Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Toward a secure and usable cloud-based password manager for web browsers

Rui Zhao, Chuan Yue *

Department of Computer Science, University of Colorado Colorado Springs, 80918, USA

ARTICLE INFO

Article history:
Received 27 November 2013
Received in revised form
18 June 2014
Accepted 6 July 2014
Available online 15 July 2014

Keywords:
Web browser
Password manager
User authentication
Security
Cloud
Storage

ABSTRACT

Web users are confronted with the daunting challenges of creating, remembering, and using more and more strong passwords than ever before in order to protect their valuable assets on different websites. Password manager, particularly Browser-based Password Manager (BPM), is one of the most popular approaches designed to address these challenges by saving users' passwords and later automatically filling the login forms on behalf of users. Fortunately, all the five most popular Web browsers have provided password managers as a useful built-in feature. In this paper, we uncover the vulnerabilities of existing BPMs and analyze how they can be exploited by attackers to crack users' saved passwords. Moreover, we propose a novel Cloud-based Storage-Free BPM (CSF-BPM) design to achieve a high level of security with the desired confidentiality, integrity, and availability properties. We have implemented a CSF-BPM system into Firefox and evaluated its correctness, performance, and usability. Our evaluation results and analysis demonstrate that CSF-BPM can be efficiently and conveniently used. We believe CSF-BPM is a rational design that can also be integrated into other popular browsers to make the online experience of Web users more secure, convenient, and enjoyable.

1. Introduction

Text-based passwords still occupy the dominant position in online user authentication (Bonneau et al., 2012; Herley and van Oorschot, 2012; Herley et al., 2009). They protect online accounts with valuable assets, and thus have been continuously targeted by various cracking and harvesting attacks. Password security heavily depends on creating strong passwords and protecting them from being stolen. However, researchers have demonstrated that strong passwords that are sufficiently long, random, and hard to crack by attackers are often difficult to remember by users (Adams and Sasse, 1999; Feldmeier and Karn, 1989; Komanduri et al., 2011; Morris and Thompson, 1979; Yan et al., 2004). Meanwhile, no matter how strong they are, online passwords are also vulnerable to harvesting attacks such as phishing (Jakobsson and Myers, 2006; Dhamija et al., 2006; Anti-Phishing Working Group). These hard problems have been further aggravated by the fact that Web users have more online accounts than ever before, and they are forced to create and remember more and more usernames and passwords probably using insecure practices such as sharing passwords across websites (Florêncio and Herley, 2007; Stone-Gross et al., 2009).

Password manager, particularly Browser-based Password Manager (BPM) is one of the most popular approaches that can potentially well address the online user authentication and password management problems. Browser integration

* *Corresponding author*.
E-mail addresses: rzhao@uccs.edu (R. Zhao), cyue@uccs.edu (C. Yue).
http://dx.doi.org/10.1016/j.cose.2014.07.003

enables BPMs to easily save users' login information including usernames and passwords into a database, and later automatically fill the login forms on behalf of users. Therefore, users do not need to remember a large number of strong passwords; meanwhile, BPMs will only fill the passwords on the login forms of the corresponding websites and thus can potentially protect against phishing attacks. Fortunately, mainly to support the password autofill and management capability, all the five most popular browsers Internet Explorer, Firefox, Google Chrome, Safari, and Opera have provided password managers as a useful built-in feature.

In this paper, we uncover the vulnerabilities of existing BPMs and analyze how they can be exploited by attackers to crack users' saved passwords. Moreover, we propose a novel Cloud-based Storage-Free BPM (CSF-BPM) design to achieve a high level of security with the desired confidentiality, integrity, and availability properties. CSF-BPM is cloud-based storage-free in the sense that the protected data will be completely stored in the cloud – nothing needs to be stored on a user's computer. We want to move the storage into the cloud for two main reasons. One is that in the long run trustworthy storage services in the cloud (Bessani et al., 2011; Bowers et al., 2009; Mahajan et al., 2011; Popa et al., 2011; Wang et al., 2012a; Windows Azure Storage Team, 2011) can better protect a regular user's data than local computers (which may not be timely and properly patched) do, especially if a storage service uses secret sharing schemes such as the (k,n) threshold scheme (Shamir, 1979) to only save pieces of the encrypted data to different cloud vendors (Bessani et al., 2011). The other reason is that the stored data can be easily accessible to the user across different OS accounts on the same computer and across computers at different locations at anytime.

We have implemented a CSF-BPM system and seamlessly integrated it into the Firefox Web browser. We have evaluated the correctness, performance, and usability of this system. We believe CSF-BPM is a rational design that can also be integrated into other popular browsers to make the online experience of Web users more secure, convenient, and enjoyable. We have followed standard responsible disclosure practices and reported those vulnerabilities to the respective browser vendors. Our vulnerability verification tools and the CSF-BPM system can be demonstrated and be shared with responsible researchers.

We provide four main contributions in this paper. First, we compare the BPMs of the five most popular browsers and identify the inconsistencies in their functionality and interface designs (Section 2). Second, we uncover the security vulnerabilities of the five BPMs and analyze how they can be exploited by attackers to crack users' saved passwords (Section 3). Third, we propose a novel CSF-BPM design to achieve a high level of security (Section 4). Finally, we present an implementation (Section 5) and evaluation (Section 6) of the Firefox version CSF-BPM system, and discuss its limitations (Section 7).

2. Related work and background

In this section, we briefly review the related password and password manager research, and provide the background information on the BPMs of the five most popular browsers.

2.1. *Related work*

Morris and Thompson pointed out long ago in 1979 that weak passwords suffer from brute-force and dictionary attacks (Morris and Thompson, 1979). Later, Feldmeier and Karn further emphasized that increasing password entropy is critical to improving password security (Feldmeier and Karn, 1989). However, strong passwords that are sufficiently long, random, and hard to crack by attackers are often difficult to remember by users due to human memory limitations. Adams and Sasse discussed password memorability and other usability issues and emphasized the importance of user-centered design in security mechanisms (Adams and Sasse, 1999). Yan et al. (Yan et al., 2004) analyzed that strong password requirements often run contrary to the properties of human memory, and highlighted the challenges in choosing passwords that are both strong and mnemonic. Recently, Florêncio and Herley performed a large-scale study of Web password habits and demonstrated the severity of the security problems such as sharing passwords across websites and using weak passwords (Florêncio and Herley, 2007). A large-scale user study recently performed by Komanduri et al. demonstrated that many Web users write down or otherwise store their passwords, and especially those higher-entropy passwords (Komanduri et al., 2011).

To help Web users better manage their online accounts and enhance their password security, researchers and vendors have provided a number of solutions such as password managers (Wu et al., 2006; 1Password; RoboForm Password Manager), Web Single Sign-On (SSO) systems (Kormann and Rubin, 2000; Sun et al., 2010; OpenAuthentication 2.0; The OAuth 2.0 Authorization Framework), graphical passwords (Davis et al., 2004; Thorpe and van Oorschot, 2007; Thorpe and van Oorschot, 2004), and password hashing systems (Halderman et al., 2005; Ross et al., 2005; Yee and Sitaker, 2006). As analyzed in Section 1, password managers especially BPMs have the great potential to well address the challenges of using many strong passwords and protecting against phishing attacks. The insecurity of third-party commercial password managers such as LastPass (LastPass Password Manager) and RoboForm (RoboForm Password Manager) are analyzed by Zhao et al. in (Zhao et al., 2013). Web Wallet (Wu et al., 2006) is an anti-phishing solution and is also a password manager that can help users fill login forms using stored information; however, as pointed out by the authors, users have a strong tendency to use traditional Web forms for typing sensitive information instead of using a special browser sidebar user interface. In addition, Web Wallet is not cloud-based. In terms of Web SSO systems, their security vulnerabilities such as insecure HTTP referrals and implementations are analyzed in (Kormann and Rubin, 2000; Sun and Beznosov, 2012; Wang et al., 2012b), their business model limitations such as insufficient adoption incentives are analyzed by Sun et al. in (Sun et al., 2010), and their vulnerabilities to phishing attacks against the identity provider (such as Google and Facebook) accounts are highlighted by Yue, 2013. Security limitations of graphical passwords are analyzed in Davis et al., 2004, Thorpe and van Oorschot, 2007, and Thorpe and van Oorschot, 2004. Security and usability limitations of password hashing systems are analyzed in (Chiasson et al., 2006;