Journal of Information Security and Applications 39 (2018) 41–57

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol

Walid I. Khedr

Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt

ARTICLE INFO

Article history:

Keywords:
Authentication
Keylogger
Shoulder-surfing
Smartphone
AVISPA

ABSTRACT

Designing a secure user authentication method that involves human in the authentication procedure is a challenging problem. Due to their high user convenience, the password is the most widely used means of authentication. However, passwords are vulnerability to compromise by disclosure using various forms of information tapping like Keylogging, phishing attack, human shoulder-surfing and camera-based recording. This paper starts with an analysis of a previous attempt that proposes two visual authentication protocols to enhance password authentication. These protocols were based on the use of user-driven visualization utilizing two-dimensional barcode and smartphones. Even though the two protocols resist some known types of attacks, our analysis reveals serious shortcomings. The first protocol is not secure against theft of a smartphone. Both protocols are not secure against shoulder surfing, camera-based recording and phishing attacks. In this paper, the deficiencies of the original scheme are demonstrated, then a two-factor authentication scheme that eliminates these deficiencies is presented. A prototype of the proposed scheme is implemented and a secured virtual on-screen keyboard (SVOSK) comprising dynamic emoticon keyboard layout is also proposed. Formal security proof and usability analyses show that the proposed scheme is secure, efficient and has a high level of usability.

1. Introduction

Due to its convenience and simplicity, password-based authentication is the most popular form of user authentication in use today. Users choose their username and text passwords when registering accounts in the authentication system. To log into the authentication system, users must enter the chosen passwords. Despite the usability and ease of deployment, passwords are exposed to various types of attacks like brute force attack [1], phishing attack, shoulder-surfing attack, keystroke logging attack etc. Keystroke logging and shoulder-surfing attacks are the most common types of password observational attacks.

Keystroke logging attack is a type of malware where attackers use a keylogger to log keyboard keystrokes on a user's computer. The keylogger can be implemented as a hardware device or a software to steal sensitive information. Keystroke logging attacks can capture information before the encryption is being performed. Although the keyboard is still the main method to enter the input on the computer, on-screen keyboards also are not secure against keyloggers [2]. Shoulder-surfing attack is a threat which is more common in public places like ATM counter, public computers, etc. Under this attack scenario, adversary observes the login information which is being entered by the genuine user and later those credentials can be used to impersonate the actual user [3]. The camera-based shoulder-surfing attack is a type of shoulder-surfing attacks, where an adversary assisted by an automatic recording tool, such as a wearable or mobile camera records and analyzes authentication sessions in detail even at the long range [4]. The widespread of high-resolution surveillance cameras in public places and the advent of wearable and mobile cameras make camera-based shoulder-surfing attacks a realistic threat. Phishing is another threat to passwords, by which attacks aim to steal private information such as usernames, passwords, and credit card details by way of impersonating a legitimate entity. Almost all phishing attacks on PCs are in the form of fake websites [5,6].

This paper focuses on a novel visual authentication scheme proposed by Nyang et al. [7]. We will refer to the scheme as the Visual Authentication Protocols (VAP) scheme in this paper. The VAP scheme proposed two visual authentication protocols: the first is a one-time-password protocol (OTP) [8], and the second is a password-based authentication protocol. Both protocols involve four participants a user, a smartphone, a user's terminal, and a server. The smartphone acts as an intermediate device between the user and the terminal. On authentication, the user invokes a user-friendly authentication via the smartphone. The interaction

E-mail address: wkhedr@zu.edu.eg

https://doi.org/10.1016/j.jisa.2018.02.003
2214-2126/

between the user and the smartphone is visualized using a Quick Response (QR) code [9].

In this paper, the VAP scheme is improved and strengthened into a new scheme. The proposed scheme eliminates the keylogging attack by avoiding entering any keystrokes either using the physical keyboard or an onscreen keyboard. Instead, the user performs the login procedure by scanning a QR code displayed on the smartphone, that contains the user's authentication credentials, using the terminal's camera. A secured virtual on-screen keyboard (SVOSK) is introduced. The proposed keyboard is used by the smartphone to prevent keylogging, shoulder-surfing and camera-based recording attacks for an infinite number of authentication sessions. Furthermore, the proposed scheme ensures the mutual authentication between the user and the server and is also immune to many other attacks such as man-in-the-middle attack, phishing attack, and session hijacking.

1.1. Contributions

In this paper, the deficiencies of the VAP scheme are demonstrated and an improved scheme is proposed. The main contributions of this work can be summarized in the following:

- The scheme eliminates the keylogging attack by avoiding entering any keystrokes either using the physical keyboard or an onscreen keyboard.
- A secured virtual on-screen keyboard (SVOSK) is introduced which is used by the smartphone to prevent keylogging, shoulder-surfing and camera-based recording attacks for an infinite number of authentication sessions.
- Web Real-Time Communication is employed to allow the user to perform the login procedure by scanning a QR code displayed on the smartphone, that contains the user's authentication credentials, using the terminal's camera.
- A prototype is implemented as an Android application running on a smartphone and a java web application running on the server which demonstrates the usability of the proposed scheme.
- The proposed scheme ensures the mutual authentication between the user and the server and is also immune to man-in-the-middle attack, phishing attack, phone theft and session hijacking.

1.2. Paper organization

The rest of this paper is organized as follows: Section 2 presents the threat and system model, assumptions, requirements, and notations used in the proposed scheme. Section 3 briefly reviews the VAP scheme and its analysis. Section 4 presents the proposed scheme. The security analysis and formal security proof of the proposed scheme are presented in Section 5. The details of the prototype implementations and the results of the user study are presented in Section 6. The usability and performance evaluation of the proposed scheme is presented in Section 7. Finally, Section 8 concludes the paper and suggests future work directions.

2. Related work

Many methods have been proposed for two-factor user authentication using an untrusted terminal. One of the most well-known works is MP-Auth [10]. MP-Auth is a scheme that prevents keylogger and phishing attacks by moving a long-term secret password input to a smartphone while the untrusted terminal only gains access to a temporary secret. The MP-Auth requires wireless bidirectional data transfer between the smartphone and the terminal. Furthermore, software installation on the untrusted terminal is required. Finally, the MP-Auth scheme is not secure against shoulder-surfing attack.

Phoolproof [11] is a public-key based scheme that utilized smartphones as authentication tokens to prevent phishing attacks. The user is required to choose a secure bookmark on the smartphone and wait for information exchange between the smartphone and terminal. To log into a website, the user should provide the issued public key and username/password combination. The phoolproof scheme requires bidirectional data transfer between the smartphone and both the terminal and the server. Furthermore, the scheme is not secure against shoulder-surfing attack and subject to password replay attack.

Another related work is QR login scheme [12]. In this scheme, the user's smartphone should be paired with an authentication server over a secure connection which generates two secret information: device secret and user PIN. These two secrets are stored on the smartphone. To log in, the user scans a QR code generated by the server using his smartphone app. A one-time password is generated using the device secret, the user PIN and the scanned QR code followed by sending of this one-time password to the authentication server. The authentication server checks the result to either authenticate or deny the user. This scheme requires a secure channel between the terminal and the server during the login process. Furthermore, the QR login scheme is not secure against shoulder-surfing attack and subject to a man-in-the-middle attack. Finally, there is no easy recovery from loss mechanism e.g. smartphone theft.

To thwart password stealing and password reuse attacks, oPass Sun et al. [13] is proposed to provide the user with a mechanism to authenticate herself to the server from an untrusted terminal without revealing confidential user information. This mechanism uses a user's smartphone and short message service (SMS) to prevent password stealing and reusing attacks. The oPass scheme requires each participating website to have a unique phone number and involves a telecommunication service provider (TSP) in registration and recovery phases. After registration, the user only needs to remember a long-term password to login to all websites. For the user to log into the website, the user submits a one-time password, from a set of precomputed one-time passwords to the server by employing Bluetooth and SMS. Bluetooth is used for communication between the terminal and the smartphone while SMS is used for communication between the server and the smartphone. The oPass scheme uses SMS service provided by telephone system which has longer time delay than the internet and does not give an acknowledgment that the message has been received or not which affect the usability of the scheme. Finally, the oPass scheme is not secure against shoulder-surfing attack and keyloggers installed on the smartphone.

Recently, Nyang et al. [7] proposed two visual authentication protocols (VAP). In the first protocol (referred to as Protocol 1), upon user request, the server sends a QR code of a fresh random string OTP encrypted with the user's public key to the user's terminal. The user decodes the QR code using his smartphone, decrypts the encrypted OTP using his private key and finally types in the OTP in the terminal with a physical keyboard. The server checks the result to either authenticate or deny the user. The second protocol (referred to as Protocol 2) assumes a password is shared between the server and the user. Upon user request, the server sends a Quick Response (QR) code of a random permutation of a keyboard arrangement (π) encrypted with the user's public key to the user's terminal. The terminal displays the QR code together with a blank keyboard. The user decodes the QR code using his smartphone which decrypts the encrypted π using the user's private key. The user uses a mouse to type his password using the blank keyboard displayed on the terminal's screen while seeing the