Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Leakage-resilient password entry: Challenges, design, and evaluation

Qiang Yan [a,*], Jin Han [b], Yingjiu Li [a], Jianying Zhou [b], Robert H. Deng [a]

[a] Singapore Management University, Singapore
[b] Institute for Infocomm Research, Singapore

ARTICLE INFO

Article history:
Received 15 May 2014
Received in revised form
22 September 2014
Accepted 17 October 2014
Available online 1 November 2014

Keywords:
User authentication
Password leakage
Leakage-resilience password entry
Mobile devices
One-time password

ABSTRACT

Password leakage is one of the most serious threats for password-based user authentication. Although this problem has been extensively investigated over the last two decades, there is still no widely adopted solution. In this paper, we attempt to systematically understand the challenges behind this problem and investigate the feasibility of solving it. Since password leakage usually happens when a password is input during authentication, we focus on designing leakage-resilient password entry (LRPE) schemes in this study. We develop a broad set of design criteria and use them to construct a practical LRPE scheme named CoverPad, which not only improves leakage resilience but also retains most usability benefits of legacy passwords. Its practicability is further verified by an extended user study.

1. Introduction

Even after two decades of attempts to replace password with other alternatives, password is still the most pervasive user authentication mechanism nowadays. Password is easy and cheap to create, use and revoke, which makes it dominant over other authentication mechanisms such as biometrics and smartcards (Bonneau et al., 2012). However, password-based authentication has its intrinsic security weaknesses, among which password leakage is a serious security threat (Long and Wiles, 2008). Password leakage can be caused by various attacks including malware, key loggers, hidden cameras, and timing analysis of user interaction. The consequence of password leakage could be catastrophic, as password-based authentication has been widely used for financial services, online social networks, and other valuable services.

It is widely believed that this threat can be effectively mitigated by using *one-time passwords* (OTPs) generated from *tamper-resistant* hardware tokens (RSA, 2011). However, the applicability of this technique is limited due to the considerable costs of manufacturing, distributing, and managing hardware tokens for service providers, and the costs of carrying hardware tokens for users. As a result, most user accounts in the cyberspace are not protected by hardware-based OTPs. Moreover, hardware-based OTP has its own vulnerabilities such as subjecting to theft (Matsumoto, 2002; Bright, 2011). In order to prevent such vulnerabilities, a hardware-based OTP is usually used together with a password, which is still subject to password leakage attacks. Besides the traditional attacks (Long and Wiles, 2008), the emergence of new

* *Corresponding author*. Current address: Google Inc. Brandschenkestrasse 110, 8002 Zurich, Switzerland. Tel.: +41 0446681800.
E-mail addresses: qiang.yan.2008@smu.edu.sg (Q. Yan), lengshan1983@gmail.com (J. Han), yjli@smu.edu.sg (Y. Li), jyzhou@i2r.a-star.edu.sg (J. Zhou), robertdeng@smu.edu.sg (R.H. Deng).
http://dx.doi.org/10.1016/j.cose.2014.10.008
0167-4048/

technologies such as Google Glass[1] further enhance an adversary's capability to capture password without being noticed.

Due to the pervasive use of passwords, extensive research efforts have been conducted on how to design leakage resilient password-based user authentication schemes (Hopper and Blum, 2001; Li and Shum, 2005; Weinshall, 2006; Wiedenbeck et al., 2006; Bai et al., 2008; Kumar et al., 2007; Sasamoto et al., 2008; De Luca et al., 2009a, b; Kim et al., 2010; Bianchi et al., 2011b, a). Despite of all these efforts, there is still no practical and widely adopted solution today. A recent study (Yan et al., 2012) provides strong evidence on the limitations of those schemes that only depend on human cognitive capabilities (Hopper and Blum, 2001; Li and Shum, 2005; Weinshall, 2006; Wiedenbeck et al., 2006; Bai et al., 2008) and concludes that it is necessary to incorporate certain secure channel in the design. The secure channel ensures that at least part of the authentication process should be invisible to an adversary so as to prevent password leakage while maintaining acceptable usability in realistic settings. However, the practicability of using a secure channel in password-based authentication has been considered questionable, as Bonneau et al. (2012) concluded that any user authentication scheme is unlikely to gain traction if it cannot retain comparable benefits provided by legacy passwords.

In this paper, we systematically investigate the underlying challenges of preventing password leakage from both security and usability perspectives. Since password leakage usually happens when a password is input during authentication, we focus on the problem of designing *leakage-resilient password entry* (LRPE) schemes in this study. We develop a broad set of design criteria, which cover three indispensable aspects in LRPE design, including the classic aspect – the tradeoffs between security and usability, and two new aspects – *built-in security*, and *universal accessibility*.

These criteria are then used to guide the design of a practical LRPE scheme named CoverPad, which aims to improve *leakage resilience* of password entry while *retaining most benefits* of legacy passwords. Unlike most prior schemes (Hopper and Blum, 2001; Li and Shum, 2005; Weinshall, 2006; Wiedenbeck et al., 2006; Bai et al., 2008; Kumar et al., 2007; Sasamoto et al., 2008; De Luca et al., 2009a, b), CoverPad is designed for increasingly popular mobile devices equipped with touchscreen, where leakage resilience is achieved by utilizing the gesture detection feature of the touchscreen in forming a *cover* for user inputs. This cover is used to safely deliver hidden messages, which break the correlation between the underlying password and the interaction information observable to an adversary. From the other perspective, CoverPad accomplishes the requirement of retaining comparable benefits of legacy passwords by following our design criteria.

Three variants of CoverPad are implemented and further evaluated with an extended user study. This study includes additional test conditions related to *time pressure*, *distraction*, and *mental workload*. These test conditions simulate common situations for a daily-used password entry scheme, which provides more comprehensive assessment on the practicability of CoverPad. Experimental results show the influence of these conditions on user performance as well as the practicability of our proposed scheme.

The rest of this paper[2] is organized as follows: Section 2 examines closely related research on the LRPE problem. Section 3 introduces the definitions and background of the LRPE problem. Section 4 identifies and analyzes the challenges of designing LRPE schemes. To mitigate the security and usability problems associated with these challenges, we develop a broad set of design criteria, which revisits the classic tradeoffs between security and usability, and extends the scope of security and usability to include built-in security and universal accessibility. Section 5 proposes a practical LRPE scheme for mobile devices equipped with touchscreen. The scheme achieves leakage resilience and retains most benefits of legacy passwords. Section 6 and Section 7 further provide security and usability evaluation to measure the practicability of the proposed scheme. Finally, Section 8 summarizes the contributions of this paper.

2. Related work

In this section, we summarize closely related work on achieving leakage resilience of password entry in three different aspects.

Although the problem of achieving leakage resilience of password entry was proposed two decades ago (Matsumoto and Imai, 1991), it is still a challenge to design a practical solution till now. Early work in this direction (Hopper and Blum, 2001; Li and Shum, 2005; Weinshall, 2006; Wiedenbeck et al., 2006; Bai et al., 2008) focused on designing schemes solely rely on the cognitive capability of human beings. Unfortunately, all such schemes with acceptable usability have been broken (Li and Shum, 2005; Weinshall, 2006; Wiedenbeck et al., 2006; Bai et al., 2008). Recent investigations (Coskun and Herley, 2008; Yan et al., 2012) provided strong evidence for the necessity to construct a partial secure channel for hiding certain user interaction during password entry in order to achieve both security and usability. The establishment of such partial secure channel may require the features only available from new user interface technologies. A few schemes (Kumar et al., 2007; Sasamoto et al., 2008; De Luca et al., 2009a, b; Kim et al., 2010; Bianchi et al., 2011b, a) were designed in this strategy. Among them, our scheme was mostly inspired by the concept of physical metaphor introduced in Kim et al. (2010). Our scheme distinguishes itself from prior work in the sense that it not only achieves leakage resilience but also retains most benefits of legacy passwords, while some of prior schemes (Sasamoto et al., 2008; De Luca et al., 2009b) are flawed in terms of security, and the others incur extra usability costs due to various reasons including: 1) using an uncommon device such as gaze tracker (Kumar et al., 2007; De Luca et al., 2009a), haptic motor (Bianchi et al., 2011b), and large pressure-sensitive screen (Kim et al., 2010), 2) requiring an extra accessory device (Bianchi et al., 2011a), and 3) inoperable in a non-stationary environment (Bianchi et al., 2011b).

[1] Google Glass is currently on sale for $1500 (Google, 2014).

[2] A preliminary version of this paper was presented at the 8th ACM Symposium on Information, Computer and Communications Security (Yan et al., 2013).