FINAL PROPOSAL DRAFT
Due on Tuesday, December 6 at 11:59 pm

TITLE OF THE PROJECT: Data breaches due to Multi-factor Authentication (MFA) attacks.

PROJECT PROPOSAL

ASHOK ADHIKARI

Department of Information Technology

Concordia University of Edmonton

aadhikar@student.concordia.ab.ca

ABSTRACT

- The problem that I plan to study is the Multi-factor Authentication (MFA) attack. Since mostly every company and individual does have multi-factor authentication set up for emails, devices, bank apps, and log-in to the system, people assume that they are secure. But with the rise in cyberattacks, there is a new kind of attack which targets users who use multifactor authentication. The attack is commonly known as MFA attack/fatigue. MFA attack/fatigue is a technique used by the cybercriminal to flood a user's authentication app with push notifications hoping that the user accepts, enabling the attackers to gain access to the account or device. People get bombarded with so many push notifications that make the user panic and accept the push notification allowing the hackers to gain access to user devices, emails, and banking info which leads to the invasion of privacy for the personal gain of cybercriminals. To protect the data/information from getting into the wrong hand, awareness about the MFA fatigue/attack seems to be important. Things that need to be considered to prevent the MFA are:
    - Limit must be set on the number of MFA push notifications that can be made before access is accepted into accounts.
    - Number matching security feature is another way to prevent the MFA attack by ensuring that a legitimate user requesting access. It is highly effective because the malicious third party who has compromised the user's credentials would need to contact the end user to ask them to input the numbers into their authenticator app.
    - Awareness Training regarding security must be provided because the attacker gains the access to passwords and data/accounts/apps via human errors. Attackers exploit the lack of awareness and human errors to get access.

Designing an app better than we have in the market like google authenticator, WebAuth, and Microsoft MFA number i.e., Verified Push is

what I think will help us prevent the MFA Attack. The apps that are currently in the market have flaws that will be addressed by the app that I am designing. The apps will have the following feature that current apps lack:

- Displays a series of numbers and wipes the serial number once the user logs into the system.
- Shorter time span to display the serial number.
- Auto update of the time zone, warning of the change in IP address and devices.

AUTHOR KEYWORD

- Phishing; Data breaches; Cybercriminals; Push Notification; Users/Victims.

INTRODUCTION

- The problem that I plan to study is the Multi-factor Authentication (MFA) attack. Since mostly every company and individual does have multi-factor authentication set up for emails, devices, bank apps, and log-in to the system, people assume that they are secure. But with the rise in cyberattacks, there is a new kind of attack which targets users who use multifactor authentication. The attack is commonly known as MFA attack/fatigue. MFA attack/fatigue is a technique used by the cybercriminal to flood a user's authentication app with push notifications hoping that the user accepts, enabling the attackers to gain access to the account or device. People get bombarded with so many push notifications that make the user panic and accept the push notification allowing the hackers to gain access to user devices, emails, and banking info which leads to the invasion of privacy for the personal gain of the cyber criminals. To protect the data/information from getting into the wrong hand, awareness about the MFA fatigue/attack seems to be important. Things that need to be considered to prevent the MFA are:

- Limit must be set on the number of MFA push notifications that can be made before access is accepted into accounts.
- Number matching security feature is another way to prevent the MFA attack by ensuring that a legitimate user requesting access. It is highly effective because the malicious third party who has compromised the user's credentials would need to contact the end user to ask them to input the numbers into their authenticator app.
- Awareness Training regarding security must be provided because the attacker gains the access to passwords and data/accounts/apps via human errors. Attackers exploit the lack of awareness and human errors to get access.

Research Questions

- What is an MFA attack?
- Why are user's seeing too many MFA attack?
- How can one protect themselves from the attack?
- Current solution in the market to address the problem of MFA attacks.
- Creating a better application to solve the problem.

BACKGROUND

Regarding the problem of the MFA attack, people have been made aware of the problem, informing users how to deal with the situation. Azura and office 365 are suggesting number matching MFA policy seems to address the problem.

My contribution to addressing the problem is making people aware of the MFA Fatigue attack, providing preventive measures, and informing people about an app like Google Authenticator, WebAuth, and Microsoft Number matching i.e., Verified

Push. which does not have push notifications while I work on designing the application.

METHOD

- **Data collection:**
  - Data about how people were affected, what measures were taken by the companies after they were targeted by the attacks, what software is used to prevent this kind of attack, solutions for big-scale industry, small-scale industry, and individuals as well.

  - I plan to collect the data by:
  - Peer reviews.
  - Online articles, news, and research papers.

- **Data Analysis:**
  - I will analyze each finding by examining the validity and correctness by checking it on multiple websites and talking with the professor and friends.
  - I will interpret all the findings in my own style so the readers can get clarity about the topic.
  - I will present all the analyzed and interpreted ideas in a good flow with graphs, visuals, and so on.

SIGNIFICANCE

- Helps the user to understand the MFA attack.
- Gives the knowledge of how to address the problem if it happens.
- Create awareness among the people who are still unknown of these kinds of attacks.

LIMITATIONS

- As this is a new kind of cyberattack, only limited information about this kind of attack is known.

- Time constraints cause the paper to limit the research to meet the deadline and implement the idea of developing the application.
- New solutions regarding attacks will not be covered.
- Limited number of resources accessed which might cause a bias.

TIMELINE

My plan for spring 2023 is to create software that will have better features than the software that is in the market like a google authenticator, Verified Push, and WebAuth. There are flaws in the software that are currently on the market so my idea to correct all the flaws and make better software to prevent the attack.

ACKNOWLEDGEMENT

I would like to thank my professor Apoorva Chauhan who supported and guided me throughout the process by teaching us how research is done, where and how to find the article related to the topic, and how the proposal should be written. I would also like to thank my reviewers who used their valuable time to read my paper and provide me with honest feedback. Thank you to everyone who supported me directly or indirectly. This paper would not have been successful without the guidance. Lastly, I would like to thank the university for providing me with the opportunity to write a research paper to help me learn more about the current problem that we are facing in the IT world.

REFERENCES

- Garrett, Keith. *VULNERABILILTY Analysis of Multi-Factor Authentication Protocols*. https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1698&context=etd.
- "Vulnerabilities in Multi-Factor Authentication." *Web Security Academy*, https://portswigger.net/web-security/authentication/multi-factor.
- Phan, Kim. *Implementing Resiliency of Adaptive Multi-Factor Authentication Systems*. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1095&context=msia_etds.

- Tolbert, Matt, et al. *Vulnerabilities of Multi-Factor Authentication in Modern Computer Networks*. https://digital.wpi.edu/downloads/2r36v157c.
- *A Case Study in Selection and Deployment of a Multi-Factor ...* https://www.researchgate.net/profile/Michael-Bumpus/publication/359078928_Issues_in_Information_Systems_A_case_study_in_selection_and_deployment_of_a_multi-factor_authentication_solution/links/6226bd723c53d31ba4b03276/Issues-in-Information-Systems-A-case-study-in-selection-and-deployment-of-a-multi-factor-authentication-solution.pdf.