International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey of Various Authentication Methods for Mobile Phones

Khalif Ahamed U [a], Tamilarasan [b]

[a] *Graduateship / Associate Membership, Computer Science, Indian Institute of Industry Interaction Education and Research*
[b] *Project Coordinator / Indian Institute of Industry Interaction Education and Research*

DOI: https://doi.org/10.55248/gengpi.4.1223.123520

ABSTRACT

Authentication is a procedure by which a system authenticates the uniqueness of a user. User authentication is the mechanism for authentication and protects user data or unauthorized access of information. The major drawback of authentication performed in mobile phones including something that the user possesses is that the physical token (the USB stick, the bank card, the key or similar) must be carried around by the user, practically at all times. Loss and theft are a risk. There are also costs involved in procuring and subsequently replacing tokens of this kind. In addition, there are inherent conflicts and unavoidable trade-offs between usability and security. The Two Factor Authentication scheme is easy through different attack i.e. dictionary attack, brute force attack, shoulder-surfing. This paper presents the survey of Multifactor authentication methods, challenges, security attack and the comparison of mobile device authentication methods.

Keywords: Reach Authentication, Two Factor authentication, Multifactor authentication, OOB

1. Introduction

Recently, Internet services have become more attractive and many users frequently use the services. The services are varied, and online shopping or auction sites are common. User authentication function is important for services that require payments. Many Internet sites still use ID/password (PW) pairs for this purpose. However, malicious attack techniques have recently improved, and thus the number of incidents has increased. In order to cope with this problem, some sites apply multifactor authentication methods, such as biometrics or One Time Password (OTP).

Multi-factor authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

Two-factor authentication (also known as 2FA) is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication.

A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.

2. Various Components of Digital Marketing

Mobile phone two-factor authentication, where devices such as mobile phones and smartphones serve as "something that the user possesses", was developed to provide an alternative method that would avoid such issues. To authenticate themselves, people can use their personal access license plus a one-time-valid, dynamic passcode consisting of digits. The code can be sent to their mobile device by SMS or via a special app. The advantage of this method is that there is no need for an additional, dedicated token, as users tend to carry their mobile devices around at all times anyway.

Some professional two-factor authentication solutions also ensure that there is always a valid passcode available for users. If one has already used a sequence of digits (passcode), this is automatically deleted and the system sends a new code to the mobile device. And if the new code is not entered within a specified time limit, the system automatically replaces it. This ensures that no old, already used codes are left on mobile devices.

2.1 Advantages of Two-Factor Authentication

No additional tokens are necessary because it uses mobile devices that are carried all the time. As they are constantly changed, dynamically generated passcodes are safer to use than fixed log-in information. Depending on the solution, passcodes that have been used are automatically replaced in order to ensure that a valid code is always available; acute transmission/reception problems do not therefore prevent login.

2.2 Disadvantages of Two-Factor Authentication

The user must share their personal mobile number with the provider, reducing personal privacy and potentially allowing spam. Text messages to mobile phones using SMS are insecure and can be intercepted. The token can thus be stolen and used by third parties. Text messages may not be delivered instantly, adding additional delays to the authentication process. Modern smart phones are used both for browsing email and for receiving SMS. Email is usually always logged in. So if the phone is lost or stolen, all accounts for which the email is the key can be hacked as the phone can receive the second factor. So smart phones combine the two factors into one factor. Mobile phones can be stolen, potentially allowing the thief to gain access into the user's accounts

3. Role of digital marketing in promoting SMEs

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. The authentication factors of a multi-factor authentication scheme may include:

1. Some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
2. Some secret known to the user, such as a password, PIN, TAN, etc.
3. Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.

3.1 Methods

3.1.1 Kodekey

KodeKey is a mobile app and Web service combination developed by Puerto Rican startup Qondado LLC. KodeKey is based on the idea that you don’t need to create and remember passwords because you already have all you need to uniquely identify yourself: your phone and your fingerprints.

Biometric authentication has been tried and tested before, but the complications and costs its previous implementations introduced had prevented it from gaining momentum. In contrast, KodeKey’s ease-of-implementation and use has made biometric authentication easier. It takes advantage of the fact that more and more users own smartphones that have fingerprint scanners and highly-secure verification infrastructure.

Each time users enter their phone number and PIN combination in the site’s login page, a notification is sent to the KodeKey app, which prompts users to confirm their identity by performing and fingerprint scan test with their phone.

3.1.2 Launch key

Launch Key is a flexible multifactor authentication platform that enables users to leverage their own mobile devices in place of traditional passwords or tokens for remote login, real-time authorization, and two-step verification.

Signing up with Launch Key-authenticated services is as easy as installing the free Launch Key Mobile app or any other app integrated with Launch Key’s white label SDK on a tablet or phone.

Launch Key Engine, the online service that handles the core functionality of the system, can be accessed through a public API, but can also be independently deployed on-premise or within private clouds. No personally identifiable information is stored in the Launch Key Engine, and sensitive authentication data never leaves the user’s device.

3.3 Clef

Clef tackles two-factor authentication from a different perspective. It uses a smartphone camera, a waveform image, and an asymmetric key combination to verify the identity of the user.

When users sign up with a service that is backed by Clef, they associate their phone with their account. Subsequently an asymmetric key is produced, the public part of which is stored on the Clef server and the private part on the user’s phone.

4. Growth Authentication on a Mobile Device

4.1. SMS One-Time Password Authentication

SMS-based OTP leverages text messaging (more specifically, short message service) to deliver a one-time password upon request. To receive the OTP, the user goes to the application website and requests the OTP. Provided that the user's mobile phone has sufficient connectivity to the mobile network, the user will receive the SMS with the one-time password. The user then types the OTP into the authentication form on the application website and gains access. As with similar systems, the OTP can be used only once, which provides much better security as compared to traditional passwords?

SMS-based one-time passwords are the least secure, primarily because of the relative insecurity of the SMS protocol. While somewhat convenient for the casual retail consumer, the SMS OTP method can cause "usability fatigue" for enterprise users who authenticate frequently during the day and therefore must wait for the SMS delivery of the OTP each time.

4.2. Device Generated One-Time Passwords

Like SMS-based OTPs, device-generated OTPs rely upon a unique password for each initial user authentication. The OTP is generated via software on the mobile phone. The software leverages a symmetric key and (typically) the phone's clock to generate the one-time password. Relative to SMS-based OTPs, device-generated OTPs are generally more secure because the one-time password is generated on the device. The enhanced security comes with a cost; device-generated OTP authentication requires software distribution, a secure process to bind the OTP to a real user, and many different software packages to support the mobile phones on the market. Device-generated OTPs are more convenient than SMS-based OTPs, because the user does not need to wait for the delivery of the SMS message.

4.3. Out-Of-Band (OOB) Authentication

The newest mobile device authentication method is out-of-band authentication. After initially contactng the application website, the user is contacted at a known phone number. The phone number can be associated with a land line or mobile phone. Once contacted, the user presses a few keys on the phone and is subsequently authenticated to the application website. Behind the scenes, the application contacts the OOB authentication service provider via a Web services request and receives a response when the user has successfully authenticated.

Of the three authentication options described here, OOB authentication generally provides the greatest security because it leverages a more secure medium for authentication -- the phone network. As with SMS-based OTPs, enterprise users may experience usability fatigue if they authenticate frequently during the day. OOB authentication also provides the greatest platform support; users can be authenticated via their home or mobile phones. The following table summarizes the ways you can help.

	SMS OTP	Device OTP	OOB Authentication
Value-added resellers (VARS)	VARS may sell the server back-end components, and in some cases the necessary platform agents.		N/A:00B authentication is a hosted service
Consultants	OTP authentication is supported in some Web access management systems, but requires configuration and light customization. In other systems, deeper integration work may be required		OOB authentication will require integration work with the organization's Web application.
Systems integrators (SIS)			
Managed service providers (MSPs)	MSPs manage the delivery of SMS messages.	Large MSPs can manage the complexity of distributing and binding device OTPS.	MSPs can host the OOB authentication method, which greatly reduces organizational burden.
Independent software vendors(ISVs)	ISVS create the back-end components (e-g.. OTP server and agents)	ISVS write the device-specific software package for mobile devices. The ISV and MSP are likely the same entity.	N/A: OOB authentication is almost always a hosted application. with no mobile device software and no on-premise components

5. Conclusion

Graphical passwords are easy to recall as compared to text based password. According to survey, it is challenging to break graphical password as compared to other authentication mechanism. Most of the methods are prone to traditional attacks like shoulder surfing, man in middle attack. The strength of authentication mechanism when it overcomes the traditional attack. In this paper analysis of authentication methods were conducted. Specific aspects of the technology were chosen for the analysis namely, two factor, Multifactor, OOB Authentication etc.

References

[1] Zippy Erlich, Moshe Zviran,“Authentication Methods for Computer Systems Security”, Encyclopedia of Information Science and Technology,ch049, 2009.

[2] The-Crankshaft Publishing, “Authentication Methods for Computer Systems Security (information science)”

[3] A. Josang and G. Sanderud, “Security in Mobile Communications: Challenges and Opportunities,” in Proc. of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003.

[4] D. de Borde, “Two-Factor Authentication,” Siemens Enterprise Communications UK- Security Solutions, 2008.