Expectations and Experiences of Implementing a Mobile Secure Communication Application

Tuomas Kari, University of Jyvaskyla, Jyvaskyla, Finland
Markus Makkonen, University of Jyvaskyla, Jyvaskyla, Finland

Lauri Frank, University of Jyvaskyla, Jyvaskyla, Finland
Eeva Kettunen, University of Jyvaskyla, Jyvaskyla, Finland

ABSTRACT

The privacy and security of communication in corporations and governmental organizations has increased enormously over the years. At the same time, a growing amount of technological solutions to support this have emerged. This study examines user expectations before and use experiences during the implementation phase of a mobile secure communication application. These are investigated from the expectation–confirmation perspective and its influence on continued adoption. The study has an exploratory approach for this investigation. To guide the investigation, the study draws from the expectation–confirmation theory (ECT) and the unified theory of acceptance and use of technology (UTAUT). Empirically, the study is qualitative and conducted in a governmental organization in Finland. The findings reveal the key user expectations and use experiences and their importance for users in terms of implementation and continued adoption of a mobile secure communication application.

KEYWORDS

Acceptance, Adoption, Implementation, Mobile Application, Organizational Context Privacy, Secure Communication, Security, Use Experience, User Expectations

INTRODUCTION

In the increasingly digital world of today, the majority of communication takes place through different digital communication channels. As people are more and more “on the move” or otherwise remotely located, the popularity and importance of different ubiquitous communication devices has exploded. This is the case in corporate, governmental, military, and personal use alike. Moreover, many things that need to be communicated contain information that is confidential or otherwise meant for certain eyes and ears only, such as, trade secrets, state secrets, or information that is otherwise sensitive or confidential. Naturally, this information can also be of interest to certain outsiders, such as industry competitors, foreign governments, or criminals. It is well known that the attempts and attacks to capture confidential information are common and increasing all the time. More and more of these attempts and attacks are also targeting mobile devices (Trend Micro, 2017). Therefore, there is a growing need, especially in corporations and governmental organizations, to ensure that critical
communication is safe and secure and the confidentiality of information is not breached. Indeed, corporations and organizations have paid an increasing consideration to information systems (IS) security and privacy during the past years. To decrease the risk posed by the prevalent security and privacy threats, different solutions have emerged to safeguard the confidentiality of communication. Some of the solutions, such as e-mail encryption software, have been around for a long time, but also more novel solutions exist. These include, for example, mobile applications meant for communication in corporations and organizations in cases where secure and confidential communication is essential.

Security and privacy management in the area of mobile communication has been studied since the early 1990s (Chan, Kwong, & Longginnou, 1993). The whole research stream of IS security and privacy dates back to the beginning of the 1970s (Bates, 1970) and has focused on various approaches and topics around security and privacy issues. Over the years, also several reviews on IS security research have been published (e.g., Baskerville, 1993; Cram, Proudfoot, & D’Arcy, 2017; Dhillon & Backhouse, 2001; Guo, 2013; Siponen & Oinas-Kukkonen, 2007; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014; Soomro, Shah, & Ahmed, 2016; Willison & Siponen, 2007), which illustrate the development of the topics and the central issues under research. Yet, as the technology, means, and needs of communication and the regarding security and privacy threats advance and are constantly evolving, there is an eminent need to keep IS security research in line with the most novel technologies.

To date, studies focusing on mobile secure communication applications for organizational use are few, and most of them have focused on the technical side. However, user-centric studies on use, use experience, and acceptance aspects of mobile services have been conducted. For example, Carlsson, Carlsson, Hyvönen, Puhakainen, and Walden (2006) examined the acceptance of personal mobile devices and services in general and found, among others, that effort expectancy, performance expectancy, and attitude influence use intention, which in turn influences the actual use of mobile devices and services. Lee, Hwang, and Kwon (2015) investigated how the perceptions of a (non-secure) mobile instant messenger affect its continued use intention in an organizational setting through perceived usefulness. They found, for example, that perceived enjoyment has a positive effect on perceived usefulness, that perceived usefulness has a positive effect on satisfaction and the continued use intention of a mobile instant messenger, and that expectation-confirmation has a positive effect on perceived usefulness. Pham, Pham, Brennan, and Richardson (2017) investigated end-users’ and IT managers’ attitudes towards performing IT security tasks and suggested that in order to enhance the probability of end-users internalizing security requirements, the regulatory processes need to shift from a mere compliance (other-directed) towards interest, enjoyment, and inherent satisfaction (self-directed). Overall, the need to deepen the user-centric research is eminent.

Security and privacy are at the forefront of mobile application usage, and the need for secure communication solutions is prevalent. As the demand and importance for secure communication in corporations and governmental organizations is increasing and the solutions to meet this are used more and more, the use of technologies providing the means for secure communication become an increasingly relevant topic to be studied. Thus, it is important to study the use experiences and to find out what kind of experiences either promote or hinder the use of these technologies. After all, technological systems can only be useful if people use them (Mathieson, 1991). Examining the use experiences provides important information about the reasons of use, adoption, and non-adoption. Understanding these reasons, and especially those related to innovation resistance, is essential because the main reason to use such technologies is typically to secure the important information of an organization, corporation, or nation. Despite the varying aspects of IS research on mobile security and privacy, there is limited research on how users adopt and experience the relatively novel mobile applications for secure communication. Studying such issues can have several important implications for the development and diffusion of these technologies as well as for implementing them into use in different kinds of organizations.

The purpose of this study is to address the aforementioned gap by qualitatively exploring the expectations that users have towards mobile secure communication applications before the
Multi Factor Two-way Hash-Based Authentication in Cloud Computing

Promoting Service Quality and Customer Satisfaction in Global Business
[www.igi-global.com/chapter/promoting-service-quality-and-customer-satisfaction-in-global-business/149730?camid=4v1a](www.igi-global.com/chapter/promoting-service-quality-and-customer-satisfaction-in-global-business/149730?camid=4v1a)