Nigerian Journal of Technology (NIJOTECH)
Vol. 43, No. 4, December, 2024, pp.706 - 715
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v43i4.11

DUAL COMBAT TECHNIQUE-BASED CYBER SYSTEMS PROTECTION AGAINST PASSWORD ATTACKS

AUTHORS:
A. I. Erike[1,*]

AFFILIATIONS:
[1]Department of Software Engineering, Federal University of Technology, Owerri, Nigeria

***CORRESPONDING AUTHOR:**
Email: azubuike.erike@futo.edu.ng

ARTICLE HISTORY:
Received: 30 April, 2024.
Revised: 09 November, 2024.
Accepted: 28 November, 2024.
Published: 31 December, 2024.

KEYWORDS:
Cyber-System protection, Brute-force, Password attack, Dual combat technique, Cybersecurity, Application system security, System protection.

ARTICLE INCLUDES:
Peer review

DATA AVAILABILITY:
On request from author(s)

EDITORS:
Chidozie Charles Nnaji

FUNDING:
None

Abstract

The rise in machine-enabled password attacks and the cost per record lost in an average case of a data breach necessitate the need for a more robust technique for combating password attacks. Organizations of different sizes and global reputation have been victims of cyber-attacks. The problem of cyber-attacks has attracted several research responses from researchers with some attending results. This article presents the Dual Combat Technique-based Cyber-Systems protection against password attack. The proposed system utilizes a-three-tier model for detection, notification, and combat. The dual combat technique involves the System Protection Model (SPM) and the User Protection Model (UPM). While the SPM implemented a time delay algorithm powered by a geometric progression model, the UPM uses a dual handshake method for data communication between the user and the server. In the first instance, the UPM sends data to the Cyber-system server through an HTTP Request over an SMS gateway to virtualize a user's account upon a trigger by the attack detection model. In the second instance, the deactivation of the virtualization operation uses the authentication of the user's email and phone number. The result of the work presents a system that introduces a time-delay after a number of login attempts defined by a certain threshold value, and a user response action for account virtualization. The application testing presented a success rate of 90.16% on the number of times the request response was induced over an eight-day period of testing and 9.84% failed attempts.

1.0 INTRODUCTION

Is cybercrime ever going to stop? Before this question is answered, the underlying cause behind this menace must be understood. Hence, a proper evaluation of the dynamics behind the problem must be studied. Cybercrime is a criminal activity that uses a computer to target other computers or websites, or a network of computers [1]. Crime on itself is simply undertaking an activity that is not ethically approved, or an action which is not publicly or generally accepted. It is apparent that for every cybercrime incidence, there is a man behind the mask. Cybercrimes exist in several forms and shapes. Kaspersky [1], [2] listed the following under types of cybercrimes: stealing financial data, sell of public data, cyber extortions, crypto jackings [1], [2]. Al Hasib [3] [4], stated Spamming, Cross-site scripting, Viruses, Worms, Phishing, Information leakage, Identity theft also as different forms of cybercrime [4]. Other forms of cybercrime include: Malware, Browser jacking, monitoring cookies, key loggers, Scum ware, Trojan

----
HOW TO CITE:
Erike, A. I. "Dual Combat Technique-Based Cyber Systems Protection Against Password Attacks", *Nigerian Journal of Technology*, 2024; 43(4), pp. 706 – 715; *https://doi.org/10.4314/njt.v43i4.11*

© 2024 by the author(s). This article is open access under the CC BY-NC-ND license

horses etc [5]. All these have a common denominator; they are carried out on the cyber space.

The major focus of cyber-attacks is to steal or to expose confidential information to unauthorized persons. The operational result is technically known as cyber breach [6]. This inadvertent exposure places firms and organizations to a fix of both reputational damage and financial loss. While the advancements in technologies help in quick developments of technological ideas to drive the society, these technologies also are a tool that promote the execution of these cyber-attacks. The average cost of cyber breach per record was estimated at $150 by IBM in their 2020 study of data breach report gathered from 524 organizations across 17 industries in 17 countries and regions. These attacks spare no one. It targets both small, medium, and large businesses. In a cyber-breach report of 2021, 26% of charities and 39% of businesses among other areas were reported to have been attacked [7].

Researchers have proposed several solutions that included the use of key-stretching techniques[8], [9], salt and pepper techniques [9], [10], [11], [12], cryptographic hashing techniques [10], [13], Honeyword generation [12], [14], [15], [16], Cyclic authentication technique[17] and so on. Other techniques involve the use of Captcha, No Captcha reCAPTCHA etc which proved very effective. All these notwithstanding, cyber systems security remains an issue till date.

Brute force attacks leverage on conceivable character permutations until it finds a matching key that can be used to perform authentication in any password-secured infrastructure [18]. However, how successful brute force attacks can be depends on the length of the user-supplied password [19]. Many brute attacks occur largely because of the user's password selection choices (selecting passwords that are easy to remember), and the use of publicly exposed default passwords created by system administrators. In all the developed methods of combating this attack, the man behind the attack is aimed. Measures have been put in place using various techniques to secure both cloud-based and non-cloud-based infrastructures.

This work developed a user-based offline approach to cyber-systems protection against brute-force password attacks in cloud-based systems using dual combat technique. It focuses on granting the user the privilege of being involved in the combat process in the face of an envisaged brute-force password attack.

The remainder of the manuscript is structured as follows: Section two presents the cyber system's protection concept and a review of some related literatures. Section three outlines the methodology employed in the research execution while section four on its own presents the results and discussion of the research implementation. Finally, section five serves as the conclusion of the work and recommendation for future work.

2.0 LITERATURE REVIEW

2.1 Cyber Systems Protection Concept

A cyber system is basically a system that integrates digital technologies with physical systems and human interactions to perform specific functions, often involving the exchange, processing, and control of information [20]. Cyber systems protection is (CSP) basically the art of ensuring that the integrity of a cyber-system is kept uncompromised. It involves a set of techniques generally set for use in safeguarding the cyber environment space of a user or an organization, and the integrity of networks, programs, and data from unauthorized accesses [21]. Undoubtedly, every cyber breach is geared towards stealing of data, defacement, alteration of data, or even profile hijacking. However, a lot of research efforts in cybersecurity domain has been centred around data protection. Many techniques and technologies have been proffered as solutions. Some of these techniques include cryptography and hashing which involves taking information or data and applying mathematical processes to it to make the message unreadable [22]. Another is the use of application firewalls for controlling data flow into a system environment and many more. Others include Intrusion detection systems for detecting unauthorized entry into a cyber-system environment, antivirus and antimalware software for detection and prevention of unauthorized software, use of multi-factor authentication which provides a complementary approach to user authentication and authorization and so on.

Attacks on cyber network infrastructures are made possible by exploitable vulnerabilities that exist in such domains. These different vulnerabilities lead to different types of attacks like the SQL injection attack. In SQL injection attacks,, where the attacker deliberately inserts malicious codes into a server that uses SQL with the sole aim of forcing the server to reveal information it normally would not [23]. Another is a denial-of-service attack which tends to flood systems, servers, or networks with heavy traffic aimed at exhausting the system's resources and bandwidth [23], [24] ,. Brute brute force attack, is yet another mode of attack which involves a repeated banging of a cyber-system's access point with every

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

https://doi.org/10.4314/njt.v43i4.11

possible combination of passwords, encryption keys or credentials until a correct one is found [25]. Still on the list are cross site scripting attack, account hijacking [26], defacement [27], fishing [28], malware [29], brute force [30], and many more.

Combat against treats is often developed using system protection models. A system protection model is a structured framework that outlines strategies, policies, and mechanisms designed to safeguard a cyber-system from vulnerabilities and threats. The concept of the dual combat technique presented in this paper refers to a protection method that utilizes two independent attack defence mechanisms to address a specific identified threat.

2.2 Related Works

Security of cyber systems involves all the actions taken to ensure proper operation of the system, ranging from making the system robust to protecting them from both intentional and unintentional malicious activities. Many Although many methods to cyber systems' protection have been developed by scholars over the years, research is still underway in that domain with the aim of curbing menace of cyber criminals. That notwithstanding, the subject of cyber systems security remains a huddle to be crossed because, the invention of new technologies and advancement of old ones open the door leading to the breaking of former security approaches and rendering them inefficient. This section presents a review of some scholarly research efforts to cyber systems protection.

To put create up a novel authentication protocol for insider attacks based on the robust cryptographic algorithm - Elliptic Curve Cryptography (ECC), [31] proposed a three-tier handshake protocol that involved a client PC in a network, the password management server (PMS) and the service provider server (SPS). Initially, all the client PCs register themselves to the PMS by sending their IDs. The PMS then encrypts the personal computer's (PC) information using a secret key and stores the master key along with the SPSs in a table. Before accessing the PMS, each client PC again registers itself to the PMS using a username and password passed through the web browser which encrypts and sends the information to the PMS. The PMS then decrypts it and computes the cypher text using the information and sends it to the SPS. The SPS only receives the encrypted password through which it can never get the original credential of the user, thus preventing the possibility of attack at any cost There is a cryptographically secure handshake protocol between the PMS and the SPS. In this handshake protocol, the SPS is just acting as a channel. The encryption and decryption lie at the far end of the user's PC and the PMS. The major drawback here is that the browser does not help the user to remember his password. This also can be viewed as an advantage because even if a user's device is stolen, access to the classified information will be denied since the device browser does not help in remembering passwords.

In their research, [32] proposed a multi-level authentication system using sound and image-based password protection. The study aimed to use text, voice and image-based authentication by taking sound as input, and then calculating the time for that sound signature alongside the image selection pattern to be done. The researchers developedThis follows a multi-level sequential technique that utilized text, audio, and image signatures for user-authentication. The user enters a particular text that he will provide the next time he visits, the start and end time stamps of the audio and then the picture pattern of images displayed at the point of registration. This way, authentication factors are increased by the number of parameters utilized in the process. During the authentication process, the user is expected to provide the same parameter he provided during the signing up process in other to be authenticated. The drawback in this approach lies in the process of recovery of the authentication parameters or the entire system recovery if the user peradventure forgets his credentials.

Password assistance was proposed by [33] with the aim of developing a system that supports users in all duties and tasks regarding their passwords, from creation of secure passwords to the recovery of same in case of loss. Their research by [33] implemented the password synchronization and backup systems using the PAsswordLess PAssword Synchronization (PALPAS) schemes, and developed a brute force resistant password generation mechanism in four building blocks as follows: Password Requirement Markup Language that was used to create password description for services. Password Requirement Crawler (PRC); an application that extracts password requirement for a service and then generates Password Requirement Description (PRD) for the service. Thirdly, a synchronization of the passwords between all the devices belonging to a user, and finally, a secure backup of the passwords as well as a built-in revocation mechanism and an emergency access for backups. The work however is presented as a roadmap to a robust open-source password assistant development project that can be implemented in parts and or in whole.

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

[34] focused on securing Enterprise Information Portals against username enumeration attack using their proposed dual combat technique. Their security framework was done using the structural systems analysis and design methodology. The technique was developed to give the user opportunity to partake in the combat process, giving the user the privilege of virtualizing and unlocking her account upon detection of either a dictionary attack or a brute-force password attack. The system was developed to track attacks targeted on the system and then to keep the user notified through an SMS sent to the user's phone. They recorded success around detection and combat of envisaged attack, and a time-to-combat response time that is 36.7% faster than the existing system. The drawback of the system is because the combat process only works with internet-enabled mobile phones, which means that a user cannot successfully virtualize his or her account if he does not have good data signal power or if he does not have an internet-enabled phone.

Further studies by [17] presented a user-driven approach for safeguarding cloud infrastructure against unauthorized deletion and modifications. This study utilized the Serpentine Multifactor Authentication Technique SeMFAT, which technically provided a cyclic sequential authentication method based on the registered authentication vectors supplied by the user. The approach has two major components: the registration by validation process for registering authentication vectors, and the authentication by validation procedure for authenticating the authentic-cation vectors. The authentication by validation action is triggered when a user-initiated action occurs, as indicated by a profile audit trail. This trail comprehensively logs all activities performed on a user's profile and initiates the authentication process to confirm that only users with authenticated privileges can perform specific actions on their profiles.

[10] proposed password protection using cryptographic hashing technique with the aim of creating a protected and crack resistant password for user authentication. They used a random cryptographic hash generation for each user registration. In there research, f For every user registration, a random cryptographic hash value is generated and stored in the database. The hashed value is then concatenated with the user password and then passed through another hash function. The produced password hash is then stored in the database. This is referred to as an iterative hash mechanism technique. This approach created a one-way high entropy password that is resistant to cracking attempts. However, unless the main user password is made to be strong, the system will still be prone to dictionary attack.

Another study by [9] proposed several improvement techniques on the MD5 hash algorithm for better password strengthening. These include: Improved hash function that involved hashing any of the following combinations – password and salt, a hash of the password and the salt, password and salt and key. Their research also suggested an iterative hashing methodology, key stretching – (simple key stretching, password key stretching, salted key stretching), password transformation before hashing, chaining method and XOR cipher approach. In the proposed approach, first, a random key string of variable length is generated. Next, the password that the user entered is transformed into a complex password through columnar transposition cipher. Then, the salt value is calculated by finding the XOR value of the random key string with the complex password, row by row. Fourthly, an additional random information string of 128 bits is generated for each user and stored in an external file. Finally, the password is hashed using a formular based on key stretching and then stored in the database. The final password output is not in hexadecimal format, so the several cracking systems that is based on hexadecimal storage failed in their attempt to crack the generated password. By XORing the output hash values from each iteration makes it almost impossible to find out the original hash output at the first round. The use of random key makes it impossible for two users using the same password to have the same output stored in the database. The challenge of this proposed solution is that the time complexity of the process will be high though the evaluation of the research was not done in that area.

A dynamic and yet a user-dependent technique for robust multi-password generation algorithm against offline attacks was proposed by [12]. This approach uses dynamic chaffing-with-tough-nuts technique to dynamically generate real-user triplicate passwords and multiple honey passwords. These combinations stored in a single password relation leaves authentication to a correct combination of the real user triplicate passwords. A password transformation function is used to transform specific yet dynamic user salts into characters whose hash values from the user supplied passwords are almost impossible to crack. This approach creates multiple passwords according the magnitude of the programmer's defined functional parameters, and thus presents multiple passwords with very high entropy.

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

All the proposed techniques except the ones in [12], [17], [34] are majorly system based. This means that the performance of the proposed solutions in combat process is application dependent. This research is focused at improving upon the work of [34] by enabling the combat process to be carried out without internet connectivity. By this, the integration of the user into the combat process will not be hampered by unavailability of data signal network around the user's vicinity at the point of attack.

The remainder of the manuscript is structured as follows: Section two presents the cyber system's protection concept and a review of some related literatures. Section three outlines the methodology employed in the research execution while section four on its own presents the results and discussion of the research implementation. Finally, section five serves as the conclusion of the work and recommendation for future work.

3.0 METHODOLOGY

A brute-force password attack systematically tries every possible combination of characters for authentication credentials, such as a User ID or Password, until the correct one is identified. So, this is a targeted attack to an existing record. The process involves keeping a known parameter constant and trying out a guess on the second parameter either manually or with the assistance of a high-speed computer. The methodology involves the integration of User Supplementary Service Data (USSDSMS) technology over an SMS gateway to perform HTTP request on the cyber system. The process follows a three-tier architecture as seen in Figure 1, which consists of three blocks: the attack block, the notification block and the combat block.

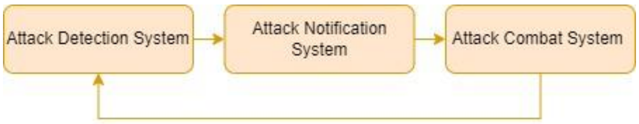

Figure 1: Three-tier cyclic architecture for cyber system protection

The attack detection block is works, based on the correctness of the login credentials in the login process; notification of the attack is performed through an SMS gateway to the user; and then, the combat process which is performed both cuncurrentlyconcurrently by the system and the user, hence the Dual Combat Technique. The correct login attempt grants the user access to the system while an incorrect login attempt logs the number of failed attempts to the database so as to prompt a system-action and a user-action when a certain threshold is reached, logging the number of failed login attempts. This process is seen in the data flow model of captured in the hybridized architecture of Figure 2.

3.1 The Attack Detection Model

The hybridized architecture of the proposed password attack model is shown in Figure 2. The architecture has different compartments. The Identity Access Management (IAM) block contains the authentication and the Access Control Lists (ACL) which grants users access to their privileged information upon successful login operation. In the event of failed login operation, the system logs the failed operation in the Access Management Log Table (AMLT). There are different parameters that are used to facilitate the attack detection operation. These include: the IP address of the attacking machine, the timestamp between attacks, the number of failed login attempts, the username U, and the password P.

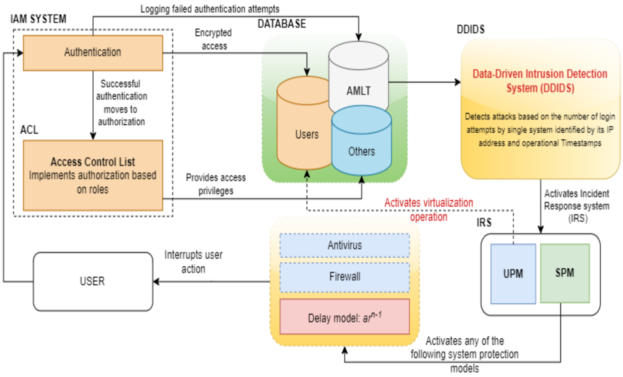
Logging failed authentication attempts
IAM SYSTEM
DATABASE
DDIDS
Authentication
Encrypted access
Successful authentication moves to authorization
ACL
Access Control List Implements authorization based on roles
Provides access privileges
AMLT
Users
Others
Data-Driven Intrusion Detection System (DDIDS)
Detects attacks based on the number of login attempts by single system identified by its IP address and operational Timestamps
Activates Incident Response system (IRS)
Activates virtualization operation
IRS
UPM
SPM
Antivirus
Firewall
Delay model: ar^{n-1}
Interrupts user action
USER
Activates any of the following system protection models

Figure 2: Hybridized architecture of the proposed password attack model

The IP address is used to detect when a repeated number of failed attempts within a specified time range determined by the timestamp was performed by a particular machine identified by the IP address. These parameters must beare identified as constant parameters within the specified time range before the improper combination of the U and P parameters are taken into consideration for attack detection. Since there are only two changing parameters of interest, the number of possible digital logic states is seen in Equation 1.

$$N_s = 2^2 x \; 1^1 \qquad (1)$$

Where, $N_s = Number\ of\ states$

Table 1 is a logic table depicting the number of possible states that the User_ID and Password can take at an instance, and the implication of each state per time. Attack will be envisaged at every other time except when the User_ID and the Password

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

https://doi.org/10.4314/njt.v43i4.11

parameters have logic state ‘1’ each at the same time. This means that the User have entered a correct User_ID and Password.

Table 1: Possible login states for User_ID and Passwords

No. of states	User_ID	Password	Status
First state	0	0	Attack suspected
Second state	0	1	Attack suspected
Third state	1	0	Attack suspected
Fourth state	1	1	Login Approved

$$Z = (\neg U \wedge \neg P) \vee (\neg U \wedge P) \vee (U \wedge \neg P) \qquad (2)$$

Let, $(\neg U \wedge \neg P) = x$; $(\neg U \wedge P) = y$; and $(U \wedge \neg P) = z$.
Where, U and P represents the User_ID and Password respectively.

Here, each of the alphabets, x, y, z represents the state at which attack will be detected. The $'\vee'$ sign represents a logical **OR** symbol, while the $'\wedge'$ sign represents the logical **AND** symbol. The ‘¬’ represents the logical **NOT** operator. Equation 2 represents the attack detection state.

$$f(w) = (Z)n, \qquad 0 \le n \qquad (3)$$

The function f(w) is an aggregation function that aggregates the possible attack states represented by Z multiplied by n. The parameter **‘n’** represents the number of failed login attempts. The number 2 is taken as the threshold value after which the system may now suspect an attack on the it, triggering the Incidence Response System (IRS) which encapsulates the System-based protection module (SPM) and the User-based protection module (UPM).

3.2 System Protection Model – SPM

Although the system protection model could be designed to activate an antivirus protection or firewall, here, it rather imposes a time delay on the system response to slow down the pace of the attack on the system to enable the legitimate user action to be taken.

$$a_n = a_1 r^{n-1} \qquad (4)$$

The system introduces a time-delay modelled in Equation 4 when the threshold of the accepted login trials has elapsed, and the time response increases by a factor that is defined by ***r*** according to the geometric sequence depicted in Equation 4 for each failed attempt ***n***. The variable ***a*** is regarded as the first term in the sequence that defines the first time the SPM is activated by a failed login attempt.

3.3 The User Protection Model - UPM

The UPM performs two operations – the virtualization, and the deactivation of the virtualization operation, albeit, through USSDSMS. This is employed to combat the trade-off of time between detection and response in using SMS-based notification and Internet-based response presented in [34], and SMS-based notification and SMS-based response that this methodology proffers as a solution in the area of user-centred attack response. The model follows a graphical approach to define the operation of this methodology.

As shown in Figure 3, the system checks the correctness of the input parameters. If they are correct, the display of E1 shows a correct login process. Otherwise, the failed attempt is logged in the database QDB2. Process 2 checks the threshold value of the incorrect login attempts and outputs two action triggered-responses depicted by the SPM and the process 3. The process 3 accesses the database at QDB3 to extract the User’s parameters in other to execute process 4. Process 4 generates access to the virtualization algorithm and sends same to the User at process 5. If the Fraud Alert SMS (FAS) is sent, the process ends, waiting for the User’s action. Next is the account virtualization and the reactivation module.

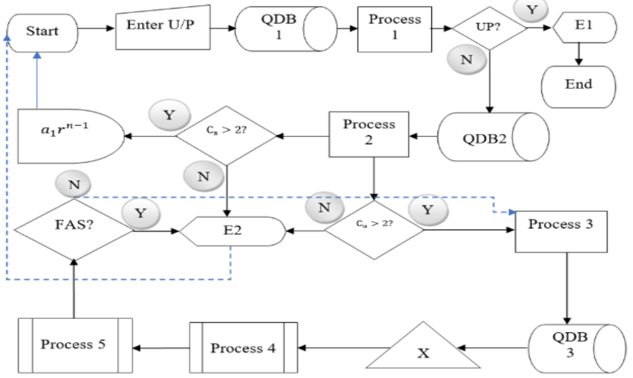

Figure 3: The Flow model of the proposed methodology

3.4 Account Virtualization and Reactivation Module

The account virtualization module is saddled with the responsibility of virtualization of the flagged user’s account simply by communicating with the Cyber-system through an HTTP REQUEST sent over an SMS gateway in response to a Fraud Alert SMS. The system of virtualization simply deactivates the attacked user’s account such that even with the right login credentials, access is denied stating that the flagged account does not exist.

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

Notice in Figure 4 that the virtualization code is checked against the authentication platform to be sure that the message has the correct virtualization code set at the onset against an account represented by the responding phone number. If it is a valid virtualization code run within a secure time frame, the next is to check the fraud log table to ascertain if the phone number responding to the call was actually the one used in sending the message.

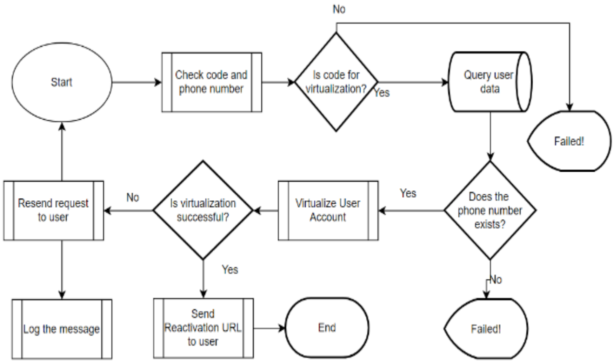
No
Start
Check code and phone number
Is code for virtualization?
Yes
Query user data
Failed!
Resend request to user
No
Is virtualization successful?
Virtualize User Account
Yes
Does the phone number exists?
Yes
No
Log the message
Send Reactivation URL to user
End
Failed!

Figure 4: Account virtualization module

If the phone number exists in the log table, then a query is raised to virtualize the account. If the check for virtualization and the authenticity of the querying phone number returns negative, the system simply fails because it assumes that a malicious attacker is making the request and hence should not be responded to. However, if the virtualization returns true, an email is sent to the user for the reactivation of the deactivated account. The choice of the User's email is so as to create a distributed channel to ensure that account recovery is by a legitimate owner of the account. If for any reason virtualization returns negative, a fraud attempt is also sent to the user and then the message is logged once again.

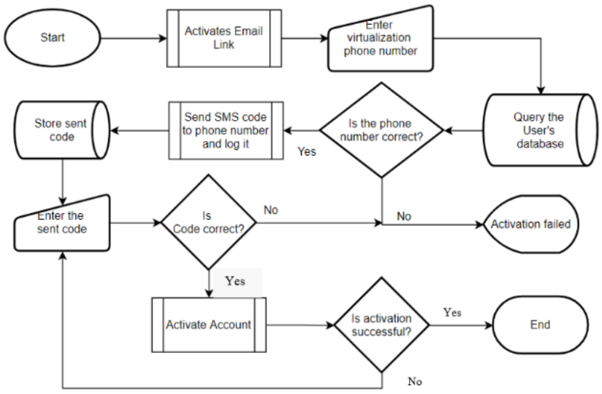
Start
Activates Email Link
Enter virtualization phone number
Store sent code
Send SMS code to phone number and log it
Yes
Is the phone number correct?
Query the User's database
Enter the sent code
Is Code correct?
No
No
Activation failed
Yes
Activate Account
Is activation successful?
Yes
End
No

Figure 5: Account reactivation module

Figure 5 is the account reactivation module. In the use-case for the reactivation of the user's account, the user clicks on a link that is sent to his email. The link takes him to the validation page that is tied to the phone number that initiated the account virtualization process. The user enters the phone number. The validation of the phone number is done and upon confirmation of the record in the database, a confirmation code is sent to the phone number. The User will be prompted to enter the code he received in a new page that would load as a way of ensuring that the user holds access to both the phone and the email. Upon authentication of the phone number through SMS, the user's account is activated.

By so doing, a malicious attacker that repeatedly tries to log into any user's account will meet the system's delay function and the user's virtualization action, hence preventing brute-force password attacks on the individual's accounts and hence enables the seamless recovery of a virtualized account.

4.0 RESULTS AND DISCUSSION

To test the robustness of the application against password attacks, deliberate attacks were lunched against the application at different times of the day for about eight consecutive days with a view of checking the delay response and the success rates of using USSDSMS-based cyber system's attack response in the event of an envisaged brute-force attack.

4.1 Success Rates

Success rates define the number of times HTTP requests that was sent through the USSDSMS gateway was successful. This is meant to validate the use of this technology to implement a remote account virtualization technique on cyber system's application as a way to combat password attacks and illegal login attempts on Cyber-Systems. Deliberate attempts were made to capture the number of USSDSMS requests made in response to FAS that really virtualized the operation by checking the database to see the instance of the User's relation. The experiment was carried out from 24th December 2022 to 31st December 2022. Table 2 contains the data of the number of trials made per day. According to the graph of Figure 6, success rates of employing USSDSMS response approach was discovered to be 90.6% with all the three selected major telecommunication carriers in Nigeria. This represents a significant proof that the USSDSMS technology can be adopted in the remote virtualization of accounts especially in the internet inaccessible areas. From the graph also, we noted that the 9.84% failure delivery is a significant portion that needs further attention in the combat process. The USSDSMS test bed utilized for the testing is a

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

sandbox environment provided by the AfricasTalking website.

Table 2: Success rates for USSDSMS requests

Date	No of Trials	Successful	Failed
12/24/2022	10	8	2
12/25/2022	5	5	0
12/26/2022	9	8	1
12/27/2022	6	6	0
12/28/2022	7	6	1
12/29/2022	8	8	0
12/30/2022	7	5	2
12/31/2022	9	9	0
Total	**61**	**55**	**6**

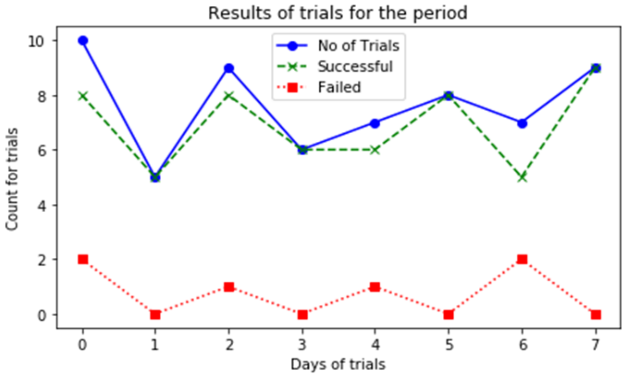

Figure 6: Success rates of implementing USSDSMS-based system account virtualization

The recorded success rates show that this technology can be used to fight against brute-force password attacks seeing that greater percentage of all the actions initiated through the USSDSMS gateway proved successful. More so, the response time is near real time in nature, meaning that as an attack is envisaged on the application, the user is alerted immediately and a response to such attack initiates an immediate action. Nevertheless, there could be a delay in sending SMS to the user which may arise due to some certain factors beyond the scope of this research.

However, the usage cost of this technique can be overwhelming with time. Nevertheless, the cost of a data breach per record when compared to the cost of utilizing this technique renders this a better alternative.

5.0 CONCLUSION

This research proposed the integration of Cyber System Users into the combat process against brute-force password attacks – The Dual Combat Technique. A review of extant literatures shows that the existing architectures neglected the user in the combat process except for the research done in [34], which integrated the User in the process though through an Internet enabled platform. The proposed methodology however utilizes an SMS gateway to execute an account virtualization action in response to an envisaged attack on the system especially during the times the user may be in a network unreached area or without an internet enabled phone. Results show that the success rate recorded by this technique proved 90.16% efficient using the three major telecom providers in Nigeria – MTN Nigeria, Globacom and Airtel Nigeria. It is therefore recommended that this technique be integrated in cyber systems development to enhance cloud infrastructural security.

REFERENCES

[1] Lusthaus, J. “Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?,” *Annu. Rev. Law Soc. Sci.*, vol. 20, no. 1, pp. 369–385, 2024, doi: 10.1146/annurev-lawsocsci-041822-044042.

[2] Wall, D. S. *Cybercrime: The Transformation of Crime in the Information Age, 2nd edition, Cambridge: Polity*, 2nd editio. Cambridge, 2024. [Online]. Available: https://www.wiley.com/en-us/Cybercrime%3A+The+Transformation+of+Crime+in+the+Information+Age-p-9780745653532

[3] Al Hasib, A. “Threats of Online Social Networks,” 2009.

[4] Al Hasib, A. “Threats of Online Social Networks,” *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 11, p. 288, 2009.

[5] Thomas, F. Stafford and Robin Poston, “Online Security Threats and Computer User Intentions,” 2010, *IEEE Computer Society*. [Online]. Available: www.grc.com/intro.htm

[6] Cheng, L., Liu, F., and Yao, D. D. “Enterprise data breach: causes, challenges, prevention, and future directions,” Sep. 01, 2017, *Wiley-Blackwell*. doi: 10.1002/widm.1211.

[7] Department for Digital Culture Media and Sport, “Cyber Security Breaches Survey 2021 Statistical Release,” London, 2021. [Online]. Available: www.nationalarchives.gov.uk/doc/open-government-licence/ or

[8] Blocki, J., Harsha, B., and Zhou, S. “On the Economics of Offline Password Cracking,” Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.05023

[9] Mary, C., Ah, K., Zhaoshun, W., and Deb, D. S. “Security Analysis of MD5 algorithm in Password Storage,” in *Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13)*, Atlantis Press, Paris, France., 2013.

[10] Preethika, S. “Password Protection Using Cryptographic Hash Technique,” *Int. J.*

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

Emerg. Technol. Eng. Res., vol. 4, 2016, [Online]. Available: www.ijeter.everscience.org

[11] Soumya, G., and Soumya, P. “Authentication by Encrypted Negative Password,” *J. Resour. Manag. Technol.*, vol. 12, no. 1, pp. 437–442, 2021.

[12] Erike, A. I, Azubogu A. C, Akpado K. A, Arinze C. O, Mshelia Y.U, “Dynamic User-Dependent Technique for Robust Multi-Password Generation Against Offline Cracking Attacks,” *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 11, no. 4, pp. 15–23, 2023.

[13] Blocki, J. and Datta, A. “CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection,” in *29th IEEE Computer Security Foundations Symposium*, Sep. 2015. doi: DOI: 10.1109/CSF.2016.33.

[14] Shubham Sawant, Pratik Saptal, Kritish Lokhande, Karan Gadhave, and Randeep Kaur, “Honeywords - Making Password Cracking Detectable,” *Int. J. Eng. Res. Adv. Technol.*, vol. 4, no. 4, Apr. 2018, doi: http://dx.doi.org/10.7324/IJERAT.2018.3218.

[15] Sailaja, C. V. and Reddy, B. T. “Creating secure and dependable honey words to increase password security.,” *Ann. Rom. Soc. Cell Biol.*, vol. 25, no. 4, pp. 19588–19594, 2021.

[16] Erguler, I. “Achieving Flatness: Selecting the Honeywords from Existing User Passwords,” *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 2, pp. 284–295, 2016, doi: 10.1109/TDSC.2015.2406707.

[17] Erike, A. I., Azubogu, A. C., and Mshelia, Y. U. “User-Driven Approach to Preventing Unsanctioned Profile Modifications and Deletions in Cloud-Based Multi-Tenant Infrastructures,” *UNIZIK J. Eng. Appl. Sci.*, vol. 2, no. June, pp. 177–186, 2023, [Online]. Available: https://journals.unizik.edu.ng/index.php/ujeas/article/view/2202

[18] Ayankoya, F. and Ohwo, B. “Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 2, pp. 7–19, 2019, [Online]. Available: https://www.academia.edu/38523734/Brute-Force_Attack_Prevention_in_Cloud_Computing_Using_One-Time_Password_and_Cryptographic_Hash_Function

[19] Farik, M. and Ali, A. S. “Analysis of Default Passwords in Routers against Brute-Force Attack,” *Int. J. Sci. Technol. Res.*, vol. 4, no. 9, pp. 341–345, 2015.

[20] Putnik, G. D., Ferreira, L., Lopes, N. and Putnik, Z. “What is a Cyber-Physical System: Definitions and models spectrum,” *FME Trans.*, vol. 47, no. 4, pp. 663–674, 2019, doi: 10.5937/fmet1904663P.

[21] Seemma, P. S., Nandhini, S., and Sowmiya, M. “Overview of Cyber Security,” *Ijarcce*, vol. 7, no. 11, pp. 125–128, 2018, doi: 10.17148/ijarcce.2018.71127.

[22] Haunts, S. "Applied Cryptography in . NET and Azure Key Vault", 2019.

[23] Saravanan, A., and Bama, S. S. “A Review on Cyber Security and the Fifth Generation Cyberattacks,” *Orient. J. Comput. Sci. Technol.*, vol. 12, no. 2, pp. 50–56, 2019, doi: 10.13005/ojcst12.02.04.

[24] Abomhara, M. and Køien, G. M. “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[25] Vugdelija, N., Nedeljković, N., Kojić, N., Lukić, L., and Vesić, M. “Review of Brute-Force Attack and Protection Techniques,” pp. 1–10, 2021, [Online]. Available: https://proceedings.ictinnovations.org/2021/paper/554/review-of-brute-force-attack-and-protection-techniques

[26] Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C. T. and Ramakrishnan, N. “Crowdsourcing cybersecurity: Cyber attack detection using social media,” *Int. Conf. Inf. Knowl. Manag. Proc.*, vol. Part F1318, pp. 1049–1057, 2017, doi: 10.1145/3132847.3132866.

[27] Hoang, X. D., and Nguyen, N. T. “A multi-layer model for website defacement detection,” *ACM Int. Conf. Proceeding Ser.*, no. October, pp. 508–513, 2019, doi: 10.1145/3368926.3369730.

[28] Conteh, N. Y., and Schmick, P. J. “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks,” *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/ijacr.2016.623006.

[29] Qamar, A., Karim, A., and Chang, V. “Mobile malware attacks: Review, taxonomy & future directions,” *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019, doi: 10.1016/j.future.2019.03.007.

[30] Bosnjak, L., Sres, J., and Brumen, B. “Brute-force and dictionary attack on hashed real-world passwords,” *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, no. May 2018, pp. 1161–

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

1166, 2018, doi: 10.23919/MIPRO.2018.8400211.

[31] Rajamanickam, S., Vollala, S., Amin, R., and Ramasubramanian, N. "Insider Attack Protection : Lightweight Password-Based Authentication Techniques Using ECC," no. May 2021, 2019, doi: 10.1109/JSYST.2019.2933464.

[32] Moyila Mounika Dev, V. Sarala, and A. Durga Devi, "Multi Level Authentication System Using Sound and Image Based Password Protection," *Mukt Shabd J.*, vol. IX, no. IV, pp. 4767–4775, Apr. 2020.

[33] Horsch, M., Braun, J., and Buchmann, J. "Password Assistance," 2017.

[34] Erike, A. I, Inyiama, H. C., and Nwalozie, G. C., "Securing Enterprise Information Using Dual Combat Technique," *Int. J. Comput. Sci. Telecommun.*, vol. 6, no. 8, pp. 12–18, Aug. 2015.

© 2024 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/