Improved Multi-layer Authentication Scheme by Merging One-time Password with Voice Biometric Factor

Amal ALRUWAILI[1†] and Saloua Hendaoui [2††]

Department of computer Science, College of Computer and Information Sciences, Jouf University, Jouf, Skaka, Saudi Arabia

Summary

In this proposal, we aim to enhance the security of systems accounts by improving the authentication techniques. We mainly intend to enhance the accuracy of the one-time passwords via including voice biometric and recognition techniques. The recognition will be performed on the server to avoid redirecting voice signatures by hackers. Further, to enhance the privacy of data and to ensure that the active user is legitimate, we propose to periodically update the activated sessions using a user-selected biometric factor. Finally, we recommend adding a pre-transaction re-authentication which will guarantee enhanced security for sensitive operations. The main novelty of this proposal is the use of the voice factor in the verification of the one-time password and the various levels of authentications for a full-security guarantee. The improvement provided by this proposal is mainly designed for sensitive applications.
From conducted simulations, findings prove the efficiency of the proposed scheme in reducing the probability of hacking users' sessions.

Key words:
cybersecurity, authentication, password, biometric, voice, recognition, three levels

1. Introduction

Authentication aims to safeguard information systems from unauthorized use, access, modification, destruction, disruption, or disclosure. It enables to ensure features of the CIA triangle that are confidentiality, integrity, and availability. Numerous authentication policies are applicable to prove that a user is authorized to enter and access system resources [1]. For instance, we cite smart cards, passwords, digital certificates, biometrics, and Kerberos [1].

We can classify authentication techniques into three main classes, as presented in figure 1. First, something you know where authentication is performed via passwords. Password is a mixture of numbers, letters, and symbols. This authentication technique can use passwords or PINs or one-time passwords (OTP), used only once for authentication [2]. Passwords can save us a little cost, but in return, they are not ideal for authentication because of attacks and password cracking. In addition, they can fall victim to eavesdropping, keystrokes, guessing, and social engineering to obtain the password [1]. Second, something you have, e.g., smart card, ATM card. Third, something you are that is known by biometrics which provides high safety, but in return, it has a high cost because it requires advanced equipment and programs. The use of smart devices and biometric factors are not always possible due to their high cost and people's fear of health problems such as eye damage. Consequently, authentication via passwords is the most used technique, whatever for business websites or official accounts.

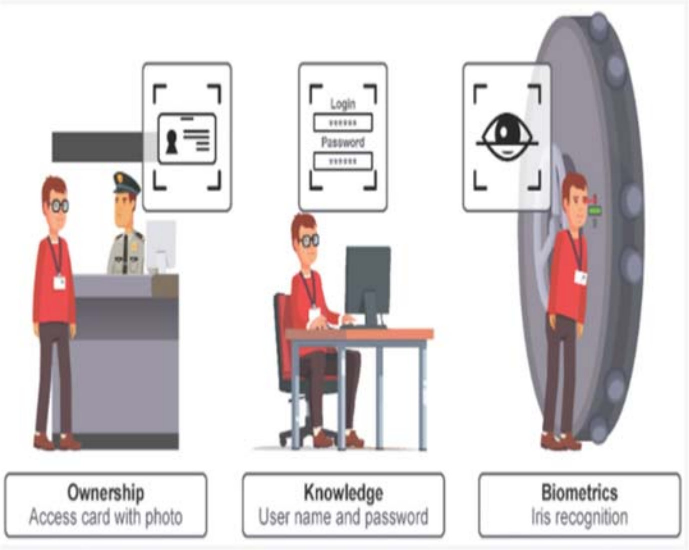


Fig. 1 Authentication methods [5]

One of the improvements to a well-secured online authentication architecture is multi-factor authentication [3]. This proposal solves the user data security problem and consists of several layers of authentication [3]. This type of authentication is a combination of any of the three categories that were mentioned above. An ATM card is an example of this type as the user owns the card in addition to knowing the personal identification number. Two-factor authentication is more reliable, stronger, and more difficult than one-factor authentication. The user can access the system only if all authentication factors are successfully bypassed, verified, and in possession of the user [3]. Multi-

Manuscript received September 5, 2021
Manuscript revised September 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.9.45

factor authentication has attracted much attention from researchers due to issues targeting passwords, classic methods of being a single point of failure, vulnerabilities, and other problems [3].

Several services and organizations apply multi-factor authentication. Most of the sensitive systems are providing their services via the internet, such as banks. Providing online banking services provides advantages for both customers and banks, nevertheless, it presents dilemmas related to security and privacy because sensitive resources must be managed and protected safely and properly [4]. The multi-factor authentication method is effective and reduces the risks targeting the single-registration process. However, studies have shown that the multi-factor authentication method is seen to provide high levels of security, but it has been classified as more difficult, less appropriate, and necessitates longer execution time, compared to passwords [3]. There are negative experiences with multi-factor authentication techniques and tools among users, and when it is adopted, it encounters a widespread negative perception due to the tedious nature of several types of multi-factor authentication [3].

The security of multi-factor authentication is evaluated based on its resistance to attacks [4]. It is not yet stable, and this may be due to the lack of a unified approach in adopting multi-factor authentication and the consequence of the presence of many protocols for heterogeneous multi-factor authentication whose ownership has been registered in the past years [4]. Several initiatives propose unifying multi-factor authentication protocols to improve their security, organizing their design and adoption to be usable and safer [4]. Better and effective strategies of enhancing security levels should be applied when rejecting users for security tools such as multi-factor authentication [3].

Evidence of the success of authentication mechanisms is the guarantee of confidentiality, integrity, and availability [4]. In system security, authentication is crucial since it allows organizations to keep their networks safe. It enables only authenticated users (or processes) to access their protected resources, including computer systems, networks, databases, websites, and other applications or network-dependant services.

Biometric factors and one-time passwords are frequently applied in current systems. However, due to misuse reasons, these methods may be insufficient. Biometrics recognition may not be reliable due to false match rates and the exponential growth of the spoofing techniques. Moreover, once a biometric factor is stolen, it will be lost forever. One-time passwords (OTP) are also usually used due to their improvements in the security level. However, the risk of spoofing them is increasing with the invention of new techniques that easily allow redirecting them to the hacker's systems. Security-sensitive applications require powerful authentication techniques that guarantee powerful protection.

We propose in this paper an adaptive authentication scheme that follows a process of three complete phases. The proposed protocol integrates the use of biometric factors with OTP. We overcome the limitations of redirecting the OTP by verifying its correctness using the voice factor. Even if this factor is stolen, the OTP will be dynamically updated hence a new signature will be generated. A recurrent authentication phase is also added to overcome the espionage and misuse of activated sessions.

In this paper, we start by giving some crucial recommendations to protect our systems. Then, we detail our proposal that aims to ensure higher safety and improve the quality of the authentication protocol that uses passwords and one-time passwords, with adaptive authentication.

The remaining of this paper is organized as follows: In section 2, we cite the main problems that conducted us to this research paper. Section 3 presents our proposed solution and section 4 presents the performance analysis of our proposed scheme. Section 5 concludes this work and opens our future perspectives.

2. Problems statements

With smarter usernames and password laws, such as minimum length and complexity stipulations, such as using capitals and symbols, vulnerabilities of authentication strategies that are using passwords can be reduced to a fascinating extent. However, password-based authentication and knowledge-based authentication are more fragile to security issues than other authentication techniques.

Most current systems use multi-factor authentication, especially two-factor authentication, based on sending a one-time password. This method is correct, easy, and it guarantees us a high level of security and confidentiality for accounts. However, saving passwords is an option available on our devices. One of its advantages is that it facilitates the usage of applications, but in return, it has risks and disadvantages. When mobile is stolen or lost, and the password is saved on this device, this induces a risk that may enable opportunists to use the account illegally, even if adopting a one-time password since the chip is still inside the mobile. Spying on the cell phone, stealing the device password are all severe risks for these authentication methods. Let's assume that an account password is saved, a colleague in the office or a member of the family may overtake in carrying out unauthorized activities and without the consent of the owner of the account. Also, there is a risk of forgetting the mobile phone unlocked anywhere and with saved passwords.

Taking some countermeasures to preserve our passwords is essential and may protect our accounts by being attentive such as avoiding sharing sensitive data and browsing malicious websites and links. However, we cannot guarantee that we are safe. Hackers are inventing new techniques to steal our data, not only passwords but also one-time passwords (OTPs) and login links. They can redirect SMS to their systems using dedicated services of text-messaging management meant for businesses. The services that redirect SMSs to the hackers' systems can be availed by just paying $16 in the US [7]. Despite that these services are designed for business usage, they are being misused by hackers, without users' permission, to reset their accounts passwords and to use some sensitive services. Therefore, multi-factor authentication that depends on a one-time password improves the security levels, but this is still insufficient because of the risks discussed above.

3. Contributions

3.1 Recommendations and improvements

The increasing use of technology forces us to improve the levels of safety and security. It is always crucial to adapt new technologies in data confidentiality, depending on the latest protocol versions. In the following, we give some recommendations that may improve the level of security and safety of our sensitive data:

- We have to maintain devices and avoid moving away from them, of course, we have to do not save passwords on devices, that have to be efficiently protected.
- Strong and complex passwords are recommended, avoid using personal information, and do not duplicate passwords on various accounts.
- We must avoid revealing our identity or password to anyone and make sure that we log out and close our accounts after using them.
- Avoid sharing personal or confidential information in any mail that we want to send to a specific destination such as a bank.
- Do not use words that are obtainable from the dictionary.
- Do not use serial numbers like 123 or keyboard styles like asdf.
- Never share the password and do not disclose any personal information such as account number, personal identification number, one-time password.
- Do not click on links in emails and use software to reduce the number of harmful emails.
- It is recommended to use an anti-virus program as well as use a personal firewall.
- Follow the latest methods to combat fraud on the Internet.
- Use multi-factor authentication for remote access to accounts.
- Prevent direct access and interaction with databases for all users except for those responsible for the database, users' access and interact with databases only through applications.
- Periodically review access rights and user identities to the systems.

3.2. multi-layer authentication scheme

As mentioned above, one-time passwords are not sufficient in protecting our systems. We can also use multi-factor authentication to improve the security level. In our proposal, we suggest a multi-factor authentication system as presented in figure 2.

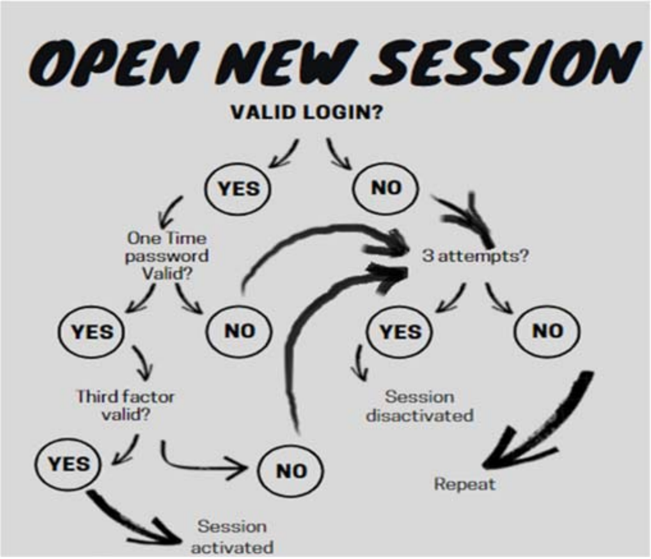


Fig. 2 Multi-levels authentication process

Based on the notation shown in Table 1, we illustrate in figure 3 the sequence diagram for the execution of our scheme.

Table 1: Notations

Notation	*Description*
UN	User Name
PWD	Password
OTP	One-Time Password
TAF	Third Authentication Factor

To activate a new session, at least two factors have to be verified, password and one-time password. Our fundamental contribution is the amelioration of OTP verification. Two main methods are useful to receive OTP by the end-user: SMS-based and TOTP-based. For the first method, the user will receive a text message containing the OTP.

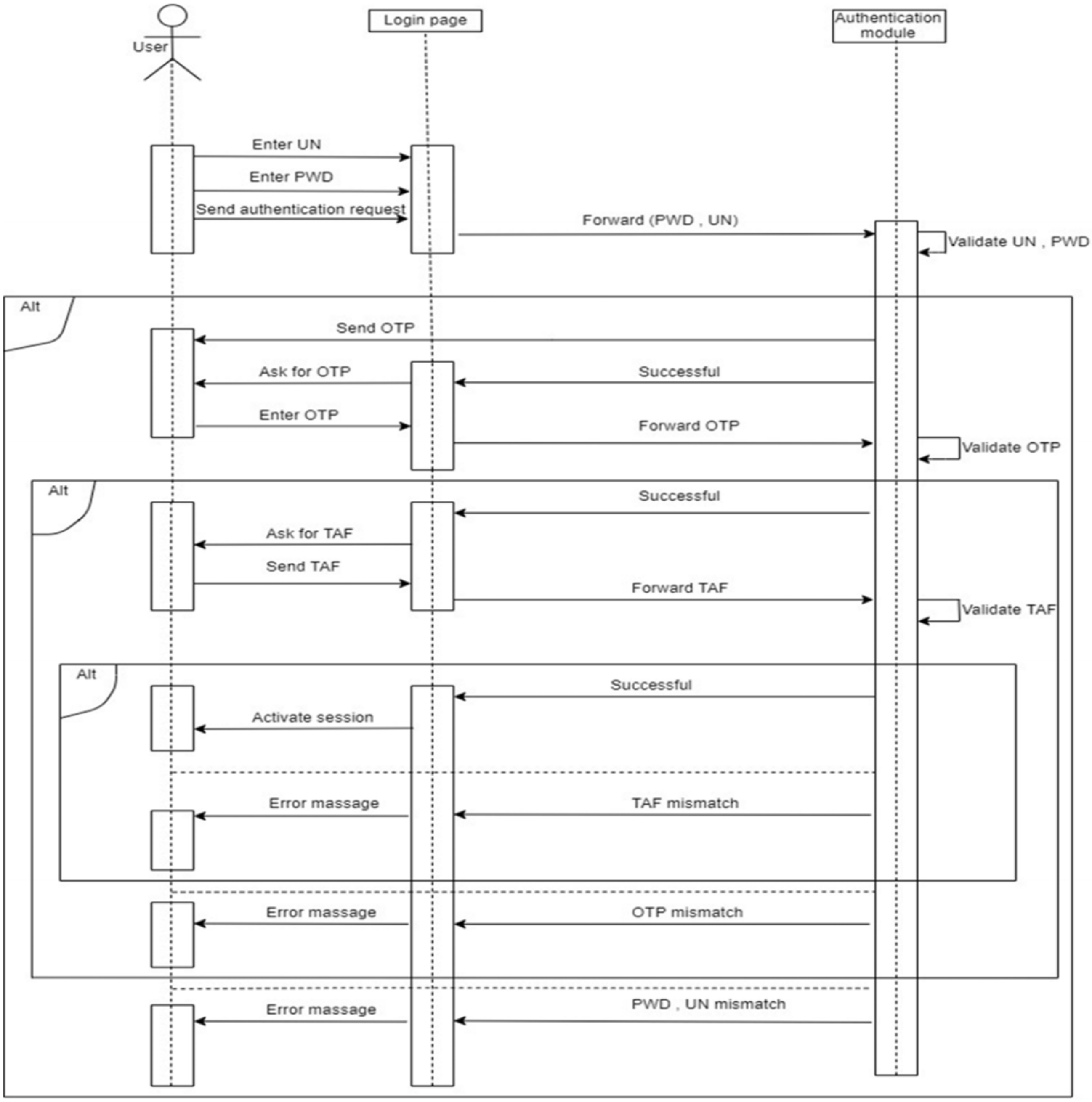


Fig. 3 Multi-levels scheme’s sequence diagram

In the second method, the user will receive a QR image that will generate a password after scanning. Whether this OTP was received via SMS or generated via TOTP, the risk of stealing this information persists with high risk, as detailed in the problem presentation section.

To surpass this problem, we suggest improving the verification of the OTP process. In fact, instead of texting the received OTP, we recommend that the user answers with his voice as a biometric factor. Subsequently, after receiving the OTP, the user may send a voice message containing the OTP. Then, the server can convert the received voice message into text data, using speaker recognition techniques. After that, the OTP can be easily verified. It is not enough to confirm that the converted text match the received OTP, but also a match of the user's voice must be established. Figure 4 summarizes this process.

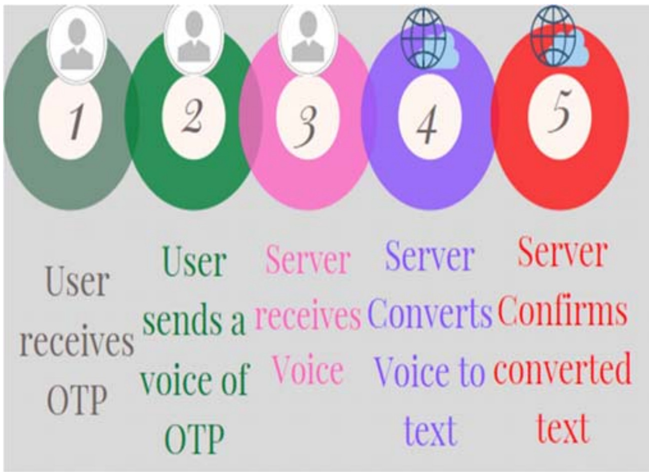

1
2
3
4
5
User receives OTP
User sends a voice of OTP
Server receives Voice
Server Converts Voice to text
Server Confirms converted text

Fig. 4. OTP verification process

Speaker recognition is an important biometric solution that identifies a user based on his voice by passing two main phases: speaker identification, to decide whether a speaker is a definite person, and speaker verification, to determine whether the speaker will be accepted or rejected [8].

The third authentication factor, that we suggest in our proposed scheme is unrestricted. The user may activate or deactivate it. Of course, in the case of sensitive applications, we recommend this factor usage to guarantee an enhanced level of security.

When the TAF is activated, our scheme will include a second level of authentication that we denote: update authentication. After a predefined period, the system performs a check of the TAF. The goal behind that is to guarantee that the session's user is legitimate. For the TAF, we recommend using the voice biometric factor, as the server uses it to verify the OTP. Here, a new OTP can be resent to the user and the OTP verification process may be re-executed.

The third level of authentication of our proposed scheme consists of re-authentication required to execute sensitive transactions. This extra level is recommended in authentication to sensitive systems such as banking transactions and governmental operations. To execute a sensitive request, even if a session is activated, a user must re-authenticate. Here, as for the periodic authentication, only the TAF must be verified. The theory of various authentication levels is summarized in figure 5.

4. Performance evaluation

To evaluate the proposed scheme, we conducted both simulations and mathematical analyses**.**

4.1 Mathematical model

In this section, we mathematically explain and evaluate the proposed scheme. According to the proposed scheme, to activate a session, three factors have to be successfully verified: PWD, OTP, and TAF

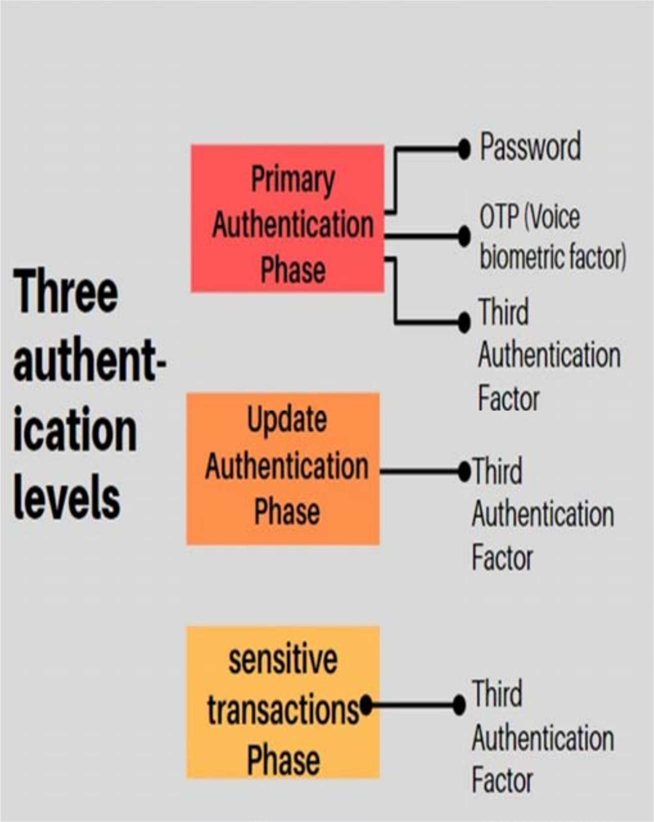

Three authent-ication levels
Primary Authentication Phase
Password
OTP (Voice biometric factor)
Third Authentication Factor
Update Authentication Phase
Third Authentication Factor
sensitive transactions Phase
Third Authentication Factor

Fig.5. Multi-authentication levels

Let's define the following events (figure 6 represents the relationship between events):

- W: Password successfully verified. P(W) is the probability that the event W happens. $P(\overline{W})$is the probability that the event W does not happen.
- O: OTP successfully verified. P(O) is the probability that the event O happens. P((Ö)) is the probability that the event O does not happen.
- T: TAF successfully verified. P(T) is the probability that event T happens. $P(\overline{T})$ is the probability that the event T does not happen.
- A: Activate a new session. P(A) is the probability that event A happens. P((Ä)) is the probability that the event A does not happen.

The conditional probability of O knowing W (probability that event O occurs knowing that event P occurs) can be represented by the formula (1)

$$PW(O)=\frac{P(W\Omega O)}{P(W)} \qquad (1)$$

$$P(\overline{W}) = 1 - P(W)$$

The conditional probability of T knowing O can be represented by the formula (2)

$$PO(T)=\frac{P(O\Omega T)}{P(O)} \quad (2)$$

$$P(\overline{T}) = 1 - P(T)$$

The probability of activating a session is modelled using a weighted tree figure 7. For this, we can consider three levels of branches: a first level which indicates the probability of the event W, then a second level which represents the conditional probabilities with the event O, and finally a third level which figures out the conditional probabilities with the event T. We deduce the probability of a (P(A)) by formula (3)

$$P(A)=P(W\Omega O\Omega T)=P(W)*PW(O)*PW\Omega O(T) \quad (3)$$

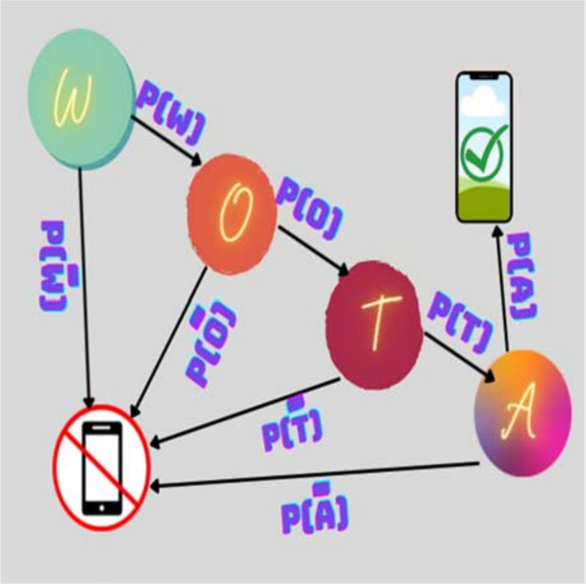


Fig. 6. Conditional relationships of events

Assuming that events W, O, and T are independent. A hacker can redirect OTP without knowing the password or may be able to spoof the TAF without knowing neither the PWD nor the OTP. We draw in figures 8 the probability of hacking a session (taking random values for the probability of the three events.

As clearly shown in figure 8, the probability of hacking a session, using our proposed solution (from 0 to 0.6) is too much less than that using either only passwords (from 0 to 1) or using both passwords and OTPs (from 0 to 0.8). Thus, a hacker must complete the three authentication levels to activate a session.

4.2 Simulations

To simulate the performance of the proposed solution, we used the well-known scyther simulator. It is a tool for the automatic confirmation, falsification, and analysis of security protocols. Also, it can be applied to detect dilemmas that result from the way the protocol is created and allow to test protocols with an unlimited number of sessions and nonces.

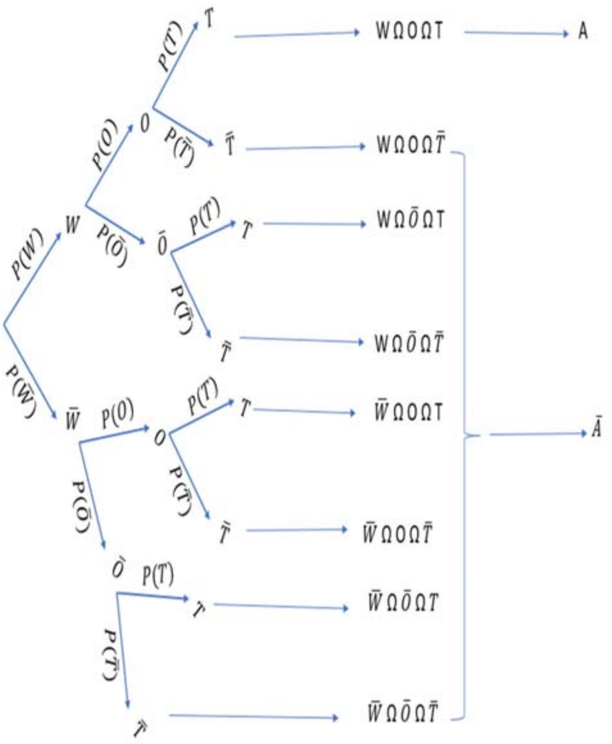


Fig. 7. Probability of activating a session using a weighted tree

It is used to describe protocols, yielding a finite representation of all possible protocol behaviors. It allows to efficiently analysis security protocols to identify possible attacks and vulnerabilities. The tool has also been used to find new multi-protocol attacks on many current protocols by verifying whether the security claims in the protocol description hold or not.

For our proposal, we assume that a trusted link is open and it connects the mobile device and the authentication server. Also, the user machine allows catching the specified biometric factor. In addition, the authentication server and the database server can verify the validity of the exchanged biometric factor. The implemented protocol consists of a translation, using scyther simulator, of the process presented in figure 3. We have a couple of events in our protocol that are received and send. We have three main agents: the authentication server, the database server, and the mobile device. Results, shown in figure 9, prove that the proposed solution is safe and guarantees a high level of security, regarding different claims. The proposal protects sensitive information from being manipulated by hackers. It resists malicious user attacks that cheat the server by accessing its services thanks to the periodic authentication as well as the re-authentication required for performing transactions.

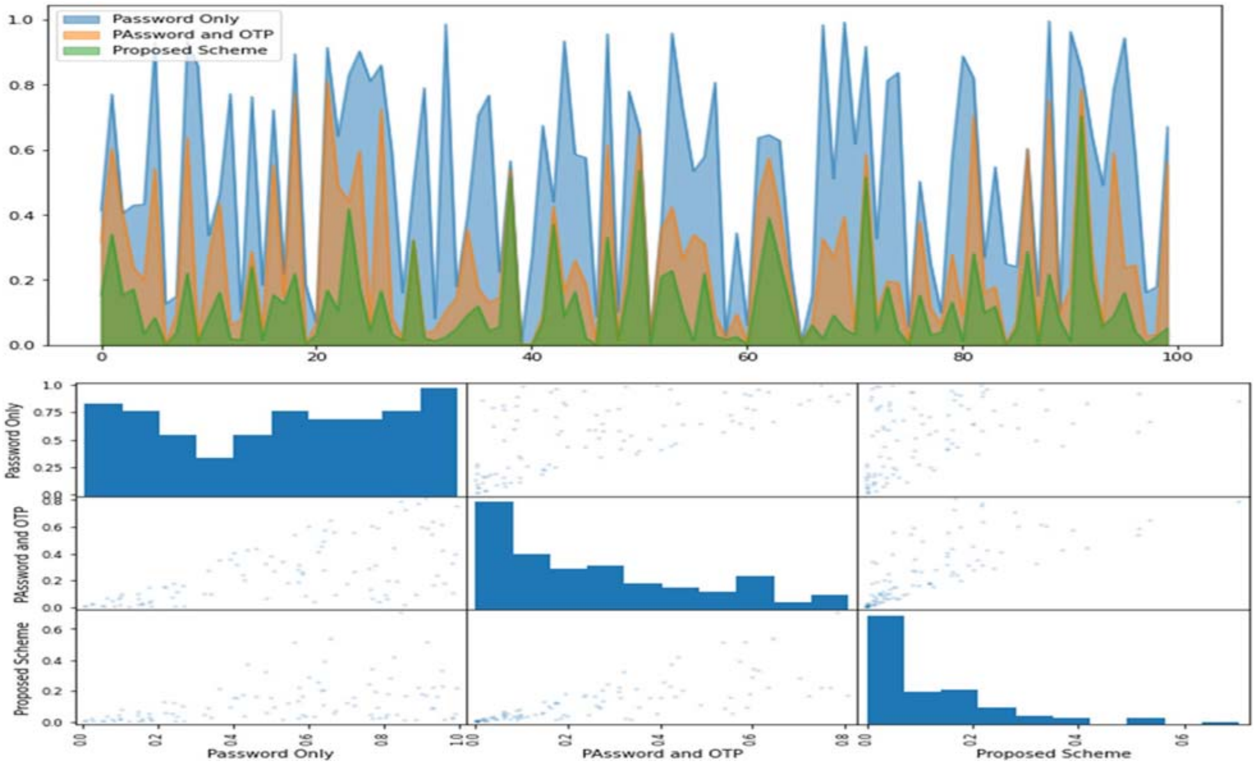
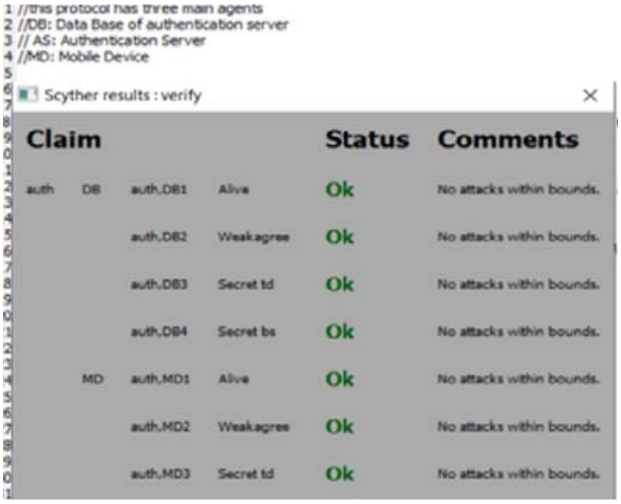


Fig. 8. Comparison of probabilities of hacking a session

We used biometric factors due to their promising advantages as during the Covid-19 pandemic, it has proven to be an advantage by utilizing facial technology with masks on as well [9]. Authors in [10] have proposed a three-level authentication process. However, if we compare our proposed protocol with their solution, we find that they only used texting factors in the three authentication levels.


```
//this protocol has three main agents
//DB: Data Base of authentication server
// AS: Authentication Server
//MD: Mobile Device
```

Claim				Status	Comments
auth	DB	auth,DB1	Alive	Ok	No attacks within bounds.
		auth,DB2	Weakagree	Ok	No attacks within bounds.
		auth,DB3	Secret td	Ok	No attacks within bounds.
		auth,DB4	Secret bs	Ok	No attacks within bounds.
	MD	auth,MD1	Alive	Ok	No attacks within bounds.
		auth,MD2	Weakagree	Ok	No attacks within bounds.
		auth,MD3	Secret td	Ok	No attacks within bounds.

Fig. 9. Claims'verification

However, we designed our solution using both texts and biometric factors including dynamic verification of the OTP using the user's voice. Another proposal [11] has been presented for sensitive banking applications by using fingerprint biometrics, along with a smart card and GSM technologies.

Despite that this solution enhances the security of authentication to the ATM systems, our solution, if adopted, will guarantee better security. In their proposal, if the user's mobile and fingerprint are stolen, the ATM system will be hacked. However, using our scheme, the

OTP has to be verified using the user's voice which even if stolen, the verification will not be performed successfully since the OTP is of single-use. The solution given in [12] uses a pair of random fingerprints from the user and converts it into a hash instead of taking a username and password. The main concern about this proposal is the use of the biometric factor only which, as mentioned above, if stolen will be lost forever. Using our solution, even if the biometric factor is stolen, the OTP conversion using the user's voice cannot be performed.

5. Conclusion and future work

Multi-factor authentication that depends on a one-time password became insufficient in guaranteeing a high-security level for our accounts particularly with the increase in technologies and the invention of new modern hacking solutions. The current paper presents a solution that is composed of a multi-level authentication: primary (using three factors), update, and pre-transaction. The proposed solution provides a high-security level for security-sensitive applications, thanks to the usage of voice recognition in the verification of the OTP. In addition, we overcome the main problem addressed in this paper which is the loss of the biometric factor.

The proposal may be costly in terms of energy consumption and the complexity of computations. However, we recommend adapting it in sensitive applications that are not frequently used and that require an extra level of security such as in banking systems. For the ordinal applications, for simplicity issues, we recommend avoiding using the third authentication factor as well as avoiding the pre-transaction authentication phase.

As future work, we may present an adaptive study that recommends which authentication level to use according to potential scenarios

Acknowledgments

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

[1] Stamp, M. (2011). Information security: principles and practice. John Wiley & Sons. ISBN: 978-1-118-02796-7, https://www.wiley.com/en-s/Information+Security%3A+Principles+and+Practice%2C+2nd+Edition-p-9781118027967

[2] Fatma Hendaoui, Hamdi Eltaief, Habib Youssef, UAP: A unified authentication platform for IoT environment, Computer Networks, Volume 188, 2021, 107811, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2021.107811.

[3] Das, S. (2020). A risk-reduction-based incentivization model for human-centered multifactor authentication (Doctoral dissertation, Indiana University). https://www.proquest.com/openview/38faf90785cf47c99733 3c8a799e1e83/1?pq-origsite=gscholar&cbl=18750&diss=y

[4] Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Nicola Zannone, A survey on multi- factor authentication for online banking in the wild, Computers & Security, Volume 95, 2020, 101745, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101745.

[5] Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-Factor Authentication: A Survey. Cryptography. 2018 Jan 5;2(1). https://doi.org/10.3390/cryptography2010001

[6] Patel C., Doshi N. (2019) Security Challenges in IoT Cyber World. In: Hassanien A., Elhoseny M., Ahmed S., Singh A. (eds) Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-01560-2_8

[7] Is your OTP safe? Here is how hackers are redirecting your SMS. https://www.businesstoday.in/latest/trends/is-your-otp-safe-here-is-how-hackers-are-redirecting- your-sms/story/433994.html. Date accessed: 06-13-2021

[8] Supeshala, Chamidu. (2017). Speaker Recognition using Voice Biometrics. https://www.researchgate.net/publication/344349873_Speaker_Recognition_using_Voice_BiometricsFigures

[9] Alston, A. (2021). A new era in cybersecurity through biometric technology (Order No. 28494739). Available from ProQuest Dissertations & Theses Global. (2537678931). Retrieved from https://www.proquest.com/dissertations-theses/new-era-cybersecurity-through-biometric/docview/2537678931/se-2?accountid=34495

[10] Mishra, Gouri & Mishra, Pradeep & Nand, Parma & Astya, Rani & ., Amrita. (2020). User Authentication: A Three Level Password Authentication Mechanism. Journal of Physics: Conference Series. 1712. 012005. 10.1088/1742-6596/1712/1/012005.

[11] B Poornima, Dr. Savadam Balaji. (2021). Cyber Security for Atm Terminals. Annals of the Romanian Society for Cell Biology, 8785–8789. Retrieved from https://www.annalsofrscb.ro/index.php/journal/article/view/3599

[12] Tabassum M., Sarower A.H., Esha A., Hassan M.M. (2020) An Enhancement of Kerberos Using Biometric Template and Steganography. In: Bhuiyan T., Rahman M.M., Ali M.A. (eds) Cyber Security and Computer Science. ICONCS 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 325. Springer, Cham. https://doi.org/10.1007/978-3-030-52856-0_9

Amal Rwily: Master student in jouf university received the B.E.. degrees, from jouf Univ

Saloua Hendaoui received the B.E. and M.E. degrees, from tunis Univ. in 2011 and 2009, respectively. She received the Dr.. degree from Cartage Univ. in 2017. Working as a assistant professor (from 2018) in the Dept. of computer Science Jouf University