International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 11, Issue 5, October 2022

A Review of Two-Factor Authentication Security Challenges in the Cyberspace

Richard Samba Omwoyo[1], John Kamau[1], Mvurya Mgala[2]
[1] School of Computing and Informatics, Mount Kenya University
[2]Institute of computing and informatics, Technical University of Mombasa

Abstract **--**Today, single-factor authentication, e.g. Passwords, is no longer considered secure in cyberspace and electronic learning environments. With the advancement of technology, passwords are becoming easier for cyber-attacks to forcibly test and eventually guess passwords or harvest them with technologies such as keystroke loggers. Two-factor authentication (2FA) has been recently introduced to overcome this problem by providing an additional layer of security using secondary means (ownership factor or inherent factor). However, the users of 2FA are still facing challenges such as delays in receiving SMS codes, expiry of codes before use, the burden of carrying hardware tokens all the time and sometimes payment for incoming SMS. A review of the literature on studies conducted on two-factor authentication security issues and challenges is done in this paper. The paper concludes that 2FA has several challenges ranging from the cost of manufacturing tokens, maintaining codes, distribution of millions of tokens to users and delays in receiving verification codes. Therefore, drawn from the findings, the study recommends that other studies be conducted on alternative multi-factor authentication schemes that are easy to use and protect users appropriately.

Keywords:- Two-factor authentication, Security, Password, cyberspace, Secondary level authentication, Token

I. Introduction

Today, cyberspace security has become a significant problem in learning institutions, banks, the healthcare industry, the military, and government agencies. Private and public companies are setting security policies and passing laws to ensure that companies and government agencies conform to these policies or face the consequences. There are several security management concerns regarding cyber-space security, with one common weak link being the password (Kuyolo & Adetoba, 2016). Two-Factor authentication (2FA) is a two-way verification process aiming to solve the existing one-factor authentication problem (Benarous & Kadri, 2017). Two-factor authentication is categorised into three authentication factors:

1. **Knowledge factor –** It is something the user knows, for example, using a password, PIN or secret word.
2. **Ownership factor –** this is something that the user has. It can vary from an identification card, security token or smartphone.
3. **Inherent factor –** something that you are, e.g., use of biometrics factors such as fingerprint, face recognition, and iris scan.

Figure 1. Authentication factors

Two-factor authentication reinforces security protocol by using two methods to validate a user's identity. This secondary layer of security makes it difficult for cybercriminals to gain access to user devices or client accounts (Niklas & Fredrik, 2017). Kaur (2022) argues that although 2FA is better than single-factor authentication, it is still not 100 % resilient. Using 2FA can provide better protection but ends up complicating the login process. He further states that 2FA involves sets of authorisation factors; if one misplaces one factor or device, it can be a cause of concern, especially if

it contains access to your bank account or other high-value data.

Katta (2015) states that, despite the security strength attached to two-factor authentication, it suffers from historical hindrances ranging from users having to carry security hardware tokens all the time, lack of equipment or know-how to navigate multi-factor authentication, extra cost charged for incoming SMS, delays in receiving codes and expiry of authentication tokens before use. These hindrances have led to an increased number of carried security tokens among users today. The growing number of carried tokens and the initial cost of maintaining and manufacturing them is also becoming a burden to clients and organisations (Fadi Alou & Syed Zahidi, 2012). A study by Emiliano & Honglu (2018) shows that most users adopt security tokens because their organisation forces them to do so; the study further reveals that most users complained that it is annoying to remember and carry security tokens all the time. A study review by Adetoba & Kuyololo (2016) outlined cyberspace security as one of the five major security challenges.

Weaknesses of Single-Factor Authentication

1. **Keyloggers Attacks:-** According to Kaspersky Lab (2021), keyloggers pose serious threats to online users by intercepting passwords and other personal information entered via the keyboard. As a result, cybercriminals are harvesting bank account details, numbers used as PIN and email passwords using this tactic. Online users aware of this fraud protect their organisations against phishing by snubbing phishing emails and avoiding entering confidential information into these bogus websites. However, users still find it difficult to identify or tell when a criminal has installed a key logger on their machines. One possible solution to keylogger programs is developing an appropriate security solution to identify keylogger programs.
2. **Fixed Password vulnerability**:- Passwords are used as proof of identity. They should ideally be easy to remember and difficult to guess. End users do not always follow these two factors as they choose easy-to-guess and remember passwords, making them vulnerable to cyberspace criminals (Gärdekrans, 2017). According to Sarohi & Khan (2014). Password is inherently weak; users have a habit of selecting simple or short passwords to recall or using the same password for several accounts. With the technological advancements, it has become simple for attackers to test and eventually guess passwords forcibly or harvest them with technology such as Key loggers (Chiasson & Bidle, 2016). Other common mistakes by users are using individual information such as date of birth, family name, name of places, and other conversant things like your favourite actor or musician. These simple factors make it easier for a criminal to guess the user's credentials and eventually launch an attack (Taneski, 2017).
3. **Reuse of passwords:-** Today, accessing any system without a password is complicated. The number of password accounts that a typical user carries has increased and continues to do so. This can be evident by the number of online users who keep dozens of internet passwords to deal with, according to a study by Jenkins (2017). Using a similar password for many accounts is a dominant occurrence that can make even the most secure systems vulnerable. An average user today can carry up to 25 protected passwords and use approximately eight each day. According to Egelman (2016), a common problem in remembering passwords is that users write them down to remember them easily. Jenkins (2017) found that once passwords have been reused across a wide range of multiple accounts, cyber criminals found it easier to track and steal those passwords from low-security websites and use them to access higher-security sites.
4. **Drawbacks of Password Policies**:- Private and public organisations are setting password policies and passing laws to ensure that organisations and government agencies comply with these policies or face the consequences. Gärdekrans (2017) states that individuals are responsible for keeping their system access login safe. Forcing people to generate complex passwords and frequently change them at fixed intervals can be an uphill task. In scenarios where changing a password is a must and users are allowed to reset their old password by adding something new to it, for instance; " frontdoor" to "frontdoor@254", users tend to do so, but in

cases where users are supposed to generate a new password they end up feeling frustrated. As a result, they write down the new password, so they do not forget it or as a way of learning it.

Two-factor Authentication Security Challenges

Two-Factor authentication (2FA) is a unique two-step verification process that solves the existing one-factor authentication problem: a simple password and username (Benarous & Kadri, 2017). It has gained popularity worldwide in securing millions of users and assets in the wake of cyber-attacks. However, it has its disadvantages:

Token drawbacks

A token is a physical or digital device used to authenticate users for services. A token may be hardware or software. Software tokens are used for digital identification. e.g. One-time password (OTP). A hardware token is a small physical handheld object which contains information for the logging process. It includes a smartcard, USB key, digital pass or mobile devices. While security tokens offer a variety of advantages to users and organisations, they can also introduce drawbacks. A survey conducted by Mare (2017) on user daily authentication behaviour using devices such as smartphones, websites, and computers and across a wide range of authentication factors such as passwords, physical tokens, and PINs revealed that users are burdened by different kinds of authenticators they carry every day. The survey revealed that 25% of participants employed physical tokens that they carry with them all the time and cannot be delegated (Busold & Wachsmann, 2018). Below is a summary of some authentication tokens that participants consider burdens added across all participants.

Table 1. summary of authentication tokens

Authenticator	Number	Comment
Credit card	60	Include work, 4 not used
House/apartment key	27	One person carried 6
Car key	19	Electric or regular
Debit card	17	
Other ID cards	16	Two expired
ID badge	15	Corporate and gym
Phone	4	phone app for password

The survey results show that participants expressed frustration over the authentication materials they manage daily. Further, they frequently encountered authentication failures and delays up to an average rate of 7-12% across a wide range of devices. The study suggested that physical tokens and simple password authentication are recommended and worthy areas of improvement.

Author (Katta, 2015) argues that, despite the security strength attached to two-factor authentication, it suffers from historical hindrances ranging from users having to carry security hardware tokens all the time, lack of equipment or know-how to navigate multi-factor authentication, extra cost charged for incoming SMS, delays in receiving codes or expiry of authentication tokens before use. This has resulted in an increased number of carried security tokens among users today. The growing number of carried tokens and the cost of maintaining and manufacturing them burden clients and organisations (Fadi Alou & Syed Zahidi, 2012). A study by Emiliano & Honglu (2018) shows that most users adopt security tokens because their organisation forces them. The study further reveals that most users complained that it is annoying to remember and carry security tokens all the time.

Biometrics Authentication Systems

Biometric technology is an advanced form of identification. Biometric authentication utilises user characteristics such as fingerprints, facial recognition, hand geometry, and eye retina and stores these data in a string (Katta, 2015). Users then utilise these characters to authenticate themselves by matching them with stored data and granting access when commonality is achieved. The advancement of this technology has its drawback, from voice mimicking in voice biometrics and fingerprint harvesting using small tape to Additional hardware devices required to detect the eye retinas and fingerprints (Ometov, 2018).

Ling (2014) conducted a quantitative study of Bio-Hash formulation to manage and control digital resources. In his research, he combined fingerprint B with a tokenised random number T, producing a set of n binary bit strings B = {b1,..., bn}. This technique makes it difficult for a malicious user to know the required authentication element (B, T) even to make the final product for successful authentication. The author states that despite biometrics providing hard-to-fake individual traits, its implementation is very costly for both the server and the client. Its acceptance has also faced drawbacks such as false recognition rate, fingerprints duplications, and additional hardware requirements. A possible solution to these drawbacks would be implementing an authentication mechanism that does not tie the user to hardware or software devices.

Cost

It will cost a company more money to shift to a two-factor authentication method than maintaining a traditional conventional password control method. 2FA carries many hidden costs for operation, deployment, licensing and maintenance. A scheme using a token or key fobs as the second authentication factor will cost an organisation between 78$ and 105$ per token. For an organisation with vast personnel and thousands of online customers, the initial cost of tokens alone could shoot up to millions of dollars. Then there is a direct cost of administrative software and hardware, the infrastructure needed to set up the server system, user training and support, the ongoing cost of keeping patches up-to-date and capital licensing. According to Pham (2017), any authentication system brings its own direct and indirect costs; some incur higher costs than others, some take months or years to be developed, others require the building to support the infrastructure, and others have layers of hidden cost. Therefore, the cost must be factored in for implementing any form of two-factor authentication.

Phone-Based Authentication Drawback

In recent years, two-factor authentications may seem like a perfect cure for securing cyberspace networks and resources. Ashok and Tanushree (2017) pointed out that this type of authentication will not protect you from many types of cyber security holes. For instance, bogus websites are commonly used by cyber-criminal to harvest personal information directly from individuals by tracking websites visited by the user in the theft of confidential information. Two-factor authentication is unable to protect users against this type of man-in-the-middle attack.

1. **SMS-based tokens:** The most common method of delivering two-factor authentications based on the liability, cost, and features found on every mobile device. Unfortunately, this technique, as much as it is an easy and faster way of communication, is the least secure for delivering two-factor authentication tokens (Thorpe, 2016). below are some drawbacks:

A. **Unavailability of service/Coverage areas:** users outside the network coverage area can face many challenges receiving tokens since tokens are sent via air. Users travelling abroad or operating outside their geographical area also face restrictions on incoming SMSs.

B. **Delay in delivery:** Once transmitted, messages traverse several network hopes before landing to the recipient. This causes delay plague because of congestion on the network courier. Two-factor authentication and a one-time password are typically time-sensitive techniques, and a delay of three to four minutes can lead to automatically timing the session.

C. **Unavailability of devices:** registered users or mobile devices must be physically available to receive SMS for a one-time password.

2. **Hardware tokens:** These are physical security tokens used for identity and controlling access management. Two-factor authentication and one-time password (OTP) commonly use hardware tokens for verifications and security control. Unfortunately, hardware tokens are vulnerable to advanced attacks such as real-time replay attacks. (Thatha, 2015). Hardware tokens also suffer from availability issues, adding an extra administrative and logistics burden on replacement. e.g., if an ATM gets lost, it can take up to five days for a replacement, inconveniencing users at the time of need. Hardware tokens are not serviceable. They require replacement at

least once every three years due to battery failure, adding extra costs to the service provider.

Two-factor authentication in the industry today

Google account developed a two-step authentication mechanism in September 2010, and many studies have been carried out concerning two-factor authentication and how to make the authentication process unbreakable. Currently, the giant tech wants to push its billions of users and industries toward enabling 2F authentication by default. Where google goes in web security, the rest of the sector often follows (Hay, 2017). A study by Shyam (2017) on two-factor authentication using security token and mobile ID show that despite organisations switching to two-factor authentication to secure their users, there is a need for the realisation of more robust authentications mechanism without having to carry software or hardware devices all the time. Opponents of 2FA say that keeping up with the token will be inconvenient (Asoke & Tanushree, 2017). E-Trade CEO Klobuchar Lou states, "If they are concerned about a secondary level of security, we're offering them a solution. If there were no inconveniences to using it, it wouldn't be much of a solution. American banks are employing different forms of two-factor authentication because the cyber threat landscape is worsening daily. A recent cyber-attack launched in Latvia using a keylogging Program by cyber criminals ended up wiring $90,000 from one of the business owners' accounts (Asoke & Tanushree, 2017). Minimising cyber-attacks for organisations and banking institutions are replacing randomly generated numbers and authentication tokens. This is attainable by allowing customers to enrol, create a username and password as the first authentication factor, and then choose a collection of images as a second authentication factor. On the next visit, the user will enter a username and password along with the selected images; if the two factors match, the user is authentic, and access is granted.

Conclusion

Two-factor authentication, an upgrade of single-factor authentication, has been introduced to provide more robust authentication options to its online users. It is regarded as the best type of authentication technique for online banking or any other institution. Microsoft and Google are pushing billions of users and industries toward enabling 2FA authentication by default. PayPal has recently used this method and integrated it into its web-based services. The major challenge today with 2FA is cyber-space security. Criminals use hybrid malicious programs such as keyloggers and rootkits to harvest confidential information from systems and web services. Delays in receiving verification codes or tokens make this technology vulnerable and susceptible to cyber security fraud. From the client's perspective, having more than one 2FA system requires carrying several tokens which are likely to get lost or stolen. The cost of purchasing, issuing, and managing these tokens is a massive disadvantage to 2FA technology. Therefore, appropriate security solutions must be improvised to make the two-factor authentication concept entirely flexible and unbreakable.

REFERENCES

[1]. Adetoba, Kuyolo, "E-learning security issues and challenges: A review." Journal of Scientific Research and Studies (2016): vol. 3(5), 96-100.

[2]. Asoke, N., & Tanushree, M. "Issues and Challenges in Two Factor Authentication Algorithms." International Journal of Latest Trends in Engineering and Technology, (2017): 325-327.

[3]. Busold, & Wachsmann. "Smart keys for cyber cars Secure smartphone-based NFC-enabled car immobiliser." In Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy (2018): 233-242.

[4]. Chiasson, & Bidle. "Helping Users Create Better Passwords." Is This the Right Approach 3rd Symposium on Usable Privacy and Security? (2013): 60-69.

[5]. Egelman, B. "It's Not Stealing If You Need It: A panel on the Ethics of Performing Research Using Public Data of Illicit Origin." Financial Cryptography and Data Security (2016): 34638-3642.

[6]. Emiliano, Honglu &. "A Comparative Usability Study of Two-Factor Authentication." Two-Factor Authentication. (2018).

[7]. Enarous, & Kadri. "A Survey on Cyber Security Evolution and Threats." Biometric

Authentication Solutions In Biometric Security and Privacy; Springer, (2017): 371-411.

[8]. Fadi Alou, & Syed Zahidi. "Multi-Factor Authentication Using Mobile Phones."

[9]. Fredrik., Niklas &. "Selecting and implementing a two-factor authentication method for a digital assessment platform." Two-Factor Authentication, (2017): 50-60. dec.

[10]. Gärdekrans, R. "Password Behaviour:." A Study in Cultrual and Gender defferences . skovede. (2017).

[11]. Hay, L. "Wired." May 2021. https://www.wired.com/story/google-two-factor-authentication-default/.

[12]. Jenkins, J. "Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals." Information Technology for Development. (2017).

[13]. Katta, S. "Two Factor Authentication System using Intervened password and Color Pattern." International Journal of Scientific & Engineering Research. (2015).

[14]. Kaur, R. "Multi-Factor Authentication: Meaning, Advantages and Disadvantages. Retrieved from: Techthisty." 25 February 2022. https://www.techthirsty.com/multi-factor-authentication-meaning-advantages-and-disadvantages/.

[15]. Lab, K., "secure list Retrieved from Keyloggers" March 2021. https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138.

[16]. Mare, S. "A Study of Authentication in Daily Life." Open access to the Proceedings of the Twelfth Symposium on Usable Privacy and Security (2017).

[17]. Ometov, A. "Multi-Factor Authentication", Cryptography (2018).

[18]. Sarohi, & Khan. "Graphical Password Authentication Schemes." Current Status and Key Issues: International Journal of Computer Science Issues (2014): 437-443.

[19]. Shyam, K. "Two Factor Authentication System using Intervened password and Color Pattern.." International Journal of Scientific & Engineering Research (2017).

[20]. Taneski, V. H. "Password security – No change in 35 years. ." 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO (2017).

[21]. Thatha, R. "Computer weekly, Limitations of two-factor authentication (2FA) technology", June 2015. https://www.computerweekly.com/tip/Limitations-of-two-factor-authentication-2FA-technology.

[22]. Thorpe, S. "SMS for 2FA: What Are Your Security Options?" January 2016. https://authy.com/blog/security-of-sms-for-2fa-what-are-your-options/.