A survey of Two Factor Authentication Methods : Advantages & Disadvantages

Shiburaj Pappu
Department of Electronics & Telecommunication Engineering,
Rizvi College of Engineering,
Mumbai, India.
shiburaj@eng.rizvi.edu.in

Dhanashree Kangane
Department of Electronics & Computer Science Engineering,
Rizvi College of Engineering,
Mumbai, India.
dhanashree.kangane@eng.rizvi.edu.in

Junaid Mandwiwala
Department of Electronics & Telecommunication Engineering,
Rizvi College of Engineering,
Mumbai, India.
junaidsir@eng.rizvi.edu.in

Dr. Varsha Shah
Principal,
Rizvi College of Engineering,
Mumbai, India.
principal@eng.rizvi.edu.in

***Abstract*— Authentication forms an important step in any security system to allow access to resources that are to be restricted. In this paper, we compare the advantages and disadvantages of two authentication methods. We begin with the details of existing systems in use and then compare the two systems viz: Two Factor Authentication (2FA), Risk-Based Two Factor Authentication (RB-2FA). We also introduce a new variation of the risk based two factor authentication system called the artificial-intelligence assisted two-factor authentication.**

Keywords—Risk- based authentication, Two- factor authentication.

I. INTRODUCTION

As the number of web applications is increasing day by day, a greater number of private data is being generated, and hence comes the need to access these resources in a protected and secure manner. Authentication and authorization form the basis in most web services in today's era for accessing protected data. Many methods of authentication exist today, each applicable to a certain type of application. There are five main authentication methods:

1. Password-based Authentication.
2. Multi-Factor Authentication
3. Certificate-Based Authentication
4. Biometric Authentication
5. Token-based Authentication.

The simplest form of authentication involves the use of a simple username and a password. With simplicity comes the problem of easily getting your account compromised. Attackers may use different techniques like brute-forcing, keyloggers, etc. to access your private resources. This may be easily protected with the help of the second method that is multi-factor authentication. In this method, the user needs to enter additional information other than the password to access their resource. This is by far the safest and most used authentication method for good security. The third method of authentication is using a certificate file generated by a certifying authority. Any access to the resource needs the user to first share the certificate with the server and get the request authenticated. If the certificate is incorrect or has expired, then the access is rejected. This type of authentication is used everywhere from your browser which uses it for SSL certificate to the server access through the terminal. The main issue with this is the user needs to have the key file always with them to authenticate. Which makes it a little inconvenient. Hence this method is restricted to advanced users and programmers. The fourth method is to use a type of biometric device to scan your fingerprint, iris, etc. to authenticate. This is a very secure method but requires additional hardware cost hence it's not feasible to be used at every website. The last method is by using token-based access. This method is mostly used by mobile applications for accessing the protected resources. But the issue with this method is that it is dependent on the first two methods to get the initial token. Hence indirectly the security of this method depends on the method that is used to get the token. From this it is clear, that for accessing the web resources the first two methods are used, most of the time. In this paper, we are going to discuss the second method (Two Factor Authentication to be more specific) in much more detail.

II. TWO FACTOR AUTHENTICATION (2FA)

A. *Basics*

Two-factor authentication methods rely on a user providing a password, as well as a second factor, usually either a security token or a biometric factor, such as a fingerprint or facial scan [1].

B. *Second Factor*

Different types of authentication factors: -

1. **Knowledge Factor**: some code you already have like PIN, shared key, etc.
2. **Possession Factor**: something the user has like a mobile device, security token, etc.
3. **Inherence Factor**: is something inherent in the user's physical self like a fingerprint, etc.
4. **Location Factor**: users' location is used as the second factor.
5. **Time Factor**: restricted access within a timeframe.

Out of the above factors, the most used is the possession factor. The most popular way of using this factor is with the help of access code on your mobile device using SMS or email id or using the google authenticator app, etc.

C. The Working of 2FA

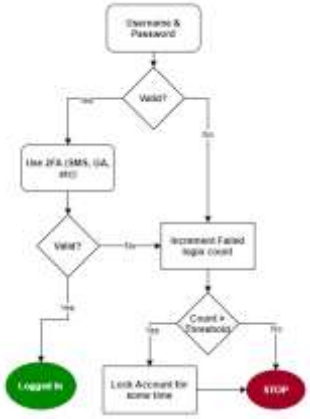

Figure 1: Working of 2FA.

The process starts with the user entering a username and password. This is then checked for validity against the data stored in the database of the server. If the credentials are valid then the user is required to enter an additional code sent to their mobile or email etc. to which the user should have access. If this code is verified, then the user is logged in to the system. If the user fails in either the first factor or at the second factor, then the server may implement a failed login counter which can be incremented. A threshold is set for how many incorrect attempts are allowed before the account gets locked out. Usually, this will be a temporary lock for some duration typically a few hours. This is done to prevent brute force and 2FA abuse.

D. Advantages of 2FA

- It is highly secure as the access to the second factor is usually with the user only.

E. Disadvantages of 2FA

- It adds complexity to the implementation.
- It adds an additional step for authentication which some users may not like.
- Huge Cost is involved if SMS & email is used for delivery of the access code.
- Time is wasted waiting for the access code.
- The user will have to carry the registered device to get the token in the case of SMS & Google Authenticator.

III. Risk-Based Two Factor Authentication (RB-2FA)

A. Basics

As explained in the previous method of authentication, the 2FA is very secure, but at the same time, it has two major drawbacks. Firstly, it adds to the cost of operation of the system as sending of SMS is costly. Secondly, every time entering the access code increases the delay to get into the users' account. The first problem can be easily accomplished by alternative methods of sending the access code like using Google Authenticator but then the users need to do an initial setup and also need to install a separate app to do so. This may not be acceptable by many of the users. So to overcome both these problems the Risk-based Two Factor Authentication Method is used.

This method at its core is analyzing the risk associated with the user during the login process. Risk-based authentication (RBA) is an adaptive security measure to strengthen password-based authentication. RBA monitors additional features during login, and when observed feature values differ significantly from previously seen ones, users have to provide additional authentication factors such as a verification code as in 2FA [2].

B. The Working of RB-2FA

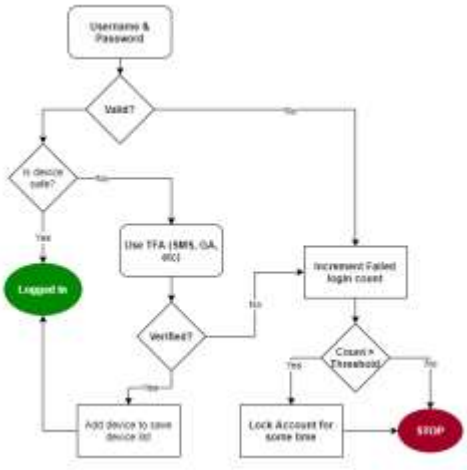

Figure 2: Working of RB-2FA.

The process starts with the users entering their credentials. This is verified by the server. If it's validated, then instead of going for 2FA the system will first check if the user agent from which the request is sent is in the safe list of devices of the particular user. If it is in the safe list, then the user is logged indirectly. If the device is encountered for the first time, then 2FA is used. After verifying the access code entered by the user the device is added to the safe list of the user [3].

C. Advantages of RB-2FA

- It is secure.
- Avoids the use of access code every time the user logs in.
- It is fast compared to 2FA.
- Low cost as access codes is sent only when accessing from a new device.
- Increases the user experience as the user has to enter the access code only once on every new device.

D. Disadvantages of RB-2FA

- Security is compromised slightly if the attacker uses the same device that was previously marked safe to attack the user's account. This is possible in the case of the user trying to access the account from a public device.
- Additional storage capacity is required to store the safety devices of the user.

Artificial Intelligence is used in predicting the user behaviour based on their browsing history [4] and then predicting the user agent with the help of appropriate Machine learning algorithms for suggesting which user authentication method to be used [5,6].

IV. Proposed Methodology

The RB-2FA solves all the major concerns of the 2FA. The main drawback of RB-2FA is the slightly reduced security due to attacks from any of the safety devices. We propose a new method in this paper which we termed as the "***Artificial Intelligence assisted Risk Based Two Factor Authentication***". In this method, we will be monitoring the user preferences/features for some time to train a model using the selected AI algorithm (KNN). Once the desired accuracy is achieved the system will be able to analyse the user based on the feature selected during login. The process starts by changing the default login form with a single login button with multiple ones each with different unique features like different colour, shape, language, position, etc. After proper training of

the AI Model the system will be able to identify an attacker from the real user by analysing the user behaviour.

A. *Advantages of AIA-RB-2FA*

- Enhances the security of the RB-2FA method.
- Reduces the cost of delivering the access code as compared to 2FA.

B. *Disadvantages of AIA-RB-2FA*

- Additional storage of all the features is required for each user.
- Saving of the model is also required for faster response time.
- Will require additional computing power in the server to run the AI.
- The model may not predict accurately if there is no sufficient data to train the AI model.

V. FUTURE SCOPE

A better analysis of this method needs to be done after a good amount of training data is available for testing this authentication method properly. Many other AI algorithms may be used instead of the KNN algorithm and proper analysis needs to be done for deciding the best algorithm suited for the proposed authentication method. Other features may also be introduced which may improve the AIA-RB-2FA method further.

REFERENCES

[1] De Cristofaro, E., Du, H., Freudiger, J., Norcie, G.: A comparative usability study of two-factor authentication. In: USEC 2014, February 2014.

[2] Cristiano C. Rocha, Joao Carlos D. Lima, M. A. R. Dantas and Iara Augustin, "A2best: An adaptive authentication service based on mobile user's behavior and spatio-temporal context", IEEE Symposium on Computer and Communication (ISCC), pp. 771-774, 2011.

[3] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono. 2020. More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In Annual Computer Security Applications Conference (ACSAC '20). Association for Computing Machinery, New York, NY, USA, 203–218. DOI:https://doi.org/10.1145/3427228.3427243.

[4] M. Misbahuddin, B. S. Bindhumadhava and B. Dheeptha, "Design of a risk based authentication system using machine learning techniques," 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/ SCALCOM/ UIC/ATC/ CBDCom/IOP/SCI), 2017, pp. 1-6, doi: 10.1109/UIC-ATC.2017.8397628.

[5] L. Chen, Y. Zhong, W. Ai and D. Zhang, "Continuous Authentication Based on User Interaction Behavior," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757539.

[6] Wiefling S., Patil T., Dürmuth M., Lo Iacono L. (2020) Evaluation of Risk-Based Re-Authentication Methods. In: Hölbl M., Rannenberg K., Welzer T. (eds) ICT Systems Security and Privacy Protection. SEC 2020. IFIP Advances in Information and Communication Technology, vol 580. Springer, Cham. https://doi.org/10.1007/978-3-030-58201-2_19.