JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 23 (2015) 44–53

Available online at www.sciencedirect.com

ScienceDirect

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

Design of a lightweight two-factor authentication scheme with smart card revocation

Dheerendra Mishra [a,*], *Ankita Chaturvedi* [b], *Sourav Mukhopadhyay* [b]

[a] *Department of Mathematics, LNM Institute of Information Technology, Jaipur, India*
[b] *Department of Mathematics, Indian Institute of Technology, Kharagpur, India*

ARTICLE INFO

Article history:
Available online 3 July 2015

Keywords:
Authentication
Smart card
Anonymity

ABSTRACT

Smart card based authentication schemes present user-friendly and secure communication mechanism over insure public channel. Recently, Li et al. designed an authentication scheme with pre-smart card authentication to present efficient login phase and user-friendly password change phase. It can quickly detect illegitimate login attempt. We analyze the security of Li et al.'s scheme, and identify the scheme insecure. Moreover, their scheme requires the computation of public key operations. To address the security and efficiency of mutual authentication design, we propose a lightweight authentication scheme, which supports smart card revocation. The proposed scheme requires the computation of only hash function and exclusive-or operations. Furthermore, we verify the correctness of mutual authentication using the widely-accepted BAN (Burrows, Abadi, and Needham) logic. Through the security and performance analysis, we show that our scheme is secure and computationally efficient than the existing schemes. Furthermore, the proposed scheme present efficient login and password change phases where incorrect login is quickly detected, and a user can freely change his password without server assistance.

1. Introduction

Advancement in Internet technology have made Internet an efficient and scalable tool to utilize for various online services. Access of resources over the insecure Internet is a subject of security and privacy risk. Thus, it is required to adopts cryptographic protocol, which can ensure secure and authorized communication over insecure public channel. The authentication protocols are designed and developed to ensure the correctness of the participants. In recent years, identity based authentication scheme is being introduced, which uses user identity in communication. It may cause identity theft and linkability of users' communications (Kuo et al., 2014; Mishra and Mukhopadhyay, 2013; Darwish et al., 2015; Wang and Wang, 2014a). In recent years, authentication schemes using smart card are also designed to ensure that only user who possesses both the smart card and the corresponding password are allowed to gain access the server to safeguard data integrity, confidentiality and availability with user privacy. Smart card based schemes support two factor authentication, and a user just need to remember memorable password to use it. These schemes are widely employed for various services due to user-friendliness.

The smart card based protocol are developed to ensure authorized and secure communication between the user and

* *Corresponding author.*
E-mail addresses: dheerendra.mishra@lnmiit.ac.in (D. Mishra), ankita@maths.iitkgp.ernet.in (A. Chaturvedi), sourav@maths.iitkgp.ernet.in (S. Mukhopadhyay).
http://dx.doi.org/10.1016/j.jisa.2015.06.001
2214-2126/

server (Wang et al., 2014; Kalra and Sood, 2014). However, smart card based remote user authentication schemes faces various attacks due to the following assumptions (Boyd and Mathuria, 2003; Eisenbarth et al., 2008; Kocher et al., 1999; Messerges et al., 2002; Nohl et al., 2008; Kim et al., 2012):

- The user holds the uniformly distributed low-entropy password from the small dictionary.
- An adversary and a participants interact by executing oracle queries that enables an adversary to perform various attacks on authentication protocols.
- The communication channel is controlled by the adversary who has the capacity to intercept, modify, delete, resend and reroute the eavesdropped messages.
- An adversary may steel user's smart card and may extract the stored information from the smart card.

To get over the security flaws, and enhance the system security, Chang and Wu (1991) introduced smart card-based remote user authentication scheme. The smart card based design of these cryptographic protocols increase the adoptability of smart card-based authentication scheme for real life applications due to feature like cryptographic capacity, low cost and portability. The smart-card-based authentication has become one of the most widely adopted authentication protocols (He and Wang, 2014; Wang and Wang, 2014b; Kuo et al., 2014; Wang et al., 2012). In the recent years many smart card based authentication schemes have been designed and developed in keeping the mind following attributes:

– Address low computational overhead and less storage requirement to design a low cost smart card.
– Achieve efficient login and password change phase to detect any unauthorized attempt.
– Resistance to different kinds of active and passive attacks such as off-line password guessing attack, impersonation attack, man-in-the middle attack, replay attack, insider attack, etc.
– Support user-friendly password change phase to allow a user to choose and change his password independently.
– Support mutual authentication to ensure correctness of participants.

In smart card based authentication protocols, smart card stores user security credentials, and using password they can be protected. On user initiation, smart card generates the login message and sends to the server. On receiving the login request, server verify the correctness of message source. If verification succeeds, User authentication holds. In 2009, Xu et al. (2009) presented an password authentication scheme using smart card to overcome the weaknesses of (Lee and Chiu, 2005; Lee et al., 2005). Xu et al. also claimed that their scheme satisfies all the desired security attributes. Although, in 2010, Sood et al. (2010) showed that Xu et al.'s scheme is vulnerable to off-line password-guessing attack and forgery attacks. They also presented an improvement of Xu et al.'s scheme. In the same year, Song (2010) also demonstrated that an adversary can extract the parameters from the legitimate user's smart card and perform user impersonation attack. Further, he presented an improvement of Xu et al.'s scheme. In 2012, Chen et al. (2014) pointed out that both Song and Sood et al. are still insecure. Chen et al. showed that Sood et al.'s scheme only achieves one way authentication instead of mutual authentication. In addition, they identified the inefficiency of Sood et al.'s scheme in the detection of incorrect input. Chen et al. also demonstrated the off-line password guessing attack on the Song's scheme. They have also proposed an efficient scheme. However, Ma et al. (2014) showed that Chen et al.'s scheme is vulnerable to off-line password guessing attack and does not provide forward secrecy. Karuppiah and Saravanan (2014) designed a public key based authentication scheme using smart card. Their scheme can efficiently resist off-line password guessing attack. However, Maitra (1502) showed that Karuppiah and Saravanan's scheme does not replay reply attack, and discussed flaws in the login phase. Recently, Li et al. (2013) also analyzed the security of Chen et al.'s scheme, and showed that Chen et al.'s scheme does not ensure forward secrecy, and fails to maintain efficient login and user-friendly password change phase. They also proposed an enhanced smart card based password authentication scheme to overcome the weaknesses of existing schemes. Later on, Islam (2014) pointed out the vulnerability of Li et al.'s scheme to insider attack, known session-specific temporary information attack and off-line password guessing attack. He also proposed an improved authentication scheme, which can efficiently resist insider attack, but does not overcome off-line password guessing attack. Unfortunately, Islam's improved authentication scheme does not protect anonymity, and has higher computation and communication overhead.

In this paper, we revisit the Li et al.'s scheme as it presents smart card pre-authentication mechanism. We demonstrate the pitfalls of Li et al.'s scheme, and then work on the design of an efficient and secure authentication scheme. We propose a lightweight authentication scheme with pre-smart card authentication. The proposed scheme supports smart card revocation mechanism. The analysis shows that proposed scheme resists various active and passive attack such as off-line password guessing attack, impersonation attack, replay attack, insider attack and stolen smart card attack. We also discuss the computation and communication overhead of the proposed scheme.

The rest of the paper is organized as follows: Section 2 presents the brief review of Li et al.'s scheme. Section 3 points out the weakness of Li et al.'s scheme. The proposed scheme is presented in Section 4. We verify the correctness of mutual authentication using the widely-accepted BAN (Burrows, Abadi, and Needham) logic in Section 5. The security and performance analysis is presented in Section 6 and 7, respectively. Finally, conclusion is drawn in Section 8.

2. Review of Li et al.'s scheme

In 2013, Li et al. (2013) proposed an improvement over Chen et al.'s (2014) password based user authentication scheme. The symbols used in the scheme is discussed in Table 1. Their scheme has four phases similar to Chen et al.'s scheme. The brief description of Li et al.'s scheme is as follows:

– Registration
– Login