Pervasive and Mobile Computing 40 (2017) 220–241

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Evaluation of user authentication methods in the gadget-free world

Kimmo Halunen *, Juha Häikiö, Visa Vallivaara

VTT Technical Research Centre of Finland Ltd, Kaitoväylä 1, P.O. Box 1100, FI-90571, OULU, Finland

ARTICLE INFO

Article history:
Received 17 June 2016
Received in revised form 29 March 2017
Accepted 19 June 2017
Available online 5 July 2017

Keywords:
User authentication
Security
Privacy
Gadget-free
Evaluation

ABSTRACT

In an ideal gadget-free environment the user is interacting with the environment and the services through only "natural" means. This imposes restrictions on many aspects of the interaction. One key element in this is user authentication, because it assures the environment and related services of the legitimacy of user's actions and empowers the user to carry out his tasks. We present five high-level categories of features of user authentication in the gadget-free world including security, privacy and usability aspects. These are adapted and extended from earlier research on web authentication methods. We survey existing authentication methods together with some emerging technologies and evaluate these according to the features in our categories. Our results show, that no single authentication method can realise all these requirements for authentication. In conclusion, we give future research directions and open problems that stem from our observations. Especially, finding combinations of authentication factors and methods that achieve all requirements is an interesting problem in the gadget-free scenario.

1. Introduction

In the present-day hyperconnected world humans are surrounded by digital distractions, which can lead to cognitive overload and attention distraction. An underlying goal of the gadget-free environment is to provide a possibility for the user to interact with the surrounding services seamlessly and effortlessly without digital distractions. In practice, the goal is to enable interaction without the hassle of different gadgets, such as mobile phones and smartwatches. The use of a wide range of emerging interaction technologies and techniques, such as printed electronics [1] and different gesture-based interaction techniques [2] have been studied in smart spaces. One critical area in gadget-free environment is privacy, especially in the process of authentication with the services. Also security and usability need to be addressed.

To interact with the services provided by ambient intelligence systems and other smart spaces, users need to be able to authenticate themselves towards the service provider and the system at large. In an ideal scenario, the user would not need any cumbersome devices to input credentials or to remember complicated secrets that would assure the system of the user's credentials. The user would be authenticated without distractions on the main task(s) at hand.

Traditionally, authentication is done through three different types of *factors*. The first type is *something-you-know*, such as a password. The second type is *something-you-have* such as a key to a physical lock or a device like a phone. The third type is *something-you-are* which means a behavioural or physical trait that you have such as a fingerprint, typing pattern or some other biometric.

In recent years also a fourth type of factor has been discussed. This has been posited either broadly as *context* [3] or more narrowly as someone-you-know [4] or other such concept not easily represented by the traditional three types of factors,

* Corresponding author.
E-mail addresses: Kimmo.halunen@vtt.fi (K. Halunen), juha.haikio@vtt.fi (J. Häikiö), visa.vallivaara@vtt.fi (V. Vallivaara).

http://dx.doi.org/10.1016/j.pmcj.2017.06.017
1574-1192/

e.g., [5]. In the gadget-free scenario, such factors become more interesting because some of the traditional means do not provide enough security, usability, privacy or other desirable properties.

As the interaction possibilities in smart spaces are usually greater than with the current desktop and laptop computers and even mobile devices, there are interesting new options for biometrics, e.g., in [6]. These possibilities can bring added usability, but also the security and privacy considerations need to be taken into account.

In this paper, we examine the possibilities for and the limitations to user authentication in a gadget-free scenario, where the user authenticates towards a smart space without any external devices. We provide an evaluation framework that is an adaptation and extension from [7]. Our framework is in some cases less fine-grained, but it also includes new aspects such as privacy, which are not as thoroughly present in [7], but are important in this broader context.

Our paper is organised in the following manner. In the next section, we shortly review relevant previous work on authentication and pervasive computing. In Section 3, we describe our framework for evaluating different authentication methods extending the previous work from [7] towards a broader view and pervasive computing. Section 4 gives the results of our evaluation of the authentication methods. In the end we discuss our findings and give concluding remarks and future research directions.

2. Related work

This section reviews some of the most relevant previous studies on authentication in the gadget-free world and the basic principles of pervasive computing.

2.1. Gadget-free world

An underlying idea behind the concept of the gadget-free world follows the early visions of ubiquitous and calm computing. Ubiquitous computing has been researched widely over the last decades. According to Mark Weiser's well-known vision of ubiquitous computing from [8]

> "most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"

> "elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence."

This early vision of ubiquitous computing is extended by the calm technology paradigm. The idea behind calm technology is that technology moves easily from the centre to the periphery of the attention and back again. It also brings more details to our periphery without being dominated by technology and causing additional information overload [9]. Pervasive computing is a term, which is commonly used in the ubiquitous computing related research. It is characterised by the following four elements: *ubiquitous access, context awareness, intelligence,* and *natural interaction* [10]. There are also a variety of other terms and research fields intertwined with the concept of ubiquitous computing, such as hidden/invisible computing, sentient computing, affective computing, everyware and ambient intelligence. These terms emphasise slightly different aspects of the field of ubiquitous computing. A common factor for all of these areas is that technology is deeply embedded to our physical environment.

Despite all the research and technology development over the last decades, Weiser's original vision on ubiquitous computing is still unreachable as currently the world is full of technologies that are capturing people's attention maybe more than ever before (see e.g. [11]). Maybe, the most visible embodiment of that is the high use of smart phones, which can be unhealthy for some mobile phone users [12]. In general, the use of smart phones decreases our ability to interact with the surrounding environment as it requires our full attention when we are using them. Our vision is highly focused on the digital content on the display, our hearing is limited with the earphones and our mind is concentrated on the movements needed to interact with the mobile device.

There are many challenges that must be won in our journey to the gadget-free world, in which people can use digital services intuitively and where these are seamlessly integrated into their daily activities without a need for carrying and operating personal devices all the time. One of the crucial challenges that must be tackled is related to privacy and authentication. Authentication process related issues in ubiquitous computing environments have been discussed widely in earlier research (see e.g. [13]). However, the concept of the gadget-free world requires extending earlier views and studying novel solutions for authentication.

2.2. User authentication

User authentication can be seen as a ritual that is performed by the user in cooperation with some system to assure the system and the service provider that the user is allowed access to the system and the service. In this paper, we use *authentication* to refer to user authentication. With computer systems this authentication is usually performed through passwords that are typed on a keyboard [14]. Other methods such as tokens e.g. [15] and biometric authentication (see [16] for a thorough introduction) are also becoming more and more frequently employed with smart devices and other systems.