Mustansiriyah Journal of Pure and Applied Sciences

www.MJPAS.com

Secure Authentication Scheme To Thwart Known Authentication Attacks Using Mobile Device

M.A. Abbas

Department of Computer Science, Al Mustansiriyah University, Iraq
mazinalwaaly@gmail.com

ABSTRACT

Recently, the use of two-factors authentication (2FA) has increased to mitigate the risk of stealing user credentials. Most of 2FA use a mobile device to complete the authentication process, but many of them require an Internet connection or a subscriber identity module (SIM) chip to activate the synchronization of the One Time Password (OTP), which may not be guaranteed all the time or may not be equipped in the user's phone in the first place. Thus, this paper attempts to overcome this problem by adopting the camera of the mobile device and QR code to verify the OTP instead of relying on the Internet connection or cellular network. The proposed approach involves encrypting keys and secret codes with symmetric and asymmetric keys for added security, and using QR to exchange those codes fast and more easily, including a code suffix to prevent phishing attacks. Security analysis proves that the scheme is immune to many well-known attacks such as MITM, Shoulder surfing Keylogger, Phishing Attacks, etc. This scheme could contribute to adding a secure, practical, and easy-to-use option to diversify of 2FA if it is adopted by service providers such as Google, Meta, and Microsoft.

Keywords: *Authentication; Two-Factor Authentication (2FA); Mobile device ; One-Time-Password (OTP); Challenge Response Protocol and Quick Response (QR) Code*

1. Introduction

Communication technologies have undeniably revolutionized the way we connect and share information. However, it is crucial to acknowledge the potential risks that come with these modern means of communication. From privacy concerns to cyber threats, it is essential to navigate this digital landscape with caution. It is imperative for individuals and organizations alike to be aware of these dangers and take necessary measures to protect themselves in this ever-evolving technological era.

In this Section, we present the most important topics related to our research as follows. Start with the username, password and the risks associated with them, then the methods that mitigate those risks used in this paper are Multi-factor authentication, Challenge response protocol and quick response code.

1.1. Username and password

The oldest traditional way to provide authentication is to use usernames and passwords. A password is a secret that the claimant keeps and uses to authenticate his or her identity [1] which is a string of characters known only to a specific person and which is used to authenticate the user identity in a computer system for allowing him to access the system resources [2], but this password is not completely secure.

The password stored by some service's accounting system can be leaked, for example, through SQL injection [3]. In recent years, we have witnessed an increasing amount of password leaks from major Internet sites [4], and Recently, In just about five hours, GPU-based architectures were able to crack eight-character NTLM passwords for Microsoft Windows [5].

To protect the password from leaking, the hash function is used which is functions that compress an input of arbitrary length to a result with a fixed length [6], and has the (Compression, Ease of computation, Uniform distribution of values) [7], and the use of salts also prevents attackers from using shortcuts. It forces the attacker to brute force the hashes one by one, rather than attacking them as a group [8].

1.2. Multi-factor authentication

It is a method of user identification that combines a some number of factor authentications which used for priority customer information and high-risk financial transactions[9] A common example is ATMs, where physical factors are combined with personal factors [10]. And the multi-factor kinds [11]:

1. Knowledge – something knows
2. Possession – something has
3. Inherence – something verifies the user is

One of the most popular multi-factor methods is SMS. The user is sent a one-time verification code via text message to his mobile phone. However, its disadvantages are delayed delivery, or lack of cellular service (such as in a foreign country or a remote location), in addition to being unsafe as mobile phone networks do not encrypt messages during their transmission, which allows attackers to conduct man-in-the-middle attacks [12]. Or the well-documented SIM swapping attack [13,14].

The second method of multi-factor is TOTP (time-based one-time password), the user first synchronizes a secret key generated by the provider to their smartphone. the user does not need to rely on a cellular provider to deliver the one-time codes.

However, it's disadvantages are that the smartphone and server must have both a clock that is reasonably in sync and users have less than 30 seconds to enter the codes because codes can be generated at any time within a 30-second period.

The third multi-factors method is pre-generated codes, which is a list of verification codes provided by the service supporter to the help user to print it. However, its disadvantage is that these codes has no specific expiring and is therefore vulnerable to brute force attack. On the other hand, the user must store the printed codes securely to protect them from theft or loss [12].

1.3. Challenge response protocol

An authentication protocol where the verifier sends a random value to the claimant which the claimant then uses to generate a response (usually using an application) to be sent to the verifier for verification [1]

1.4. QR quick response

The origin of the QR code goes back to the Japanese automobile industry and it facilitates the communication between real objects and digital contents such that Internet contents [15]. Most mobile phones equipped with cameras have the ability to read QR codes to access Internet addresses automatically [16].

2. Related Works

In this Section, we present some research related to our paper, which is classified as follows:

2.1. Mobile

Recently, there has been great reliance on multi-factor to support secure login [17-20] as it makes the stealing user credentials is difficult. Some researchers [20,31-39] are satisfied with the browser available on the computers or choose a specific browser such as google chrome [17,37], but other researchers [17-19,21-30] mainly use the mobile phone for this purpose as it is commonly used and available to most users almost all the time,, even Alhothaily [21] believes that using smartwatch is equal to the use of a mobile phone.

Varshney [17] uses some of the mobile features such as the Bluetooth address as the user’s name or the IMEI number to confirm the user’s identity [25].

Sabzevar [24] also prefer to use the mobile to permanently store keys and passwords in it which saves the user the trouble of remembering them, but storing important codes inside the mobile phone may pose a major security risk due to the possibility of them being stolen by hackers or the mobile phone itself being stolen, Therefore, some researchers [17,25] do not prefer to store it in the mobile phone for those reasons.

Storing codes in a mobile phone is not the only reason for using it in the authentication process. Rather, the mobile phone’s ability to communicate is exploited to confirm the user’s identity by receiving an SMS [28] or an email [20].

This also has its drawbacks, as it is not possible to guarantee the availability of an Internet connection always and everywhere, and the SMS message may be delayed or may not arrive when moving to another country, for example, or a place that does not have mobile phone network coverage, or due to server problems.

Therefore, [18,19,22,25,27,29,30] uses the mobile phone camera to read the Quick Response (QR) code, which is used to encode information and transfer it from one device to another quickly and accurately, which was used in the proposed scheme.

2.2. One Time Password (OTP)

Many malicious programs trying to stealing the user password in various ways, and to avoid stealing password, researchers [17-23,25-27,29,34,36] resort to use one time password OTP because it changes constantly in every session. Rather, Varshney and Alhothaily [17,21] uses one time user name such as Bluetooth, as we mentioned above. To generate OTP, researchers [17-19,21-23,25,26,29,36] uses key generation, and in order to protect OTP and some important information such as passwords, encryption is used by researchers [17,18,21,22,24,25,27,29,30] which is done either by using the symmetric key or the public key [18,21,25,29]. Other cryptographic techniques such as hashing are used to encrypt the password [21].

It is usually added salt [17,18,22,23] In order to prevent cracking password attacks that use precompiled tables (e. g. , rainbow tables).

Due to the great security importance provided by OTP, it was mainly used in the proposed scheme in addition to symmetric and asymmetric encryption techniques to achieve a high level of security for the user.

2.3. Virtual Keyboard

Instead of using multi-factor, some researchers focus primarily on entering the password securely and use virtual keyboard for this purpose. For example, the alphabet appears on an empty keyboard and the user clicks the appropriate button for the password [18]. Or the user may be asked to locate his passwords in the specified an M x N grid [33,35], or the user may choose a specific color from among the basic colors on a wheel containing random letters and numbers [34].

Hamid uses a random number generator RNG keyboard and Keypad Scrambler pseudocode to scramble the position of the buttons [26]. Nand designed PassBoard which is an extension for Google's browser as a special virtual keyboard [37]. To avoid spyware that using screenshot, Lim displays a partial keyboard at every moment in the browser [39].

Kumar differs from other researchers by using the eye instead of the hand to enter the password with the Gaze-based Password Entry method [31].

Despite all the efforts made to create secure virtual keyboards, they remain relatively difficult to learn and are not sufficiently robust against some attacks such as screen recording attacks. Therefore, some researchers came up with other methods away from traditional virtual keyboards, as is the case in the innovative RPTPA technique [36] where the pattern (number of random places or index) is displayed to the user to arrange the password during login stage, then the user enters the password elements according to this pattern and then retrieving the user's password from the server side according to this pattern, or as Herley [38] suggested a simple method by clicking anywhere in the browser except the password field, then typing random keys, then one letter of the password, and so on to avoid Keylogger software.

Unlike existing works, in proposed scheme it us Challenge Response Code which is sent to the server and received OTP from the server using QR and camera which provides great ease to the user along with security.

Our approach is to scan the OTP using the user's smart devices and cryptographic primitives of symmetric and asymmetric encryption

3. Proposed Scheme

In this section, main components of our system model will discussed and how to implement it, which divided into two stages. Table 1 consists of the Description for the abbreviations used in this paper:

Table 1. Abbreviation and Description

Abbreviation	Description
UPass	User Password
uPrK	User Private Key
uPuK	User Public Key
aPrK	Attacker Private Key
aPuK	Attacker Public Key
CAPA	Computer Application of the Proposed Approach
CRC	Challenge Response Code

ePrK	Encrypted Private Key
Key Gen.	Key Generator
MAPA	Mobile Application of the Proposed Approach
OTP	One Time Password
PrKeC	Private Key Encryption Code
SCS	Server Code Suffix

3.1. Setup stage

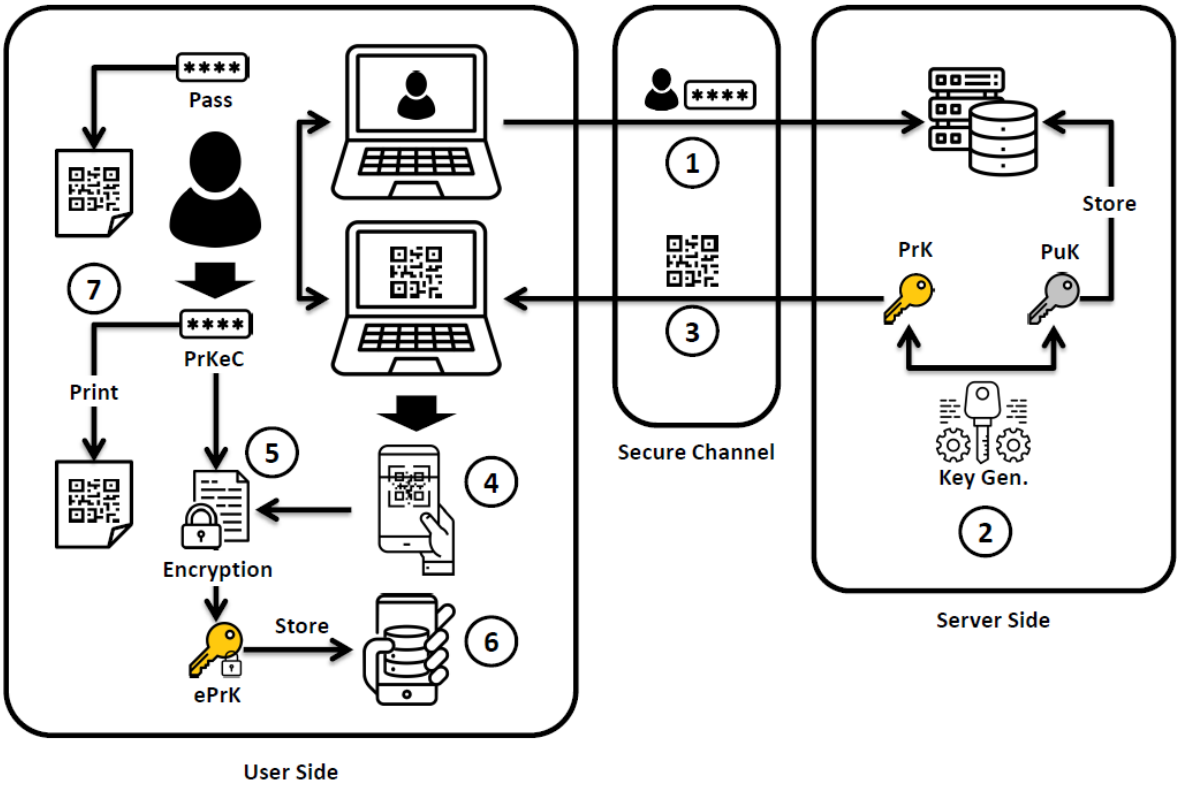
Our system model consists of four main entities, and at the setup stage all these entities must be secure.

1. User: He and his mobile device must be secure against spy or directly or by using a hidden camera directed at them.
2. Browser (usually on the computer): It should well protected with anti-virus and anti-spyware software against authentication attacks such as Keylogger Attack, Shoulder surfing attacks, Phishing Attacks, Video Recording Attack, Man-in-the-Browser Attack,. . etc. As optional, it is equipped with a camera (built-in or webcam), and Computer Application of the Proposed Approach (CAPA).
3. Mobile phone: The same requirements as a computer (in 2), in addition, Mobile Application of the Proposed Approach (MAPA).
4. Server: it must be secured against authentication attacks such as Insider Attack, SQL Injection Attack, Replay Attacks,. . etc. , and use hypertext transfer protocol secure connection (https).

These conditions are necessary at this stage because they involve transferring the user's private key, and any security violation will result in the entire proposed scheme being compromised. These are the conventional requirements for any secure connection between the user and the server, except for some conditions specific to the proposed scheme (such as the availability of a mobile phone with a camera and a specific application).

As shown in Figure 1, sign-in stage begins as usual registration process as follow:

1. Through the browser, the user provides username and password (UPass) to the server that will store on the server database (after Hashing with Salt).
2. Server creates asymmetric keys which are the private key (uPrK) and the public key (uPuK), then, uPuK stores in the server database and assigns to the user (the server generating these keys for each user).
3. uPrK converting to a Quick-Response Code form (QR) and sends to the user using a secure connection.



4. When QR appears on the user browser, the user scans QR using the Mobile Application of the Proposed Approach (MAPA) by mobile camera to retrieve the digital form again.
5. MAPA requests user to entering the Private Key Encryption Code (PrKeC) which must meet the security criteria for the standard password [40].
1. , then, MAPA encrypts the uPrK using PrKeC to produce Encrypted Private Key (ePrK).
6. MAPA store ePrK permanently in the mobile storage.
7. As an optional procedure, Computer Application of the Proposed Approach (CAPA) offers the user on the server side (browser), to print the UPass in QR format, and MAPA on the user side (mobile phone), to print PrKeC in QR format as well.

Printing these codes in QR format relieves the user of remember effort as well as writing down in the login stage, in addition to a security benefit, but QR must be printed in the smallest possible size that make the user mobile camera can recognize it, while a spying cannot recognize it even with a camera.

Figure 1. Setup Stage

3.2. Login stage

As shown in Figure 2, this stage begins when the user provides username and UPass to the server, Optionally, the user directs the UPass as QR printed paper to the computer camera (if available), where CAPA scans the QR and retrieve UPass then paste it into the password field instead of writing it manually by the user to reduce time and effort for the user in addition to avoiding Keylogger.

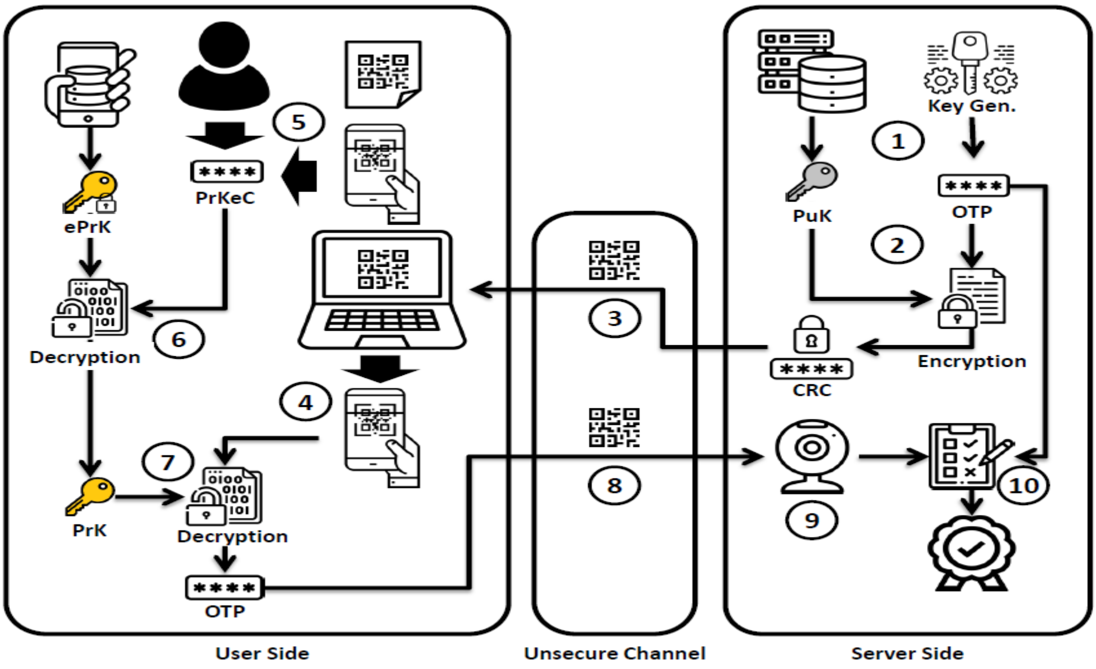
At this point, the registration process can be considered completed

3.3. 2FA stage

In the Proposed Approach, we assume that the user prefers to use Two-Factor Authentication (2FA), thus, the registration process will proceed as follows:

1. The server randomly g enerates the One Time Password (OTP) which must meet the security randomness requirements [41].
2. The server adds the Server Code Suffix (SCS) as follow:
   For example, if server is Google then, the server adds (google-) to OTP to produce google-XXXXXXXX, where XXXXXXXX represents the OTP.
   SCS must be store in MAPA so that it can later identify the server through it.
   Then, encrypts the OTP with uPuK to produce Challenge Response Code (CRC).
3. CRC displayed on the user's browser after converting it into QR form.
4. The user, in turn, scans QR using the mobile camera.
5. MAPA prompt user to write PrKeC or (optionally) scans printed QR of PrKeC.
6. MAPA decrypt the Encrypted Private Key (ePrK) by using PrKeC to produce uPrK.
7. MAPA use uPrK to decrypt the CRC and produce OTP.
8. When the correct OTP is obtained, MAPA displays the OTP on the mobile phone screen for the user to type in the OTP field on the browser, or (optionally) MAPA converts the OTP into a QR form and displays it on the phone screen The user points the screen to the computer camera that captures the OTP code, then CAPA pastes the code into the OTP field automatically.

The server then compares the password generated with the password submitted by the user,



and if it matches, the login process ends successfully.

Figure 2. Sign in Stage

4. Security Analysis

In this section, possible attack scenarios on the proposed scheme will be discussed. The focus will be on the login phase, especially the 2FA stage. The details of the setup stage (where it is assumed to be fully protected as mentioned previously) will not be addressed, nor the sending the name and uPass process of because it is outside the proposed scheme goal, however, is that despite using an Hypertext Transfer Protocol Secure (https), the worst scenario will be assumed, which is that the attacker obtains the username and password in some way.

4.1. Man-in-the-Middle Attack

An attack on the authentication protocol where the attacker is between the user and the server so that it appears to the server as the user and appears to the user as the server, and can view and modify all data sent between the user and the server [42].

There are two types of data sent over the network between the user and the server, CRC and OTP, both in QR form, but that makes no difference to the attacker. This scenario will be divided into A and B

Case A: The attacker intercepts the CRC sent from server to user and tries to change its value, but changing CRC value requires possession of uPuK, and here the attacker may use the Attacker Public Key (aPuK), and thus MAPA will detect the presence of the attacker after decryption, because the CRC is encrypted with aPuK and decrypted with uPrK, so CRC cannot be recovered. in addition, the original SCS does not appear as agreed between the user and the server.

Case B: In this case, the worst scenario will be assumed, whereby the attacker able to stealing uPuK from the server in some way. The attacker use uPuK to create a fake OTP, then add the original SCS and then encrypt it to create a fake CRC and send it to the user. Since the uPuK used to encrypt the CRC is compatible with the uPrK used to decrypt it, in addition use the original SCS, MAPA will recover the fake OTP and send it to the attacker.

But in this scenario, the attacker cannot send the fake OTP to the server because it does not match the OTP that the server generated, and thus the server will detect the presence of the attacker.

In addition to detecting the attacker, it is noted that in both cases the attacker does not obtain valuable data such as (uPrK and ePrk) and thus the attack fails.

In the following attack scenarios, the details mentioned in the Man-in-the-Middle Attack scenario will not be repeated. Rather, only the differences will be mentioned. Attacks that have the same effect on the proposed scheme will be combined.

4.2. Replay Attacks and Man-in-the-Browser Attack

Replay Attacks: The attacker copies the data, user credentials, or important information that is transferred between the user and the server and then uses it for malicious purposes [43].

Man-in-the-Browser Attack: These attacks are a special type of Man-in-the-Middle attack, which steals user authentication data, changes it, and uses it for malicious purposes [44].

In this scenario, using an OTP that is valid for only one session is sufficient to nullify both Replay Attacks and Man-in-the-Browser Attacks.

4.3. Shoulder surfing attacks, Keylogger Attack, Video Recording Attack and Trojan attack

Shoulder surfing attacks: A type of spying where the attacker spies on the user to obtain the password and monitors the user to discover what keyboard keys were pressed [45]

Keylogger Attack: is a computer program or device that captures keystrokes made by a user for the purpose of stealing a password [46].

Video Recording Attack: In this type of attack, attackers can use the mobile camera or any other camera to record a video of the user who enters the password and then analyze it to obtain the user's password [47].

It was assumed that the mobile device is completely protected from spyware, and therefore this scenario concerns the computer and the persons around the user. In this case, the use of 2FA with OTP as well as QR in a reduced size leads to making this attack seem impossible as (with the exception of uPass) there is no value to what the attacker gets by this type of attack.

4.4. Insider Attack and SQL Injection Attack

Insider Attack: An insider attack is a type of malicious attack that occurs within the organization, in which attackers take advantage of their spatial presence near the server to steal important data from the database [48].

SQL injection attack: is the process of injecting malicious code into databases which is used to attack websites and log in to them using administrator privileges [49]

As mentioned previously in Man-in-the-Middle Attack, even if the attacker manages to obtain uPuK, he will be detected by the server for sending a fake OTP to the server.

4.5. Phishing Attacks

It is a type of attack in which the attacker impersonates the original website by creating an identical website to the original and even a domain name similar to the original to steal user credentials [50].

In this scenario, the attacker can steal the username and the uPass, but the uPrK, ePrK, or PrKeC cannot be stolen, i. e. it will be stopped in the 2FA stage.

4.6. Brute Force Attacks: Dictionary Attack

Brute force attacks: In this type of attack, all possible combinations of the password are tried for the purpose of cracking it [51]

Dictionary attack: In this type of attack, it tries to match the password with most of the dictionary words or the most used words in daily life, and it is relatively faster than the brute force attack [52]

It has been assumed in the supposed scheme that the uPass PrKeC, and the OTP apply to [40] [41] security standards and are therefore immune to this type of attack

4.7. Mobile device theft

In the supposed scheme, uPass and PrKeC are not stored on the computer or on the user's mobile device, but are kept in the user's memory (or a printed QR that is kept in a safe place). When the mobile device is stolen, the attacker gets only ePrK

In the mobile device theft scenario, the user replace the uPrK and uPuK after connecting to the server and proves his identity using other authentication factors (such as an sms message or an email message on another account, etc.), then he can encrypt the new uPrK with the same old PrKeC without alteration.

Although the scheme uses two 2FA factors, the user actually has three factors, and the reason is due to the second factor CRC on the server side, which requires two factors on the user side, ePrK and PrKeC. :

1. uPass: something you know (user memory) or something you have (printed QR)
2. ePrK: Something you own
3. PrKeC: something you know (user memory) or something you have (printed QR)

The reason for the classification difference in the first and third factors is due to the difference in the user’s preference in terms of using the printed QR or relying on remembering.

It is clear from the three factors that the proposed scheme is immune to a wide range of attacks, and the attacker can only succeed in stealing the three factors combined, as follows:

1. Stealing uPass via Phishing Attacks, Brute Force Attacks, Dictionary Attack or Man-in-the-Browser Attack and so on, or by (stealing as QR printed on paper *)
2. Stealing ePrK by stealing the user's own mobile phone or (using spyware to steal ePrK remotely **)
3. Stealing PrKeC via Shoulder surfing attacks or (it captures the keys while the user is typing them on the mobile keyboard**) or via (taking a snapshot of the QR code on the mobile screen*) or (stealing as QR printed on paper *)

* Represents optional user states

** The proposed scheme assumes that there is no spyware on the user's mobile device

It is emphasized here that the attacker will not succeed if he is able to fulfill one or two of these conditions, and that the probability of achieving all three conditions together is very small, especially taking into account the user's keenness to protect the mobile phone from spying and to keep the printed QR in a safe place.

5. Conclusion

In the security analysis section, all possible attack scenarios in the proposed scheme are discussed, and the worst possible possibilities were taken into consideration, whether in the attacker obtaining the username and password by spying on the network between the user and the server, or in intercepting the CRC code sent from the server to the user, Or in stealing uPuK from the server by hacking the server database, which are considered unlikely cases. In the first case, https is used to encrypt data sent through the network between the user and the server, and in the second case, the server's protection measures are assumed to be applied and sufficient to prevent these attacks.

It is worth noting the importance of using OTP, QR, CRC and SCS in the proposed scheme and how to protect the user from most known attacks, which can be summarized as follows:

1. Using mainly OTP in the proposed scheme reduces the risk of password theft because the attacker still needs a new OTP every time he tries to log in.
2. Using a digital QR makes the registration process easier and faster for the user, as you only need to point the camera at the QR code and it does not require writing the code manually.
3. Using a printed QR reduces the risk of shoulder surfing, as the attacker cannot know the original code except by using a QR scanner, and it certainly cannot happen in front of the user's eyes. It also removes the user from the trouble of remembering it.
4. Using CRC prevents impersonation of the user because it requires the correct Prk to decrypt it, which only the user has.
5. Using SCS prevents server impersonation as MAPA can detect the source of the CRC if the attacker does not use the correct Puk in the encryption process.

As is clear in the previous section, the proposed scheme is well protected against most attacks (which were mentioned in detail in the previous section), and the attacker is only successful in the proposed scheme if he obtains uPass, ePrK, and PrKeC all together, which is almost impossible.

The proposed scheme also takes into account the server being hacked and thus the attacker obtaining uPuK, which is (as mentioned previously) a scenario that does not constitute a threat to the proposed scheme.

In addition to the features of safety and ease (because when printing codes in QR form, the user does not need to write any code except the user name, nor to save any code) that the proposed scheme provides for the user, it does not require subscriber identity module (SIM) card to receive Short Message Service (SMS) messages, nor synchronization as in Authenticator applications, nor even an Internet connection.

References

[1] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., ... & Theofanos, M. F. (2016). Draft nist special publication 800-63b digital identity guidelines. *National Institute of Standards and Technology (NIST), 27.*Turan, Meltem Sönmez, et al. "Recommendation for password-based key derivation. " NIST special publication 800 (2010): 132

[2] Kontaxis, G., Athanasopoulos, E., Portokalidis, G., & Keromytis, A. D. (2013, November). Sauth: Protecting user accounts from password database leaks. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 187-198).IEEE data breach: 100K passwords leak in plain text. http://www. neowin. net/news/ieee-data-breach-100k-passwords-leak-in-plain-text.

[3] New 25 GPU Monster Devours Passwords In Seconds. http://securityledger. com/new-25-gpu-monsterdevours-passwords-in-seconds/.

[4] Preneel, B. (1993). *Analysis and design of cryptographic hash functions* (Doctoral dissertation, Katholieke Universiteit te Leuven).Galbreath, Nick. Cryptography for Internet and database applications: developing secret and public key techniques with Java. John Wiley & Sons, 2003.

[5] Mirante, D., & Cappos, J. (2013). Understanding password database compromises. *Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02.*Smart Card Alliance (Randy Vanderhoof), “Smart Card Technology Roadmap for secure ID applications”,2003.

[6] Rathgeb, C., & Uhl, A. (2010, June). Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In *International Conference Image Analysis and Recognition* (pp. 296-305). Berlin, Heidelberg: Springer Berlin Heidelberg. and Recognition. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[7] Reddy, B. K. K., & Reddy, B. I. (2018). A comparative analysis of various multifactor authentication mechanisms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(5), 8.Reese, Ken, et al. "A usability study of five {two-factor} authentication methods. " Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). 2019.

[8] Andrews, N. (2018). " Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers for Sim-Swap Attacks and Wireless Provider Liability. *Nw. J. Tech. & Intell. Prop., 16*, 79.Mulliner, Collin, et al. "SMS-Based One-Time Passwords: Attacks and Defense: (Short

Paper). " Detection of Intrusions and Malware, and Vulnerability Assessment: 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings 10. Springer Berlin Heidelberg, 2013.

[9] Aktaş, C. (2017). *The Evolution and Emergence of QR Codes*. Cambridge Scholars Publishing..

[10] Law, C. Y., & So, S. (2010). QR codes in education. *Journal of Educational Technology Development and Exchange (JETDE)*, *3*(1), 7.

[11] Varshney, G., Misra, M., & Atrey, P. (2018). Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks. *Journal of Information Security and Applications*, *42*, 1-17.

[12] Nyang, D., Mohaisen, A., & Kang, J. (2014). Keylogging-resistant visual authentication protocols. *IEEE Transactions on Mobile Computing*, *13*(11), 2566-2579.

[13] Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrag, M. A., & Janicke, H. (2021). Cybersecurity revisited: Honeytokens meet google authenticator. *arXiv preprint arXiv:2112.08431*.

[14] Matiushin, I., & Korkhov, V. (2021, December). Passwordless Authentication Using Magic Link Technology. In *CEUR Workshop Proceedings* (Vol. 3041, pp. 434-438).

[15] Alhothaily, A., Hu, C., Alrawais, A., Song, T., Cheng, X., & Chen, D. (2017). A secure and practical authentication scheme using personal devices. *IEEE access*, *5*, 11677-11687.

[16] Spafford, E. H. (2015, May). Enhancing Passwords Security Using Deceptive Covert Communication. In *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings* (Vol. 455, p. 159). Springer.

[17] Lei, M., Xiao, Y., Vrbsky, S. V., & Li, C. C. (2008). Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing. *Computer Communications*, *31*(18), 4367-4375.

[18] Sabzevar, Alireza Pirayesh, and Angelos Stavrou. "Universal multi-factor authentication using graphical passwords. " 2008 IEEE international conference on signal image technology and internet based systems. IEEE, 2008.

[19] Chow, Y. W., Susilo, W., Au, M. H., & Barmawi, A. M. (2015). A visual one-time password authentication scheme using mobile devices. In *Information and Communications Security: 16th International Conference, ICICS 2014, Hong Kong, China, December 16-17, 2014, Revised Selected Papers 16* (pp. 243-257). Springer International Publishing.

[20] Hamid, H. R. M. H., & Abdullah, N. Y. (2015, October). Physical authentication using random number generated (rng) keypad based on one time pad (otp) concept. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (pp. 135-139). IEEE..

[21] Kao, Y. W., Luo, G. H., Lin, H. T., Huang, Y. K., & Yuan, S. M. (2011, October). Physical access control based on QR code. In *2011 international conference on cyber-enabled distributed computing and knowledge discovery* (pp. 285-288). IEEE.

[22] AlZomai, M., Josang, A., McCullagh, A., & Foo, E. (2008, December). Strengthening sms-based authentication through usability. In *2008 IEEE International Symposium on Parallel and Distributed Processing with Applications* (pp. 683-688). IEEE.

[23] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An improved Time-Based one time password authentication framework for electronic payments. *Int. J. Adv. Comput. Sci. Appl*, *11*(11), 359-366..

[24] McCune, J. M., Perrig, A., & Reiter, M. K. (2005, May). Seeing-is-believing: Using camera phones for human-verifiable authentication. In *2005 IEEE Symposium on Security and Privacy (S&P'05)* (pp. 110-124). IEEE.

[25] Kumar, Manu, et al. "Reducing shoulder-surfing by using gaze-based password entry. " Proceedings of the 3rd symposium on Usable privacy and security. 2007.

[26] Nielsen, F. (2013). Logging safely in public spaces using color PINs. *arXiv preprint arXiv:1304.6499*.

[27] Kim, S. H., Kim, J. W., Kim, S. Y., & Cho, H. G. (2011, February). A new shoulder-surfing resistant password for mobile environments. In *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication* (pp. 1-8).

[28] Phatak, S. (2019). *Implementing Colour Shuffling with OTP as a defence against Shoulder Surfing* (Doctoral dissertation, Dublin, National College of Ireland).

[29] Hsu, S. C., Huang, C. T., Weng, C. Y., & Wang, S. J. (2019, February). A logging-in scheme in virtual keyboard protection from shoulder surfing and screenshot capturing. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)* (pp. 440-444). IEEE..

[30] Abbas, M. A., Mahmood, S. A., & Hussien, K. A. (2018). RPTPA: Random Pattern Technique Based Password Authentication. *Iraqi Journal of Information Technology*, *9*(2 اللغة الانكليزية).

[31] Nand, P., Singh, P. K., Aneja, J., & Dhingra, Y. (2015, March). Prevention of shoulder surfing attack using randomized square matrix virtual keyboard. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 916-920). IEEE.

[32] Herley, C., & Florencio, D. (2006, July). How to login from an Internet café without worrying about keyloggers. In *Symposium on Usable Privacy and Security (SOUPS)* (Vol. 6)..

[33] Lim, J. (2007, July). Defeat spyware with anti-screen capture technology using visual persistence. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 147-148).

[34] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., ... & Theofanos, M. F. (2016). Draft nist special publication 800-63b digital identity guidelines. *National Institute of Standards and Technology (NIST), 27*.

[35] Keller, Sharon, and Timothy A. Hall. "The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS). " NIST Information Technology Laboratory (2009).

[36] Ouafi, K., Overbeck, R., & Vaudenay, S. (2008). On the security of HB# against a man-in-the-middle attack. In *Advances in Cryptology-ASIACRYPT 2008: 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings 14* (pp. 108-124). Springer Berlin Heidelberg..

[37] Syverson, P. (1994, June). A taxonomy of replay attacks [cryptographic protocols]. In *Proceedings The Computer Security Foundations Workshop VII* (pp. 187-191). IEEE.

[38] Dougan, T., & Curran, K. (2012). Man in the browser attacks. *International Journal of Ambient Computing and Intelligence (IJACI)*, *4*(1), 29-39.

[39] Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In *21st international conference on advanced information networking and applications workshops (AINAW'07)* (Vol. 2, pp. 467-472). IEEE.

[40] Sapra, K., Husain, B., Brooks, R., & Smith, M. (2013, October). Circumventing keyloggers and screendumps. In *2013 8th International Conference on Malicious and Unwanted Software:" The Americas"(MALWARE)* (pp. 103-108). IEEE.

[41] Fujita, K., & Hirakawa, Y. (2008, September). A study of password authentication method against observing attacks. In *2008 6th International Symposium on Intelligent Systems and Informatics* (pp. 1-6). IEEE.

[42] Duncan, A. J., Creese, S., & Goldsmith, M. (2012, June). Insider attacks in cloud computing. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications* (pp. 857-862). IEEE.

[43] Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In *Proceedings of the IEEE international symposium on secure software engineering* (Vol. 1, pp. 13-15). IEEE.

[44] Huang, C. Y., Ma, S. P., & Chen, K. T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications*, *34*(4), 1292-1301..

[45] Adams, C., Jourdan, G. V., Levac, J. P., & Prevost, F. (2010, August). Lightweight protection against brute force login attacks on web applications. In *2010 Eighth International Conference on Privacy, Security and Trust* (pp. 181-188). IEEE.

[46] Narayanan, A., & Shmatikov, V. (2005, November). Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security* (pp. 364-372).