An Analysis of a Three-Factor Authentication Scheme and Its Improved Fix

Songsong Zhang, Xiang Li, and Yong Xie(✉)

Department of Computer Technology and Application,
Qinghai University, Xining 810016, China
mark.y.xie@qq.com

Abstract. With the development of Internet technology, a single authentication method for username and passwords can't satisfy the basic requirements of system security. A multi-server authentication scheme is a useful authentication mechanism in which a remote user can access the services of multiple servers after registering with the registration center (RC). Biometric information is difficult to simulate, therefore biometrics is used for multi-factor authentication. Recently Reedy *et al.'s* proposed a three-factor authentication scheme. They claimed their schemes can resist all types of attacks. But unfortunately, after analyzing the scheme, we demonstrate their scheme cannot defend against impersonation attack and offline guessing attack. At last, we propose improved fix to overcome its deficiency.

Keywords: Multi-factor authentication · Password authentication scheme · Impersonation attack · Offline guessing attack

1 Introduction

After the emergence of Internet technology, the network-based information industry has developed rapidly and developed into multi-server ubiquitous network that starting as single point-to-point wired network. The network-based severs in our daily life, production and even military field show a broad application prospect [2]. Data has been the main part of people's production and life. Now, the mobile terminal is pushing the application of network to another climax. However, more and more incidents of information leakage and virus spreading have also reached another climax [3]. It is for the reason that data security becomes indispensable. It's why we need cryptography and effective encryption architecture to protect our data security.

When attacking a target, an attacker often interprets the user's password as the beginning of the attack. As long as an attacker can guess or determine the user's password, he can gain access to the machine or network and access any resources that the user can access. This is extremely dangerous if the user has domain administrator or root user privileges [12].

Password attack is the hacker's favorite method of intruding into the network. Hackers obtain the passwords of system administrators or other special users, obtain the management rights of the system, steal system information, files on disk and even destroy the system.

X. Sun et al. (Eds.): ICAIS 2019, LNCS 11633, pp. 597–605, 2019.
https://doi.org/10.1007/978-3-030-24265-7_51

Authentication is a process of providing access authorization verification for the person who want to access or a process of giving user the identification [13]. That is applied to mutual authentication between server and user to assure each other exclusively. Apart from traditional username - password authentication method, by means of biometric authentication to establish a key also began to blossom. This process of participating in certification through biometrics is called as mutually authenticated key agreement [1].

Multi-server authentication schemes ca be divided into two main parts: password-based multi-server authentication and smartcard-based multi-server authentication schemes [19]. We can store a large secret parameters for in smartcard-based authentication [20, 21]. Smartcard-based multi-server authentication schemes prevent an adversary from successfully implementing the password-guessing attack. However, it is very inconvenient for users to carry smart cards and smart cards must participate in every process in login authentication [8]. On the contrary, password-based multi-server authentication schemes are easy to use and convenient for practical applications because they do not require a smartcard and card reader [22, 23]. However, the emergence of biometric authentication has made up for the shortcomings of the above two authentication methods and so the biometric authentication began to flourish.

Since Lamport [15] first proposed a password-based authentication in 1981, a series of single-server password-based authentication schemes are proposed. But these schemes are greatly increased burden on users because of one-on-one authentication method [15]. In 2001, Tsaur [16] proposed the smartcard-based password authentication which initiated remote user identity authentication for multi-server environment. Yoon *et al.* [5] demonstrated an anonymous authenticated key agreement scheme for multi-server environment by using elliptic curve cryptography [5]. Soon afterwards, he and Kim [17] pointed out that Yoon *et al.*'s scheme cannot resist masquerade attack, inside attack, stolen smartcards attack and offline password guessing attack and then he proposed the improved scheme. Afterwards, Chuang and Chen [18] proposed scheme that recommended using hash to meet practical application. But Mishra *et al.* [4] proved several weaknesses.

In 2015, Jiang et al. [23] and Odelu et al. [24] proposed biometric key agreement protocol for multi-Server applications. But in the three schemes, RC participates in the authentication stage, the registry load is too high, which is easy to cause a node failure, which not applicable to the actual situation [27, 28]. In addition, they put forward in the password update phase which has security problems and is vulnerable to masquerade attack, inside attack. There are clock synchronization problems in the protocol. As a result, they have put forward improvement plans. In 2016, Wan et al. [25] pointed out Chuang et al. 's [18] schemes can't resist the masquerade attack and proposed a improvement plans. At the same time, Amin et al. [26] also pointed out that the previous schemes have various shortcomings and gave an improved authentication protocol for remote users in multi-server environment [29].

Recently, to resistant to impersonation attack, Reedy *et al.* [1] proposed a design of mutually authenticated key agreement scheme resistant for multi-server environment. They claimed their scheme withstand all types of known attacks. Unfortunately, we find that their scheme cannot resist offline password guessing attack, user impersonation attack and lacks user anonymity protection. We present an improved fix to overcome these deficiencies at last.

We are organized this paper as follows: (i) Firstly, our preparations introduce the attack model and elliptic curve knowledge. (ii) Next, we review Reedy *et al.*'s scheme and point out the drawbacks of the scheme Reedy *et al.*'s. That is, cryptographic analysis. (iii) We present an improved fix to overcome these deficiencies at last.

2 Preliminaries

2.1 Discrete Logarithm Problem of Elliptic Curve

The security of the entire scheme is guaranteed based on the discrete logarithm of the elliptic curve. The discrete logarithm problem is also the basis of the Reedy's scheme. We need briefly talk about the elliptic curve involved in the scheme.

Addition definition of elliptic curve: If we delimit an elliptic curve: $E_{\mathrm{p}} : y^2 = x^3 + ax + b$ and $4a^3 + 27b \neq 0$. Assuming P and Q are the point on the elliptic curve. We define $P + Q = R$ where R satisfies the point R is the negative point of the only intersection where the line passing through the two points P and Q intersects the elliptic curve. Additionally, $P = Q$, the tangent to the point P is crossed to the negative point where the elliptic curve is R, $R = 2P$. However $3P = P + P + P = 2P + P$, we can compute the by this way. Consequently, when a point P is known, the "the number N operate the point $NP(\mathrm{N} \in \mathrm{Z})$" is not difficult, because of the nature of the addition, the operation can be faster [10]. But in turn, "the problem of knowing the point $NP(\mathrm{N} \in \mathrm{Z})$ for N" is very difficult, because only each N can be traversed. This is the "discrete logarithm problem on elliptic curves" used in elliptic curve cryptography [30].

- Which is the following parameters are known:
  - an elliptic curve: $E_{\mathrm{p}} : y^2 = x^3 + ax + b$
  - a point P on the elliptic curve (base point)
  - $NP(\mathrm{N} \in \mathrm{Z})$ on the elliptic curve $E_{\mathrm{p}} : y^2 = x^3 + ax + b$

We need solve:

- N

Because of the difficulty, the security of the elliptic curve cipher is guaranteed.

2.2 Security Model

In recent years, the adversaries model of the remote password authentication scheme has always used the classic Dolev-Yao's model [6], that is the adversaries can arbitrarily monitor, capture, insert and delete the information on the public channel [7]. In recent years, with the development of Internet technology, the ability of adversaries are increased. Adversaries can analyze the message on the smartcards and enhance ability to attack. This paper introduce Wang et al. [7] and Huang's [9] adversaries model.

In this mode, there are enumerated six kinds adversaries model and increments them according to their capabilities [11]. But for Three-factor Mutually Authenticated

Key Agreement schemes, an adversary $\mathcal{A}$ have capabilities which could obtain two of the authentication factors but have no affects to another. The details are shown as following.

(1) $\mathcal{A}$ captures the smartcards and the password, but A can't threaten the biological factors of user.
(2) $\mathcal{A}$ have abilities to obtain password and biological factors, but have inability to get smart card parameters.
(3) $\mathcal{A}$ get the smartcards and the biological factors, but the password is security.

In Huang et al.'s [9] schemes, the probability of success is rare in case 1 or 2. Because the biological factors are fuzzy and extremely difficult to recover. Security parameters of high information entropy are often stored in smart cards [14]. In summary, Scenario three poses a great threat because of the development of the low information entropy and dictionary attack technique.

3 Review of Reedy et al.'s Scheme

In this subsection, we will briefly review Reedy *et al.'s* scheme. Their scheme include six compositions: Registration Server Initialization phase, Application Server Registration phase, User Registration phase, Login phase, Mutually Authenticated Key Agreement phase, Password And Biometrics Change phase, Dynamic Addition Of Application Server phase, User Revocation/Re-Registration phase. In order to save time and space, we simply recall the central few parts.

Registration Server Initialization phase, we will not elaborate on this. This phase are ready for initialization which the registration server RS generates following parameters. RC (RC is registration server) generates an elliptic curve $E_p : y^2 = x^3 + ax + b(\mathrm{mod}\,\mathrm{p})$, where P is a larger prime number, private key USK, ASK and finally publishes the parameters $\{E_p, \mathrm{p}, h(\cdot)\}$.

3.1 Application Server Registration Phase

(1) S_j sends SID_j to RC securely.
(2) RC computers $K_j = h(\mathrm{SID_j} \parallel \mathrm{ASK})$ and stores them in its database.
(3) RC responds to S_j the parameters and stores $\{K_j, h(\mathrm{ASK}), \mathrm{P}\}$.

3.2 User Registration Phase

A user must register with RC to become a legitimate user. $\mathrm{U_i}$ need do the according following steps to register with RC via a private channels.

(1) U_i chooses ID_i and PW_i Meanwhile, users need generate a random number $r_i \in Z_p^*$ and compute $PID_i = h(\mathrm{ID_i} \parallel \mathrm{r_i}), \mathrm{PWD_i} = h(\mathrm{PW_i} \parallel \mathrm{r_i})$ and send a request messages $\{PID_i, \mathrm{PWD_i}\}$

(2) RC verifies the whether a registered user and computes $\mathrm{Q_j} = h(\mathrm{PID_i} \parallel \mathrm{K_j})$, $\mathrm{R_j} = \mathrm{Q_j} \oplus \mathrm{PWD_i}$.
Finally, RC reserves $\{\mathrm{SID_i}, \mathrm{R_j}\}$ in $\mathrm{T_i}$ table and $\{PID_i, \mathrm{C_i}, \mathrm{T_R} = 1\}$ in T_c table where $\mathrm{T_R} = 1$ means U_i registered initially and is in active state. RC computes $W_j = h(\mathrm{PID_i} \parallel \mathrm{USK})$ and personalizes $\{W_j, \ \mathrm{T_i}, \mathrm{h(ASK)}\}$ into the smartcards to be delivered to U_i.

(3) U_i scans his/her BIO_i at the provided sensor with card reading machine, and computes $X_j = W_j \oplus PWD_i$, $C_i = h(\mathrm{ID_i} \parallel \mathrm{W_j})$, $(\sigma_i, \theta_i) = \mathrm{Gen(BIO_i)}$, $\mathrm{V_i} = \mathrm{r_i} \oplus \mathrm{h(\sigma_i)}$ U_i replaces W_j with X_j and stores $\{C_i, \mathrm{V_i}, \theta_\mathrm{i}\}$ on smartcards. Therefore, the smartcards finally contains $\{X_j, \mathrm{V_i}, C_i, \ \mathrm{T_i}, \theta_\mathrm{i}, P, h(\cdot), h(\mathrm{ASK})\}$.

3.3 Login Phase

User can transmit the login request by inserting smartcards and enter ID_i, PW_i and $\mathrm{BIO}_i^{'}$ to get login privileges.

Smartcards compute $\sigma_i^{'} = \mathrm{Re}\,p(\mathrm{BIO}_i^{'}, \theta_i), \mathrm{r_i} = \mathrm{V_i} \oplus \mathrm{h}(\sigma_i^{'}), \mathrm{PID_i} = \mathrm{h}(\mathrm{ID_i} \parallel \mathrm{r_i})$, $\mathrm{PWD_i} = h(\mathrm{PW_i} \parallel \mathrm{r_i})$, $W_j = X_j \oplus PWD_i$. Finally, smartcards need verify whether the parameter $C_i \overset{?}{=} h(\mathrm{ID_i} \parallel \mathrm{W_j})$ are correct. If the value doesn't correspond, the login request is terminated.

User choose the server S_j by assessing the list $\mathrm{T_i}$ and extract $\mathrm{R_j}$ at the same time. User compute $\mathrm{Q_j} = \mathrm{R_j} \oplus \mathrm{PWD_i}$. Smartcards generate random number $\mathrm{N_1} \in \mathrm{Z_p^*}$ and compute $B_{ij} = PID_i \oplus h(\mathrm{SID_i} \parallel \alpha \parallel \mathrm{h(ASK)})$, $\mathrm{D_{ij}} = \mathrm{h}(\mathrm{PID_i} \parallel Q_i \parallel \alpha)$, $\alpha = N_1 P$. Smartcard send out the login request include $\{B_{ij}, \mathrm{D_{ij}}, \alpha\}$ by public channel.

3.4 Mutually Authenticated Key Agreement Phase

This phase mainly introduce the process which U_i and S_j authenticate each other and establish a secure long-term channel for further communication over public channel.

(1) S_j computes $PID_i = B_{ij} \oplus h(\mathrm{SID_i} \parallel \alpha \parallel \mathrm{h(ASK)})$ and $\mathrm{Q_j} = h(\mathrm{PID_i} \parallel \mathrm{K_j})$ when receive the login request. Afterwards, S_j authenticates U_i only if $\mathrm{D_{ij}} \overset{?}{=} \mathrm{h}(\mathrm{PID_i} \parallel Q_i \parallel \alpha)$ matching the condition. Otherwise, the process terminates.

(2) S_j generates a random number $\mathrm{N_2} \in Z_p^*$ and computes $\beta = \mathrm{N_2 P}$, $\mathrm{K_{ij}} = \mathrm{N_2}\,\alpha$, $\mathrm{SK} = \mathrm{h}(\mathrm{Q_j} \parallel \mathrm{K_{ij}} \parallel \mathrm{PID_i})$, $\mathrm{E_{ij}} = \mathrm{h}(\mathrm{SK} \parallel \mathrm{SID_j} \parallel \beta \parallel \alpha \parallel \mathrm{Q_j})$. And then S_j send $\{\mathrm{E_{ij}}, \beta\}$ to smartcards by a public channel.

(3) U_i computes $\mathrm{K_{ij}} = \mathrm{N_1}\,\beta$, $\mathrm{SK} = \mathrm{h}(\mathrm{Q_j} \parallel \mathrm{K_{ij}} \parallel \mathrm{PID_i})$ and verifies $\mathrm{E_{ij}} \overset{?}{=} \mathrm{h}(\mathrm{SK} \parallel \mathrm{SID_j} \parallel \beta \parallel \alpha \parallel \mathrm{Q_j})$. If the condition holds, U_i authenticates S_j and U_i computer $\mathrm{F_{ij}} = \mathrm{h}(\mathrm{SK} \parallel \mathrm{SID_j} \parallel \beta \parallel \alpha \parallel \mathrm{Q_j})$ Otherwise, the process terminates. Smartcards launches $\mathrm{F_{ij}}$ to S_j via a public channel.

(4) S_j verifies condition $\mathrm{F_{ij}} \overset{?}{=} \mathrm{h}(\mathrm{SK} \parallel \mathrm{SID_j} \parallel \beta \parallel \alpha \parallel \mathrm{Q_j})$ and reconfirms the authenticity of U_i. They complete each other certification and rebuild communication channel.

4 Cryptanalysis of Reedy et al.'s Proposed Scheme

After we analyzed the Reedy *et al.* 's scheme and established the basic attack model, we begin to analyze the security of the scheme. We show that the scheme is not resistant to offline password guessing attack and impersonation attack. The following is a description of the Reedy *et al.*'s scheme.

(1) We have established an adversary model in the previous section, that is, two factors are known to determine whether it can threaten the third factor. The proof of the impersonation attack is given in the scheme including user and application. In the proof a, assume $\mathcal{A}$ wants to impersonate a legitimate user, he/she can performs guessing the username and the password. Apart from this, $\mathcal{A}$ need build the message $\{\mathrm{B_{ij}}, \mathrm{D_{ij}}, \alpha\}$. And then $\mathcal{A}$ compute the parameters $\sigma_i^{'}$, $\mathrm{r_i}$ $\mathrm{PID_i}$, $\mathrm{PWD_i}$, W_j and test C_i. Reedy deems the adversaries can't correct credentials. In the proof b, Reedy consider that $\mathrm{Q_j}$ is unique for each S_j. Therefore, $\mathcal{A}$ can't have the session key. The scheme is considered security.

But in the scheme, store the long-term private key h(ASK) of the RC in every user's smartcard. If A can obtain h(ASK), he/she will initiating an impersonation attack.

Firstly, $\mathcal{A}$ can capture $\{\mathrm{B_{ij}}, \mathrm{D_{ij}}, \alpha\}$ and $PID_i = B_{ij} \oplus h(\mathrm{SID_i} \parallel \alpha \parallel \mathrm{h(ASK)})$. Then he/she computes $Q_j = R_j \oplus PWD_k$ which the R_j is extracted from T_k and compute $\alpha^* = N_1^*P$, $B_{ij}^* = PID_i \oplus h(\mathrm{SID_j} \parallel \alpha^* \parallel \mathrm{h(ASK)})$, $\mathrm{D}_{ij}^* = h(\mathrm{PID_i} \parallel \mathrm{Q_j} \parallel \alpha^*)$ to S_j, D_{ij}^* is successful verification.

(2) Guessing attack means that as long as the adversaries can guess or determine the user's password, he can gain access to the machine or network and access any resources that the user can access. The key point is the vulnerability of the user's choice of password. If $\mathcal{A}$ can obtain the message on the smartcards like $\{X_j, \mathrm{V_i}, C_i, \ \mathrm{T_i}, \theta_\mathrm{i}, P, h(\cdot), h(\mathrm{ASK})\}$, then he/she get the biological factors $\mathrm{BIO_{i'}}$ of user. $\mathcal{A}$ can initiate a password guessing attack:
Firstly, $\mathcal{A}$ can compute $\sigma_{i'} = \mathrm{Re}p(\mathrm{BIO_{i'}}, \theta_i)$, $\mathrm{r_i} = \mathrm{V_i} \oplus \mathrm{h}(\sigma_{i'})$. And then $\mathcal{A}$ can guessing the ID, PW. Follow the steps to continue calculating the formula $PWD^* = h(\mathrm{PW} \parallel \mathrm{r_i})$, $\mathrm{W}_j^* = X_j \oplus PWD^*$. We can verify the $\mathrm{C}_i^* = h(\mathrm{ID}$ $rallelW_j^*) \overset{?}{=} C_i$.

Since the actual identity and password space is very limited space ($|D_{id}| \leq |D_{pw}| \leq 10^6$), attacks can be completed within a limited time. Through the establishment of the attack model and the analysis of the above scheme, we show that C_i is the key for adversaries. The C_i parameter is the correctness parameter for the login verification in the smartcard. If adversaries gets the password, they can choose a random number and calculate the $\mathrm{B_{ij}}, \mathrm{D_{ij}}$ for login the S_j. The scheme does not involve the complexity of the time space for offline guessing attack. So the solution is not safe for offline guessing attack.

The user is completely unaware of the circumstances which adversaries get messages from the channel. $\mathcal{A}$ only need derive Q_j with $\mathrm{h(ASK)}$. It is not difficult to find that the above attack is caused by the same security parameters from RC and S_j stored in the user's smartcards. It can be seen that the analysis of this agreement proves to be incomplete.

The user is completely unaware of the circumstances which adversary gets messages from the channel. $\mathcal{A}$ only need derive Q_j with $\mathrm{h(ASK)}$. It is not difficult to find that the above attack is caused by the same security parameters from RC and S_j stored in the user's smartcards. It can be seen that the analysis of this agreement proved to be incomplete.

5 Possible Fix

We put forward a solution that may figure out this problem in the light of the problems above. The critical points that the basis of the analysis above is whether the third factor of the first two factors is known to be reliability. Three factors synthesize into parameter to ensure the security of verification. We mainly modify the registration phase and the login phase. The login phase can be executed as following.

U_i chooses ID_i and PW_i. Meanwhile, users need generate random number $r_i \in Z_p^*$ and compute $PID_i = h(\mathrm{ID_i} \parallel \mathrm{r_i}), \mathrm{PWD_i} = h(\mathrm{PW_i} \parallel \mathrm{r_i})$ and send a request messages $\{PID_i, \mathrm{PWD_i}\}$

RC verifies the whether a registered user and computes $\mathrm{Q_j} = h(\mathrm{PID_i} \parallel \mathrm{K_j})$, $\mathrm{R_j} = \mathrm{Q_j} \oplus \mathrm{PWD_i}$.

Finally, RC compute a random number IDR_i reserves $\{\mathrm{SID_i}, \mathrm{R_j}, IDR_\mathrm{i}\}$ in $\mathrm{T_i}$ table and $\{PID_i, \mathrm{C_i}, \mathrm{T_R}= 1\}$ in T_c table where $\mathrm{T_R} = 1$ means U_i registered initially and is in active state. RC computes $W_j = h(\mathrm{PID_i} \parallel \mathrm{USK})$ and personalizes $\{W_j, \mathrm{T_i}, \mathrm{h(ASK)} \oplus IDR_\mathrm{i}\}$ into the smartcards to be delivered to U_i.

U_i scans his/her BIO_i at the provided sensor with card reading machine, and computes, $(\sigma_\mathrm{i}, \theta_\mathrm{i}) = \mathrm{Gen(BIO_i)}$, $\mathrm{V_i} = \mathrm{r_i} \oplus \mathrm{h}(\sigma_\mathrm{i})$, $C_i = \mathrm{h}(\mathrm{PID_i} \parallel PWD_i \parallel \sigma_i \parallel \theta_i)$, U_i stores $\{C_i, \mathrm{V_i}, \theta_\mathrm{i}\}$ on smartcards. Therefore, the smartcards finally contains $\{W_j, \mathrm{V_i}, C_i, \mathrm{T_i}, \theta_\mathrm{i}, P, h(\cdot), h(\mathrm{ASK})\}$.

Next, login phase is executing as following.

Smartcards compute $\sigma_i' = \mathrm{Re}p(\mathrm{BIO}_i', \theta_i), \mathrm{r_i} = \mathrm{V_i} \oplus \mathrm{h}(\sigma_i'), \mathrm{PID_i} = \mathrm{h}(\mathrm{ID_i} \parallel \mathrm{r_i})$, $\mathrm{PWD_i} = h(\mathrm{PW_i} \parallel \mathrm{r_i})$. In particularity, we need proving the parameters $C_i \overset{?}{=} \mathrm{h}(\mathrm{PID_i} \parallel PWD_i \parallel \sigma_i \parallel \theta_i)$. Finally, smartcards need verify whether the parameter are correct. If the value doesn't correspond, the login request is terminated.

User chooses the server S_j by assessing the list $\mathrm{T_i}$ and extract $\mathrm{R_j}$ and IDR_i at the same time. User compute $\mathrm{Q_j} = \mathrm{R_j} \oplus \mathrm{PWD_i}$. Smartcards generate random number $\mathrm{N_1} \in Z_p^*$ and compute $B_{ij} = PID_i \parallel IDR_\mathrm{i} \oplus h(\mathrm{SID_i} \parallel \alpha \parallel (\mathrm{h(ASK)} \oplus IDR_\mathrm{i}))$, $\mathrm{D_{ij}} = \mathrm{h}(\mathrm{PID_i} \parallel Q_i \parallel \alpha)$, $\alpha = N_1 P$. Smartcard send out the login request include $\{B_{ij}, \mathrm{D_{ij}}, \alpha\}$ by public channel.

In Mutually Authenticated Key Agreement phase, S_j inquiry the number IDR_i, and then compute $PID_i \parallel IDR_\mathrm{i} = B_{ij} \oplus h(\mathrm{SID_i} \parallel \alpha \parallel \mathrm{h(ASK)} \oplus IDR_\mathrm{i})$ and compute the parameter PID_i, $\mathrm{Q_j} = h(\mathrm{PID_i} \parallel \mathrm{K_j})$ when receive the login request. Afterwards, S_j authenticates U_i only if $\mathrm{D_{ij}} \overset{?}{=} \mathrm{h}(\mathrm{PID_i} \parallel Q_i \parallel \alpha)$ matching the condition. Otherwise the process terminates.

6 Conclusions

In this paper, we demonstrate that Reedy *et al.'s* scheme can't withstand some common attacks. More concretely, we analysis the Reedy's proof on the basis of the Wang *et al.* and Huang *et al.*'s [9] rigorous security model. Unfortunately, we find that Reedy *et al.'s* scheme can't be secure against guessing attack and impersonation attack with limited domain offline passwords. Next, we propose the improved scheme to overcome their scheme's flaws. The proposed improved scheme can overcome the flaws of the Reedy *et al.'s* schemes and be more practically and secure.

Acknowledgments. The work was supported in part by the National Natural Science Foundation of China under Grants 61862052 and the Science and Technology Foundation of Qinghai under Grants 2019-ZJ-7065.

References

1. Reddy, A.G., Yoon, E.J., Das, A.K., et al.: Design of mutually authenticated key agreement scheme resistant to impersonation attacks for multi-server environment. IEEE Access **PP**(99), 1 (2017)
2. Wang, D., Wang, P.: Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secur. Comput. **15**(4), 708–722 (2018)
3. He, D., Tian, M., Chen, J.: Insecurity of an efficient certificateless aggregate signature with constant pairing computations. Inf. Sci. **268**(2), 458–462 (2014)
4. Mishra, D., Das, A.K., Mukhopadhyay, S.: A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Syst. Appl. **41**(18), 8129–8143 (2014)
5. Yoon, E.J.: Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J. Supercomput. **63**(1), 235–255 (2013)
6. Dolev, D., Yao, A.C.: On the security of public key schemes. IEEE Trans. Inf. Theory **29**(2), 198–208 (1981)
7. Wang, D., Wang, P.: On the anonymity of two-factor authentication schemes for wireless sensor networks. Comput. Netw. **73**(C), 41–57 (2014)
8. Wang, D., He, D., Wang, P., et al.: Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans. Dependable Secur. Comput. **12** (4), 428–442 (2015)
9. Huang, X., Xiang, Y., Chonka, A., et al.: A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans. Parallel Distrib. Syst. **22**(8), 1390–1397 (2011)
10. Veyrat-Charvillon, N., Standaert, F.-X.: Generic side-channel distinguishers: improvements and limitations. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 354–372. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_20
11. Wang, D., Zhang, Z., Wang, P., et al.: Targeted online password guessing: an underestimated threat. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 1242–1254. ACM (2016)

12. Wang, D., Wang, P.: On the implications of Zipf's law in passwords. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9878, pp. 111–131. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45744-4_6
13. Boyd, C., Mathuria, A.: Schemes for authentication and key establishment. In: Schemes for Authentication and Key Establishment, pp. 3215–3230. Springer (2003)
14. He, D., Wang, D.: Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst. J. **9**(3), 816–823 (2015)
15. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(24), 770–772 (1981)
16. Tsaur, W.-J.: A flexible user authentication scheme for multi-server internet services. In: Lorenz, P. (ed.) ICN 2001. LNCS, vol. 2093, pp. 174–183. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-47728-4_18
17. Kim, H., Jeon, W., Lee, K., Lee, Y., Won, D.: Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme. In: Murgante, B., Gervasi, O., Misra, S., Nedjah, N., Rocha, Ana Maria A.C., Taniar, D., Apduhan, Bernady O. (eds.) ICCSA 2012. LNCS, vol. 7335, pp. 391–406. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31137-6_30
18. Chuang, M.C., Chen, M.C.: An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Int. J. Netw. Secur. **18**(5), 997–1000 (2014)
19. Tsai, J.L., Lo, N.W.: A new password-based multi-server authentication scheme robust to password guessing attacks. Wirel. Pers. Commun. **71**(3), 1977–1988 (2013)
20. Chang, C.C., Lee, J.S.: An efficient and secure multi-server password authentication scheme using smart cards. In: International Conference on Cyberworlds (2004)
21. He, D.: Security flaws in a smart card based authentication scheme for multi-server environment. Wirel. Pers. Commun. **70**(1), 323–329 (2013)
22. Juang, W.S.: Efficient multi-server password authenticated key agreement using smart cards. IEEE Trans. Consum. Electron. **50**(1), 251–255 (2004)
23. Jiang, P., Wen, Q., et al.: An anonymous and efficient remote biometrics user authentication scheme in a multi server environment. Front. Comput. Sci. **9**(1), 142–156 (2015)
24. Odelu, V., Das, A.K., Goswami, A.: A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans. Inf. Forensics Secur. **10**(9), 1953–1966 (2015)
25. Wan, T., Liu, Z.X., Ma, J.F.: Authentication and key agreement protocol for multi-server architecture. J. Comput. Res. Dev. **53**(11), 2446–2453 (2016)
26. Khan, M.K., Kim, S.K., Alghathbar, K.: Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Comput. Commun. **34**(3), 305–309 (2011)
27. Shivraj, V.L., Rajan, M.A., Singh, M., et al.: One time password authentication scheme based on elliptic curves for Internet of Things (IoT) (2015)
28. Qi, X., Na, D., Wong, D.S., et al.: Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. Int. J. Commun. Syst. **29**(3), 478–487 (2016)
29. Zhong, J., Liu, Z., Xu, J.: Analysis and improvement of an efficient controlled quantum secure direct communication and authentication protocol. Comput. Mater. Contin. **57**(3), 621–633 (2018)
30. Fong Cheang, C., Wang, Y., Cai, Z., Xu, G.: Multi-VMs intrusion detection for cloud security using Dempster-Shafer theory. Comput. Mater. Contin. **57**(2), 297–306 (2018)