Communications and Network, 2017, 9, 172-178
http://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

Enhancing Multi-Factor Authentication in Modern Computing

Ekwonwune Emmanuel Nwabueze[1], Iwuoha Obioha[2], Oju Onuoha[3]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria
[3]Department of Computer Science, Abia State Polytechnic, Aba, Nigeria
Email: ekwonwuneemmanuel@yahoo.com

How to cite this paper: Nwabueze, E.E., Obioha, I. and Onuoha, O. (2017) Enhancing Multi-Factor Authentication in Modern Computing. *Communications and Network*, **9**, 172-178.
https://doi.org/10.4236/cn.2017.93012

Received: May 5, 2017
Accepted: August 6, 2017
Published: August 9, 2017

Abstract

Most network service providers like MTN Nigeria, currently use two-factor authentication for their 4G wireless networks. This exposes the network subscribers to identify theft and users data to security threats like snooping, sniffing, spoofing and phishing. There is need to curb these problems with the use of an enhanced multi-factor authentication approach. The objective of this work is to create a multi-factor authentication software for a 4G wireless network. Multi-factor authentication involves user's knowledge factor, user's possession factor and user's inherence factor; that is who the user is to be presented before system access can be granted. The research methodologies used for this work include Structured System Analysis and Design Methodology, SSADM and Prototyping. The result of this work will be a Multi-factor authentications software. This software was designed with programming languages like ASP. NET, C# and Microsoft SQL Server for the database.

Keywords

Enhanced Multi-Factor Authentication, Rapid Prototyping, Security Threat, Encryption, Hackers, Phishing, Malware, Tokens

1. Introduction

Multi-factor authentication (MFA) is a method of computer access control in which a user is granted access only 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 only two different components. Two-factor authentication is a type of multi-factor authentication, but it is not enhanced to allow for presentation of three or more factors of authentication [1]. 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.

Enhanced multi-factor authentication involves the requirement of the user to present at least three of different authentication factors before access can be granted to the resource sought for. Enhanced multi-factor authentication requires that the user must present knowledge factor or factors like passwords or PIN, possession factor or factors like SIM card or ATM card and then an inherence factor or factors like fingerprint, iris color or voice tone; before he/she is granted access to the system.

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-for example a building or data, being protected by multi-factor authentication then remains blocked [2]. 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 or a SIM-subscriber identification module.

2) Some secret known to the user, such as a password or PIN-personal identification number.

3) Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed or pattern in key press intervals.

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate. A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication [3]. Many multi-factor authentication techniques rely on password as one factor of authentication. Variations include both longer ones formed from multiple words (a passphrase) and the shorter, purely numeric, personal identification number (PIN) commonly used for ATM access. Traditionally, passwords are expected to be memorized. Many secret questions such as "Where were you born?" are poor examples of a knowledge factor because they may be known to a wide group of people, or be able to be researched.

Possession factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems [4]. A security token is an example of a possession factor. Disconnected tokens

have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user. Connected tokens are devices that are physically connected to the computer to be used, and transmit data automatically. There are a number of different types, including card readers, wireless tags and USB tokens.

Inherence factor are authentication factors associated with who the user is. They usually biometrics which include the user's fingerprint, retina-iris color or voice.

The major drawback of authentication involving something that the user possesses, is that the physical token (the USB stick, the bank card or SIM) 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. 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-that is something that only the individual user knows, 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 [5]. 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 [6]. For added security, it is possible to specify how many incorrect entries are permitted before the system blocks access. Security of the mobile-delivered security tokens fully depends on the mobile operator's operational security and can be easily breached by wiretapping or SIM cloning by national security agencies.

2. Theoretical Framework

Enhanced multi-factor authentication is a type of authentication protocol which requires the user or one who wants to gain access into a system to present at least 3 valid basic authentication factors before he/she can be granted access. These 3 basic authentication factors include:

1) Knowledge factor; which is what the user knows which includes usernames, PIN, password or pattern.

2) Possession factor; which is what the user has which involves the presentation of tokens like ATM card, SIM card or even a phone device.

3) Inherence factor; which is who the user is. This involves fingerprint, iris color or voice recording.

Computing involves the use of computers to solve problems. Modern compu-

ting involves the use of state-of-the-art computer systems like smart devices, laptops and servers, for provision of solution to real-life problems or all surrounding problems which may include machine or user problems.

2.1. Roles of Enhanced Multi-Factor Authentication in Modern Computing

The following are some roles multi-factor authentication can play in modern computing:

1) Curbing of the presentation of weak user credentials, this is achieved by ensuring compulsory presentation of at least three valid authentication factors before access is granted.

2) Rendering the intension of stealing and stealing of user credentials useless. Using enhanced multi-factor authentication, even if the hard token of the user which can be an ATM card is stolen by a hacker, it will still not guarantee the hacker access to the system since a knowledge factor and an inherence factor are still required for authentication.

3) Enhanced multi-factor authentication protects companies from losing huge finances to security breach attacks like hacking, snooping, sniffing, spoofing and identity thieves [7].

4) Identity theft is mitigated to a high degree by the use of enhanced multi-factor authentication process. This is because it will be difficult for a hacker to easily present the minimum three main authentication factors for access into the system.

5) Small-scale business vulnerable to cheap hacks are effectively protected by use of enhanced multi-factor authentication [8]. Even with advanced firewalls and anti-virus systems in place without user authentication, you are leaving the front door wide open to intruders.

6) Enhanced multi-factor authentication has updating and upgrading features that ensure that it constantly improves on its effectiveness in curbing the activities of identity thieves.

7) Cross-Platform Protection on web affairs: Multi-factor authentication protects data from hacking and phishing attacks by confirming the user's identity during the login process, and can be seamlessly integrated into a number of third-party platforms used across the organization. Real-time, mobile-based solutions to authenticate employees have proven to be a cost-effective way to significantly increase the level of security without requiring the user to learn a new authentication method for every application they try to access [7]. A cross-platform approach, therefore, boosts user satisfaction and cuts the number of security applications the IT admin is required to manage.

8) Reduction of Complexity and Ensured Access: Fighting complexity in the IT department is a constant battle. Every new module or upgraded system can threaten to set off a chain reaction of tweaks and adjustments to processes that can irritate users and keep them offline. It is important to find an authentication system that can be easily installed, deployed and administered [9]. Multi-factor

authentication approaches exist that offer policy-driven administration and can protect multiple platforms on a global scale. Enhanced MFA integrates seamlessly with today's most popular remote access systems and cloud applications.

9) Flexibility boost and Security of Remote Workers: The modern staff is working from home more than ever, supported by great advancements in remote access for critical business applications. The IT department is responsible for facilitating the ability of the remote workforce to perform its functions from outside the office environment, which means its authentication strategy must make it as easy as possible to safely access business applications from anywhere, at any time [10]. Multi-factor authentication fits that bill. It enables administrators to adapt the level of support needed using contextual information, such as login behavior patterns, geo-location and type of login system being accessed. For example, if the user is logging in from a trusted location where they have logged in before, they will not be prompted for a One-Time Passcode in order to authenticate. This allows end users the needed security with greater ease of use while working off-premise.

10) Multi-factor authentication generally boosts users' confidence with the obvious guaranteed security protocols. This can lead to users keeping more sensitive data on modern smart systems like the cloud, than physically storing them in vulnerable places around them [11].

2.2. Considerations in Enhanced Multi-Factor Authentication Implementation

Some factors to consider while trying to implement enhanced multi-factor authentication include:

1) Implementing enhanced multi-factor authentication require the use of multi-factor enabled devices like smart phones with fingerprint readers, high pixels camera for eye retina capture and analysis. It might also require multi-factor configured software like biometric fingerprint database manager and structured inherence query software.

2) There is need for users to have some basic technical skills required during provision of the authentication factor especially when using soft tokens which involves the use of time-based one-time passwords from tokenization devices.

3) Enhanced multi-factor solutions require additional investment for implementation and costs for maintenance [12]. Most hardware token-based systems are proprietary and some vendors charge an annual fee per user. Deployment of hardware tokens is logistically challenging. Hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed. In addition to deployment costs, multi-factor authentication often carries significant additional support costs.

4) According to proponents, multi-factor authentication could drastically reduce the incidence of online identity theft and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to

their information. However, many multi-factor authentication approaches remain vulnerable to man-in-the-browser, and man-in-the-middle attacks [13]. This man-in-the-middle could be the person that registered your account at the registration center or the person(s) managing the queried databases. Multi-factor authentication may be ineffective against modern threats, like ATM skimming, phishing, and malware.

3. Summary

Modern computing involving the use of smart devices and laptops is currently having issues of identity theft, porous authentication, snooping and sniffing. This is due to the use of poor authentication protocols. This paper achieved the objective of defining and explaining the role enhanced multi-factor authentication will play to curb these disturbing issues in modern computing. The research methodology used in this research is the Rapid or throw-away prototyping which is a type of the prototyping methodology. It involves the creation of a simple working model to visually show the users what their requirements may look like when they are implemented into a finished system. The result of this paper is the achievement of an in-depth understanding of how enhanced multi-factor authentication works and its need to be integrated into all facets of modern computing.

4. Conclusion

Enhanced multi-factor authentication ensures information security for business enterprises and prevents them from crashing or losing money. It curbs identity theft involving someone imitating who he or she is not, presenting an authentication factor and gaining access into a system as known user meanwhile he or she is a foreign malicious entity. Enhanced multi-factor authentication provides cost effective user validation that is flexible, convenient and has no complexities for remote workers. It involves the use of a complete security strategy to protect critical data from malicious actors.

Recommendation

It is strongly recommended that IT professionals and hardware manufacturers adopt and integrate the use of enhanced multi-factor authentication in their newer products for enhanced security and mitigation of identity theft, pharming, sniffing, snooping, phishing and outright theft of possession factors of authentication.

References

[1] Adam, B. (2014) Biometrics for Identification and Authentication. Eprint Publishers, Westpoint, USA.

[2] Brian, K. (2006) Security Fix—Citibank Phish Spoofs 2-Factor Authentication. Washington Post Press, Washington, USA.

[3] Bruce, S. (2005) The Failure of Two-Factor Authentication. Schneier Publishers, New York, USA.

[4] DeBorde, D. (2012) Two-Factor Authentication Exposed. Goldman Publishers, New York, USA.

[5] Howard, S. (2016) How Web Sniffing Works. Bellingcat Press, New York, USA.

[6] Hangman, G. (2016) All about iCloud Technology. Kinjo Press, Minnesota, USA.

[7] Mann, J. (2016) Mobile Two Factor Authentication. Pcisecurity Publishers, London, GB.

[8] Tim, K. (2015) The Failure of Two-Factor Authentication. Kinjo Press, Minnesota, USA.

[9] Rosenblatt, S. and Cipriani, J. (2015) Two-Factor Authentication: What You Need to Know (FAQ). Retrieved from https://www.cnet.com/

[10] Syracuse, F. (2013) Secure Configurations for Network Devices. WestPoint Printers, Virginia, USA.

[11] Sean, A. (2016) Usable Two-Factor Authentication Based on Ambient Sound. Usenix Publishers, New York, USA.

[12] Thomas, J. (2015) Two-Factor Authentication: All You Need to Know. CNET Press, Ohio, USA.

[13] Van, T., Henk, C. and Jajodia, S. (2011) Encyclopedia of Cryptography and Security. Volume 1, Springer Science & Business Media, New York, USA.