A Two Factor User Authentication Scheme for Medical Registration Platform

Di Liu
China United Network Communications Group Company Limited Postdoctoral Workstation, Beijing, China

Zhi-Jiang Zhang
China United Network Communications Group Company Limited, Beijing, China

Ni Zhang
China Unicom Research Institute, Beijing, China

***Abstract*—This paper proposes a two factors user authentication scheme for Beijing medical registration platform, in order to protect user personal information on the platform. This scheme overcomes the shortcoming that there is no authentication process during user log on the platform. The reason that builds a two factor authentication scheme for the system is that this way is safer than traditional single factor user authentication methods, e.g., typing username and password, or biometric authentication. For the proposed two factor user authentication scheme, we give three different solutions, including SMS-OTP solution, NFC-enabled device solution, and biometrics based solution. Finally, an optimal solution is chosen as the formal one to the platform through comparisons at a different angle among these three solutions.**

Keywords-two factor authentication; SMS-OTP; NFC; biometrics

I. INTRODUCTION

Many public service infrastructures have been established in Beijing recently, e.g., Beijing public transportation inquiry platform, Beijing social security card platform, Beijing medical registration platform, etc. Especially, the Beijing medical registration platform [1] is convenient for patients to make pre-registration on web, instead of queuing and waiting for a long time for medical registration when they go to hospital very early. When a user uses the platform at the first time, he or she is required to make a new user registration, which the user should input his or her basic personal information, such as real name, gender, age, mobile phone number, ID card number, etc. After the user fills in all the information, an information confirmation is conducted by sending a SMS with confirmation code to user's mobile phone which just register. Then, the user inputs the code just received, and click confirmation button. The registration process has been completed successfully.

However, if user wants to log on, the only information they inputs are his or her name, and ID card number, without any security measurements, e.g., typing password. Once user's ID card gets lost, is stolen, or attacker remembers the contents of ID card. The attackers can easily log on by user's ID, fetching user's privacy information, misusing, i.e., doing some illegal or bad operations on user accounts. To avoid this, a user authentication process should be considered when users log on. Straightforwardly, a typing username and password authentication mechanism can be added on the platform. But this is not reasonable that attacker can easily use brute-force way, or dictionary attack [2] way to guess the password. In addition, biometrics [3], e.g., face [4], voice [5], palmprint [6], finger vein [7], or iris [8] authentication seems to be a good way to protect user privacy information. However, due to statistical characteristic of biometrics, performance of this way is not steady. Thus a better authentication way should be considered. Multiple factor authentication [13] provides a significant increase in security. It not only requires user input username and password, but also requires user verify using other channel, e.g., using SMS with OTP code by mobile phone, or smart card to make a double check for user's identity.

To make up the drawback of the current medical registration platform, a two factor user authentication scheme is proposed in this paper, which enables to keep user privacy information away from the attackers. No longer will users encounter the case that an un-secured password provides enough information to a hacker to allow a breach in security.

The rest of this paper is organized as follows. Section II discusses current user authentication schemes, such as username-password way, and biometrics. Section III presents the proposed two factor authentication method. Three two factor user authentication solutions in detail for the medical registration platform, namely SMS-OTP, NFC-enabled device, and biometrics based solution are presented in turn. Then section IV makes a comparison at a different angle among these three solutions, and choose optimal one as formal two factor user authentication scheme for the platform. Finally, a conclusion will be conducted at last.

II. RELATE WORKS

This section discusses traditional authentication schemes, such as username-password way and biometrics way, and shows drawbacks of these current ways.

A. Traditional username and password way

The most prevalent authentication type in use today is single factor authentication. In short, single factor authentication is a combination between user basic username and password. The single factor in this case is something user knows, i.e., password. Most business networks and most internet sites use basic username/password combination to allow access to secured or private resources. However, the existing way to log in by password has some drawbacks:

1. For convenience, user usually uses a rather simple password, which faces a high security risk.

2. In order to enhance security, user sets up a complicated password. Maybe user writes down some visible places, e.g., papers in the office table. This is unsafe that imposter can get the password without any technical methods.

Published by Atlantis Press, Paris, France.

3. Traditional password is not difficult to divulge as imposter fetches user's the date of birth, and ID card number. One way is that they use dictionary attack to guess password.

4. Sometimes an account may be occupied by multiple persons at the same time. Yet the system can not get to know which time logs on by a genuine. This would give rise to a legal dispute once the account gets involved with any illegal operations.

B. Biometric authentication

Biometrics is a human identity detecting technique by authentication or identification algorithms with human being's biometric samples collected by sensors, e.g., human's face image, fingerprint, palmprint, finger vein, voice, iris, etc. Despite biometrics can be used for authentication, the sole use of biometrics still exists some drawbacks as follows.

1. The privacy of biometric samples still should be considered carefully. For example, attacker is likely to fetch user fingerprint from the cup user touched. For another example, a hidden camera will take a photo of user iris when he or she is unconscious.

2. Due to the statistical characteristic of biometric samples, it has intra-class fuzziness. The fuzziness is referred as to the case that the same person's biometric samples acquired by sensors have more or less difference among them under a variety of circumstances, e.g., different illustrations, places, angles, background conditions, etc.

3. Most of biometric template is not discrete, but a real vector obtained by certain signal processing algorithm in serial domain.

4. Biometric samples are subverted by a large amount of noises.

III. THE PROPOSED METHOD

In order to overcome challenges from attackers, a two factor user authentication scheme for the Beijing medical registration platform should be considered. Based on the practice of two factor authentication, three solutions are proposed as below.

A. SMS-OTP based solution

When users log on the Beijing medical registration platform, this solution requires users not only type their username and password, but also type another One Time Password (OTP) [9] received by SMS. This means the platform automatically send an OTP to registered mobile number when a user inputs both their username and password, and want to log on. The users finish logging on until user input the correct OTP from SMS to webpage of the Beijing medical registration platform. Note that the registered mobile phone number should be correlated with user's identity. This SMS-OTP can be viewed as an additional verification measure for traditional username-password user authentication.

The steps of SMS-OTP solution for medical registration platform are shown in the figure 1.

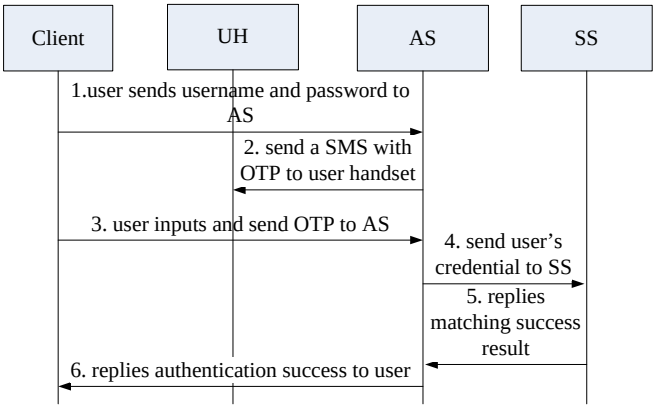

Figure 1. SMS-OTP solution

Step 1. User who wants to makes a request of logging on by using claimed id and password from Client on computer to Authentication Server (AS).

Step 2. AS send a SMS with OTP back to user's handset (UH).

Step 3. User inputs OTP on client, which sends this OTP to AS.

Step 4. AS receives user's credentials including username, password, OTP, etc, and sends them to Storage Sever (SS) which is a user database.

Step 5. If authentication matching is successful, SS replies authentication success message to AS.

Step 6. AS replies an authentication successful result to the client. The whole of user authentication procedure is finished.

There are two advantages in SMS-OTP solution:

1. This solution provides a secure two factor authentication scheme, protecting against hacker attacking, phishing [10], etc.

2. The solution has been widely accepted by many companies due to high security, especially the Beijing medical registration platform.

B. NFC-enabled device based solution

Another high secure two factor solution for the medical registration platform is to employ NFC-enabled mobile device. NFC [11] is a promising mobile identity-based technique widely employed on field of mobile banking, physical access, logical access, electronic ticketing, etc. NFC-enabled mobile phone can get close to a special POS terminal to verify mobile phone holder identity. Because user's identity is correlated with NFC-enabled mobile phone which user's identity credential are stored in the SE module of the NFC-enabled device. Once user inputs username and password, the system gives a prompt that uses NFC-enabled device for additional authentication procedure to user. The user puts the NFC-enabled device near to POS terminal device to accomplish the additional authentication.

The steps of NFC-enabled device based solution for medical registration platform are shown in the figure 2.

Step 1. User who wants to makes a request of logging on by using claimed id and password from Client on computer to AS.

Step 2. AS sends a message to user's handset, giving a prompt that makes a NFC authentication via POS terminal.

Step 3. The user uses NFC-enable device, e.g., NFC-based handset, get closed to the specific POS terminal, sending user's credential stored in SE of the handset to AS.

Step 4. AS receives user's credentials including username, password, NFC user information, etc, sending them to SS.

Step 5. If authentication matching is successful, SS replies authentication success message to AS.

Step 6. AS replies an authentication successful result to the client. The whole of NFC-enabled device based two factor user authentication procedure is finished.

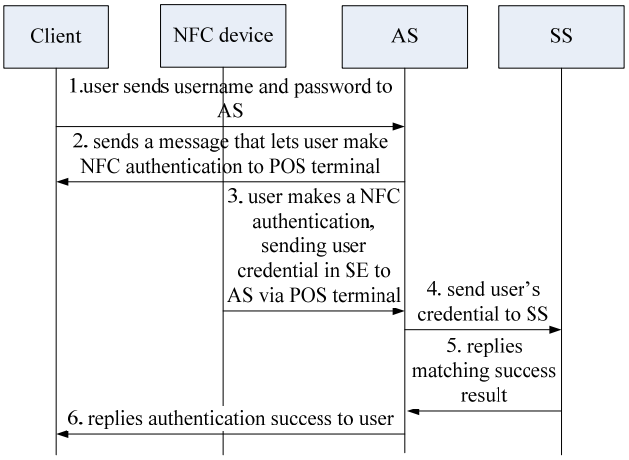

Figure 2. NFC-enabled device based solution

The advantage of NFC-enabled device-based solution is to protect against phishing, Man-in-the-Middle attack [12], and web browser attack.

C. Biomerics based solution

Biometrics detects user's identity by authentication or identification algorithms with human being's biometric samples collected by biometric sensors. That it incorporates within a multiple factor authentication scheme is a secure way.

The steps of biometrics based solution for medical registration platform are shown in the figure 3.

Step 1. User who wants to makes a request of logging on by using claimed id and password from Client on computer to AS.

Step 2. AS sends a message to user's handset, giving a prompt that provides a biometric sample to AS via biometric sensor. Note that the choice of biometric type is depend on factors of scenario, cost of the sensor, accuracy, etc. Not all biometric identifiers can be used for authentication. For face, it often requires capture enough clear face image. Noise, occlusion, or complex background all result in bad verification accuracy. For fingerprint, its authentication scheme is so sophisticated that it is widely used on computers. But it is an obstacle to integrate within fingerprint extraction sensor on all the phones with the consideration of cost. For palmprint, it is impossible to fasten the users' hands by phone, capturing a fine palmprint picture for user authentication. For voice, handset and computer can easily acquire users' voice biometrics by its mic without any extra cost consideration. Hence voice biometrics is a reasonable biometric way to make a user authentication on handset and computer, protecting user identity based information.

Step 3. The user uploads biometric sample via certain specific biometric sensor, e.g., handset mic, computer webcam, fingerprint reader etc to AS.

Step 4. AS receives user's credentials, including username, password, user's biometric sample, etc, sending them to SS.

Step 5. If both password and biometrics authentication matching are successful, SS replies authentication success message to AS.

Step 6. AS replies an authentication successful result to the client. The whole of biometrics based two factor user authentication procedure is finished.

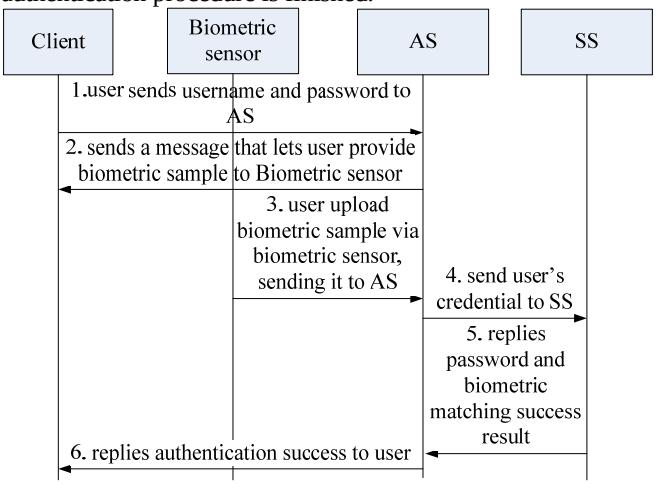

Figure 3. Biometric based solution

IV. DISCUSSION

TABLE I. A COMPAISON OF THREE TWO FACTOR AUTHENTICATION SOLUTIONS

Solutions	Accuracy	Acceptance	Novelty	Cost	Efficiency	Security	Complexity

Solutions	Accuracy	Acceptance	Novelty	Cost	Efficiency	Security	Complexity
SMS-OTP	High	High	Low	Low	High	High	Low
NFC-enabled	High	Low	High	High	High	Very High	Middle
Biometrics	Middle	Low	Middle	High	Middle	Very High	High

This section makes a comparison among three proposed 2-factor user authentication solutions mention above. And choose the best one as the proposed method for user authentication of the Beijing medical registration platform. The comparisons from different aspects are shown on the Table 1. For accuracy, both OTP and user credential stored in the SE of NFC device are very accurate. But biometrics has statistical nature, sometime is inaccuracy in bad environments, such as noise, complex background, occlusion etc. For acceptance, the SMS-OTP is widely accepted by public. But the NFC solution requires users who want to log on the medical registration platform buy some NFC-enabled device, e.g., NFC handset, or NFC-enabled tablet and POS terminal. And the biometrics-based solution requires user buy a biometric sensor except voice in handset environment. Therefore, users may dislike NFC-enabled and biometrics based solutions because of the NFC device and biometrics expense. For novelty, the NFC-enabled solution with NFC technology is really new one. For cost, both NFC-enabled solution and biometrics-based solution need users pay more like discussed in the aspect of acceptance. For efficiency, both the SMS-OTP and NFC solution are faster than the biometrics one. This is because biometric authentication spends a period of time to calculate matching score between testing biometric sample and template then making a decision. For security, all three solutions are safer than the traditional single factor ways. For complexity, the SMS-OTP method is straightforward. NFC-enabled solution is more complicated than the SMS-OTP one. It must consider issues like NFC storage, SE module security etc. The biometrics-based solution is most complex one than any others. The manufacturer of the platform needs to consider building a special user database with biometric samples.

To summarize, the SMS-OTP two factor user authentication solution is most reasonable one for Beijing medical registration platform.

V. CONLUSION

This paper proposes a two factors user authentication scheme for Beijing medical registration platform, in order to safeguard user privacy information on the platform and protect against attacker abuse. The SMS-OTP solution is chosen as the optimal way for user authentication of the Beijing medical registration platform. This scheme helps the platform to make up user authentication process during user log on. Users are glad to accept this way, because most of them have another factor device except computer, i.e., mobile phone. And the platform enables to send OTP for free. Therefore, the SMS-OTP scheme can be considered as a straightforward and low-cost two factor user authentication solution for the platform.

REFERENCES

[1] Beijing Medical Registration Uniform Platform. HTTP:// http://www.bjguahao.gov.cn/comm/index.php.

[2] Alsaleh M, Mannan M, Oorschot P C. Revisiting Defenses against Large-Scale Online Password Guessing Attacks[J]. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, p.128-141, 2012.

[3] Hollingsworth K P, Darnell S S, Miller P E, Woodard D L. Bowyer K W, Flynn, P J. Human and Machine Performance on Periocular Biometrics Under Near-Infrared Light and Visible Light[J]. IEEE Transactions on Information Forensics and Security, Vol.7, No.2, p.588- 601, 2012.

[4] Ben-Yacoub S, Abdeljaoued Y, and Mayoraz E. Fusion of face and speech data for person identity verification[J]. IEEE Transaction on Netrual Network, Vol. 10, No. 5, p.1065-1074, 1999.

[5] NAKAGAWA S, Wang L, Ohtsuka S. Speaker Identification and Verification by Combining MFCC and Phase Information[J]. IEEE Transactions on Audio, Speech, and Language Processing, Vol. 20, No.4, p.1085-1095, 2012.

[6] Kong A, Zhang D and Kamel M. A survey of palmprint recognition[J]. Pattern Recognition, Vo. l 42, No. 7, p. 1408-1418, 2009.

[7] Li Z, Sun D, Liu D, Liu H. Two Modality-Based Bi-Finger Vein Verification System[C], The 2010 International Conference on Signal Processing, p.1690-1693, 2010.

[8] J. Daugman, "Combining Multiple Biometrics", Available on http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html.

[9] Wang H, Fan C, Yang S, Zou J, Zhang X. A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP)[C]. 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, p.1-4, 2011.

[10] Kirlappos I, Sasse M A. Security Education against Phishing: A Modest Proposal for a Major Rethink[J], IEEE Security & Privacy, Vol.10, No.2, p. 24-32, 2012.

[11] Morak J, Kumpusch H, Hayn D, Modre-Osprian R, Schreier G. Design and Evaluation of a Telemonitoring Concept Based on NFC-Enabled Mobile Phones and Sensor[J], IEEE Transactions on Information Technology in Biomedicine, Vol.16, No.1, p.17-23, 2012.

[12] Fayyaz F, Rasheed H. Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network Environment[J]. IEEE Potentials, Vol.31, No.4, 35-37, 2012.

[13] Chaudhari S, Tomar S S, Rawat A. Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for webmail access in multi trust networks[C]. 2011 International Conference on Emerging Trends in Networks and Computer Communications, p.27-32, 2011.