User-Friendly Security Patterns for Designing Social Network Websites

Khalid Alemerien, Tafila Technical University, Tafila, Jordan

ABSTRACT

The number of users in Social Networking Sites (SNSs) is increasing exponentially. As a result, several security and privacy problems in SNSs have appeared. Part of these problems is caused by insecure Graphical User Interfaces (GUIs). Therefore, the developers of SNSs should take into account the balance between security and usability aspects during the development process. This paper proposes a set of user-friendly security patterns to help SNS developers to design interactive environments which protect the privacy and security of individuals while being highly user friendly. The authors proposed four patterns and evaluated them against the Facebook interfaces. The authors found that participants accepted the interfaces constructed through the proposed patterns more willingly than the Facebook interfaces.

KEYWORDS

Design Patterns, Privacy, Security Patterns, Security, Social Networking Sites, Usability, User Interface

INTRODUCTION

Social network sites (SNSs) have attracted millions of users around the world. Approximately half of the Internet users are members in one or more SNSs (Liu et al., 2011). Users create their personal profiles and share their private information and interests with others (Sledgianowski & Kulviwat, 2009). With information sharing in social networking applications, private information may be disclosed unintentionally. For example, a users' position is visible to others when he/she uses a location based service. The exploratory nature of social networking websites requires a user friendly interface while virtual communications need a secure protection on private information. This paper proposes the concept of user-friendly security patterns that provide developers the solutions to address the usability and security issues together.

A social network website has a set of distinct features, different from other websites (Marin et al., 2010; Vorakulpipat et al., 2011; Gao et al., 2011). First, it is challenging to automatically authenticate contents due to the diversified information, which includes various multimedia contents, texts, instant messages or requests that are closely related to a specific context. It is, therefore, hard to automatically validate information in social networking websites. Second, a SNS facilitates virtual communication among a large number of users. It contains a large repository of personal profiles and contents, which make it challenging to have a user-friendly yet powerful interface to differentiate sensitive information from public information. Third, a SNS is an open platform for third-party developers and businesses. For example, Application Platform Interfaces (APIs) allow third-party developers to create applications that are hosted by SNSs. Fourth, SNSs have diversified services, such as content tagging, messaging, circle of friends, wall posts, status updates, and etc., which need a sophisticated mechanism to enhance secure information sharing (Kitsantas et al., 2016) .

DOI: 10.4018/IJTHI.2017010103

The above characteristics of SNSs have introduced several challenges (Truta et al., 2015). A major challenge is to protect users' privacy while being user-friendly as well. For example, the open architecture of SNSs allows any third party developer or person to send requests to the user, which may potentially jeopardize a user's privacy. SNSs have to provide an efficient graphical user interface (GUI) to verify various requests. Also, the diverse social interactions should provide different levels of access to users' private information. Therefore, GUIs should provide a flexible yet powerful mechanism to balance user-friendliness and privacy. In addition, SNSs allow the users to upload their contents for others to access and tag. This kind of tags may reveal users' private information to the others. This requires GUIs to give users a control to protect their contents and information. Therefore, SNS developers should emphasize on user-friendliness to encourage users to keep active in a virtual community. However, user-friendliness should not sacrifice security and privacy. Instead, when developing social network websites, developers must consider the usability and security aspects at the same time (Braz et al., 2007), since both security and usability are important properties of Social Network Sites. On one hand, numerous security and privacy issues remain as an open problem (Marin et al., 2010; (Vorakulpipat et al., 2011; Gao et al., 2011). On the other hand, "usability" (Fox & Naidu, 2009) has been one of the critical factors of SNSs, even if it is still one of biggest dilemmas faced by SNS developers, particularly when considering the security and privacy features (Lipford et al., 2008).

The primary objective of this study is to encourage developers to consider the usability, security and privacy issues during the SNS development process. Developers must support security features in a usable manner by providing users with visual feedbacks (Muñoz-Arteaga et al., 2011; Rode et al., 2006). Currently, design patterns in software engineering play a significant role in developing software (Marin et al., 2010; Cuevas et al., 2009). Patterns help developers to understand and realize the solutions offered by experts in both usability and security. Various security patterns for SNSs have thus been proposed. These patterns are related to image tagging, participation and collaboration among users of SNSs, and location based services (Marin et al., 2010; Marin et al., 2011). However, they only focus on security aspects without considering usability aspects. On the other hand, (Muñoz-Arteaga et al., 2011) proposed a set of patterns which provide visual feedbacks for secure websites in general. However, little work has been done on user-interface patterns which focus on the usability while also handling security and privacy issues (Boyko et al., 2002; Van & Trætteberg, 2000).

Two distinctions make this work different from previous patterns. First, the proposed patterns integrate usability and security. Second, four key services of social network websites were studied in this paper, friendship requests, application requests, friend lists, and content sharing. In summary, a set of user-friendly security patterns in social network websites are presented to help developers in designing secure yet highly usable social network sites. These patterns are: Secure Friendship Request, Secure Application Request, Restricted Information Sharing and Protected Friend Lists.

In order to evaluate the proposed patterns, Facebook was selected to conduct a study that compared these patterns with the current Facebook interfaces. The rest of this paper is organized as follows. Section II discusses related works. Section III illustrates the security and privacy issues in SNSs. Section IV demonstrates the proposed user-friendly security patterns. Section V discusses the evaluation of the proposed patterns. Section VI presents the discussion and Section VII concludes the paper with possible future work.

RELATED WORK

The relationship between security and usability has been discussed in various scenarios (Rode et al., 2006; Mathiasen & Bødker, 2011; Lampson, 2009; (Norman, 2009; Whitten & Tygar, 1999). (Rode et al., 2006) focused on usability characteristics of privacy and security activities and provided the user with information to understand the implications of his/her interactions. (Mathiasen & Bødker, 2011) presented acting out security as tools to design a mobile digital signature for daily uses. (Lampson,