International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.11-20
http://dx.doi.org/10.14257/ijsia.2014.8.5.02

Weakness Cryptanalysis of Liao's Scheme and Improved Remote User Authentication Scheme for Mobile Device

Hie Do Kim[1] and Kwang Cheul Shin[2*]

[1]Department of Military Science(Naval Information Communication), Gang Neung Yeong Dong College, #357, Gong Je Ro, Gang Neung -Si, Kang Won-Do, 210-792, South Korea
[2]Division of Industrial Management Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea
[1]skcskc12@sungkyul.ac.kr, [2]hdkim@gyc.ac.kr

Abstract

Liao et al.'s has recently announced the suitable authentication scheme for mobile device environment, which can authenticate remote users by using QR code. However, Liao et al.'s scheme cannot satisfy several important security requirements. The biggest drawback of Liao et al.'s scheme is that it is not able to satisfy the mutual authentication between remote users and SP since it is vulnerable to eavesdropping, man-in-the-middle, theft and loss of mobile devices and forgery attack.

This paper aims to analyze the problems of Liao, et al., scheme and propose a safe authentication scheme using password based QR code that has fixed the aforementioned vulnerabilities.

Keywords: *mobile device, authentication scheme, QR Code, impersonation attack*

1. Introduction

The user authentication is essential for e-commerce and m-commerce in terms of accessing important resources. The user authentication protocol registers information that will allow users to confirm their identity from the servers providing services in advance. It also let users use services provided by the servers anytime and anywhere when they want to use services.

Recently, mobile devices are providing portability along with various functions such as PC, camera, recorder, *etc.*, Due to the fact that it has become easy for anyone to produce and distribute mobile contents in an open environment, the likelihood of security threat is on the rise. QR (Quick Response) code based OTP (One Time Password) authentication protocol [1], eliminates the usage of the password verification table and also is a cost effective solution since most internet users already have mobile phones.

There are many advantages to use the QR code [2] in mobile phones such as Omni-direction readability and error correction capability [3]. In 2010, Liao, *et al.*, proposed a user authentication scheme based on QR Code in which users may send a login request message without using their password [4].

Liao, *et al.*, scheme does not utilize the password table and realize the cost efficiency by using the decryption and encryption algorithm and the hash function [5-7].

However, the reasons why Liao, *et al.*, scheme cannot provide a perfect mutual authentication between users and SP (Service Provider) are as follows.

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

First, third parties are able to disguise themselves by tapping messages at the login phase for server access. Second, third parties are able to extract and use the information saved in mobile devices as though they are legitimate users after they stole and owned mobile devices.

Third, SP does not have any function to authenticate whether a message received from a user at the login phase is a legitimate message sent by users. Fourth, users do not have a function to verify whether third parties are performing the role of a server in disguise of SP. Fifth, for such results as mentioned, a safe mutual authentication between users and SP is lacking.

In this paper, we propose a safe mutual authentication scheme in mobile device environment, which complements the aforementioned drawbacks.

The proposed method is based on ownership (mobile device) and knowledge (password) factors. It combines the above factors challenge response methods without requiring any time synchronization or OTP between user's mobile phone and service provider's server for authentication purpose [8].

The rest of the paper is organized as follows section 2, 3 presents literature review, section 4 describes the motivation for the work and the contributions of this paper. Section 5 discusses the proposed scheme and its details. Section 6 presents the analysis of the scheme and finally Section 7 presents the conclusions.

2. Review of Liao, *et al.*,'s Authentication Scheme

This section reviews a user authentication scheme proposed by Liao, *et al.,* The scheme participants include a remote user and a service provider. For simplicity, we denote the remote user A by U_A, and the service provider by SP.

The scheme assumes that each authorized user can request service from SP with granted access rights. In addition, each user hold a mobile phone with embedded camera, therefore he can take a picture of the QR code image and then decode it. Liao, *et al.,* scheme consists of two phases: registration phase and authentication phase.

The registration phase is performed only once per user when a new user registers itself with the service provider. The authentication phase is carried out whenever a user wants to gain access to the service provider. Before the registration phase is performed for the first time, the service provider SP decides on the following system parameters: a one-way hash function h and a cryptographic key s. The key s is kept securely the service provider. The notation is employed throughout this paper.

Table 1. Notation and Description

U_A	User A
ID_A	Identifier of User A
pwa	Password of User A
$h(\cdot)$	An one-way hash function
$E_{QR}(\cdot)$	A function that encodes data into QR code image
$D_{QR}(\cdot)$	A function that decodes the QR code image captured in an embedded camera device
s	SP’'s long term secret key
*T*1, *T*2	Time stamps
$\|$	Concatenation operation
$\oplus$	XOR operation

A. Registration Phase

Assume that a U_A with an embedded camera mobile device wants to join the system. Then, SP and U_A carry out the following registration procedures.
step 1 : U_A sends his identity ID_A to SP.
step 2 : SP computes
$X_A = h(ID_A \parallel s)$
and sends X_A to U_A's mobile device via a secure channel.
step 3 : U_A's mobile device stores X_A as the long term secret key.

B. Verification Phase

The verification phase is shown as follows.
step 1 : U_A sends ID_A and T1 to SP, where T1 is the time stamp attached by the User A.
step 2 : SP examines whether the time stamp T1 is correct.
If it is invalid, then rejects it. Otherwise, he chooses a random number r, computes
$X_A = h(ID_A \parallel s)$, and $\alpha = r \oplus X_A$
and then sends $E_{QR}(\alpha)$, $h(r \parallel T1 \parallel T2)$, and T2 to U_A, where T2 is the time stamp attached by the SP.
step 3 : User A examines whether the time stamp T2 is correct. If it is invalid, then rejects it. Otherwise, he derives r by computing
$r = D_{QR}(E_{QR}(\alpha)) \oplus X_A$
with his embedded camera devices. After that, U_A examines whether $h(r \parallel T1 \parallel T2)$ is correct. If holds, then U_A sends $h(r \parallel T2 \parallel T3)$ and T3 to SP.
step 4 : SP examines whether the time stamp T3 is correct. If it is invalid, then rejects it. Otherwise, he checks whether $h(r \parallel T2 \parallel T3)$ is correct. If holds, then SP is convinced that U_A is validated. Otherwise, the request is rejected.

3. Security Analysis of Liao et al.'s Scheme

In this section, we will discuss the security drawbacks in Liao, *et al.*,'s QR code based remote user authentication Scheme. Since the message in login phase and verification phase are transmitted via an insecure channel, we assume that the third parties (attacker) can control the insecure channel.

3.1. Man-in-the-middle Attack

According to Sun, *et al.*,'s article(2009), the man-in-the-middle attack is defined as a form of active wiretapping attacks in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association [7].

Attackers are able to tap and read messages exchanged between U_A and SP. U_A is vulnerable to the main-in-the-middle attack since SP generates an authentication information $\alpha(r \oplus X_A)$ as to U_A without any verification procedure when U_A sends $<ID_A \parallel T1>$ to SP.

3.2. Stolen Attack

Assuming that U_A lost a mobile device or a third parties stole a mobile device, third parties would be able to disguise themselves as a legitimate U_A by extracting the confidential information (X_A) saved in a mobile device.

Third parties find out the random number r generated by SP by decoding α through the decoder of a mobile device. Third parties own the confidential information X_A and r of a legitimate U_A. Then, they generate h(r1 ∥ T2 ∥ T3) and T3 in accordance with the following scenario and pass the authentication process by sending them to SP.

3.3. User Spoofing Attack

Assuming that third parties extract the secret value X_A from the mobile device of a legitimate user, which they acquired through stolen attack, these third parties attempt to obtain an authentication after sending the log-in message <ID_A ∥ T1> to SP by disguising themselves as legitimate users. SP would verify the login message after receiving <ID_A ∥ T1>.

Next, SP would generate and send EQR(α), h(r ∥ T1 ∥ T2) and T2 to third parties. Third parties extract r by computing h(DQR(EQR(α)). Then, third parties obtain the time stamp T3 and send h(r ∥ T2 ∥ T3) to SP to get an approval as though they are legitimate users.

3.4. Server Spoofing Attack

Third parties that are in disguise of a server compute the following after receiving <ID_A ∥ T1> from a legitimate U_A.

They select a random number r' and generate a random X_A'. Then, they calculate and send decode(EQR(α')), h(r' ∥ T1 ∥ T2) on α' from α'=r'⊕X_A' to U_A. U_A calculates r'(=α'⊕X_A') by using the confidential information X_A as regarding it as a message sent from a legitimate SP. X_A' is randomly generated by third parties; thus, the value of r' must be trusted. U_A authenticates third parties as SP since it trusts r' generated by third parties and generate and sends h(r' ∥ T2 ∥ T3) and T3 to SP.

4. Description of the Proposed Authentication Scheme

In this section we proposed a password-based and use of the deployed widespread QR code in order to remote user authentication scheme which enhances on previous scheme.

The convenient integration of the web based application and the mobile devices usage makes our scheme more practical.

The proposed scheme involves two parties: a service provider (SP for short) and remote users. Each authorized user can request service from SP with the granted access rights. In addition, each user hold a mobile phone with embedded camera, therefore he can take a picture of the

QR code image and then decode it. Our scheme is divided into four phases: Registration, Login, Verification and Password change phases.

As mentioned earlier, our scheme improves over Liao et al.'s scheme in five ways:

(1) it does not require synchronized clocks between in the network by using password.

(2) it can withstand the password guessing attack even though the attacker has stolen some user's mobile device or gained access to it and extracted the secret values stored in it,

(3) it is secure against a service provider impersonation attack and a user impersonation attack, man in the middle attack and stolen attack.

(4) SP confirms whether U_A의 is a legitimate user by verifying the login messages of U_A, whereas U_A는 authenticates SP by verifying whether X_A can be generated. In this way, 2-way communication can be implemented.

(5) The application module of a mobile device is operated only when password is entered. Therefore, it cannot be disguised even when it is stolen by third parties. Also, it allows for users to change the password whenever necessary.

There are four phases in our scheme including registration, login, authentication and password change phase. Detailed steps of these phases of the proposed scheme are described as follows.

A. Registration Phase

Before the U_A logins to the SP, the user needs to perform the following steps.
Step 1: Firstly, U_A send the U_A's ID, ID_A to SP via a secure channel.
Step 2: Next, SP compute X_A as follow:
X_A=h (ID_A ∥ s), Where s is a secret key generated by the SP.
Step 3: Lastly, SP sends X_A to U_A via a secure channel.
Step 4: U_A chooses a password pwa and compute hpwa=h(pwa ∥ ID_A), A=h(X_A), and B=hpwa ⊕A on the mobile device.
Step 5: U_A's mobile device stores B as the long-term secret key.

B. Login Phase

Whenever the U_A wants to login to the remote SP, he/she must perform the following steps.
Step 1: When U_A enters ID_A and pwa, a mobile device confirms whether it is a legitimate user of a mobile device as the module application calculates the following. In other words, it verifies whether the password has been correctly entered.
A=B⊕h(ID_A ∥ pwa)=h(h(ID_A ∥ s)
B'=h(pwa ∥ ID_A)⊕B
A=?B⊕h(pwa ∥ ID_A), accept or reject.
step 2: Calculate the following if it is a legitimate owner of a mobile device in step 1.
random number ri, time stamp T1 select
Ci=h(ID_A ∥ A ∥ T1)⊕ri, Where T1 is the time stamp attached by the U_A.
step 3 : At last, U_A sends the message ID_A, Ci, T1 to SP.

C. Authentication Phase

After SP receiving the login message (ID_A, Ci, T1), Sp perform the following steps to mutual authentication.
Step 1: ID_A, T1 check. Reject or accept. SP examines whether the time stamp T1 is correct. If it is invalid, then reject it. Otherwise, he computes X_A and ri.
X_A=h(ID_A ∥ s), A=h(X_A).
ri=Ci⊕h(ID_A ∥ h(X_A) ∥ T1)
After compute X_A and ri, SP first verifies whether Ci=? h(ID_A ∥ h(X_A) ∥ T1). If it holds, SP believes that U_A is authenticated and then computes the following message to provide mutual authentication between SP and U_A.
Step 2: SP computes the follows:
α=h(ri⊕h(X_A) ∥ T2), Where T2 is the time stamp attached by the SP, compute E_{QR}(α).
Step 3: SP sends the message E_{QR}(α), T2 to U_A.
Step 5: U_A examines whether the time stamp T2 is correct. If it is invalid, then reject it. Otherwise, U_A derives α by computing D_{QR}(E_{QR}(α))=h(ri⊕h(X_A) ∥ T2) with his embedded camera device.

After that, U_A examines whether $h(ri \oplus h(X_A) \parallel T2)$ is correct. If hold, then U_A is convinced that SP is validated. Otherwise, the request is rejecting.

D. Password Change Phase

According to the above-mentioned requirements, U_A can freely change the password, pwa, to a new password, pwa'. It can be finished without the help of the SP.
The steps of changing password are as follows.
step 1: Calculate h(A) after operating the password modification application by entering password.
$B=B \oplus h(pwa \parallel ID_A)=h(A)$
Step 2: A mobile device calculates the following when a new password pwa' is entered.
$B'=h(A) \oplus h(pwa' \parallel ID_A)$
Step 3: Replace B with B'

5. Security Analysis of the Proposed Scheme

We now analyze the security of the proposed scheme, considering password guessing attack, impersonation attacks, stolen mobile device attacks, man-in-the middle attack and providing proper mutual authentication.

In the Table 2-3, we compare the proposed scheme with previously published Liao et al.'s scheme.

5.1. Resist Stolen Mobile Device Attack

From Liao, *et al.*, scheme, we have seen that a mobile device was used improperly when a legitimate user lost it or a third party acquired it. Third parties send $<ID_A \parallel T1>$ by operating the remote authentication module in a mobile device of a legitimate user. SP that received a message does not have a function to verify whether it is a message sent from a legitimate user. SP calculates $\alpha = r \oplus X_A$ by selecting a random number r and sends it along with $h(r \parallel T1 \parallel T2)$ and T2 to third parties after conducting $encode(E_{QR}(\alpha))$ on α.

Third parties own a mobile device of a legitimate user; therefore, they get an authentication by extracting r by means of the saved X_A and sending $h(r \parallel T2 \parallel T3)$ and T3 to SP.

However, in the proposed paper, third parties are not able to find pwa of legitimate users and the confidential information X_A of SP even after they picked up a mobile device. The information saved in a mobile device is $B(=hpwa \oplus h(X_A))$; thus, it is not possible to calculate $h(X_A)$ without knowing the accurate password of users. Furthermore, X_A calculates B with the hash value; thus, it is safe in terms of loss and theft of a mobile device.

5.2. Resist Man-in-the Middle Attack

In our scheme, the remote server only has to maintain secret information, s, without storing the password tables. An attack may try to derive X_A from the intercepted messages ID_A, Ci, T1. But it is computationally infeasible because of the property of the one-way hashing function.

If the illegal user intercepts the message ID_A, Ci, T1 from user i and try to masquerade as the remote server. It is impossible for the user to compute the message Ci unless he/she knows the secret information X_A and U_A's password, pwa.

An illegal user may try to fabricate fake request login messages to cheat the remote server into believing it is a legal remote login request (masquerade attack) in the login phase. It does not work unless he/she could modify Ci correctly.

Table 2. Comparison of Security Properties between Our Scheme and Liao, *et al.,* Scheme

	Liao, *et al.*,'s	Our proposed scheme
Password guessing attack	N/A	resistance
Impersonation attack	non-resistance	resistance
Replay attack	resistance	resistance
Man-in-the middle attack	non-resistance	resistance
Stolen attack	non-resistance	resistance
Password change	N/A	possible
Proper mutual authentication	non-proper	proper

Table 3. Comparison of Computation and Communication between Our Scheme and Liao, *et al.,* Scheme

	Liao, *et al.*,'s	Our proposed scheme
Registration	1Th	3Th
Login	1Th	3Th
Authentication	4Th	4Th
Password change	x	2Th
Communication	3-way	2-way

5.3. Resist Impersonation Attacks

Impersonation attack is about an attacker who obtains a legitimate right by disguising him/herself as a legitimate user or SP after participating in the protocol.

Our scheme can resist two impersonation attacks, which are a service provider impersonation attack and a user impersonation attack.

An attacker cannot extract the confidential information X_A within a mobile device. Moreover, he/she can no longer forge a valid response message <α> or a valid login request message <Ci> although an attacker obtains the information (*i.e.*, B) saved in a mobile device. A legitimate user utilizes hpwa=h(pwa$\oplus$$ID_A$) in the registration phase; thus, insiders of SP or external third parties are not able to find it out. In order for a third party to disguise him/herself as an attacker, he/she should know the confidential information X_A of SP.

However, it is saved along with user password in the form of B=hwpi$\oplus$A in a mobile device after SP conducted A=h(X_A) on X_A=h(ID_A∥ s) by the harsh value. In other words, it is safe since B cannot be extracted from X_A. In addition, third parties should be able to extract X_A in order to disguise themselves as a server. If they are able to extract X_A, then they will be able to calculate a random number ri and generate legitimate α. However, X_A는 is calculated by the hash value h(X_A) and saved as the value of B in a mobile device. Thus, it is safe for user/server spoofing attacks since it is not able to generate legitimate α.

5.4. Proper Mutual Authentication

The proposed scheme can provide proper mutual authentication. U_A sends the message(ID_A, Ci, T1) to SP. SP first check the validity of U_A's ID, ID_A, time stamp T1, then compute $X_A=h(ID_A \| s)$, $A=h(X_A)$ and $ri=Ci\oplus h(ID_A \| h(X_A) \| T1)$, compare the compute $h(ID_A \oplus h(X_A) \oplus T1)$ value with the receiving Ci value. If they are equal, SP is a valid U_A. U_A believes that SP is able to calculate A easily as long as it is legitimate. U_A authenticates that SP is legitimate when the value of α matches the value calculated by U_A after A decoded the value of $E_{QR}(\alpha)$ by the value that was hashed as a result of connecting the secret key s of SP to ID_A.

5.5. Free Password Change

If the legal user lost his/her mobile device, it is difficult for any adversary to derive or change the password because he/she cannot pass the password verification. The illegal request will be rejected.

6. Performance Comparisons and Functionality Analysis

In this section, we evaluate the performance and functionality of our proposed scheme and make comparisons with Liao, *et al.,* scheme. To analyze the computational complexity of the schemes, we define the notation Th as the time complexity for hashing function. Because exclusion-OR operation requires very few computations, it is usually negligible considering its computational cost.

Table 3 shows the Performance Comparison of our scheme and Liao, *et al.,* scheme. As you can see Table 3, In Liao, *et al.,* scheme, the computation cost of registration phase, login phase, and authentication phase are 1Th, 1Th and 4Th, respectively. In our improved scheme, the computation cost of registration phase, login phase, and authentication phase are 3Th, 3Th and 4Th, respectively. But our scheme can achieve the proper mutual authentication and can resist man-in-the middle attack, stolen attack, impersonation attack *etc.,* in Table 2.

7. Conclusion

This paper reviewed and analyzed the authentication scheme of Liao et al. that was based on QR code. As a result of the analysis, it was found that Liao, *et al.,* authentication scheme was vulnerable to several attacks of a third party. In conclusion, Liao, *et al.,* authentication scheme does not provide a safe authentication between users and SP.

This paper proposed an enhanced authentication scheme using password based QR code for prevention of theft and spoofing attack of mobile devices and safe mutual authentication.

The differentiated point of the proposed paper from Liao, *et al.*, authentication scheme is that users hash their password and the confidential information X_A of SP in the registration phase and save them in a mobile device and consequently, users are able to select and renew a random password. Therefore, it can resist spoofing attacks, loss and theft associated attacks and man-in-the-middle attacks toward users and SP and also reduce the communication traffic for mutual authentication from three times to two times.

References

[1] K. C. Liao and W.-H. Lee, "A Novel User Authentication Scheme Based on QR-Code", Journal of Networks, vol. 5, no. 8, **(2010)** August 8, pp. 937-941.

[2] A. S. Narayanan, "QR Codes and Security Solutions", International Journal of Computer Science and Telecommunications, vol. 3, Issue 7, **(2012)** July.

[3] N. Harini and Dr. T. R Padmanabhan, "A New Two Factor Authentication Scheme Using QR-Code", International of Engineering and Technology, vol. 5, no. 2, **(2013)** May, pp. 1087-1094.

[4] J.-S. Wang, F.-Y. Yang and I. Paik, "A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices", International Journal of Computer Science and Network Security, vol. 11, no. 6, **(2011),** pp. 12-19.

[5] Y. Lee, J. Kim, W. Jeon and D. Won. "Design of a Simple User Authentication Scheme Using QR-Code for Mobile Device", Information Technology Convergence, Secure and Trust Computing, and Data Management Lecture Notes in Electrical Engineering, vol. 180, **(2012),** pp. 241-247.

[6] T. Falas and H. Kashani, "Two-Dimensional Bar-code Decoding with Camera-Equipped Mobile Phones," Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, **(2007)** March 19-23, pp. 597-600.

[7] X. Li, J.-W. Niu, J. Ma, W.-D. Wang and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 34, **(2011)** pp. 73-79.

[8] "OTP Authenticators", Retrieved, **(2009)** November, from: http://www.safenetinc.com/Products /Data_Protection/Multi-Factor_Authentication/OTP_Authenticators.aspx.

[9] M. Kim, B. Lee, S. Kim and D. Won, "Weaknesses and Improvements of a One-time Password Authentication Scheme", International Journal of Future Generation Communication and Networking, vol. 2, no. 4, **(2009)** December.

[10] W. C. Kuo, Y. C. Lee, "Attack and improvement on the one-time password authentication protocol against theft attacks", Proc. of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, **(2007)** August, pp. 19-22.

Authors

Hie Do Kim, Department of Military Science (Naval Information Communication), Gang Neung Yeong Dong College, #357, Gong Je Ro, Gang Neung -Si, Kang Won-Do, 210-792, South Korea, hdkim@gyc.ac.kr Education & Work experience: 2007, Ph.D. degree in Information and Communication Security Engineering, Sungkyunkwan University. Currently: Professor in Dept. of Military Science, Gang Neung Yeong Dong College. Tel: 82-033-610-0316.

Kwang Cheul Shin, Division of Industrial Management Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, skcskc12@sungkyul.edu education & Work experience: 2003, Ph.D. degree in Information and Communication Engineering, Sungkyunkwan University. Currently : Professor in Dept. of Industrial Management Engineering, Sungkyul University. Tel: 82-031-467-8916.