International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 5 Issue: 1 25-Mar-2015,ISSN_NO: 2321-3337

An efficient and practical solution to secure password-authenticated scheme using smart card

R. Deepa [1], R. Prabhu M.Tech [2],
PG Research scholor[1], Head of the Department[2]
Dept.of Information Technology , Chennai, Tamil Nadu, India [1, 2].
Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College[1,2]

ABSTRACT— *This paper outlines and discusses about the smart card based password authentication scheme. Smart cards are the commonly used security mechanism used for several application especially security related ones. This paper addresses the two recently proposed protocols: i) attacker with pre-computed data ii) attacker with different data. Therefore, we propose an improved scheme to overcome the weakness and to improve the benefits of our new scheme. In addition, our improved scheme is secure under both online and offline dictionary attack.*

Keywords— *Authentication, Key Exchange, Dictionary attacks, Smart card, Network Security.*

1. INTRODUCTION

In the current trend, security plays an important role. Smart cards are secure portable storage devices, which provide security, data portability, convenience etc.., smart card usually consists of a microprocessor, memory and some interface. The memory card used in smart card simply store data and can be viewed as a small floppy disk with optional security. A microprocessor card on the other hand can add, delete and manipulate information in its memory on the card. In order to authenticate the clients or users, password based security mechanisms have been widely used in many remote login systems because they are easily implemented. To provide a secure authentication system, password based methods are often used in many remote login servers. To date, many smart card based password authentication schemes have been proposed, but they are limited to high communication and computational cost.

2. PREVIOUS WORK

Smart card based password authentication scheme involves the two entities i.e.., the server and the user. This consists of three phases: first, is the registration phase, where the server issues the smart card to the user. Thus, the smart card is personalized by the user information. Second is the login phase, where the user logon to the server using his smart card, runs an authentication session with the server. For subsequent secret communication, the user and the server need to establish the session key after the authentication session. Last phase is a password changing phase, if the user wants to change his password for the smart card under some situation, he is free to change his/her password using his smart card for the future use. In 2005, fan et.al proposed a robust remote authentication with smart cards [4]. They claimed that their proposed scheme satisfy the properties of low computation, no password table. the major drawback of their scheme is that it has no ability of anonymity for the user and it has higher computational cost because of using Rabin's public key cryptography. Using the two recently proposed protocols as case studies ([2], [3]) we demonstrate two new types of adversaries with smart card. In order to reduce the computational and communication cost, Juang, Chen and Liaw [2] described a robust and efficient password authenticated key agreement scheme using smart card, by introducing a pre-computation phase i.e., the costly operations are completed in the offline phase. It is claimed in [2] that their scheme can prevent offline dictionary attacks even if the secret information stored in a smart card is compromised. Although the scheme of Juang et al. has many benefits, we find that it suffers from three weakness: 1) inability of the password-changing operation; 2) the session-key problem; and 3) inefficiency of the double secret keys. That is, it fails to fully meet the security requirement that this type of scheme should achieve. To overcome the aforementioned weaknesses, sun et al. proposed an improved scheme, which consists of the parameter generation phase, the registration phase, the authentication phase and the password generation phase.

Juang-chen-liaw's scheme was improved by sun et al, who shows that attackers can successfully impersonate the user with old password and old data in the smart card. Sun et al scheme employs the cipher block chaining mode [5] to provide a protection against unauthorized data modification such as deletion or insertion. The functionalities of the sun et al scheme includes: 1) usability of password changing operation 2) desirable key properties 3) small verification table and 4) more identity protection.

3. SYSTEM ANALYSIS

3.1 Existing System

3.1.1 Review of Juang-Chen-Liaw's scheme

In order to reduce the communication and computational cost, Juang-Chen-Liaw proposed a password authenticated key agreement scheme using the smart card, by introducing the pre-computation phase. The main drawback of using this scheme is that, local password change not allowed. If the user forgot the password, it s straight forward for the thief to hack all the information's of the user.

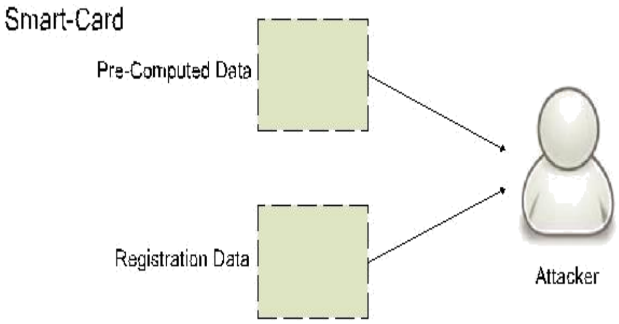

Fig.1. Adversaries with pre-computed data

Pre-Computation phase [2]

1) Smart Card selects a random number r and calculates
$e = r \times G$ and $c = r \times P_s$.
2) Smart Card writes (c, e) on its memory, i.e.,
Smart Card = $\{b_i, V_i, ID_i, CI_i, b, c, e\}$.

Password-Changing phase [2]

1) Smart Card and Server have a shared session key S_k at the end of the log-in phase.

2) Smart Card → Server:
$\{E_{Sk}\,(ID_i, h(P\ W_i^*\_b^*))\}$.

$P\ W_i$: A new password chosen by the user with identity ID_i.

b: A random number chosen by the user with identity ID_i

3) Server → SmartCard:
$\{E_{Sk}\,(b_i)\}.b_i = E_s(h(P\ W_i\_b)\_ID_i\_CI_i\_\text{AuthTag})$. AuthTag $= h(ID_i\_CI_i\_h(P\ W_i^*\_b^*))$.

4) Smart Card decrypts $E_{Sk}\,(b^*{}_i)$ with S_k and adds $(b^*{}_i, b^*)$ into its memory

3.1.2 Review of Sun et al scheme

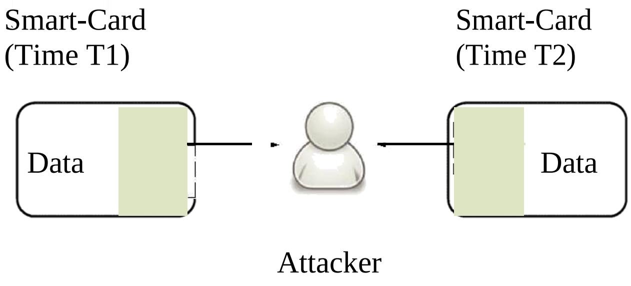

Fig.2. Adversaries with different data

Comparing with Juang-Chen-Liaw scheme, sun et al [3] provides the usability of password changing operation and several desirable key properties.

Parameter generation phase

S chooses an elliptic curve E over a finite field F such that the discrete logarithm problem is hard in E(F). The set of all the points on E is denoted by E(F). S also chooses a point G € e(f) such that subgroup generated by G has a large order n. S publishes the parameters (p, E, G, n).

Password-Changing phase

1) User U inserts Smart Card = $\{V, IM\}$, and enters the old password $P\ W$ together with a new password $P\ W^*$.
2) Smart Card replaces V with V, where

$$V = V + h(P.W\ )+h(P\ W.) = h(ID||K_S\ )+h(P\ W^{\cdot}).$$

3.2 Proposed System

To overcome the aforementioned weaknesses, we propose an improved scheme, which consists of registration phase, authentication phase and password changing phase. Thus a new scheme was proposed to fix that flaw, together with several other new properties such as forward secrecy and password changing without any interaction with the server. The security analysis made in indicates that the improved scheme remains secure under offline-dictionary attack in the smart-card loss case.

4. FEATURES OF OUR IMPROVED SCHEME

4.1 Analysis

In most smart-card based password authentication schemes, smart cards only store the data produced during the registration phase. As a result, an adversary with the smart card can only obtain the data generated in that phase. However, this is different in Juang-Chen-Liaw's protocol, where the smart card contains the data not only produced during the registration phase but also generated during the pre-computation phase. Thus an adversary with smart card can obtain both types of data. As one can see, the essential reason behind the online and offline dictionary attack on is the design of the smart card in registration phase, where V is calculated for the purpose of performing password-changing without any interaction with the server.

To make the protocol secure, we can calculate V in a different way. An improvement of Juang et al scheme was recently introduced by sun et al, that scheme provides the password changing operations and several desirable key properties. In this paper, we consider an adversary who is able to extract the data stored in the smart card of a specific user more than once. Such an adversary can successfully guess the password chosen by the user in sun et al. so we proposed a new scheme that's robust sun et al scheme for smart card password authentication.

4.2 Robust SUN Et Al.'s Scheme

User login and Admin verification is done here. Local password change is done using the Diffie-Hellman key exchange algorithm. Admin monitors the mini statement and activities with smart card. If the user forgot the password, he is free to change his/her password. Our feature is further extended by using an ideal scheme.

4.3 IDEAL Scheme

This scheme provides the Zero Attack which is Secure channel Authentication. Local password change is done in an ideal scheme. There is no chance of adversary to hack the user details. Resistance to the smart card lost case. Here, the password is not stored in the server, instead the values will be stored as keys i.e., cipher1, cipher2, Prime, A value and B value using the IDF algorithm.

5. SECURITY ANALYSIS

To evaluate the security of our improved scheme, we need to assume the capabilities that the attacker may have under the smart-card-based authentication environments. Two attacking methods are:

Method 1: attacker can inject, modify, block and delete messages at will. All authentication schemes must thwart this kind of attacker.

Method 2: attacker compromises either smart card or password but not the both.

We divide the security of the scheme in three cases as general one (attacker has all capabilities as method 1), smart card loss case (attacker has the capability of method 1 and compromises smart card as in method 2) and password loss case (attacker has the capability of method 1 and compromises password as in method 2). Our improved scheme is secure under all the three cases. so we can say that our improved scheme is secure under the aforementioned 2 methods.

6. SYSTEM DESIGN

System Design involves identification of classes their relationship as well as their collaboration. In object or, classes are divided into entity classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that is helpful only after the construction of the class diagram.

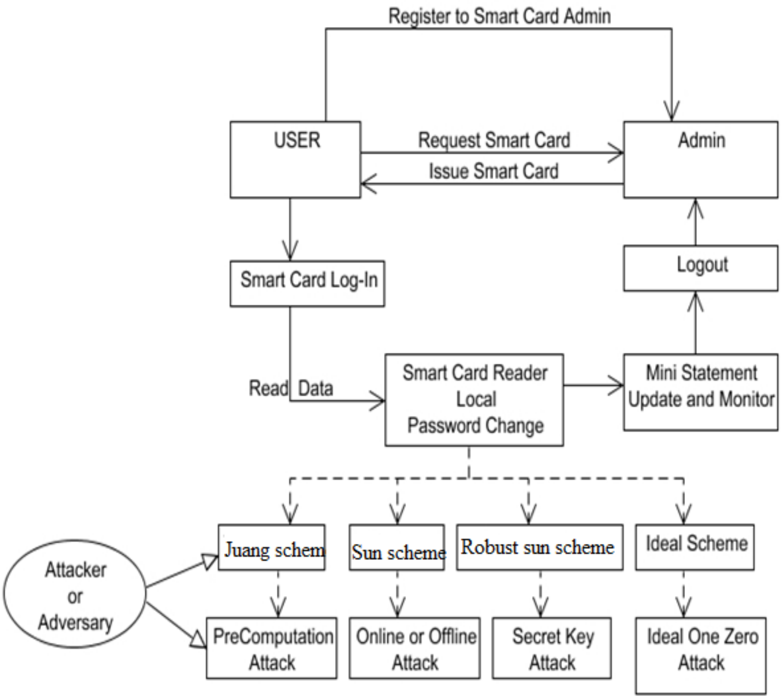

Fig.3. Architecture of improved scheme

7. CONCLUSION AND FUTUREWORK

Recently, Juang et al and Sun et al proposed a password authenticated key agreement scheme using smart cards. In this paper, we have shown the weakness of both the Juang et al and Sun et al scheme and further proposed an improved scheme. Our improved scheme, not only satisfies the benefits of the existing scheme, but also fixes its weakness by introducing a Robust Sun et al scheme. In addition, our improved scheme is further extended by introducing the ideal scheme, where the password won't be saved in the server. Instead, the key values will be saved. Therefore, we believe that our improved scheme is more suitable for real life applications than any other scheme.

8.REFERENCES

[1] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, "further observations on smart card based password-authenticated key agreement in distributed systems", IEEE Trans. Parallel and distributed systems, vol.25, No.7, July 2014.

[2] W. S. Juang, S. T. Chen, and H. T. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551-2556, Jun. 2008.

[3] D. Z. Sun, J. D. Zhong, and Y. Sun, "Weakness and improvement on Wang-Li-Tie's user-friendly remote authentication scheme," *Appl. Math. Comput.*, vol. 170, no. 2, pp. 1185-1193, Nov. 2005.

[4] C.-I Fan, Y.-C Chan, and Z.-K Zhang, "Robust remote authentication scheme with smart cards". *Comput. Secur.*, vol. 24, no. 8, pp. 619-628, Nov. 2005.

[5] NIST, Recommendation for block cipher modes of operation, NIST special publication 800-38A 2001 Edition, dec 2001, Washington DC:U.S. Dept Commerce/NIST

[6] X. Huang, Y. Xiang, A. Chonka, J. Zhou and R.H. Deng, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems", *IEEE Trans. Parallel Distrib. Syst*, vol. 22, no. 8, pp.1390-1397, Aug. 2011.

[7] C.L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards", Comput. Stand. Inter., vol. 26, no. 3, pp. 167C169, May 2004.

[8] L. Lamport, "Password authentication with insecure communication," *Commun. ACM.* vol. 24, no. 11, pp. 770-772, Nov. 1981.

[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks,"
IEEE Trans. Computers., vol. 51, no. 5, pp. 541-552, May. 2002.

[10] J. Xu, W-T. Zhu, and D-G Feng, "An improved smart card based password authentication scheme with provable security", Comput. Stand. Inter., vol. 31, vol. 4, pp. 723C728, Jun. 2009.