Journal of Information Security and Applications 42 (2018) 1–17

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks

Gaurav Varshney[a,*], Manoj Misra[a], Pradeep Atrey[b]

[a] Department of CSE, IIT Roorkee, Roorkee, Uttarakhand, India
[b] Computer Science Department, State University of New York at Albany, NY, USA

ARTICLE INFO

Article history:

Keywords:
Phishing
Malicious browser extension
Bluetooth
RT MITM
CR MITM
Authentication
Chrome
Smartphone
Credentials
Deception
Multifactor authentication
QR code
OTP
CAPTCHA

ABSTRACT

Securing user credentials against phishing attacks is an important and challenging research problem. These days phishing is carried out by real time (RT) and control relay (CR) man in the middle (MITM) attacks or by malicious browser extensions. Existing user authentication schemes are either incapable of handling these attacks or they are complex to learn and use or they require users to purchase and carry additional hardware such as a security key. In this paper, we propose a new secure authentication scheme for anti-phishing, which uses the Bluetooth address of the user's smartphone for user identification along with App instance ids and a user password for authentication. The analysis of the results of our experiments shows that the proposed scheme is safe against RT MITM and CR MITM phishing attacks and the attacks launched via malicious browser extensions. It is also efficient in terms of memory and CPU utilization. The comparison of the proposed scheme with the existing schemes in terms of usability and deployability shows that it is better than the schemes that can provide the same level of security.

1. Introduction

Phishing [1–16] is a cyber-fraud which uses deception techniques to break secure authentication schemes. Most of the existing authentication schemes, either one way (user authenticates himself to the website) or two way (the website and user both authenticate each other), are vulnerable to the latest cyber phishing attacks [14,15,17] such as Real Time (RT) and Control Relay (CR) Man In The Middle (MITM) phishing attacks [18–21] and malicious browser extension based phishing (MEP) attacks [22–28]. MEP attacks generally involve keylogging, password & form data sniffing, screen logging etc. The consistent number of phishing attacks [29–32] can be inferred as an indirect indication of the ease with which existing authentication schemes can be compromised.

- *RT MITM Phishing:* In an RT MITM [18–21] phishing attack, attackers place themselves between a client and a server by means of a phishing website appearing as a genuine one. The attacker captures the authentication information entered by the user on the phishing website and relays this information to the genuine website in real time via manual or automated means, thereby gaining access to the user's account. RT MITM, unlike traditional phishing, can utilize remote desktop monitoring modules, malicious browser extensions/screen loggers that can help in providing the additional information (keystrokes, CAPTCHAs, QR codes etc.) in real time to break the authentication scheme [Appendix]. QRLjacking [33] is an example of an RT MITM phishing attacks.
- *CR MITM Phishing:* CR MITM [19–21] is more invasive. In a CR MITM phishing attack, the attacker relays his desktop over the user's terminal, eventually deceiving the user into entering his credentials directly on his computer. Both one-way and two-way authentication [34,35] schemes are vulnerable to such attacks as an authentication token provided by the user can be captured on the phishing website and can be relayed to the genuine website in real time to complete a successful authentication. Only separate hardware token based schemes or schemes which store at least one part of user credentials over the client can handle such attacks.
- *MEP Attacks*: Malicious browser extensions [36–41] can also be used to perform phishing attacks for stealing user credentials. Schemes for malicious browser extension detection have been proposed in the past [22–28,36,41–43], but little work has been

* Corresponding author.
E-mail addresses: gauravdtsi@gmail.com (G. Varshney), manojfec@iitr.ac.in (M. Misra), patrey@albany.edu (P. Atrey).

https://doi.org/10.1016/j.jisa.2018.07.001
2214-2126/

done in this area. Malicious browser extensions can acquire permissions needed for carrying out any stealth activity by providing a functionality to the users in the foreground that requires the same set of permissions. For example, a malicious browser extension can provide grammar checking facility to the users in the foreground and hence can get permissions to access the contents of websites opened in the browser and tab related data (URL typed in the tab's address bar). Using these permissions malicious browser extensions can carry out credential stealing, spying and phishing activities in the background. Malicious browser extensions can also be installed covertly by an insider on the victim's PC. A malicious browser extension can perform key logging, screen logging, or password sniffing to steal credentials. No matter whether the scheme is a CAPTCHA based scheme [20,44], a picture password-based scheme [45], or a dynamic security skin based scheme [46], it can be compromised if a malicious browser extension running on a user's PC captures the screen and relays this information to the attacker in real time. A malicious browser extension can sniff the information entered on the browser even before the application or transport layer (TLS) encrypts it, hence password manager based schemes can also be compromised. In one of our recent publications, we have discussed in detail the attacks which can be launched via malicious browser extensions [40]. Also, see the [Appendix] for MEP attack examples.

Most of the existing multifactor [47] authentication schemes are incompetent in handling the attacks described above. Our experiments show that OTP/PIN-based schemes [48–50], QR/Barcode based schemes [19,21], Password manager [51], and push notification based login schemes [52–54] are vulnerable to these attacks. Graphical password-based schemes [20,44,55] can be phished using a malicious browser extension that can log the screen when the user enters his password or CAPTCHA on the website opened in the browser. Also, graphical password based schemes are not user-friendly [56]. Biometric authentication [57–59] is still not 100% accurate, robust, mature, and user-friendly. Environment and usage can affect the measurements and they also need additional hardware [60]. User-friendly biometric schemes which are commercialized (such as fingerprints, facial recognition etc.) can be spoofed [59,61,62]. Separate hardware token based schemes (such as Yubikey U2F [63], RSA SecurID [64], DUO [65] etc.) provide a better layer of security compared to the other schemes but they have following drawbacks.

- Firstly, the user needs to buy and carry these hardware tokens always which makes them nonuser friendly [50].
- Secondly, some of the hardware token based schemes that use security keys for OTP/PIN generation and their subsequent entry on browsers can be compromised via malicious browser extensions through sniffing of HTML form data during its submission.
- Thirdly security keys such as Yubikey and RSA SecurID tokens can also be compromised through reverse engineering and spoofing onto other hardware [66].

New protocols such as Yubikey U2F may handle most of the sophisticated attacks but the need for buying and carrying a separate authentication token makes them unattractive. Also, attacks that weaken the strength of RSA key generation on Yubikey has been recently recorded in October 2017 [67]. This can be inferred from the ratio of the number of users who use separate hardware authentication tokens to log in over websites to the number of users who use soft tokens generated from Authenticator Apps installed on their smartphones or OTPs as a second factor for authentication [50].

Hence there is a need for immediate research and development of secure authentication schemes which can address the latest phishing threats from the latest cyber phishing attacks. The schemes should also be easy to use and must use existing hardware and/or technology so that the cost incurred for carrying out login authentication can be reduced. In this paper, we propose a secure authentication scheme which uses a commonly used hardware, smartphone to provide better security against the latest phishing threats. The main contributions of the paper include:

1. We analyze the security of existing popular multifactor authentication schemes against latest phishing attacks launched via RT MITM, CR MITM and malicious browser extensions. Our analysis shows that most of these schemes can't handle these attacks. Only some of the schemes such as Yubikey U2F, Tricipher [68] can handle these attacks but they require the user to purchase and carry extra hardware device.
2. We propose a secure authentication scheme that can handle RT MITM, CR MITM and malicious browser extension based phishing attacks and uses a smartphone, a device commonly used by the Internet users.

Section 1 introduces the latest phishing attacks and establishes the motivation to work in this area. It also describes the main contributions of the paper and its organization. Section 2 describes latest and popular multifactor authentication schemes that are currently used by the websites for authentication. Recent proposals which claim to handle RT MITM and CR MITM phishing attacks have also been described. The section ends with a discussion of research gaps in this area. Section 3 explains the design and working of the proposed secure authentication scheme that addresses the research gaps identified in section 2. Section 4 provides information regarding the implementation, performance, security evaluation of the proposed scheme and a comparison with existing schemes in terms of usability, deployability and security. Section 5 mentions the key limitations of the proposed scheme and concludes the paper. The scope for future work is also given in the section.

2. Literature survey

2.1. Existing multifactor authentication schemes

Two Factor Authentication via OTP /PIN: Google 2 step [49,69] verification is a two-factor authentication scheme which uses OTP as a second factor. The server sends OTP to the user's registered mobile number after receiving the user credentials. OTP, if entered correctly by the user, allows him to login onto the website. SAASPASS [48,70] is another two-factor authentication scheme which uses App generated PINs in place of SMS based OTPs. This reduces the cost of sending OTPs at every login. The user installs the SAASPASS App on his/her smartphone and links it with his/her personal web account. SAASPASS generates and displays a 6-character PIN to the user which is synchronized with the server and changes every 30 seconds. The user enters the PIN as the second factor for login verification. RSA Soft token, DUO also generate similar authentication code/PIN through Apps for login. These schemes are vulnerable to MITM phishing attacks as the OTP/PIN can be acquired by a phishing website or through a malicious browser extension [Appendix].

Authentication using QR Codes: In Xie et al.'s [21] approach, a user submits the username and password to the website using a browser extension. The server generates and sends a barcode to the user. This barcode is displayed on the user's browser. The user scans the barcode using his smartphone App and after verification generates a vouch request in the form of a barcode which is scanned by the PC camera. The browser extension sends the vouch request to the server for final authentication. The approach claims to solve the problem of MITM phishing attacks and utilizes