THE ROLE OF ENHANCED MULTI-FACTOR AUTHENTICATION IN MODERN COMPUTING

Obioha Iwuoha, Chidiebere C. Oparah
Computer Science Department,
Federal Polytechnic Nekede Owerri, Imo State.
Email: ohaobi@yahoo.com, canonchychuks@yahoo.com

Abstract: *Modern computing involving the use of smart devices and laptops is currently having issues of identity theft, porous authentication, phishing and sniffing. This is due to the use of poor authentication protocols. This paper has 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 to be 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.*

Keywords: Enhanced Multi-Factor Authentication, Rapid Prototyping, Security Threat, Encryption, Hackers, Phishing, Malware, Tokens.
Received for Publication on 20 April 2017 and Accepted in Final Form 8 May 2017

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 (“Biometrics for Identification and Authentication”, 2014).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.

Authentication Factors

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 (Brian,2006). 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

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 (Bruce, 2005). 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

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 (DeBorde, 2012). 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 factors

These are factors associated with the user, and are usually biometric methods, including fingerprint readers, retina scanners or voice recognition.

Mobile phone two-factor authentication

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 smart phones 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 pass code consisting of digits. The code can be sent to their mobile device by SMS or via a special app ("How Russia Works", 2016). 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 pass code available for users. If one has already used a sequence of digits (pass code), 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 ("How to extract data", 2016). 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.

THEORETICAL FRAMEWORK

Roles of enhanced multi-factor authentication

Some of the roles of enhanced multi-factor authentication include;

1. Cross-Platform Protection:
   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 ("Mobile Two Factor Authentication", 2016). A cross-platform approach, therefore, boosts user satisfaction and cuts the number of security applications the IT admin is required to manage.
2. 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 (Rosenblatt & Cipriani, 2015). 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.

3. 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 ("SANS Institute, Critical Control 10", 2013). 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 Pass code in order to authenticate. This allows end users the needed security with greater ease of use while working off-premise.

4. Multi-factor authentication can be used in Office desktop applications for enhanced and detailed log in to Office client applications with a higher level of security than a user-selected password. This is achieved by users being required to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password ("Sound-Proof: Usable Two-Factor Authentication", 2016). Only after this second authentication factor has been satisfied can a user sign in.

5. Secure Cloud generates encryption keys and provides full key lifecycle management. Anyone with

the Security Administrator role has the privilege to download encryption keys from the Secure Cloud server. With enhanced multi-factor authentication in place, Secure Cloud can determine if the user logging on is indeed the account owner. Enhanced multi-factor authentication mitigates the risk of an account being hacked ("The Failure of Two-Factor Authentication - Schneier on Security", 2015). Secure Cloud applies enhanced multi-factor authentication on a role-basis and implements two-factor authentication (or two-step verification), which implements Time-based One-time Password (TOTP) algorithm and requires account owners to provide the compulsory three factors of authentication.

Reasons why enhanced Multi-Factor Authentication is necessary

The following are some reasons why the need for enhanced multi-factor authentication cannot be over-emphasized;

1. Weak or stolen user credentials are hackers' preferred weapon and are exploited in 76 percent of all network breaches.
2. The hackers are winning the war. From 2012 to 2013, the number of successful breaches went up by 20 percent ("Two-factor authentication: What you need to know", 2015). Not only that, but they also took longer to be discovered and ended up costing the victim companies 30 percent more.
3. Identity theft is the fastest-growing type of crime, and is now more profitable than drug-related crimes. It is an easy, low-risk, high-reward type of crime and a threat to all businesses.
4. The big brands may be the ones making headlines when

they are hacked, but they are not the only ones being targeted. Thirty-one percent of all targeted attacks were aimed at businesses with fewer than 250 employees.

5. Even with advanced firewalls and anti-virus systems in place without user authentication, you are leaving the front door wide open to intruders.
6. Hackers don’t just steal information. Often they destroy data, change programs or services or use servers to transmit propaganda, spam or malicious code.
7. Hackers constantly improve their effectiveness in stealing passwords through phishing, pharming, key loggers and other methods.

Security issues in enhanced multi-factor authentication

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 (Vanetal, 2011). 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.

Enhanced multi-factor authentication implementation considerations

Many multi-factor authentication products require users to deploy client software to make multi-factor authentication systems work. Some vendors have created separate installation packages for network login, Web access credentials and VPN connection credentials. For such products, there may be four or five different software packages to push down to the client PC in order to make use of the token or smart card. This translates to four or five packages on which version control has to be performed, and four or five packages to check for conflicts with business applications. If access can be operated using web pages, it is possible to limit the overheads outlined above to a single application. With other multi-factor authentication solutions, such as "virtual" tokens and some hardware token products, no software must be installed by end users. There are drawbacks to multi-factor authentication that are keeping many approaches from becoming widespread. Some consumers have difficulty keeping track of a hardware token or USB plug. Many consumers do not have the technical skills needed to install a client-side software certificate by themselves. Generally, multi-factor solutions require additional investment for implementation and costs for maintenance (“What are 2 factor authentications?” 2015). 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.

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.

CONCLUSION

As hackers persist with their attacks, creating increasingly sophisticated threats, IT administrators should be diligent in finding effective methods to defeat them at every turn. Right or wrong, when a breach occurs, company executives point the finger of blame at the IT admin. It is the IT admin's responsibility to protect all users and all platforms, but not to the extent that access becomes difficult or that the budget goes bust. Multi-factor authentication provides secure user validation that is convenient, reduces complexity and increases flexibility for remote workers. It is a crucial aspect of a complete security strategy to protect critical data from malicious actors.

RECOMMENDATION

It is strong 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

Biometrics for Identification and Authentication - Advice on Product Selection. (2014). Retrieved from http://eprint.iacr.org/2014/135.pdf

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

Bruce, S. (2005). The Failure of Two-Factor Authentication. Schneier publishers, New York, USA.

DeBorde, D. (2012). Two-factor authentication.pdf. Retrieved from www.archivedpdfcs.com

How Russia Works on Intercepting Messaging Apps – bellingcat. (2016). Retrieved from www.bellingcat.ru

How to extract data from an iCloud account with two-factor authentication activated. (2016). Retrieved from www.iphonebackupextractor.com

Mobile Two Factor Authentication.pdf. (2016). Retrieved from www.securenvoy.com Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (2016). Retrieved from www.pcisecuritystandards.org

Rosenblatt, S. & Cipriani, J. (2015). Two-factor authentication: What you need to know (FAQ). Retrieved from www.cnet.com

SANS Institute, Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. (2013). Retrieved from www.eag.net

Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound | USENIX. (2016). Retrieved from www.usenix.org

The Failure of Two-Factor Authentication - Schneier on Security. (2015). Retrieved from www.schneier.com

Two-factor authentication: What you need to know (FAQ) - CNET. (2015). Retrieved from www.cnet.com

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

What are 2 factor authentications? (2015). Retrieved from www.securenvoy.com

Reference to this paper should be made as follows: Obioha Iwuoha, Chidiebere C. Oparah (2017), The Role of Enhanced Multi-Factor Authentication in Modern Computing. *J. of Engineering and Applied Scientific Research,* Vol. 9, No. 2, Pp. 13-24