Chapter 1.26
Security for Ubiquitous Computing

Tobias Straub
Fraunhofer Institute for Secure Information Technology, Germany

Andreas Heinemann
Technical University of Darmstadt, Germany

ABSTRACT

Taking typical ubiquitous computing settings as a starting point, this chapter motivates the need for security. The reader will learn what makes security challenging and what the risks predominant in ubiquitous computing are. The major part of this chapter is dedicated to the description of sample solutions in order to illustrate the wealth of protection mechanisms. A background in IT security is not required as this chapter is self-contained. A brief introduction to the subject is given as well as an overview of cryptographic tools.

INTRODUCTION

Mark Weiser's vision of ubiquitous computing (UC) raises many new security issues. Consider a situation where a large number of UC peers interact in a spontaneous and autonomous manner, without previously known communication partners and without a common security infrastructure. Such extreme conditions make it difficult to apply established security methods that have been tailored for "classical" information technology (IT). Virgil Gligor emphasizes this by comparing the Internet cliché where "processing is free and physically protected, but communication is not" with the new cliché about UC where "neither processing nor communication is free and physically protected" (Gligor, 2005).

This chapter gives a systematic introduction into the field of security for UC. It is structured as follows: first (the section "Four UC Settings"), we illustrate the diversity of UC systems and applications in order to raise the reader's awareness of security questions. Our discussion focuses on four representative UC settings. For each of them, a characteristic application scenario is given. The diversity of the settings, for example, concerning presumed knowledge about components or

system complexity, has direct implications for which mechanisms are appropriate to achieve a desired IT security objective.

The section "A Taxonomy of UC Security" starts with an introduction to basic terminology explaining the objectives of IT security as well as the threat model. UC security can be regarded from two different viewpoints: The special characteristics of UC may lead to known and new security risks, if not addressed appropriately. In addition, limitations concerning resources and infrastructure pose a number of challenges in order to achieve desired security objectives.

A compact overview of cryptographic tools suitable to enforce those objectives is given in the section "Overview of Cryptographic Tools". A brief explanation of cryptographic primitives like ciphers, hash functions, and signatures is provided for the nonspecialist reader. A discussion of the potential and limitations of cryptography in UC concludes the section.

After having learned the particularities and challenges of UC systems with respect to security, we look at sample solutions to mitigate these limitations. A selection of elaborated approaches for secure UC systems is given in the section "Sample Solutions". They tackle the issues of privacy and availability as well as the establishment of secure communication.

A brief summary and a list of references for further reading conclude this chapter.

FOUR UC SETTINGS

In order to pave the way for the development of a systematic view on UC characteristics and limitations in the section "A Taxonomy of UC Security", we sketch four representative settings. Each setting exhibits one or more security-related properties. They are termed *mobile computing*, *ad hoc interaction*, *smart spaces*, and *real-time enterprises*.

Mobile Computing

Mobile computing supports *mobile* users with connectivity and access to services and backend systems while being on the move. A synonymous term is nomadic computing, emphasizing the goal of providing a working environment more or less equivalent to that of a desktop user. The widespread availability of cellular networks and 802.11 WiFi allows a field worker to connect to an arbitrary service on the Internet or to the company's backend at almost any place and at any time.

Mobile computing relies on a given infrastructure managed by a provider, for example, a cellular network company. This fact has implications for security: In order to access a service, a user needs to register with a provider. Thus, the user group is closed and the provider controls access to the infrastructure. In addition, users are not able to act in an anonymous manner.

Mobile devices can easily get lost, for example left behind in the proverbial taxi (see http://www.laptopical.com/laptops-lost-in-taxi.html). In case of theft, an attacker might be able to impersonate the legitimate device owner or learn her private data like business contacts or personal email. This physical threat is given whenever mobile devices are considered.

Scenario 1: The Mobile Salesman

While on the road, a salesman needs to regularly download up-to-date client reports from his company's databases. His laptop is equipped with several wireless communication interfaces which can be used to connect via different service providers depending on what kind of service/infrastructure is available.
At the client's office, there is a WiFi network the salesman can access. There are also some networked printers available for guests. However, it is unclear to what extent the infrastructure can be trusted.