Anti-Phishing Technology: Using Multi-Factor Authentication (MFA) for preventing many credential-based attacks.

Dorado, Benjie Q.
Maharlika Magkapitbahayan,Bagumbong,Caloocan City
09568720898
doradobenjie@gmail.com

ABSTRACT

The purpose of this research is for us to be able to have knowledge of what is Multi-Factor Authencation is, how it works, and how it prevent many phishing attacks.

Keywords:*Phishing,Multi-Factor Authencation,ransomware attacks*

INTRODUCTION

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.[1]

The past twelve months has been not a revolution in the attackers' methods but an evolution, and 2020 is on target to see a 15% increase in phishing incidents compared with last year. This year we found that phishing incidents rose by a staggering 220% compared to the yearly average during the height of global pandemic fears. Fraudsters were quick to seize upon the confusion and we saw large spikes in phishing activities that closely coincide with various lockdown rules and the increase in homeworking. Using certificate transparency logs, we found that at its peak, there were almost 15,000 active certificates using "covid" or "coronavirus" in their names. On the topic of encryption, the use of HTTPS also rose sharply across all phishing sites with an impressive 72% making use of digital certificates and TLS encryption. The dramatic increase in phishing activity at the beginning of lockdown could well be a factor in the sharp rise of stolen payment cards discovered in May and June of this year. The number of cards of seven major global banks found on darknet markets was almost double a similar peak period in 2019.

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.[2]

The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.[3]

MFA works by requiring additional verification information (factors). One of the most common MFA factors that users encounter are one-time passwords (OTP). OTPs are those 4-8 digit codes that you often receive via email, SMS or some sort of mobile app. With OTPs a new code is generated periodically or each time an authentication request is submitted. The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could

simply be a counter that is incremented or a time value.[3]

When should I use MFA?

Stopping all online crime is not a realistic goal, but simple steps can massively reduce the likelihood you'll be the next victim.

You should use MFA whenever possible, especially when it comes to your most sensitive data—like your primary email, your financial accounts, and your health records. While some organizations require you to use MFA, many offer it as an extra option that you can enable—but you must take the initiative to turn it on. Furthermore, if a business you interact with regularly, say your health organization, wants to provide you with convenient online access to health records, test results, and invoices, but only offers a password as a way to protect that data, consider saying: 'no thanks, not until you provide MFA to secure my information.'

REVIEW OF RELATE LITERATURE AND STUDIES

The results obtained from the descriptive study revealed that when MFA is adopted the knowledge-based factor is usually chosen as the first factor to overcome the problem of 'sniffing password' when the authentication is performed (Erlich and Zviran, 2008). Thus, the proposed methods used in the experimental study used KBA as the first factor because it does not provide an adequate level of security. This finding parallels the results from Chapter 4 as all the banks investigated via the survey used KBA as the first factor when MFA was adopted.

Assessing Usable Security of Multifactor Authencation
By: Maha Mohammed Althoabaiti
SOURCE:
https://core.ac.uk/download/pdf/77028828.pdf

Multi-factor authentication improves online data security by implementing multiple factors in addition to single factor sign-on. Usability of such security technologies often comes across as a challenge for security practitioners, researchers, designers, and developers. Through systematic literature review (N = 623) we aimed at understanding the current trends of MFA research and studies. We analyzed the gaps in the existing literature for future user studies (n = 57) which can align with the risk perception of individuals. Our study reveals that there are identifiable trends in MFA studies that reveals a considerable amount of focus on new authentication technologies but lacks risk perception analysis. Additionally, we noted that cultural and demographic biases in user study designs. Many studies performed usability testing of existing or proposed new MFA (21 out of 57), however, a two of them discuss implementation and adoption of MFA in large scale organizations. Furthermore, the studies overall show recruitment bias to individuals who come from universities (Khan & Chefranov 2018). We provide actionable recommendations to pave future research scope, primarily aiming to include more diverse population for user study evaluations which can be effective for general adoption of MFA.

Evaluating User Perception of Multi-Factor Authentication A Systematic Review
By: S. Das, B. Wang, Z. Tingle, and L. Jean Camp
SOURCE:
https://arxiv.org/ftp/arxiv/papers/1908/1908.05901.pdf

REVIEW OF RELATED STUDIES

A very promising direction of the MFA development is therefore in the area of neural networks and Big Data . Here, many successful applications have been known to the community for more than a decade. Examples could be found in where conventional factors, such as iris, retina, fingerprints, etc., are considered. Utilizing neural networks for the next-generation biometrics is the most likely way to proceed due to presently high levels of the analysis complexity .
In summary, biometric technology is a prominent direction driven by the mobile device market. The number of smartphones to be sold only in the US is expected to reach 175 million units by 2018 with the corresponding market to exceed $50.6B in revenues by 2022 . It is believed that a strong push towards the utilization of biometrics in many areas of life is imminent, since most of the flagman devices are already equipped with the fingerprint scanner and facial recognition technology in addition to convention PIN codes.
This work provided a systematic overview of the state-of-the-art in both technical and usability issues, as well as the major challenges in currently available MFA systems. In this study, we discussed

the evolution of authentication from single- through two- and towards multi-factor systems. Primarily, we focused on the MFA factors constituting the state-of-the-art, future possible directions, respective challenges, and promising solutions. We also proposed an MFA solution based on the reversed Lagrange polynomial as an extension of Shamir's Secret Sharing scheme, which covers the cases of authenticating the user even if some of the factors are mismatched or absent. It also helps qualify the missing factors without disclosing the sensitive data to the verifier.

Multi-Factor Authentication: A Survey
Aleksandr Ometov , Sergey Bezzateev , Niko Mäkitalo , Sergey Andreev , Tommi Mikkonen and Yevgeni Koucheryavy

Department of Security of Cyberphysical Systems, ITMO University, St. Petersburg RU-197101, Russia; bsv@aanet.ru

Correspondence: aleksandr.ometov@tut.fi

Multi-Layered Security for Increased Protection and user Confidence Improving the overall security of consumer-facing services is vital to financial institutions , Nuclear and military facilities, transactions , banging , airplane and jetfighters . The risk of doing business with unauthorized or incorrectly identified persons in an Internet environment can result in financial loss and reputation damage. Online financial services customers need confidence that their financial institution is protecting confidential personal information and account access. Financial and business institutions therefore need to not only improve security, but bolster customer confidence in order to drive adoption of their online brokerage channel. multi-factor authentication and risk evaluation services that improve security without increasing complexity for users . Multi-factor Authentication & Security applications offer rapidly deployable options that can be configured to meet your most demanding online security needs. Our solutions are designed to ensure that users feel safe and secure every time. Through the use of secure, multi-factor user and transaction authentication able to monitor and enforce business rules to prevent fraud, protect privacy and support regulatory compliance. All above are the advantages of multi-factor-authentication
[4]Security of Multifactor Authentication Model to Improve Authentication Systems

Mrs. Tamara Saad Mohamed

Lecturer, Department of Computer Science Cihan university \ Sulaimaniah \

Iraq E-mail : tamara_ttt@yahoo.com

REFERENCE

[1] https://www.imperva.com/learn/application-security/phishing-attack-scams&

[2] https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

[3] https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

[4] https://www.researchgate.net/publication/322288752_Multi-Factor_Authentication_A_Survey/link/5a5366d1aca2725638c7fb9b/download

[5] https://core.ac.uk/download/pdf/234671705.pdf

Benjie Q. Dorado, He was born on December 02 1999 in Province of Roxas,Capiz. He Graduated on schools of Congress Elementary School, Sampaguita High School, Immaculate Mother Academy Inc.
Now, he is third year college at University of Caloocan City with the course of Bachelor Science in Information Technology.

He is good in solving puzzle and he like to play board games, He is knowledgeable in programming such as C, Java and Vb.net but he most focus on web development specially in backend programming. He polishing his skills by reading and studying document and software trends ,his end goal is to become database developer.