Information Sciences 321 (2015) 162–178

Contents lists available at ScienceDirect

Information Sciences

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

Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity

Ding Wang [a,c,*], Nan Wang [b], Ping Wang [b,c], Sihan Qing [b]

[a] School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
[b] School of Software and Microelectronics, Peking University, Beijing 100260, China
[c] National Engineering Research Center for Software Engineering, Beijing 100871, China

ARTICLE INFO

Article history:
Received 5 April 2014
Received in revised form 20 March 2015
Accepted 30 March 2015
Available online 3 April 2015

Keywords:
Password authentication
User anonymity
De-synchronization
Random oracle model

ABSTRACT

Due to its simplicity, portability and robustness, two-factor authentication has received much interest in the past two decades. While security-related issues have been well studied, how to preserve user privacy in this type of protocols still remains an open problem. In ICISC 2012, Kim–Kim presented an efficient two-factor authentication scheme that attempts to provide user anonymity and to guard against various known attacks, offering many merits over existing works.

However, in this paper we shall show that user privacy of Kim–Kim's scheme is achieved at the price of severe usability downgrade – a de-synchronization attack on user's pseudonym identities may render the scheme completely unusable unless the user re-registers. Besides this defect, it is also prone to known key attack and privileged insider attack. It is noted that our de-synchronization attack can also be applied to several latest schemes that strive to preserve user anonymity. As our main contribution, an enhanced scheme with provable security is suggested, and what we believe is most interesting is that superior security and privacy can be achieved at nearly *no* additional communication or computation cost. As far as we know, this work is the *first* one that defines a formal model to capture the feature of user un-traceability and that highlights the damaging threat of de-synchronization attack on privacy-preserving two-factor authentication schemes.

1. Introduction

With the rapid proliferation of wireless network technologies and micro-electromechanical systems, it is becoming more and more convenient for subscribers to enjoy desired services/resources from distributed service servers by using mobile devices (e.g., PDAs, PMPs, Smart phones) at any time and anywhere [78,85]. Meanwhile, it is of utmost importance to ensure that a system's services will not be consumed by unauthorized users in a fraudulent manner. Among numerous methods available for validating a remote user, password-based authentication is one of the most prevalent and effective approaches. Since the introduction of the seminal work (known as encrypted key exchange) of Bellovin–Merritt [5], there have been a

* Corresponding author at: Room 560, 2#, Chuangchunxinyuan, University, No. 5 Yiheyuan Road, Haidian District, Beijing 100871, China. Tel.: +86 185 1134 5776; fax: +86 010 6276 5808.
E-mail addresses: wangdingg@mail.nankai.edu.cn (D. Wang), wangnan@ss.pku.edu.cn (N. Wang), pwang@pku.edu.cn (P. Wang), qsihan@ss.pku.edu.cn (S. Qing).

http://dx.doi.org/10.1016/j.ins.2015.03.070
0020-0255/

number of remarkable proposals (e.g., [1,12,48]) with various levels of security and complexity, catering for diverse application scenarios.

In password-based authentication schemes, the server has to *store a sensitive verifier table* that contains the passwords (or the salted passwords, e.g., by using Hash or symmetric encryption) of all the registered users. One prominent issue is that once this sensitive password-verifier table is leaked (hacked), all the users' passwords will be endangered. These days it is no surprise to see news about a catastrophic leakage of thousands of millions of passwords in the headlines [19,24], and the prevalence of zero-day attacks [6] will further aggravate the situation. Recently, two-server password-only schemes (e.g., [47,109]) are suggested to solve the server compromise problem, yet they are helpless to deal with another emerging problem – password leakage at the user side (e.g., malwares and social engineering [34,62]). As deeply investigated in [105], the latter security threat can only be well addressed (i.e., achieving both reasonable security and acceptable usability) by incorporating certain trusted devices.

Owing to its portability, cryptographic capacity and tamper resistance nature, smart cards are usually introduced to serve as the "second line of defense". In this new type of schemes (see Fig. 1), only the user with the valid smart card and the correct password can pass the verification of the remote server, while a compromise of either factor (but not both factors) would pose no danger to the system, which ensures the so-called '*two-factor security*' [40,87]. This sort of schemes has been widely adopted in various security-critical applications, such as e-commerce [27] and e-health [28].

In 1991, Chang and Wu [14] introduced the first smart-card-based password authentication scheme, yet it was not until 2005 that the first scheme that can achieve "truly two-factor security" was given in a seminal work by Fan et al. [30]. Despite the provision of two-factor security, Fan et al.'s scheme [30] fails to support some necessary properties like session key agreement and password update. To eliminate these weaknesses, a number of schemes were further developed [23,39,46,49,60,79,93,104]. Unfortunately, most of them have been demonstrated either insecure against some basic attacks or lack of some important properties (e.g., users cannot freely choose their own passwords). The past thirty years of research on password-based authentication scheme (i.e., single-factor) has proven to be not an easy task [48,74], the design of a practical smart-card-based password authentication scheme (i.e., two-factor) can only be harder, for the designers are faced with the challenging task of reconciling stringent usability, efficiency and security requirements [64,69,88]. To gain a better grasp of the difficulties and challenges in designing a secure and efficient two-factor scheme, readers are referred to the "break-fix-break-fix" history of this area in Fig. 1 of [88].

What further complicates matters is that, smart cards can no longer be deemed as fully tamper-proof devices. Recent research has reported that, the secret parameters stored in common commercial smart cards can be extracted by side-channel attacks such as power analysis [66,67], reverse engineering [3,70] and fault injection attacks (e.g., launched on software-supported Java Cards) [10,54]. In other words, the previous practice of resting complete trust in the physical security of smart cards (e.g., the schemes in [17,23,49,84,93]) is highly risky in the presence of state-of-the-art side-channel attacks. In addition, there is a constant arms race going on between attackers and security practitioners. Even though the physical security of smart cards may be evaluated by independent laboratories or certified by third-party certification authorities (e.g., FIPS-201 [68] and ETSI-TS-102 [29]) at the time of their production, how much confidence can we have that they are still tamper-proof after two years of circulation? Considering this, it is more prudent and desirable to assume that the smart cards can be somehow tampered when they are in the hands of the attacker.[1]

Here we give a concrete example to show that, under the new (but practical) assumption that smart cards can be somehow tampered when lost, two-factor schemes which were traditionally regarded secure may *no longer* be secure anymore. Consider a two-factor scheme in the client–server remote authentication environment, a user-chosen password is used to unlock the smart card which stores the user's private key, and a standard challenge response protocol (e.g., authenticated key exchanged protocol [51]) between the card and server (which keeps the user's corresponding public key) is used to prove user authenticity. This kind of design is quite intuitive and the resulting scheme is indeed secure if the smart cards are assumed to be tamper-proof. However, such an assumption about smart cards, as mentioned earlier, would not always be the case in reality. Once the sensitive data in the card is extracted, the proof-of-concept two-factor scheme will fall: an attacker with the victim's lost card can extract the private key stored in the card memory, and then use this key to impersonate the victim to the server. One may wonder what if the user's private key is not stored in plain-text but encrypted by user password? This case has been investigated in [94] and it falls short of two-factor security, too.

While security-related issues have long been the focus of the community, much less attention has been paid to how to design a privacy-preserving two-factor scheme. These years, with privacy concerns being raised rapidly among individuals and human rights organizations [2,7], user anonymity becomes an admired property of such schemes. Instead of a unique notion of what it means to be "user anonymity", there are a variety of flavors such as sender identity protection, sender un-traceability, sender k-anonymity, blender anonymity, controllable anonymity and so on [38,41,42], and quite varied (sometimes even contradictory) notions may be implemented in different application environments [53,81]. As for remote user authentication, the notion of user anonymity is defined against the public (eavesdropping attackers) rather than the server because the server has to obtain the user's real identity for revoking, accounting and/or billing purposes [65]. Basically, this notion means user identity-protection (i.e., "initiator anonymity" in [41] or "basic user anonymity" in [38]),

[1] As deeply investigated in [88], even if smart cards are assumed to be non-tamper-proof when they are in hands of the attacker for a relatively long period of time (e.g., a few hours), smart-cards-based schemes are still much more robust than common-memory-sticks-based ones in practice.