Security Analysis of an Authentication Scheme Using Smart Cards

Gaurav Tiwari, Amit K. Awasthi and Neha Shukla

Department of Applied Mathematics,
School of Vocational Studies & Applied Sciences,
Gautam Buddha University, Greater Noida, 201312, UP, India.
{gtiwari506@gmail.com, awasthi.amitk@gmail.com, nehshuk.28@gmail.com}

Abstract. In 2010, Sood et al [3] proposed a secure dynamic identity based authentication scheme using smart cards. They claimed that their scheme is secure against various attacks. In this paper, we improve their scheme for outsider attack as well as insider attack. To remedy these security flaws, an improved scheme is proposed to withstand these attacks.

[1] Introduction

With the rapid increasing need of remote digital services and electronic transactions; authentication schemes that ensure secure communication through an insecure channel are gaining popularity and have been studied widely in recent years. In 1981, Lamport [4] proposed first remote user password based authentication scheme by employing a one way hash chain, in an insecure and untrusted network, but this scheme has a. That is why, Smart cards major drawbacks of its dependency on verification table. Smart cards implementation solved this problem of dependency on verification tables and ensures secure communication based authentication scheme are becoming day by day more popular.

The paper is organized as follows: Section 2 reviews Sood et al's authentication scheme. Section 3 describes our proposed scheme followed by security analysis in Section 4. Finally, we conclude the paper in Section 5.

[2] Phases of Sood et al's Scheme

The dynamic identity based authentication scheme proposed by Sood et al in 2010, consists of four phases: registration phase, login phase, verification and session key agreement phase and password changing phase. The notations used throughout the paper are summarized below:

Notations and Symbols used in paper

Ui	Legitimate ith user
IDi	Identifier of Ui
PWi	Password of Ui
S	The Server
x	Secret key of the server S
yi	Server's random value
ski	Session Key
T	Current date and time of inpute device
T'	Current date and time of the server S
δT	Expected time interval for a transmission delay
H(.)	Secure one way Hash Function
$\oplus$	Bitwise Exclusively or (XOR) operation
$\|$	Bitwise concatenation operation

[3] Our Proposed Scheme

In this section, we propose an upgraded authentication scheme, that preserves the properties of Sood et al's scheme and resolves all the identified weaknesses of their scheme and make it secure and efficient for practical applications. The scheme consists of four phases: registration phase, login phase, verification & session key agreement phase and password changing phase.

[3.1] Registration

When the user Ui wants to register, he chooses his identity IDi and password PWi, and send it to the server S via a secure communication channel. Then, the server S chooses random value yi for ith user and computes:

$$Ni = H(PWi) \oplus H(yi\|IDi) \oplus H(x) \oplus yi ,$$
$$Bi = H(yi) \oplus H(PWi) ,$$
$$Vi = H(IDi\|PWi) \oplus PWi ,$$
$$Di = H(H(yi) \| IDi) ,$$

S chooses the value of yi, in such a way that the value of Di must be unique for each user. The server S stores (Ni, Bi, Vi, H(.)) into smart card and sends it to Ui, via a secure channel.

[3.2] Login Phase

The user Ui, inserts the smart card into the card reader and keys in IDi$*$ and PWi$*$, then the smart card computes

$$Vi* = H(IDi* \| PWi*) \oplus PWi*$$

and checks whether computed Vi∗ is equal to the Vi or not. If they are equal, the requested user is the legitimate bearer of the smart card otherwise rejects the login request. To resist offline password guessing attack, the card reader locks the card if Ui enters either wrong identifier or wrong password more than limited number of times. After verifying the legality of the user, the smart card computes:

$$yi = Bi \oplus H(PWi) ,$$

$$H(x) \oplus yi = Ni \oplus H(PWi) \oplus H(yi \| IDi) ,$$

$$CIDi = H(H(yi) \| IDi) \oplus H(H(x) \oplus yi \| T) ,$$

$$Mi = H(H(x) \oplus yi \| H(H(yi) \| T) ,$$

and sends the login request message (CIDi, Mi, T) to the server S.

[3.3] Verification and Session Key Agreement Phase

Upon receiving the login request, S first checks the validity of time stamp Tby checking $(T'-T) \leq \delta T$ to accept/reject the login request.If it finds incorrect, the login request is rejected else the server S computes

$$Di* = CIDi \oplus H(H(x) \oplus yi \| T)$$

and recompute IDi and yi using its secret information x. Then the server computes

$$Mi* = H(H(x) \text{ c } yi \| H(H(yi) \| T)$$

and verifies computed Mi∗ with the received Mi. If it finds true, then Ui is authenticated and the login request is accepted else the connection is interrupted. Finally, S and Ui computes session key ski = H(IDi‖H(yi)‖H(x) ⊕ yi‖T) of the transmission.

[3.4] Password Change Phase

Whenever Ui wants to update his password, he inserts his smart card into the card reader and presents the credentials such as identifier IDi and current password PWi. After verifying the legality of the user by verifying Vi, the smart card ask Ui to input new password PWinew to replace the value of Ni, Bi, Vi, with the Ninew, Binew, Vinew where

$$Ninew = Ni \oplus H(PWi) \oplus H(PWinew)$$
$$Binew = Bi \oplus H(PWi) \oplus H(PWinew)$$
$$Vinew = H(IDi \| PWinew) \oplus PWinew$$

To resist offline password guessing attack, the card reader locks the card if Ui enters either wrong identifier or wrong password more than limited number of times.

[4] Security Analysis

In this section, we analyze the security of our scheme under the assumption that the secret information stored in the smart card could be extracted by some means.

[4.1] Denial of Service Attack

To resist password guessing attack, the card reader locks the card if someone enters either wrong identifier or wrong password more than limited number of times.

[4.2] Malicious User Attack

A legal but malicious user Ua can get the value of H(x) from his own card, which is same for each user. But from H(x), Ua may not be able to compute yi, which makes the proposed protocol secure against malicious user attack.

[4.3] Impersonation Attack

As both CIDi and Mi are protected by secure one way hash function, any modification in login request message (CIDi, Mi, T) will be detected by the server by verifying Mi. So, because the attacker has no way to find PWi and yi of the legitimate user Ui, he cannot modify login request message, which makes this protocol secure against impersonation attack.

[4.4] Offline Password Guessing Attack

After gathering the information on legitimate user Ui's smart card, an attacker can intercept the login request message (CIDi, Mi, T) during the login transaction, and try to guess out IDi, PWi, yi and x, but it is not possible to guess out all the parameters correctly at the same time, which makes this protocol secure against offline guessing attacks.

[4.5] Stolen Smart Card Attack

An attacker can extract security parameters (Ni, Bi, Vi, H(.)) from legitimate user Ui's smart card. But, this information does not help him to find out the value of server's secret parameter yi corresponding to the ith legitimate user. He cannot use this information to generate fake login request. He is also not able to play as man in middle by using any information on card. Thus, the proposed protocol is secure against stolen smart card attack.

[4.6] Insider Attack

Any privileged insider user can obtain H(x) from his registered legal smart card, but without knowing the password of ith user, he cannot compute yi and secret key x of the server and not use the secret information for personal benefit. Thus, this protocol is secure against an insider attack.

[5] Conclusion

In this paper, we analyzed Sood et al's dynamic identity based authentication scheme using smart cards and its immunity against various attacks. We got that their scheme is insecure for practical applications and vulnerable to outsider and insider attacks. To remedy these security flaws, we proposed an upgraded protocol for authentication scheme that preserves the similar properties of their scheme and resolves all the identified weaknesses of their scheme and make it more secure and efficient for practical purpose.

References

1. Awasthi A.K. (2004) Comment on a dynamic id-based remote user authentication scheme. Transaction on Cryptology 1(2), 15-16.

2. Cryptography / Network Security, Douglas R. Stinson, Fall 2013

3. Sood S.K., Sarje Singh K. (2010) An improvement of liao et al's authentication scheme using smart cards. In: Proc. IEEE 2nd International Advance Computing Conference, pp. 240-245.

4. Lamport L. (1981) Password authentication with insecure communication. Communication of the ACM, 24(11), 770-772.