International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 3, Issue 11, 2016

Cryptanalysis of Biometric Based Authentication Protocol

Rahul Kumar[1] Saru Kumari2,

1Department of Mathematics, S.S.V P.G College, Hapur, Utter Paradesh, India

2Department of Mathematics, Ch. Charan Singh University, Meerut, Utter Paradesh, India

ABSTRACT

He-Wang presented a ECC and biometric based smart-card lightweight authentication scheme for multi-server environment in 2014. In this article, we cryptanalyze the scheme of He-Wang and identify that it is not secure against session specific information and user impersonation attack. Furthermore, the proposed protocol of He-Wang is unable to provide the facility of re-registration and user-revocation in the case of smart card stolen attack. There are also some design issues in He-Wang's scheme like invalid password login and invalid password modification during password update stage.

.

Keywords ***Authentication protocol, Multi-Server, Smart Card, Impersonation***

I. INTRODUCTION

Due to the fast development of e-commerce applications and wireless communication networks, the demand of protecting the user's credentials has increased[1]. In recent years, a large number of transactions have been implemented on wireless networks or internet due to their feature of transferability for various mobile devices like smart phones, smart cards, tablets and laptops [2]. So, the key agreement and authentication schemes have become important part for the communication systems. A reasonable security features like privacy of client's credentials, mutual-authentication and Sk security are required to be well-thought-out to secure the important information from any illegal user or adversary [3, 4].

I. REVIEW OF HE-WANG'S SCHEME

The protocol introduced by He-Wang [5] is reviewed in this section. The common used notations throughout the article are listed down in the Table 1. He-Wang's protocol consists on two stages named as: i). Registration stage and ii). Authentication and key agreement stage. The description of all these stages is as follow.

A. Registration stage

This stage comprises of two phases namely i) Server- registration and ii) User-registration.

1) In server-registration stage, a server S_i selects the SID_i and forwards to the registration center through private channel. After getting SID_i the registration center calculates $s_i = H(SID_i||s)$ and transmits it back to S_i over secure channel. After getting S_i from the RC, server stores it.

2) In user registration stage, a user U_j initiates a message and gets a smart-card SC_j along-with the

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 3, Issue 11, 2016

components required for authentication, like following:

Step1: The user U_j selects his id_j, pw_j and inserts biometric impression B_j. Furthermore, U_j calculates $(\sigma_j, \theta_j) = Gen(B_j)$ and forwards the registration request towards $R = (id_j , H(pw_j,\sigma_j))$ RC over private channel.

Step2: After getting the request of registration R, RC calculates $s_i = H(id_j \| s)$, $z_j = s_j \oplus H(pw_j,\sigma_j)$ and keep z_j into smart-card.

TABLE I
COMMON USED NOTATIONS

Notations	Description
RC	Registration Center
S	Private key of RC
g,p	Large prime number
F_p	Finite field
E_p	An elliptic curve over GF_p
G	An additive group on E_p
P	Generator of G
P_{pk}	Public key of RC
S_i	The i^{th} server
SID_i	The identity of server S_i
s_i	Private key of server S_i
C_j	Tthe j^{th} client
id_j	The identity of j^{th} client
pw_j	Pasword of j^{th} client
s_j	An authentication parameter of C_j
sc_j	Smart card of C_j
A	An adversary
$H(.)$	Hash funcation
$\|$	Concatenation operator
$\oplus$	XoR operator
Enc_s/Dec_s	Encryption and Decryption key

B. *Authentication and key agreement stage*

In this stage, both U_j and S_i makes mutual-authentication and maintains the SK.

Step1: The user U_j enters smart-card into a reader and insert id_j, pw_j and B_j' at sensor. After that U_j produces a random number a and calculates $\text{Rep}(B_j^{',\theta_j)=\sigma_j}$, $s_j = z_j \oplus H(pw_j,\sigma_j)$, $X=Ap$, $L_1= aP_{pk}$, $cid_j = id_j \oplus H(L_1)$ and $h_1 = H(id_j \| SID_j \| s_j \| X \| L_1)$.Then user U_j sends the message $msg_1 = cid_j \| X \| h_1)$.to S_i.

Step2: After obtaining the msg_1, S_i chooses a number b randomly and calculates $Z = bP$, $L_2= bP_{pk}$, $h_2 = H(cid_j \| X \| h_1 \| SID_i \| s_j \| Z \| L_2)$. and $CSID_i = SID_i \oplus H(L_2)$. Then S_i send the message $msg_2 =\{ cid_j , X , h_1 , CSID_i , Y, h_2 \}$.to RC via a public channel.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 3, Issue 11, 2016

Step3: After getting the message msg_2 from the server, RC calculate $L_3 = sZ(=L_2)$, $SID_i = CSID_i \oplus H(L_2)$.and $s_j = H(SID_i \| s)$, then registration center verifies that either $h_2 = H(cid_j \| X \| h_1 \| SID_i \| s_i \| Z \| L_3)$ satisfies or not. If this condition does not satisfy then session will be terminated. Else, RC calculates $L_4 = sX$ $(=L_1)$, $id_j = cid_j \oplus H(L_4)$ and $s_j = H(id_j \| s)$, the registration center checks either $h_1 = H(id_j \| SID_i \| s_j \| X \| L_4)$ satisfies or not. If this condition fails then the session will be terminated. Otherwise, RC calculates $tid_j = id_j \oplus H(Z \| L_3 \| s_i)$, $h_3 = H(id_j \| tid_j \| X \| SID_i \| Z \| s_i)$, $TSID_i = SID_i \oplus H(X \| L_4 \| s_j)$ and $h_4 = H(id_j \| X \| L_4 \| SID_i \| Z \| s_j)$. Then RC transmits the message $msg_3 = \{ tid_j \| h_3 \| TSID_i \| h_4 \}$ to S_i over public channel.

Step4: After getting the message msg_3, S_i calculates $id_j = tid_j \oplus H(Z \| L_2 \| s_i)$ and determines either the identity of client id_j is legal or not. If this check is failed then session will be terminated. Else, S_i test either $h_3 = H(id_j \| tid_j \| X \| SID_i \| Z \| s_i)$ satisfies or not. If this check fails then the session will be terminated. Otherwise, S_i calculates the session key $SK = bX = abP$ and $h_5 = H(id_j \| SID_i \| X \| Z \| X \| h_4)$.At the end, S_j forwards message $msg_4 = \{TSID_i \| Z \| h_4 \| h_5 \}$ to user over public channel.

Step5: After getting msg_4 from S_i , U_j calculates $SID_i = TSID_i \oplus H(X \| L_1 \| s_j)$ and tests either $h_4 = H(id_j \| X \| L_4 \| SID_i \| Z \| s_j)$ satisfies or not. The session will be stopped if this check fails. Otherwise, session key $SK = aZ = abP$ and verifies that $h_5 = H(id_j \| SID_i \| X \| Z \| h_4)$ is satisfies or not. If this check fails then the session will be aborted. Else, U_j calculates $h_6 = H(SID_i \| id_j \| X \| Z \| SK \| h_4)$ and forwards message $msg_5 = \{h_6\}$ to S_i over public channel.

Step5: Upon getting msg_5 from U_j , S_i verifies that $h_6 = H(SID_i \| id_j \| X \| Z \| SK \| h_4)$ satisfies or not. and forwards message $msg_5 = \{h_6\}$ to S_i over public channel. If this condition passes then it is confirmed by S_i that the user U_j is legal. Otherwise, the session will be terminated.

III. *CRYPTANALYSIS OF HE-WANG'S SCHEME*

In this section, we have presented the cryptanalysis of He-Wang's scheme. The proposed scheme of He-Wang is vulnerable to the following issues.

A. Session specific information attack

If the randomly choosen number a is exposed to an dishonest user *A* then, the scheme of He-Wang will suffer from various disadvantages like as follows:

- *A* can easily compute $SK = aZ = abP$ by stealing random number a.

- The registration center *RC* will not be able to identify the both entities U_j and S_i respectively whenever they wish to maintain a session key. So, a valid server S_i can behave as a valid user U_j and can take the services from other servers S_i.

Due to above mentioned drawbacks the discussed scheme is unable to facilitate the session key security.

B. User impersonation attack

In registration stage of U_j, the *RC* calculates the parameter s_j of U_j using the id_j of user and private key s of *RC* as $s_j = H(id_j||s)$. As we know that the authentication parameter is not dynamic and registration stage is not capable to point out re-registration with similar credentials. That's why U_j will not be able to re-register himself using same identity.So,*A* can obtain the secret parameter of authentication by getting re-registered with the identity of honest id_j, because no identity information table is maintained by RC. So, A can get the parameter used for authentication of an honest user and can behave as an honest user.

C. Non provision of re-registration and revocation

If the smart card of any user is stolen or lost then revocation of card is key security need of scheme to facilitate the user with strong security. There must be a mechanism to protect the smart-card from misuse if any user loss his/her smart- card. Otherwise, A can deceive any honest user because user registration stage doesn't have any ability to identify the re- registration process using same identity. The authentication scheme presented by He-Wang does not provide the facility of re-registration and revocation if smart-card of a legal user is stolen or lost.

IV. CONCLUSION

The scheme proposed by He-Wang is crypt analyzed in this manuscript, and it is found that their scheme is not secure against session-specific information attack. Furthermore, their proposed protocol is insecure against user impersonation at- tack. We have also highlighted the scheme of He-Wang is not able to facilitate user with re-registration and revocation.

REFERENCES

[1] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Transac- tions on Industrial Informatics*, vol. 9, no. 4, pp. 2004– 2013, 2012.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: motiva- tion, taxonomies, and open challenges," *IEEE Communi- cations Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2013.

[3] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2001, pp. 453– 474.

[4] M. Bellare, R. Canetti, H. Krawczyk *et al.*, "A modular approach to the design and analysis of authentication and key exchange protocols," in *STOC*, vol. 98, no. 50, 1998, pp. 419–428.

[5] D. He and D. Wang, "Robust biometrics-based authentica- tion scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2014.