SECURE USER AUTHENTICATION (QR CODE, EMAIL VERIFICATION, ONE TIME PASSWORD (OTP)) SCENARIO

CENG 3544, COMPUTER AND NETWORK SECURITY

Ali Tiryaki
alitiryaki@posta.mu.edu.tr

Saturday 8th June, 2024

Abstract

This paper discusses a brief understanding of the secure user authentication techniques such as QR code, email verification, and One-Time Password (OTP). It is to discuss the aforementioned methods and its application to improving security of the user. Through these methods the study also notes the benefits, drawbacks and possible usage of all the methods studied. It will also be of immense benefits to the students and researchers who are in need of appropriate secure authentication mechanisms.

1 Introduction

Because many services go through the internet now, user authentication security has become more significant in the current world. This is vital as the usage of the internet and widely connectivity increases the exposure to threats and vandals. This study explores three popular authentication methods: decoding a QR code, confirming an email address, and using one-time passwords.

As known as quick response codes,[1] QR layout is an effective way of allowing users to be authenticated through a mobile device by scanning a certain code.[2] Email verification as another kind of the validation process involved sending a verification link to the user's email address in order to prove their identity. Passwords are a set of letters and numbers that must be entered on the website and can be received on a phone as OTP's for a certain amount of time, making it more secure. All these methods come with their endemic merits and disadvantages thus being appropriate to be used in particular circumstances.

Thus, the goal of this study is to describe the mentioned authentication methods, assess its performance, and reveal its practices. The structure of the study is as follows: Section 2 introduces each approach in detail, Section 3 focuses on the literature review and Section 4 discusses the system design, Section 5 presents the actual deployment and Section 6 evaluates the outcome. Last but not least, Section 7 presented the key findings of the research and suggestions for further studies.

2 Fundamentals

2.1 QR Code Authentication

QR codes are quick response codes in that they are two-dimensionalbarcodes that are read using a smartphone or a QR code scanner.[3] Some of the application of this authentications includes the following: In the case of authorization a QR code can be created and then captured on a login page. With the use of their device the user is require to scan a QR code which in turns check the code with the server to allow the user in.

2.2 Email Verification

The process of email verification is set up through the sending of a verification link through an email. After clicking the link, the user is verified, and if valid, the access to the relevant application is granted.[4] It is used often during registration of accounts or where passwords have been forgotten or lost.

2.3 One-Time Password (OTP)

OTP is a password that is generated by static and dynamic factors to ensure user's identification.[5] Of the account passwords, an OTP is a password that is only allowed for a single login or transaction. It is commonly delivered via the user registered mobile number or the email id. The entered OTP is to be used for completing the authentication process within a specific period of time.

3 Related Works

Several studies have explored various authentication methods to enhance user security. For instance, research on QR code authentication has shown its effectiveness in providing a seamless user experience while maintaining security. Email verification is widely adopted in many systems due to its simplicity and effectiveness in confirming user identity. OTPs are popular in banking and financial services, where high security is required.[6]

There are extensive sources of research works that investigate different aspects of security concerning QR codes, email authentication, and OTPs. Saranya et al. (2016) also explained the present-day uses of QR codes for security with the intention of emphasizing on their capability in secure authentication. Chen et al. (2020) proposed an analysis of the email sender authentication discussing how the inadequate authentication methods are critical to using emails. Literature review revealed that Parmar et al. (2012) developed a method that can also create one-time passwords using image authentication to secure the passwords and avoid use of traditional OTPs. Narayanan (2012) discussed on the security solutions offered by QR codes and the research revealed that such a tool could improve the degrees of security. These works offer benefit to the literature as a whole and can help further the research on the specific topics of QR codes, email verification, and OTPs for secure authentication.[7, 8, 9, 10]

This study builds on existing research by providing a comparative analysis of QR codes, email verification, and OTPs in various scenarios.

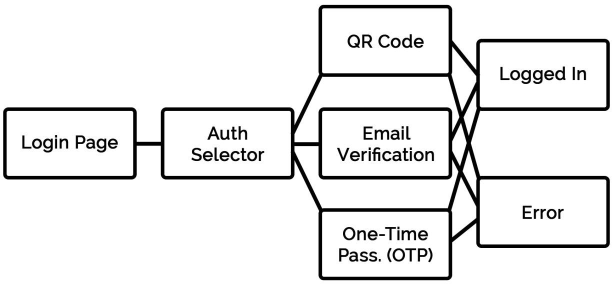

Figure 1: Demo System Architecture

4 System Proposal

The proposed system firstly involves the use of a QR code, followed by the verification of the email that the user provides, and then OTP authentication to improve the system's security and convenience. The overall system consists of three main components:

QR Code Generator: Generates a unique QR code for each authentication request. Email Verification System: Sends a verification email with a secure link to the user. OTP System: Generates and sends a one-time password to the user's phone or email.

4.1 System Architecture

The system architecture is presented in the following Figure 1. This consists of a front end with control panel, server to authenticate the users and DBMS. Of the three methods of option, the user selects one and sets processes the stage for authentication. The request is taken to the server which in turn produces the relevant code or link and then authenticates the user.

5 Implementation

The prototype system is developed in Python platform and uses Flask for the web application development. The system does not rely on any specific hardware and it can be deployed on virtual environment.

You can find this study's demo inside this GitHub repo.

5.1 QR Code Authentication

The system establishing QR code authentication is developed using a QR code generation library, base64 decode library and python imaging library (PIL). If the user chooses QR code authentication, the server then produces a QR code that appears on the screen to the user. The user uses his/her mobile app to scan the given QR code (the user must logged in within the app), while the server authenticates the code.

5.2 Email Verification

The email verification system incorporates the help of a server support method (SMTP) to send the verification emails. Selecting the email verification option, the server in turn sends to the user's email address, a unique hyperlink. The user proceeds and clicks on the link so as to confirm his or her identity.

5.3 One-Time Password (OTP)

The OTP system that is used is an implementation PyOTP. Whenever the OTP authentication is chosen by the user, the server will then automatically generate a one time password and send it in the phone or in the email of the said user. The OTP is then typed in by the user where the server authenticates it on the same login page. For easy connection, the server creates a qr code that can be scanned by an authenticator app.

6 Results and Discussion

The proposed system was tested in various scenarios to evaluate its effectiveness and user experience. The results showed that:

- **QR Code Authentication**: QR Code Authentication provided a quick and seamless user experience but required a smartphone with a QR code scanner. The response time was minimal, making it suitable for fast-paced environments.
- **Email Verification**: Email verification was easy to implement and use but depended on the reliability of the email service. Users reported delays in receiving emails in some cases, which could hinder the login process.
- **One-Time Password (OTP)**: OTP authentication offered the highest security but required users to have access to their phone or email. The OTPs were valid for a short duration, reducing the risk of misuse but adding an extra step for the user.

The comparative analysis of these methods is shown in Table 1. The table highlights the key aspects of each authentication method, including security, user experience, and implementation complexity.

Table 1: Comparison of Authentication Methods

Aspect	**QR Code**	**Email Verification**	**OTP**
Security	Medium	Medium-High	High
User Experience	High	Medium	Medium
Implementation Complexity	High	Low	Medium

The study found that combining these methods can provide a flexible and robust authentication system. By leveraging the strengths of each method, it is possible to create a secure and user-friendly authentication process that meets diverse needs.

7 Conclusion

This study analyzed and compared three secure user authentication methods: QR codes, email verification, and OTPs. Each method has its own strengths and is suitable for different scenarios. By integrating these methods, the proposed system provides a secure and user-friendly authentication process. Future work will focus on improving the system's scalability and exploring additional authentication methods.

Acknowledgement

In the implementations, I would like to thank `freecodecamp.org` and Abhishek Saud for tutorials. I would like to thank ChatGPT for correcting the grammatical errors.

References

[1] J.-P. Lacroix, S. Lacroix. QR Codes whitepaper. 2011. Go to Article

[2] T. Chen; Y. Ishino. Study on Popularization of QR Code Settlement in Japan. Springer, 2019. Go to Article

[3] C. Chengsheng. QR Code Authentication with Embedded Message Authentication Code. Springer, 2016. Go to Article

[4] J. Diaz. On securing online registration protocols: Formal verification of a new proposal. ScienceDirect, 2014. Go to Article

[5] H. Wang. A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP). IEEE Xplore, 2011. Go to Article

[6] A. Menshchikov; A. Komarova. Comparison of Authentication Methods on Web Resources. Springer Link, 2017. Go to Article

[7] K. Saranya; R.S. Reminaa; S. Subhitsha. Modern applications of QR-Code for security. IEEE Xplore, 2016. Go to Article

[8] J. Chen; V. Paxson; J. Jiang. Composition Kills: A Case Study of Email Sender Authentication. Usenix.org, 2020. Go to Article

[9] H. Parmar; N. Nainan; S. Thaseen. Generation of Secure One-Time Password Based on Image Authentication. CS & IT-CSCP 2012, DOI: 10.5121/csit.2012.2417. Go to Article

[10] A. Sankara Narayanan. QR Codes and Security Solutions. International Journal of Computer Science and Telecommunications (IJCST), 2012. Go to Article