Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Area Six

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Moving Towards a Password-less Authentication Future

[1]Sarumi, Jerry Abayomi, [2]*Oduroye, Ayorinde P., [3] Amadi, Chinadu & [4] Oworu, Theophilus
[1]Lagos State University of Science and Technology, Ikorodu, Lagos, Nigeria
[2,4]Computer Science Department, Caleb University, Imota, Lagos, Nigeria
[3,4]Computer Science Dept, School of Postgraduate Studies, Caleb University, Imota, Nigeria
E-mail: jerrytechnologies@yahoo.co.uk; poduroye@yahoo.co.uk; amadichinedu@gmail.com
oworutheiophilus@gmail.com

ABSTRACT

Since time immemorial, the twin concepts of safety and privacy have always been paramount to man. Hence, early man used boulders to barricade cave entrances, then doors emerged, in the middle ages Roman sentries would demand a password or watchword from anyone attempting to enter a certain area, and would only grant access to an individual or group if they were cognizant of the requisite password. Upon the birth of the internet, passwords retained its relevance and transitioned smoothly to the web and have since taken over as the primary method of web authentication. However, although password authentication has improved over the course of decades, this system has been plagued by persistent and inevitable security and usability issues. Developers in the computer security sector think that by implementing asymmetric challenge-response protocols for authentication, security and usability can be advanced.

Keywords: Moving, Password-less, Authentication, challenge-response, usability, security

Proceedings Citation Format
Sarumi, Jerry Abayomi, Oduroye, Ayorinde P., Amadi, Chinadu & Oworu, Theophilus (2022): Moving Towards a Password-less Authentication Future. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 89-95
www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P15

1. INTRODUCTION

However, despite calls for change by academia and the industry to improve web authentication, passwords still remain dominant in this field. Hence, the aim of this dissertation would be to shed illuminating light on:

- The definitions of password and authenticators.
- The challenges encountered by passwords.
- The genesis and impact of passwordless authenticators and

Statement of the Problem

Passwords without doubt are subject to consistent and unavoidable operability and security issues hence the need to transition to passwordless authentication. Therefore, it behooves on this essay to elaborate on methods which would facilitate the migration to passwordless authentication.

2. LITERATURE REVIEW

Since ancient times, people have used passwords to manage access. Passwords migrated naturally to the web with the development of the internet, and they have since taken over as the primary method of web authentication (Alex Takakuwa, 2019). For internet security researchers, the persistent dominance of passwords over all other forms of end-user authentication is a significant embarrassment. Passwords persists and proliferates with every new website even as web technology advances rapidly in other areas. Detailed discussions of different authentication methods have not yielded any definitive conclusions.

Research conducted over the span of 40 years has shown that passwords have numerous security flaws and are publicly despised by users (Joseph Bonneau et al 2012). Authentication is the foundation for a secure digital transformation. Beyond that, it is a cornerstone of the Fourth Industrial Revolution, whose widespread adoption is anchored on reliable authentication. However, the persistent reliance on passwords as the primary authentication method presents a significant obstacle to further advancement. Password usage and dependence interrupt the user experience, which is quickly emerging as one of the most crucial brand selling points (Andrew Shikiar, 2020).

Using passwords for authentication compels users to create and commit to memory complex integrations of numbers, symbols, letters and to change their passwords frequently; and to try to avoid using the same password across many accounts. Users must handle anywhere between 25 and 85 passwords, and the amount of information sources and tools available to them is exponentially growing. They want to login on to digital tools quickly and easily, but they find it difficult to do so, therefore they resort to using the same passwords (Andrew Shikiar, 2020). According to Okta, for more than 50 years, the core of digital identification and security has been traditional authentication using a login and password.

However, the ever-increasing number of user accounts has given rise to a number of additional problems, including the need for end users to remember numerous passwords, support expenses, and—most importantly—the security concerns posed by stolen credentials. The value of passwords is now outweighed by these new difficulties. The argument for removing passwords from the authentication process is becoming more vehement. Password elimination has gone from a hypothetical possibility to a genuine possibility thanks to evolving passwordless security requirements, increasing consumer and consumer-like experience demands, and rising expenses.

3. RESEARCH METHODOLOGY.

This section would discuss the methods used in conducting research for this topic. For this study, the method employed for research is Secondary data collection. This is defined as information that was first gathered for a different reason and is now being used to answer a new research topic (J J. Hox & H R. Boeije, 2005). The rationale for this method is to facilitate a wider approach in addressing the subject matter. Relevant data was extracted from previous works which had carried out comprehensive analyses of the subject matter and left no stone unturned in the discourse of the title. This essay aims to analyze the shortcomings of passwords and emphasize the stance that it is pertinent at this juncture to transition to passwordless authenticators drawing research primarily from two academic dissertations.

For the first study (Oskar Persson & Erik Wermelin, 2017), two research questions were posed by the authors which are:

1. Comparing their passwordless model to current authentication methods, can it offer any relevant security benefits against popular attacks?
2. Also, password-less authentication is now offered by Google and other companies to combat security vulnerabilities with weak passwords. It is crucial that the proposed model be as user-friendly as possible because password-less authentication might not only provide improved security but also increased usability. So when compared to current alternatives, does this approach offer more user-friendly functionality?

Literary analysis was then conducted to gather data on comparable systems and outlining topics in order to construct a theoretical model. The model was created in order to preserve both the protection that two-factor authentication provides and the usability of less secure approaches. The system architecture was crucial for validating a real-world implementation that could be implemented in contrast with alternative approaches. Potential shortcomings of current authentication technologies were examined to help the authors find the answers to the concerns of the study. The same procedure was then used in their model to see if it shared any of the same flaws. The authors selected two of Google's two-factor authentication systems since they are so widely used. The first one is Google Authenticator, an open source mobile application that makes use of two different kinds of one-time passwords. The second was a passwordless solution, which was ultimately unnecessary because there was insufficient data to compare it to their approach in terms of security.

In a bid to gather information, strings such as "Passwordless authentication", "two factor authentication", "two factor authentication utilizing mobile phones", "two factor authentication security", "biometric authentication", and "password security" were used in Google Scholar searches to gather resources. For the second Essay (Syed W. Shah & Salil S. Kanhere 2017), the authors resorted to using Authentication mechanism based upon the knowledge factor. Recall that passwords, PINs, and other conventional knowledge-based authentication methods have been repeatedly proved to be vulnerable to attack? Researchers have suggested a variety of additional mechanisms that depend on the knowledge component (i.e., what you know) in light of this. The Authors provided a different approach that creates location-based authentication questions by focusing on episodic memories in a spatiotemporal context. The user of this work had to choose some pre-defined areas during the enrollment process, he then choose the matching spot on the map for authentication (not entered as a text or selected from multiple options).

Any location that was within 30 meters of the right response was regarded as accurate. According to evaluations, users can recall the answers to these questions with a high rate since the maps used to answer the questions aid recollection. Additionally, this strategy demonstrates a respectable level of resistance to both near adversaries (such as partners or friends) and strangers.

4. CHALLENGES ENCOUNTERED BY PASSWORDS

Authentication is the validation of an individual or process identity. A password is a secret string of characters that in conjunction with user's ID, grants access to networks, systems, applications, or information (Southern University Password policy, 2019). Passwords have undoubtedly played a central role in web security for more than 50 years, however, it is beset with a plethora of challenges and must be put to rest for the pertinent advancement of web security. Challenges encountered by passwords include;

Poor Account Security; Passwords have given rise to a whole group of identity and security-driven attacks; account takeover attacks may be launched using compromised passwords as a result of credential breaches, phishing, password spraying, or other security flaws (Okta, 2020). According to Verizon Data Breach Report 2017, In 81% of hacking-related breaches, the passwords were either weak or stolen.

Difficulties with Remembering the Password; The biggest criticism regarding passwords is that most people have trouble remembering them. Customers use passwords that are simple for attackers to predict or note them down, or do both when they are expected to remember them (Ross J Anderson,2010).

Issues with Reliable Password Entry; Another problem with passwords is that users may have trouble successfully typing a password if it is too long or complicated. If the task they are trying to execute is urgent, a long alphanumeric password may mislead the person typing it, which could have safety or other ramifications (Ross J Anderson,2010).

Web Attack; Malicious websites are run by web attackers and can be exploited to steal credentials. Phishing is the most typical kind of web assault. With thousands of operational phishing websites targeting hundreds of businesses, phishing has evolved into a mainstream technique for stealing account information (Alex Takakuwa, 2019). The Anti-Phishing Working Group claims that phishing is a criminal tactic that uses both technological and social engineering deception to obtain customers' financial account information and personal identity information. This may involve the use of spoof emails or fake websites made with the intention of stealing information, like usernames and passwords. Despite the fact that phishing is not a novel technique, prior attempts to reduce its efficacy were ineffective**.**

Passwordless authenticators.
As has been discussed in the preceding paragraphs, the continued use of passwords as the dominant means of authentication is a major point of concern especially as it truncates the user experience (Andrew Shikiar, 2020). Also, passwords are incredibly challenging to safeguard: on one hand, users continue to reuse them, while companies struggle to handle and safely store them. The solution then is passwordless authenticators. Essentially, these are authenticators which do not require passwords.

4.1 Advantages of Passwordless Authenticators;

Higher revenues, lower costs
Since cybersecurity has historically been seen as a cost center, the financial aspect is likely the most important justification for businesses to think about switching to passwordless authentication. Not only does it reduce the expenses of password management and data breaches, but it also boosts profits through higher productivity and client retention (Andrew Shikiar, 2020).

Boosts Employee Productivity
A recent survey by State of Password and Authentication Security Behaviors found that employees globally spend approximately 11 hours typing or changing their password each year. For a business with an average of 15,000 employees, this totals productivity loss of $5.2 million. Indeed, there will be expenses related to moving toward a password-free ecosystem, but they are anticipated to be promptly balanced out by the productivity increase alone (Andrew Shikiar, 2020).

Reduce Costs in Case of Data Breach
Weak or stolen passwords are a factor in 80% of data breaches, and assaults utilizing the latter account for 29% of all attacks. The average cost of a data breach globally in 2019 is $3.92 million, up 1.5% over the previous year. The capacity of cybercriminals to acquire and exfiltrate data is severely hampered if there are no passwords to steal or infer. Criminals can employ password hashes as well since they can brute force them with no restrictions from the authentication server. From a risk management standpoint, this suggests that switching to passwordless authentication enables businesses to reduce by 4/5 the costs linked to their exposure to breach risk. This immediately results in cheaper cyber insurance premiums (Andrew Shikiar, 2020).

Approaches for going Passwordless
Passwords can be eliminated, and passwordless systems can be implemented, using a variety of methods which this essay would discuss below:

Email Magic Links: Passwordless authentication using email has become quite popular. At its core, this technique is a password reset sequence; the user receives a hidden link that enables them to reset their password without having to enter their old one. The majority of people are familiar with it because they have used it multiple times. Apps like Medium and slack helped make this authentication mechanism widespread. Solid passwordless authentication takes the password reset flow a bit further. The password (and any associated reset procedures) are eliminated by app designers, who instead deliver a secure, time-limited, one-time link to the user's email address. The user is authenticated when they click that link, and a cookie with a lengthy lifespan is placed to keep them signed in. This is an extremely enticing feature, especially for mobile devices, as the user never has to set, type, or save any passwords. Consumer apps find this passwordless authentication solution to be particularly appealing because it has no hardware requirements (Okta, 2020).

WebAuthn: Using registered devices (phones, laptops, etc.) as factors, WebAuthn is a standards-based passwordless authentication system that enables online applications to secure and simplify user authentication.

With this new standard, these authenticators can now be used by any web application that runs in browsers that supports WebAuthn to reliably authenticate users (Okta, 2020).

Authentication with facial biometric technology: Facial recognition and document scanning can now be used to check persons remotely and on a large scale thanks to recent technological advancements in smartphone cameras and machine-learning models. To put it simply, when creating a fresh account on an online platform, users take a snapshot of their government ID, and the application matches it to the photo of the user who took the photo. Users can access their accounts without a password by utilizing facial biometric authentication (Andrew Shikiar, 2020).

Authentication with Behavioral Analyses: Behavioral authentication verifies authenticity by using non-identifiable yet distinctly individual factors. Users might not see a password prompt when logging in, but their identity will be verified in the background using things like their login history, network information like their IP address, the browser they are using, and non-identifiable behavior attributes like mouse movements and typing habits. Even while each of these anonymous elements is insufficient on its own, when they join together as a single security mesh, authentication is both secure and undetectable (Andrew Shikiar, 2020).

5. CONCLUSION

To date, the majority of authentication solutions have been knowledge-based, single-factor, and they have caused a wide range of problems, from consumer and reputational harm to excessive expenses for help desks and data breaches. Transcending passwords should be a short-term goal for businesses that are ready to enter the new digital world. Passwordless authentication is not a goal in and of itself, even if it is the next step. Security measures frequently fail because criminals learn to bypass them. Because of this, a robust authentication system should be based on a long-term strategy that promotes inclusivity, security, privacy, sustainability, and user experience. Many different directions will be taken by authentication in the future, including ones that we are just beginning to investigate, including cryptocurrency self-sovereign identities and zero trust network. However, the direct route for online companies is to jettison passwords and embrace passwordless authentication.

REFERENCES

1. Alex Takakuwa (2019). Moving from Passwords to Authenticators https://www.semanticscholar.org/paper/Moving-from-Passwords-to-Authenticators-Takakuwa/57b8b32d80e439f067a2f0a9e81430d44e6024df
2. Andrew Shikiar (2020). Passwordless Authentication https://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf
3. Hox, J. J. & H.R Boeije (2005). Data collection, primary versus secondary https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2693952 https://www.subr.edu/assets/subr/DoIT/Password-Policy-April-2019.pdf
4. Joseph Bonneau, Cormac Herly, Paul Ooschot & Frank Stajano (2012). The Quest to Replace Passwords:A Framework for Comparative Evaluation of Web Authentication Schemes https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf

5. Okta (2020). Move beyond Passwords https://www.okta.com/resources/whitepaper/move-beyond-passwords/
6. Oskar Persson & Erik Wermelin, (2017). A Theoretical Proposal of Two-Factor Authentication in Smartphones https://www.divaportal.org/smash/get/diva2:1114318/FULLTEXT02
7. Ross J. Anderson (2010). Security Engineering. https://www.cl.cam.ac.uk/~rja14/book.html
8. Southern University Password Policy (2019) https://www.subr.edu/assets/subr/DoIT/Password-Policy-April-2019.pdf
9. Syed W. Shah & Salil S. Kanhere (2017). Recent Trends in User Authentication - A Survey. https://ieeexplore.ieee.org/document/8784263