Workshop Proceedings of the 11th International Conference on Intelligent Environments
D. Preuveneers (Ed.)

doi:10.3233/978-1-61499-530-2-43

Establishing Secure Intelligent Environments

Wolfgang APOLINARSKI
Networked Embedded Systems, Universität Duisburg-Essen, Essen, Germany
wolfgang.apolinarski@uni-due.de

Keynote

One of the main goals of intelligent environments is to create environments that provide users with seamless and distraction-free task support. Often, the task support is realized by so-called pervasive applications that are running on devices integrated into everyday objects. The set of everyday objects is not limited to devices that are already regarded as *smart* such as smart phones, but also include devices like refrigerators, coffee machines, light controls, power switches and other devices from everyday life. Furthermore, smart street lamps, smart ticketing and payment systems, smart homes and smart cars are already extending the size of such environments from small, local and isolated solutions to a ubiquitous, worldwide intelligent environment.

During the realization of this vision, we face several challenges. One of the challenges is the acquisition of context information through sensors that are often built into these smart devices. Additionally, the devices usually feature actuators that need to be configured such that they can be used to manipulate the physical world. Since the devices are highly integrated, they are also heterogeneous with regard to many aspects such as processor type, RAM size and power consumption. If we now consider additional factors such as mobility, it becomes clear that we are dealing with a highly dynamic environment. The configuration of such an environment and the introduction of common communication protocols or middlewares are therefore further challenges. Since it needs permanent adaptation to be able to cope with such an environment, manual adaptation by the user is not distraction-free nor feasible. As a consequence, another important challenge is the automated adaptation usually also performed by a middleware.

The security aspects of these challenges are often disregarded, since the first priority is usually to provide a working (technical) solution to each challenge. Nowadays, there already exist several approaches that solve (parts of) the problems of intelligent environments. Often, these approaches were created without security in mind and are thus inherently insecure. This is why we need to introduce security now, either by adapting existing approaches or by re-designing them. Establishing secure intelligent environments is a complex challenge that opens several questions, for example: Why do we trust a device? Why do we trust a sensor? How do we make sure the gathered context is really perceived by a sensor? Who is allowed to create a configuration for intelligent environments? Who is allowed to access data? How to detect a valid user?

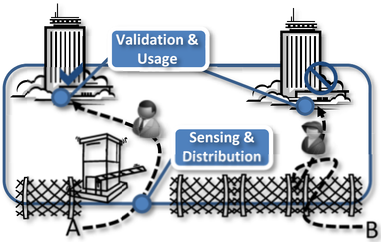
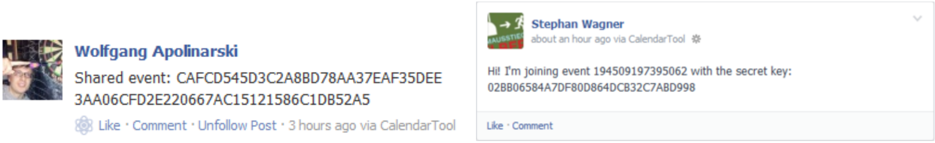


Figure 1. Secure Peer-based Context Distribution



Wolfgang Apolinarski
Shared event: CAFCD545D3C2A8BD78AA37EAF35DEE 3AA06CFD2E220667AC15121586C1DB52A5
Like · Comment · Unfollow Post · 3 hours ago via CalendarTool

Stephan Wagner
about an hour ago via CalendarTool
Hi! I'm joining event 194509197395062 with the secret key: 02BB06584A7DF80D864DCB32C7ABD998
Like · Comment

(a) Shared key, at the event's wall

(b) User-level key, at a participant's wall

Figure 2. Keys exchanged with PIKE in Facebook

At first, we show that security is an important aspect of automated configured intelligent environments and is usually a requirement for privacy. Imagine an adaptation decision that results in displaying a secret document on a public screen set up by a malicious user. The screen could easily be programmed to copy the document against the intents of the document authors. Similarly, while this would only result in intellectual property being stolen, devices like doors or smart cars without a proper security implementation will result in the theft of real goods. To overcome these issues, we present our approaches that are a first step towards secure intelligent environments.

The adaptation of intelligent environments depends on the detection of valid context information. We present a mechanism for secure context distribution [1] that allows a secure, distributed, peer-based verification of context, even when using resource-constrained devices such as sensors. Additionally, it does not require that all devices, which form one infrastructure, are part of one network. Instead, sensors can sense context independently and issue a context token that can later be validated (e.g., to open a door at an office building as shown in Figure 1). The provided context information can then be used to create a secure role assignment [2], which allows the secure, automated adaptation of intelligent environments. Here, trust and security are provided by using a simple but effective trust system with certificate hierarchies, allowing to establish an Internet-grade security level. As we elaborated further about trust, we came to the conclusion that users are already defining trust between each other in online collaboration platforms such as Google Calendar or Facebook. We therefore present our approach PIKE [3] that exchanges secure keys which are later used for secure, privacy-preserving communication between users, transferring trust relationships from the virtual to the real world. While PIKE can be used to establish mutual keys, it can also be used to identify participants at a shared event such as a conference or party. Examples of a PIKE-initiated key exchange can be seen in Figure 2.

Although the feedback we get from these first approaches are promising, there is still a lot of work waiting. During the talk, we outline past and current work and show gaps that need further attention. In the end, we will have a clearer view on what is needed to really establish secure intelligent environments.

Acknowledgments

This work is supported by UBICITEC e.V. (European Center for Ubiquitous Technologies and Smart Cities) and BESOS (Building Energy Decision Support Systems for Smart Cities) funded by the European Commission under FP7 with contract number FP7-SMARTCITIES-2013-608723.

References

[1] W. Apolinarski, M. Handte, and P. J. Marrón: *A Secure Context Distribution Framework for Peer-based Pervasive Systems*. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on, pages 505–510, 2010.

[2] W. Apolinarski, M. Handte, and P. J. Marrón: *An Approach for Secure Role Assignment*. Intelligent Environments (IE), 2012 8th International Conference on, 26-29 June 2012

[3] W. Apolinarski, M. Handte, M. U. Iqbal, P. J. Marrón: *Secure interaction with piggybacked key-exchange*. Pervasive and Mobile Computing, Volume 10, Part A, February 2014, Pages 22–33, ISSN 1574-1192