BOOK CHAPTER | Chains Break at The Weakest Point

Weak Credential Information as a Threat to Online Security

Cyprian Danso Darko
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: login2cyprian@gmail.com
Phone: +233201692746

ABSTRACT

Weak credential information poses lots of threats to online security. Online credentials form an integral part of online activities with the increasing number of activities of human life now on the web like transactions involving the transfer of funds, social media handles, medical records and other sensitive data hosted in the clouds which can be accessed from anywhere using the web. It is important to have strong online credentials that would curb if not remove the threats it poses when weak credentials are chosen. This paper looks at weak credential information as a threat to online security, review current situation and evaluate the need for a stronger credential information as a means to reduce the threat to online security. Another objective of this paper is to suggest better ways to choosing stronger credential information on the web like biometric authentication.

Keywords: Passwords, Authentication, Complexity, Memorability, Cybercrime, cyber safety,

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Cyprian Danso Darko (2022). Weak Credential Information As A Threat To Online Security . SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 35-40. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P6

1. INTRODUCTION

Online activities increasing at fast rate comes with lots of benefits to users and on the other side is the threats that are associated with these activities, users and the system. Choosing a weak credential information online for various accounts held can pose a serious threat to the user being compromised or hacked. As a results, personal data can be altered and the worse is when your credential information is used as a gateway to have access to the whole system which also houses other users' data and or information. It is in the light of this that this paper looks at the security threats that would be posed to the online users and systems. Weak credential itself is a flaw in all systems as can easily be compromised.

This paper is necessitated by the rise in cybercrime that are committed online and one major cause is weak credential information that is making it easy for cyber criminals and posing lots of threats to the entire web space. Credential information which includes user name, passwords and other authentication methods to access the web should be strong and or complex enough to make it difficult for cyber criminals to guess or easily find it in clear text.

The greater part of the authentication systems nowadays utilizes a blend of a username and password for confirmation. Generally, alphanumeric passwords are being utilized for authentication and are known to have security and convenience issues. Vaz and et al. (2017), says a computer Information security system ought to likewise consider the human issues, for example, effortlessness of utilization and openness and that, current security systems endure in light of the fact that we generally disregard the significance of some social and human factors in security. They further said that a password is a mystery that is shared by the verifier and the client. "A secret password is a private key that is shared by the verifier and the End user. "Passwords are just a private key that is given by the End-User upon solicitation by a recipient." These passwords are regularly put away on a server in an encrypted format with the goal that a penetration of the system does not uncover password records.

2. RELATED WORKS

This section looks at related work and reviews the work with reference to choosing user names and passwords through to authentication of such credentials on systems and online platforms. A research conducted by Kumar and Bilandi (2014) indicated that an authentication system should energize vigorous passwords while keeping up the ease of use and memorability.

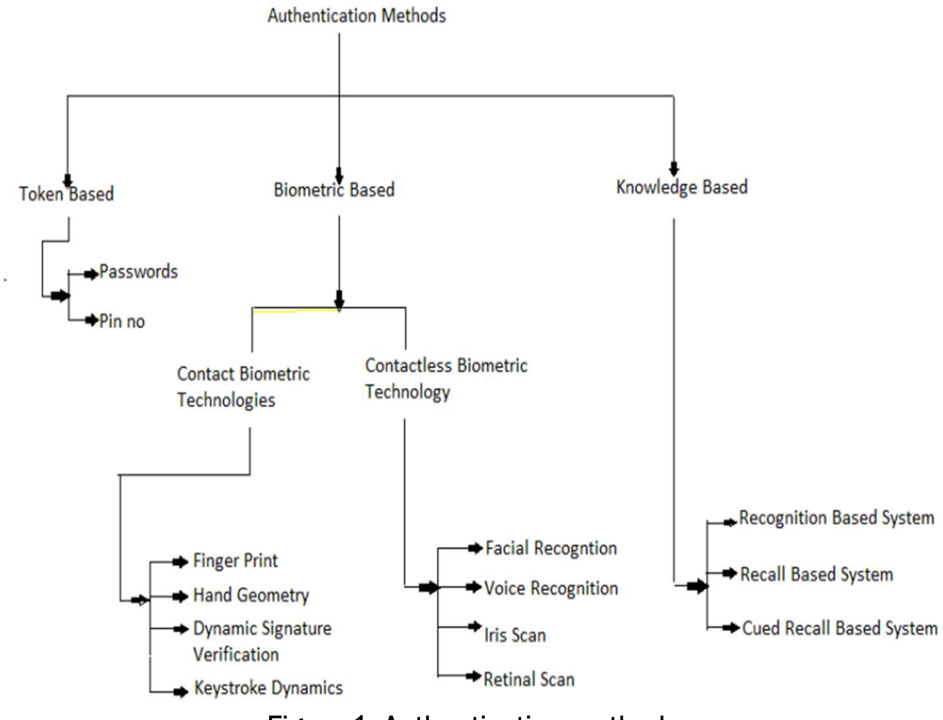

Figure 1. Authentication methods
Source: https://www.preprints.org/manuscript/202008.0268/v1

According to Gordon (2017) there are three authentication mechanisms, which is something you know, something you have, and something you are. Authentication techniques square measure comprehensively characterized into three principle areas. Token-based Authentication which is commonly known as two-factor authentication, Biometric based authentication which is also known as three-factor authentication and a Knowledge-based authentication which is a single factor authentication (https://www.preprints.org › manuscriptuthentication)

A research conducted by Kumar and Bilandi (2014) show authentication methods and I think employing the biometric based one online would proof more secured.

Weak passwords always play a major role in any hack. For the ease of user, sometime applications do not enforce password complexity and as a result of that users use simple passwords such as password, password123, Password@123, 12345, god, own mobile number etc. Weak password does not always mean length and the characters used, it also means the guessability. Name@12345, it looks quite complex password but can be guessable (https://www.sciencedirect.com/topics/computer-science/weak-password)

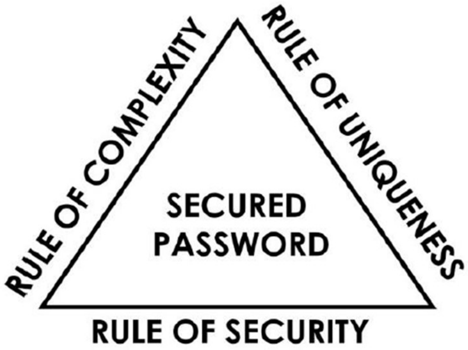

Fig. 2a: Theoretical Framework of Password Management

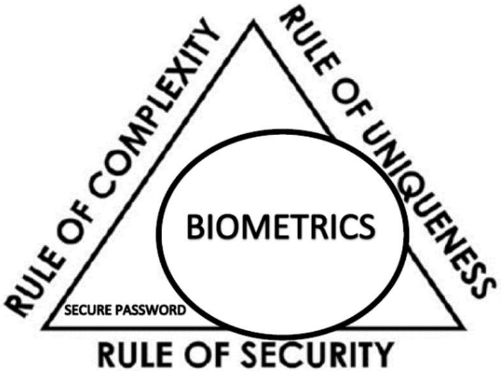

Fig.2b: Revised Theoretical framework of Password Management
Sources: Burnett and Kleiman (2006); Cyprian D.D (2022)

3. RESEARCH GABS AND FINDINGS

From the above modification of the Theoretical Framework Password of Management to a now Secure Credential Authentication Framework, the gab that has been left is being closed. This framework when implemented by all would reduce the cyber threats of online activities and many other systems that uses such credentials to access the needed data and information. Dean Nicolls 2019 , in his article What is biometric authentication? says Juniper Research forecasts that biometric authentication will increase from an estimated 429 million in 2018 to over 1.5 billion in 2023. (source: Mobile Payment Security: Biometric Authentication & Tokenisation 2018-2023).https://www.jumio.com/what-is-biometric-authentication

According to the 2019 Verizon Data Breach Investigations Report, 80% of hacking related breaches are due to compromised, weak, and reused passwords. Passwords provide a broad attack surface with many vulnerabilities. In the midst of increased cyberthreats and fraud, voice and face biometrics reduce risks while offering a simpler way for users to login. Unlike passwords, PINs, and “secret” questions, biometrics require nothing for users to remember and nothing that can be stolen, “phished,” found on the dark web, or shared.
https://www.idrnd.ai/biometric-login

Weak credential information was being mitigated with password encryption which still had some form of weakness and could still pose a threat to online security.
https://www.sciencedirect.com/topics/computer-science/weak-password

There are credential spills, spoofing, etc. because the credential information is mostly weak and poses threat to the users. Again, it was found that threats for weaker credential information did not only affect the very system and user but have ripple effect on other users and other systems.
https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

Chromebook have biometrics as part of its login requirements to allow users have secure login credentials that would not pose security threats to its users. You can use the fingerprint and pin to log in to supported websites or apps. You must set up your fingerprint before you log into websites and apps with your fingerprint.
https://support.google.com/chromebook/answer/10364313?hl=en

4. CONCLUSION

Weak credential information poses so much threat to online security and must be looked at with all urgency. Though it is difficult to memorize a strong password that forces most users to request reset of passwords, it also makes it difficult to guess thus increasing the security and reducing threats. However, the weak credential information could resort to biometrics to curb the threat and damages it would cause.

5. RECOMMENDATION FOR POLICY AND PRACTICE

The use of clear text usernames should be transformed to abstract characters as they are being entered to prevent eavesdroppers from seeing the username and trying to guess the password. Users must learn to have unique passwords for different platforms so that when one password is compromised, the other accounts managed by the same user on different platforms would not be compromised.

Further, biometric authentication methods should be used in authenticating logins on online systems by providing the needed hardware in computers and other devices that would allow such biometric authentications anywhere one is accessing the web. International Professional and standardization organizations like IEEE and ISO should make it a policy to collaborate with other stakeholders to set out rules for the use of biometrics in online platforms to login instead of the current alphanumeric user names and passwords that are in use. They could achieve this by enforcing a policy that would coerce technological device manufacturers to add biometric scanners or data captures to every device produced.

5.1 Cyber Safety in Africa and implementation of policies and best practices

Africa is gradually positioning itself in the technological world with seven African tech companies included in the forum's 2021 cohort of 100 Technology Pioneers. In his article, Cyber security in Africa: The boring technology story that matters´' Hood S. Mukiibi, 2019 stated that A limitless cyberspace, little to no boundaries, and eroding national borders is making Africa vulnerable to cyber threats and potential harms, Cybersecurity represents a serious economic and national security challenges which needs to be properly defined and contextualized". https://www.researchgate.net/publication/33751971

Weak online credentials can collapse the African economy if cyber safety is not implemented. African Union (AU) must encourage its member states to implement cyber safety polices in government settings and enforce the same with every entity to make cyber safety (strong credential information on the web and systems) a corporate social responsibility

6. DIRECTIONS FOR FUTURE WORKS

Future research work must consider researching how best biometric authentication could help reduce the threats associated with weak online credential information, Further research could also consider the if there are any inherent weaknesses associated with using biometric credentials online.

REFERENCES

1. Enhancing Password Authentication Using Association Password Technique: An Ecological Theory of Memory and Data.Vaz and et al. (2017)
2. https://www.sciencedirect.com/topics/computer-science/weak-credential-Vidhyacharan Bhaskar, in Engineering Science and Technology, an International Journal, 2018
3. https://www.preprints.org › manuscriptuthentication.
4. https://www.jumio.com/what-is-biometric-authentication
5. https://www.idrnd.ai/biometric-login
6. https://www.preprints.org/manuscript/202008.0268/v1
7. https://www.sciencedirect.com/topics/computer-science/weak-password
8. https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report
9. https://support.google.com/chromebook/answer/10364313?hl=en
10. https://www.researchgate.net/publication/337519711.