhaps, legislative homogeneity may be possible in the future but while that is achieved, some methods are needed to face the heterogeneity related issues.

Acknowledgments:

AWARE project has been partially funded by the Spanish Ministry of Economy and Competitiveness. (Ref. TEC2011-28397). The authors would like to thank CITSEM Research Center from the UPM.

Author Contributions:

All authors are involved in this project.

Conflicts of Interest:

The authors declare no conflict of interest.

References and Notes

1. García-Mexía, Pablo (2013) La Internet de las Cosas y sus repercusiones jurídicas. Regulación en la Red. ABC. http://www.abc.es/blogs/ley-red/public/post/la-internet-de-las-cosas-y-sus-repercusiones-juridicas--15395.asp (accessed on 12 May 2014).
2. García-Mexía, Pablo (2012) El potencial revolucionario de la privacidad por diseño". Privacidad y protección de datos. ABC. http://www.abc.es/blogs/ley-red/public/post/el-potencial-revolucionario-de-la-privacidad-por-diseno-14670.asp (accessed on 12 May 2014).
3. Miguel S. Familiar, José F. Martínez, Lourdes López, Pervasive Smart Spaces and Environments: A Service-Oriented Middleware Architecture for Wireless Ad Hoc and Sensor Networks, International Journal of Distributed Sensor Networks, 2012, Article ID 725190, 1-11 pages, . http://dx.doi.org/10.1155/2012/725190
4. Rodríguez-Molina, Jesús; Martínez-Ortega, José-Fernán; Rubio-Cifuentes, Gregorio; Hernández-Díaz, Vicente. A proposal for an Internet of Things-based monitoring system composed by low capability, open source and open hardware devices. Proceedings of 3rd International Conference on Sensor Networks, Lisbon, Portugal 7th January 2014; v.3, pp. 87-94. http://dx.doi.org/10.5220/0004697900870094
5. Project Sun SPOT, Oracle Labs, http://www.sunspotworld.com/ (accessed on 12 May 2014)
6. Cuadrado Gamarra Nuria. Aplicación de los sistemas expertos al campo del derecho; Facultad de Derecho de la Universidad Complutense de Madrid, Spain, 2004, 524p. ISBN: 84-8481-042-9
7. Sánchez-Alcón, José-Antonio; López-Santidrián, Lourdes; Martínez-Ortega, José-Fernán; Castillejo-Parrilla, Pedro. Automated determination of security services to ensure personal data protection in the Internet of Things applications. Proceedings of the Innovative Computing Technology (INTECH), 2013 Third International Conference, London, 1st August 2013, pp. 71-76. http://dx.doi.org/10.1109/INTECH.2013.6653704