# Chapter 7.15
# Towards Adaptive Security for Ubiquitous Computing Systems: MOSQUITO and Serenity

**Volkmar Lotz**
*SAP Research, France*

**Luca Compagna**
*SAP Research, France*

**Konrad Wrona**
*SAP Research, France*

## ABSTRACT

The flexibility and dynamism of ubiquitous computing systems have a strong impact on the way their security can be achieved, reaching beyond traditional security paradigms like perimeter security and communication channel protection. Constant change of both the system and its environment demand adaptive security architectures, capable of reacting to events, evaluating threat exposure, and taking evolving protection needs into account. We introduce two examples of projects that contribute to meeting the challenges on adaptive security. The first focuses on an architecture that allows for adaptive security in mobile environments based on security services whose adaptation is guided by context information derived from sensor networks. The second addresses engineering aspects of secure ubiquitous computing systems through making security solutions accessible and deployable on demand and following emerging application-level requirements.

## INTRODUCTION

A major challenge in securing ubiquitous computing systems is to cope with the increased flexibility and dynamism these systems show: the actual structure and behavior of a system at a particular point of time during its operation is not known in advance and depends on the physical and application context at that time. Consider

a service-oriented architecture (cf., the chapter "Ubiquitous Services and Business Processes"), where a business service providing access to a resource—for example, performing a transfer to a bank account—is used in two applications being composed on demand and referring to a different business environment—for example, invoicing in a supply chain management application, and monthly employee payment in a human resources application. Otherwise, in a spontaneous interaction scenario (cf., the section "Ad-Hoc Interaction" of the chapter "Security for Ubiquitous Computing") the number of participants in a communication as well as their roles change over time, with the particular type of interaction depending on the location of an entity, the networking capabilities available, and the particular features of the devices being used.

The flexibility of ubiquitous computing systems has a strong impact on security. The constant change of characteristics of both the system and its environment leads to different protection goals and exposure to threats over the system lifespan. Security thus needs to be adaptive: the security architecture, comprising both policies and mechanisms—as explicated in section "Sample Solutions" of the chapter "Security for Ubiquitous Computing"—needs to react to events, to evaluate the current threat exposure, and to take the actual protection needs into account. For example, the bank transfer service, being used in the human resources application environment, is likely to be subject to privacy regulations and confidentiality requirements protecting the information about an employee's salary, whereas the same service, in a supply chain management environment, is probably required to provide strong traceability of transfers and to enforce the four-eye principle on their approval. The service might only be permitted to run on a mobile device in cases where the transferred amount does not exceed a given threshold, due to the increased vulnerability of wireless communication and the mobile environment to eavesdropping, unless it deploys strong authentication and encryption mechanisms.

The challenge of security solutions adapting to the system's context occurs in development, deployment and operation of ubiquitous computing systems. In a service-oriented architecture, applications are designed on demand in a composite manner through orchestrating services, while taking advantage of the reuse of services in different application contexts. This asks for the application designer to specify the individual protection needs and security policies, and the service ecosystem (cf., the chapter "Ubiquitous Services and Business Processes") and infrastructure to support the selection and the set-up of the appropriate security architecture as well as its configuration, all being accessible to an application designer not assumed to be a security expert. Such an effort needs to take into account that the system as well as its environment and protection needs might change over time; thus, events indicating a security relevant change—for example, change of a physical condition or location—need to be identified, the actions to be taken upon detection of the event—for example, the modification of the access control policy or the strength of encryption—need to be specified, and the monitoring of the events as well as the execution of the appropriate actions need to be enforced.

The remainder of this chapter introduces two examples of projects that contribute to meeting the challenges on adaptive security. The first focuses on an architecture that allows for adaptive security in mobile environments based on security services that—like application services in a service ecosystem—can be composed on demand to meet individual security requirements, and whose adaptation is guided by context information derived from sensor networks. The second addresses engineering aspects of secure ubiquitous computing systems through making security solutions accessible and applicable—in terms of integration and operation—on demand and following emerging application-level requirements.