Journal of Network and Computer Applications 34 (2011) 1292–1301

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Using one-time passwords to prevent password phishing attacks

Chun-Ying Huang[a,*], Shang-Pin Ma[a], Kuan-Ta Chen[b]

[a] Department of Computer Science and Engineering, National Taiwan Ocean University, No. 2 Pei-Ning Road, Keelung 202, Taiwan
[b] Institute of Information Science, Academia Sinica, No. 128 Academia Road, Section 2, Nankang, Taipei 115, Taiwan

ARTICLE INFO

Article history:
Received 13 July 2010
Received in revised form
20 December 2010
Accepted 22 February 2011
Available online 2 March 2011

Keywords:
Anti-phishing
Identity management
In-band password delivery
One-time password
Web security

ABSTRACT

Phishing is now a serious threat to the security of Internet users' confidential information. Basically, an attacker (phisher) tricks people into divulging sensitive information by sending fake messages to a large number of users at random. Unsuspecting users who follow the instruction in the messages are directed to well-built spoofed web pages and asked to provide sensitive information, which the phisher then steals. Based on our observations, more than 70% of phishing activities are designed to steal users' account names and passwords. With such information, an attacker can retrieve more valuable information from the compromised accounts. Statistics published by the anti-phishing working group (APWG) show that, at the end of Q2 in 2008, the number of malicious web pages designed to steal users' passwords had increased by 258% over the same period in 2007. Therefore, protecting users from phishing attacks is extremely important. A naïve way to prevent the theft of passwords is to *avoid using passwords*. This raises the following question: *Is it possible to authenticate a user without a preset password?*

In this paper, we propose a practical authentication service that eliminates the need for preset user passwords during the authentication process. By leveraging existing communication infrastructures on the Internet, i.e., the instant messaging service, it is only necessary to deploy the proposed scheme on the server side. We also show that the proposed solution can be seamlessly integrated with the OpenID service so that websites supporting OpenID benefit directly from the proposed solution. The proposed solution can be deployed incrementally, and it does not require client-side scripts, plug-ins, nor external devices. We believe that the number of phishing attacks could be reduced substantially if users were not required to provide their own passwords when accessing web pages.

1. Introduction

Phishing is a malicious activity whereby an attacker (phisher) tries to trick Internet users into providing confidential information (Dhamija et al., 2006). It is a serious problem because phishers can steal sensitive information, such as users' bank account details, social security numbers, and credit card numbers. To achieve this goal, a phisher first sets up a fake website that looks almost the same as the legitimate target website. The URL of the fake website is then sent to a large number of users at random via e-mails or instant messages. Unsuspecting users who click on the link are directed to the fake website, where they are asked to input their personal information. Although the process of setting up a fake website sounds complicated, reports show that it is much easier than before as there are now "phishing kits" (McMillan, 2006; Danchev, 2008) that can create a phishing site in a very short time. Users believe that responsible enterprises should protect them from phishing attacks; thus, in addition to the risk of personal information leakage, successful phishing attacks can seriously damage business enterprises, especially a company's brand reputation (McDonnell, 2006; O'Brien, 2006).

1.1. Anti-phishing techniques

As phishing is a serious threat to both users and enterprises, several anti-phishing techniques have been developed. In general, the techniques can be classified as either list-based or heuristic-based technologies. List-based techniques maintain a black list or a white list, or both. Many anti-phishing mechanisms use a black list to prevent users from accessing phishing sites. However, the effectiveness of black list filtering depends on the coverage, freshness, and accuracy of the list. The URLs are usually reported by Internet users or collected by web crawlers, and list maintainers are responsible for verifying whether or not the listed URLs are really phishing sites. Though a well maintained black list can filter most well-known phishing sites, it obviously cannot filter unreported, uncollected, or unanalyzed URLs. No list can

[*] Corresponding author.
E-mail addresses: chuang@ntou.edu.tw, huangant@gmail.com (C.-Y. Huang), albert@ntou.edu.tw (S.-P. Ma), swc@iis.sinica.edu.tw (K.-T. Chen).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.02.004