Challenges and Solutions of Secure Smart Environments

Eila Ovaska and Antti Evesti, VTT Technical Research Centre of Finland
Eila.Ovaska@vtt.fi, Antti.Evesti@vtt.fi

Abstract – Security challenges of smart spaces, e.g., smart homes, smart buildings, and smart cities based on Internet connected devices and systems, are related to the main philosophy of smart environments; the freedom to use available devices for the purpose in hand of end-users, and to make it happen easily and hopefully without human-intervention. But what are the security solutions that promote the business and technology development of smart space owners, device manufacturers and smart application developers? Because information security is a cross-cutting issue of the software intensive systems, it needs extra-ordinary solutions for balancing user-friendliness and trust-worthy behaviour of smart environments. This paper introduces an approach and related solutions developed in an ongoing Artemis-EU project, Sofia, for secure-enabled smart environments and user-friendly adaptation in a situation-based manner. A list of topics to be discussed in the workshop is also introduced.

1. Challenges of secure smart spaces

A smart space is a logical entity of an environment that provides information about users' physical surroundings via inherently dynamic applications. The goals of smart spaces are: i) to increase the visibility of opportunities, ii) to support context understanding and iii) ultimately to provide the correct information when and where it is required, even if not explicitly requested, with its content and format optimally adapted to the user situation and profile [1]. The purpose of the space sets security requirements for what information is provided, who could use the space and how the validity of information is guaranteed. The free use of information provided by smart spaces brings out the following challenges related to information security:

- A smart space must provide the facilities for a user, device and application to authenticate with different security means, e.g. ID, password, public key exchange, biometrics, etc. Authentication is required before different kinds of interactions and actions can be performed.
- A smart space has to keep controlling the accesses of appliances and related authorizations. Thus, when a user or application tries to access to a smart space, the space has to check that the requester has access to information or an appliance in question. This also regards any software update, which should not breach access control.
- A smart space is to guarantee integrity and privacy of (shared) information. First, information about the entities connected to the smart space has to be protected while transmitted from an information provider to an information consumer. Second, the space should provide solutions that prevent unauthorized corruption of transmitted information. Thirdly, privacy is the must; information related to persons and their preferences/behaviours in the smart space is to be secured.
- A space might have to support non-repudiation of performed operations and requests. Thus every action performed by a user or an application must be logged and associated to the source of the action. For example, the action performed by a building maintenance staff has to be associated to the person who completed the task.

- Users and smart spaces should protect themselves from infections. Moreover, use and forwarding of harmful content to users and applications are to be prevented.
- A space should provide the means of (real-time) auditing the used security mechanisms and the achieved security levels of applications and the space itself.

The above-mentioned challenges are based on the requirements derived from a large set of application scenarios identified and defined for smart personal spaces, smart indoor spaces and smart cities. Although not all of them are required for all kinds of spaces, they all are the architectural requirements of high importance.

2. Solutions for managing information security at run time

Our approach to solve the above-mentioned challenges is based on the use of the Information Security Metrics Ontology (ISMO) [5] and a specific service that stores and brokers information as RDF triples. The RDF Information Base Solution (RIBS) [2] is a backbone implementation of the service; this way devices and applications exchange information in smart spaces. The RIBS is able to ensure communication confidentiality, integrity, and authentication by a means of Transport Layer Security (TLS). In addition, these security attributes can be ensured even thought communication parties are utilizing different TLS versions or implementations [2]. A TLS connection also facilitates user authentication.

The micro architecture for measuring and adapting security of smart space applications is based on the Monitoring, Analysis, Prediction and Executing (MAPE-K) model that exploits security knowledge by a means of the ISMO [3]. The micro architecture works as a guideline to build secure-aware smart space applications and presents how the ISMO is used in the different phases of the control loop, i.e., the MAPE-K model. First, context information for security taxonomy [3] offers an input to decide required securities in different situations. Second, the ISMO offers input for security measuring and adaptation.

In order to fulfill security requirements in smart spaces the achieved security level has to be measured. The ISMO makes it possible to present security measures in a generic and reusable form. In addition, it provides a possibility to modify the used measures and reasoning rules dynamically. Currently, the ISMO contains example measures for password based authentication. However, the measuring part is generic and measures to other authentication mechanisms, e.g., public key, biometrics, etc., and other security attributes, e.g., non-repudiation and integrity, can be easily added. The monitor component is also designed. The component is able to measure the security level of a smart space application based on information from the ISMO. [5]

Security measuring triggers context-based security adaptation. The adaptation occurs, when a user joins to the smart space and/or a significant change happens in the smart space. The ISMO also guides to make adaptation in a way that the required security characteristics are achieved also in the changed situation. In our implementation, adaptation is triggered by using the measures on risks levels [4] and the properties of the used passwords [5].

3. Open issues for discussion

There are still several issues and options that need further developments:

- How should the space manage a join process of new users? First option: a user arriving into a new space can directly join to the smart space without any control. Second option: a registration process is required before joining. In some situations direct joining is reasonable, for instance, information consuming in a smart city environment. However, producing information always requires controlling, e.g., only registered users are able to produce information, or a space administrator has to check information before publishing (legislation might set constraints).

- Can a user trust on the smart space and the offered (or claimed) security level? Security problems and vulnerabilities are found all the time even from static and strictly designed software systems. Hence, is it possible to achieve reasonable security in dynamic and evolving smart spaces? This requires that security issues are taken into account in all levels and during the whole lifecycle of the smart space. Moreover, security knowledge has to be updated constantly and autonomous reasoning based on information from different sources is needed. Thus, smart spaces shall have self-protecting and self-healing capabilities.
- Who is producing and maintaining trust information of different users and smart spaces? One option is that a trusted third party maintains this information. However, is this traditional way suitable for smarts spaces? Another option is that users compose trust values for different smart spaces based on recommendations made by other users (friends, colleagues, etc.). From the administrative point of view, the smart space can monitor user behaviour and give additional permissions to well behaving users. However, how does this approach match to the privacy objectives?

References

[1] Weiser, M. (1993). Some computer science issues in ubiquitous computing, *Communication of the ACM*, 36 (7), 75-85.

[2] Suomalainen, J., Hyttinen, P., Tarvainen, P. Secure Information Sharing between Heterogeneous Embedded Devices. The First International Workshop on Measurability of Security in Software Architectures (MeSSa 2010). Copenhagen, Denmark, 23 August 2010

[3] Evesti, A., Pantsar-Syväniemi, S. 2010. Towards micro architecture for security adaptation. ACM International Conference Proceeding Series, ss. 181-188. 4th European Conference on Software Architecture: Doctoral Symposium, Industrial Track and Workshops, ECSA 2010. Copenhagen, Denmark, 23-26 Aug. 2010.

[4] Evesti, A., Ovaska, E. 2010. Ontology-based security adaptation at run-time. Proceedings 2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. SASO 2010, Budapest, 27 Sep. – 1 Oct. 2010, ss. 204 - 212. Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems.

[5] Evesti A, Savola R, Ovaska E, Kuusijärvi J. Design, Instantiation, and Usage of Information Security Measuring Ontology. The Second International Conference on Models and Ontology-based Design of Protocols, Architectures and Services (MOPAS 2011), Budapest, Hungary, April 2011.

.