Chapter 23

Mobile Embedded System: Your Door Key Evolved with Your Smartphone – A User Evaluation of a Two-Factor Authentication

Pei-Lee Teh
Monash University, Malaysia

Huo-Chong Ling
Multimedia University, Malaysia

Soon-Nyean Cheong
Multimedia University, Malaysia

Pervaiz K. Ahmed
Monash University, Malaysia

ABSTRACT

The use of smartphone is pervasive. With device pocketability driving user engagement throughout the day, it is highly probable that smartphones will replace daily items (e.g., keys and credit cards) that people now carry around. The idea presented here is a significant step in this direction. This chapter details the authors' design and development of a smartphone access control system using Near Field Communication (NFC) Encrypted Steganography Graphical Password (ESGP). The primary objective is to leverage the technical capability of NFC-enabled smartphones in developing a two-factor authentication system connecting physical resources (i.e., premises) and virtual resources (i.e., password knowledge). This involves a novel integration of token-based, graphical-password authentication, cryptography and steganography. The second objective is to evaluate users' behavior intention to use the system. New insights for researchers and business world interested in the unified solutions for NFC-compatible smartphone, access control and mobile security are provided.

DOI: 10.4018/978-1-5225-7909-0.ch023

INTRODUCTION

A smartphone is a quintessential device in today's world. In fact, smartphones are omnipresent in people's daily life (Xia, Ding, Li, Kong, Yang & Ma, 2013). According to International Data Corporation (IDC) (International Data Corporation, 2013), more than half of the population in the United States uses smartphones. More interestingly, it is found that 79 percent of smartphone users carry their phones with them for all but two hours of their waking day (International Data Corporation, 2013). The use of smartphone has become engrained in people's daily behavior. Given that smartphones are pocketable, people engage with smartphones whilst engaging in everyday activities such as reading, ticketing and purchasing. It is likely that smartphones will supplant loose items (e.g., keys, credit cards and paper-based money) that people are now carrying around (Opperman & Hancke, 2011).

Currently systems that enable individuals to access any physical or virtual facilities have a significant limitation since they are relatively inflexible and lack interoperability (Bauer, Garriss, McCune, Reiter, Rouse & Rutenbar, 2005). For example, access to premises such as home and office is usually linked to the possession of a hardware key or a smartcard both of which are not interoperable (Bauer et al., 2005). In contrast, access to virtual resources relies on knowledge-based password or token-based authentication (e.g., SecureID) for generating time-varying passwords (Bauer et al., 2005). The primary goal of this chapter is to propose an access control system that utilizes the always-in-hand smartphone as a two-factor authentication technology to consolidate access control to both physical as well as virtual resources. In addition, the chapter assesses user's behavioral intention to use the proposed system. The motivation of this chapter is twofold. First, it is important to consider smartphones and people (users) as mutually dependent and dynamically emergent phenomena. The authors believe that smartphones can transmute into two-factor authentication devices that represent a shift in lifestyle for smartphone users. Currently, authentication behavior is determined by user habits but with increased smartphone usage, the usability of keys and smartcards is changing. The authors do not expect smartphones to completely replace other token-based authentication systems. Nonetheless, smartphones provide an alternative that could complement the conventional access control system using old-fashioned key, smartcard and password knowledge that do not interoperate. Second, when integrated well, smartphones are able to incorporate two-factor authentication technology. This chapter aims to address the security issue that underlies such smartphone authentication system. Specifically, this chapter presents an ingenious design and development of a two-factor smartphone authentication system, incorporating recognition-based graphical password, steganography and cryptography techniques. This proposed system is named as Near Field Communication (NFC) Encrypted Steganography Graphical Password (ESGP) smartphone access control system. This system is engineered as a practical, secure NFC-enabled smartphone access control to both physical and virtual resources.

This chapter is organized as follows: In the background section, the authors review related work on two-factor authentication systems, graphical passwords, steganography and cryptography techniques. This section also presents the architecture of NFC ESGP smartphone access control system, and its authentication protocol. This is followed by the experiment setting and user evaluation of the proposed system. The results and analysis are discussed in the section of system evaluation and recommendation. This chapter concludes by elucidating research implications and future research directions.

Related Content

Awareness, Knowledge, and Ability of Mobile Security Among Young Mobile Phone Users

River Yan (2017). *International Journal of Cyber Behavior, Psychology and Learning (pp. 73-81).*

www.irma-international.org/article/awareness-knowledge-and-ability-of-mobile-security-among-young-mobile-phone-users/190808

The Construction of a Personalised and Social U-Learning Environment for Third Level Education

Olapeju Latifat Ayoolaand Eleni Mangina (2012). *International Journal of Cyber Ethics in Education (pp. 45-56).*

www.irma-international.org/article/the-construction-of-a-personalised-and-social-u-learning-environment-for-third-level-education/90236

Health-Related Online Support Communities

Neil S. Coulsonand Sumaira Malik (2012). *Encyclopedia of Cyber Behavior (pp. 671-688).*

www.irma-international.org/chapter/health-related-online-support-communities/64794

E-Learning and the Global Workforce: Social and Cultural Implications for Workplace Adult Education and Training

K. Remtulla (2007). *Linguistic and Cultural Online Communication Issues in the Global Age (pp. 276-305).*

www.irma-international.org/chapter/learning-global-workforce/25576

Cyberbullying in the World of Teenagers and Social Media: A Literature Review

Sophia Alim (2016). *International Journal of Cyber Behavior, Psychology and Learning (pp. 68-95).*

www.irma-international.org/article/cyberbullying-in-the-world-of-teenagers-and-social-media/158159