Comments on ‘A Dynamic ID-Based Remote User Authentication Scheme’

Mohammed Khan

Abstract —*This paper presents cryptanalysis of ‘a dynamic id-based remote user authentication scheme’ proposed by Das et al. We identify that their work is susceptible to hacking and can be cryptanalyzed. We demonstrate that a hacker can generate a forge login message and bypass the authentication. We also indicate that Das et al.’s method only provides unilateral authentication and there is no mutual authentication between user and remote system. Therefore their work is vulnerable to the server spoofing attack. Furthermore, we identify that Das et al.’s scheme has practical loopholes and infeasible to practical deployment.*

Index Terms —Authentication, security, smart card, attacks.

I. INTRODUCTION

Remote authentication is a method to authenticate the remote users over an insecure communication network. In 1981, Lamport is the first who presented a remote user authentication technique using password [1]. Later in 2000, Hwang and Li [2] identified that Lamport’s work suffers from hacking and changing the password database. Hwang and Li then came up with a novel remote user authentication scheme without using the password database. This work was based on El-Gamal public key technique [3]. To improve the previous works, many remote user authentication algorithms have been proposed in the literature [4-34].

Recently, Das et al. [16] presented a dynamic id-based remote user authentication scheme. Their work is new and secure, because dynamic identity for each transaction session can avoid the risk of id-theft. Their work uses one way hash functions. In their work, users can freely choose and change passwords without any problems [16]. They claimed that their work is more secured against some well-known attacks e.g. replay, forgery, guessing, insider, and stolen verifier etc. However, a number of researchers found that their scheme is vulnerable to attacks against their claims and has some loopholes of security.

Awasthi [17] first found that Das et al.’s work has low security and insecure. Awasthi also found that Das et al.’s work lacks basic needs of authentication theory. Afterwards, Chien and Chen [18] found out that Das et al.’s scheme fails to protect the anonymity of remote users and then they came up with an improved remote authentication technique, which achieves users anonymity. Ku-Chang [19] also pointed out some vulnerabilities of Das et al.’s work. They demonstrated that Das et al.’s work is susceptible to the impersonation attack. Ku-Chang pointed out that Das et al.’s scheme has problems of insider adversary and cannot be easily improved.

In this paper, we present further cryptanalysis of Das et al.’s scheme and point out that their scheme suffers from practical pitfalls. We also show that an adversary or a legitimate user of the system himself can easily forge a valid pair of login message, so their scheme is vulnerable to the forgery attack. Furthermore, we discuss that Das et al.’s work only provides unilateral authentication. It is also susceptible to the server spoofing attack. We also delineate that their scheme is insecure, inefficient, and not feasible for practical environment.

II. DESCRIPTION OF DAS ET AL.’S SCHEME

There are four phases in Das et al.’s scheme, namely; registration, login, authentication, and password change. The notations used throughout this paper are as follows:

U_i denotes the user of the system

Pw_i denotes the password of the user

CID_i denotes the dynamic Id of the user

S denotes the remote server

$h(.)$ denotes the one way hash function

x denotes the secret key of the remote server

y denotes the remote system’s secret number

$\oplus$ denotes the bitwise XOR operation

$A \Rightarrow B: M$ denotes a message from A to B over a secure channel

$A \rightarrow B: M$ denotes a message from A to B over an insecure channel

A. Registration Phase

In the registration phase, user U_i chooses his password Pw_i and submits to the registration server. The remote system performs the following steps:

1. Calculates a nonce $N_i = h(pw_i) \oplus h(x)$, here x is a secret key of the remote server.
2. Personalizes the smart-card with the secure parameters $h(.)$, N_i , and y ; where y is remote server’s secret key stored in each registered smart card.
3. $S \Rightarrow U_i$: Remote system sends smart card and password to the user over a secure channel.

A. Login Phase

In the login phase, user inserts his smart card in the input device and keys his password. The smart card performs the followings operations:

1. Computes $CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T)$, where T is the current time stamp of the user.
2. Computes $B_i = h(CID_i \oplus h(pw_i))$

3. Computes $C_i = h(T \oplus N_i \oplus B_i \oplus y)$
4. $U_i \rightarrow S : CID_i, N_i, C_i, T$

A. Verification Phase

The remote system receives the message from the user and performs the following operations at time T^* :

1. Verify the validity of the time interval; if it is invalid, the server rejects the login request.
2. Computes $h(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T)$
3. Computes $B_i = h(CID_i \oplus h(pw_i))$
4. Checks whether $C_i = h(T \oplus N_i \oplus B_i \oplus y)$. If it is valid, the remote system accepts the login request, otherwise terminates the operation.

D. Password Change Phase

This phase is invoked whenever user wants to change his password. Following operations are performed in this phase:

1. User inserts his smart card into the reader and submits his password. If user is validated, then he requests to change his password.
2. User chooses a new password i.e. pw_i^*
3. The smart card computes

$$N_i^* = N_i \oplus h(pw_i) \oplus h(pw_i^*)$$
which yields

$$h(pw_i^*) \oplus h(x)$$
4. The N_i will be changed by N_i^* . Now the password is changed and user terminates the operation.

III. CRYPTANALYSIS OF DAS ET AL.'S SCHEME

The Das et al.'s scheme is vulnerable to the attacks and can easily be cryptanalyzed. In the following section, we show the cryptanalysis of their scheme.

A. Forgery Attack

In Das et al.'s scheme, we know that the value of N_i i.e. $N_i = h(pw_i) \oplus h(x)$ is fixed until user changes his password. To get login into the system, user sends his login information over an insecure channel. Assume an adversary Bob or any other registered disgruntle user intercepts this information i.e. $\{CID_i, N_i, C_i, T\}$ then he performs the following operations:

1. Computes $CID_b = h(pw_b) \oplus h(N_i \oplus y \oplus T')$, where T' is the current time stamp of the adversary.
2. Computes $B_b = h(CID_b \oplus h(pw_b))$
3. Computes $C_b = h(T' \oplus N_i \oplus B_b \oplus y)$
4. Now Bob sends CID_b, N_i, C_b, T' to the remote system, which is a forged message.

After receiving the forged message from Bob, the remote system validates the T' . If T' is valid, the remote system performs the following:

1. Computes $h(pw_b) = CID_b \oplus h(N_i \oplus y \oplus T')$
2. Computes $B_b = h(CID_b \oplus h(pw_b))$
3. Remote system checks $C_b = h(T' \oplus N_i \oplus B_b \oplus y)$

Here, C_b holds true and remote system accepts the login request from the Bob who is an adversary. Finally, it is proved that Das et al.'s scheme logs in any body that chooses a random password and uses intercepted value of N_i . Thus their scheme is equivalent to the no password scheme.

B. Server Spoofing Attack

Das et al.'s scheme provides unilateral authentication i.e. only client authentication and there is no authenticity of the remote system. Thus, in their scheme there is no mutual authentication between remote user and remote system that is vulnerable and insecure from the practical point of view. The user only sends the message $\{CID_i, N_i, C_i, T\}$ and gets no acknowledgement, which can authenticate the authenticity of the remote system. Hence, their scheme can not withstand the server spoofing attack.

IV. COMMENTS ON PRACTICAL PITFALLS OF DAS ET AL.'S SCHEME

In this section, we discuss the weaknesses and pitfalls which make Das et al.'s scheme vulnerable and susceptible to use.

1. In the registration phase of Das et al.'s system, user only submits his password to the remote authentication server. In their scheme there is no user-id stored in the table to identify the user, which is important from the practical point of view. In practice, users may have same passwords but ID is always unique, which is used as a primary key in the table or database [20] e.g. Social security number or telephone number.

It is very important that every user should have at least one static and unique identifier in the table, because users are given rights or privileges based on that unique identifier which is only associated with that specific user. In case, if there is no unique identifier of users, then system does not have any information that which user can access which facilities provided to him.

Moreover, if a user has to delete from the system or blacklist in the system, then Das et al.'s scheme has no way to perform these operations. So, their scheme is practically infeasible to implement.

2. In the login phase, Das et al. compute CID_i and B_i in which $h(pw_i)$ is calculated twice. If the value of $h(pw_i)$ is saved in one variable e.g. $P = h(pw_i)$ then there is no need to calculate $h(pw_i)$ two times. So in the login phase of Das et al.'s scheme, there are five hash calculations which can be reduced to only four hash function calculations to improve the computational speed of the login phase or even the whole system.

3. Das et al. used the secret number of the remote system i.e. y which is stored in the smart card of each registered user. But unfortunately, this secret number y has no worth in maintaining the system's security, because it is public to all registered users and is saved on the smart card without any encryption or transformation.

Here, we assume that there are thousands of registered users in the system who are using the same remote system's secret number i.e. y and because of some reasons the remote administration wants to change this secret number, then it becomes a cumbersome job and it is practically difficult to do so. One solution is to change the smart cards of all the registered users, which is an inefficient solution. Thus, this drawback also makes the Das et al.'s scheme infeasible for the real environment.

4. In Das et al.'s scheme, N_i is available to each registered user and also sent over the insecure channel. If a user wants to calculate the value of $h(x)$, which is the hashed value of server's secret key then user uses $h(x) = h(pw_i) \oplus N_i$. Each user already knows the value of N_i so he can easily get the value of $h(x)$. Now a user can play administrator's role to register fake users in the system. As an example, we assume that Bob is a registered user of the system and wants to register Carol, who is a fake user. Because Bob knows $h(x)$, so he can register Carol by calculating $N_c = h(pw_c) \oplus h(x)$. Now Carol is also a registered user of the system in Das et al.'s scheme and enjoys the system facilities without being registered by the original server.

In our opinion, if Das et al. calculate N_i by $N_i = h(pw_i \oplus x)$, then it is very difficult for any body to register fake users in the system. One more benefit for $N_i = h(pw_i \oplus x)$ is only one hash function calculation instead of calculating two hashes $h(x)$ and $h(pw_i)$, which also decrease the performance of Das et al.'s scheme.

V. CONCLUSION

In this paper, we have presented the cryptanalysis and comments on the Das et al.'s scheme. We have demonstrated that their scheme is vulnerable to the forgery attack, and an adversary can easily impersonate or pass the system authentication. In addition, we have pointed out that Das et al.'s scheme does not provide mutual authentication between client and remote system, thus their scheme is susceptible to the server spoofing attack. Moreover, we have also discussed some practical pitfalls, which make Das et al.'s scheme insecure, inefficient, and infeasible for the practical deployment.

REFERENCES

- [1] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, vol.24, no.11, pp.770-772, 1981.
- [2] Hwang, M.S., and Li, L.H. "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.
- [3] T. El Gamal, "A Public Key Cryptosystem and Signature Scheme Based on the Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 469-472, 1985.
- [4] S. J. Wang and J. F. Chang, "Smart Card Based Secure Password Authentication Scheme," *Computers and security*, vol. 15, no. 3, pp. 231-237, 1996.
- [5] W.H. Yang and S.P. Shieh, "Password Authentication Schemes with Smart Cards," *Computers and Security*, vol.18, no.8, pp.727-733, 1999.
- [6] H. M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958-961, 2000.
- [7] C. C. Lee, M. S. Hwang, and W. P. Yang, "A Flexible Remote User Authentication Scheme Using Smart Cards," *ACM Operating Systems Review*, vol.36, no.3, pp.46-52, July 2002.
- [8] J. J. Shen, C. W. Lin, and M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol.49, no.2, pp.414-416, May 2003.
- [9] C. C. Chang and K. F. Hwang, "Some Forgery Attacks On a Remote User Authentication Scheme Using Smart Cards," *Informatics*, vol. 14, No. 3, pp. 289-294, 2003.
- [10] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol. 49, No. 4, pp. 1243-1245, Nov 2003.
- [11] C.L. Hsu, "Security of Chien et al.'s Remote User Authentication Scheme Using Smart Cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.
- [12] M. Kumar, "New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no.2, pp. 597-600, May 2004.
- [13] Lin, C.H., and Lai, Y.Y., "A Flexible Biometrics Remote User Authentication Scheme", *Computer Standard and Interfaces*, vol. 27, no. 1, pp. 19-23, 2004.
- [14] W.C. Ku, S.T. Chang and M.H. Chiang, "Further Cryptanalysis of Fingerprint-based Remote User Authentication Scheme Using Smartcards", *IEEE Electronics Letters*, vol. 41, no. 5, 2005
- [15] E. J Yoon, E. K Ryu, K.Y Yoo, "An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication Scheme", *Computers and Security*, vol. 24, pp. 50-56, 2005.
- [16] M.L Das, A Saxena, V.P Gulati, "A Dynamic ID-based Remote User Authentication Scheme", *IEEE Transactions on Consumer Electronics*, vol. no. 50, no. 2, pp. 629-631, May 2004.
- [17] A.K Awasthi, "Comment on A Dynamic ID-based Remote User Authentication Scheme", *Transactions on Cryptology*, vol. no. 1, issue no. 2, pp. 15-16, August 2004.
- [18] H.Y Chien, C.H Chen, "A Remote Authentication Scheme Preserving User Anonymity", *Intl. Conf. on AINA'05*, vol. no. 2, pp. 245-248, March 2005.
- [19] W.C Ku, S.T Chang, "Impersonation attack on A Dynamic ID-based Remote User Authentication Scheme Using Smart Cards", *IEICE Transactions on Communication*, vol. E88-B, no.5, pp. 2165-2167, May 2005.
- [20] C.J Date, "An Introduction to Database systems", *Pearson Addison Wesley*, 2005.
- [21] Horng, S.J. Tzeng, S.F. Pan, Y. Fan, P. Wang, X. Li, T. Khan, M.K., "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", *IEEE Transactions on Information Forensics Security*, 2013, 8, 1860-1875.
- [22] Z. Liu, X. Huang, Z. Hu, M.K. Khan, H. Seo, L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age", *IEEE Transactions on Dependable and Secure Computing*, pp. 99, 2017, pp. 237-248
- [23] S.F Tzeng, S.J Horng, T. Li, X. Wang, P.H. Huang, M.K Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", *IEEE Transactions on Vehicular Technology*, vol 66, no. 4, pp. 3235-3248, 2017
- [24] A.K Das, M. Wazid, N. Kumar, M.K Khan, K.W.R Choo, Y.H Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment", *IEEE Journal of Biomedical and Health Informatics*, vol. 22, issue 4, pp. 1310-1322, 2017
- [25] P.W Tsai, M.K Khan, J.S Pan, B.Y Liao, "Interactive Artificial Bee Colony Supported Passive Continuous Authentication System", *IEEE Systems*, Vol. 8, Issue, 2, 2014
- [26] X. Li, J. Niu, Muhammad Khurram Khan, J. Liao, "An Enhanced Smart Card based Remote User Password Authentication Scheme", *Journal of Network and Computer Applications*, Elsevier Science, pp.1365-1371, volume 36, issue 5, September 2013

- [27] Muhammad Khurram Khan, Soo-Kyun Kim, Khaled Alghathbar, "Cryptanalysis and Security Enhancement of a 'More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme'", Computer Communications, Elsevier Science, vol. 34, Issue 3, pp. 305-309, March 2011
- [28] A.S Tolba, M.K Khan, Khaled A, "Systems and Methods for Three-Factor Authentication", US Patent No. 8862888, 2014
- [29] M.K Khan, "Fingerprint Biometric-based Self and Deniable Authentication Schemes for the Electronic World", IETE Technical Review, vol. 26, issue 3, pp. 191-195, May-June, 2009
- [30] A. Waqar, A. Raza, H'. Abbas, M.K Khan, "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata", vol. 36, issue 1, pp. 235-248, Journal of Network and Computer Applications, 2013
- [31] M.K Khan, K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'", Sensors, vol. 10, Issue 3, pp. 2450-2459, 2010.
- [32] M. Aalsalem, W.Z. Khan, W. Gharibi, Muhammad Khurram Khan, Q. Arshad, "Wireless Sensor Networks in Oil and Gas Industry: Recent Advances, Taxonomy, Requirements, and Open Challenges", Accepted for Publication, Journal of Network and Computer Applications, Elsevier, April 2018
- [33] V. Odelu. AK Das, M.K Khan, KKR Choo, M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts", vol 5, pp. 3273-3283, IEEE Access, 2017
- [34] W.Z Khan, M. Alsalem, S. Sohrab, M. Atiquzzaman, Muhammad Khurram Khan, "A Reliable Internet of Things Architecture for Oil and Gas Industry", 19th IEEE International Conference on Advanced Communications Technology (ICACT'17), 2017, Korea