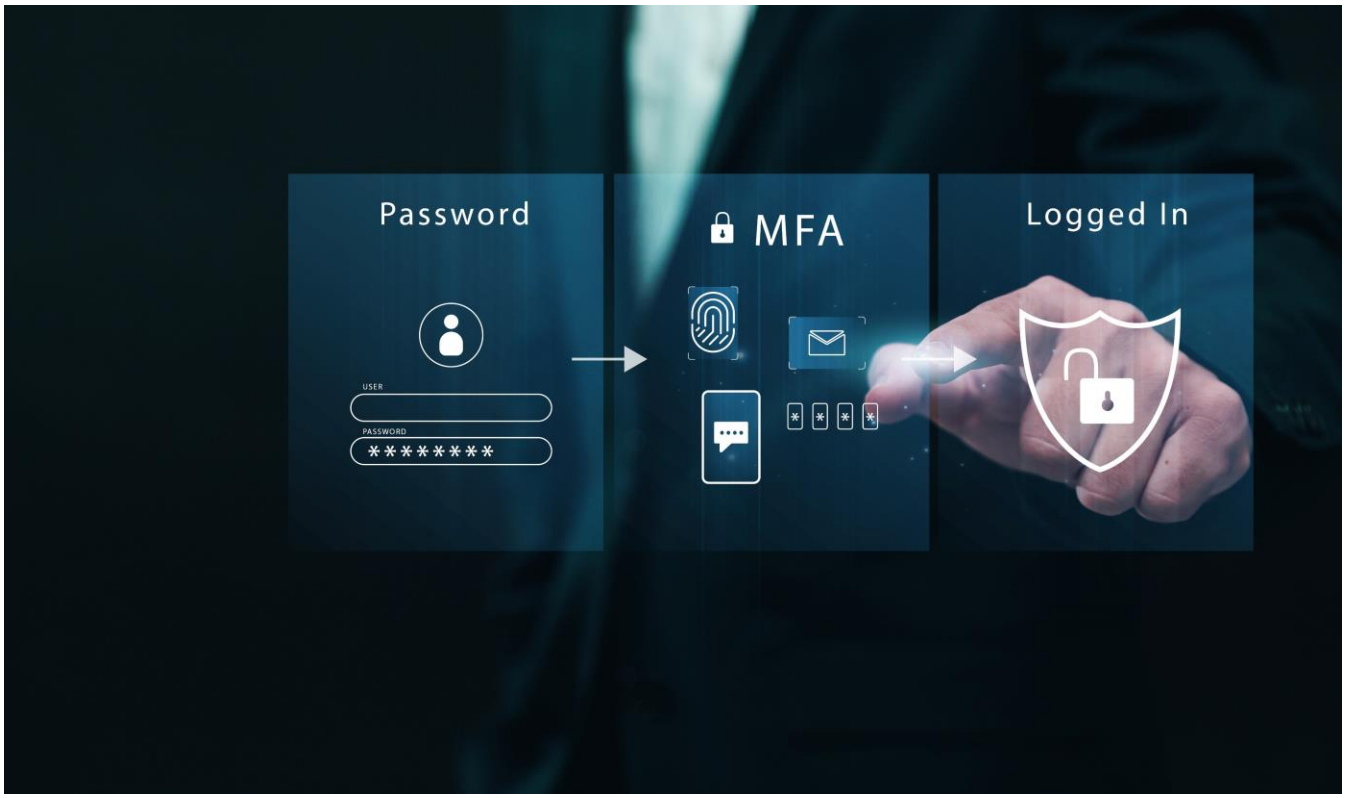
NPCore
New Paradigm Core

| 2024 NPCore Monthly Technical White Paper

The Limitations of Multi-Factor Authentication (MFA)



The Limitations of Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a crucial security measure that adds an extra layer of protection beyond traditional password-only methods. However, despite its benefits, MFA is not foolproof and can be vulnerable to certain attacks and exploits. This article explores the key limitations of MFA and the implications for security.

Phishing and Social Engineering

Phishing remains a significant threat to MFA security. Attackers use deceptive methods such as fake login pages or emails to trick users into revealing their MFA credentials. Even sophisticated MFA systems can be compromised if users are not vigilant. For example, an attacker may set up a phishing site that captures both the password and the MFA code, allowing them to bypass the intended security measures and gain unauthorized access.

SIM Swapping and SMS Vulnerabilities

SIM swapping is a technique where attackers transfer a victim's phone number to a new SIM card under their control. This allows them to intercept SMS-based MFA codes, which are commonly used as a second factor in two-factor authentication. The vulnerability of SMS for MFA has been highlighted in several high-profile attacks, emphasizing the risks associated with this method.

Man-in-the-Middle (MitM) Attacks

In MitM attacks, attackers intercept the communication between the user and the authentication system. They may set up a fake interface to capture MFA codes and credentials. Once they obtain the necessary information, they can access the system as the legitimate user. This type of attack can bypass MFA when codes are sent through insecure channels.

MFA Fatigue Attacks

MFA fatigue involves bombarding a user with numerous authentication prompts, often through push notifications. Attackers hope that the user will eventually approve one of these prompts out of frustration or confusion. This method was notably used in a breach of Uber's internal systems, demonstrating its effectiveness in certain scenarios.

Biometric Vulnerabilities

Biometric authentication, while generally secure, is not immune to exploitation. Techniques such as fingerprint replication, deepfakes, and other advanced methods can potentially bypass biometric systems. Additionally, biometric data, unlike passwords, cannot be reset if compromised, posing a significant long-term security risk.

Physical Security and Token Theft

Physical devices used for MFA, such as USB tokens or smart cards, can be stolen or lost. If an attacker gains physical access to these devices, they can potentially use them to bypass security measures. Moreover, malware on a user's device can capture authentication tokens or codes, further compromising security.

Weak Passwords and Account Security

MFA cannot fully mitigate the risks associated with weak passwords. If a password is compromised and the secondary factor is weak or flawed, attackers can still gain access. This underscores the importance of maintaining strong password practices in conjunction with MFA.

Configuration and Implementation Flaws

Improper implementation of MFA can introduce vulnerabilities. For example, if a system does not properly separate the authentication steps, attackers might bypass the second factor entirely. Additionally, not all MFA solutions are equally secure; for instance, email-based 2FA can be less secure if the associated email account is compromised.

Real-Life Cases of MFA Bypass and Attacks

Multi-Factor Authentication (MFA) is a widely adopted security measure that provides an extra layer of protection beyond simple passwords. However, even MFA is not foolproof, and there have been notable real-life cases where attackers successfully bypassed MFA using various techniques. Here are some examples:

1 MFA Fatigue Attacks

MFA fatigue attacks, also known as MFA push notification spam, involve bombarding a victim with repeated push notifications to approve a login attempt. Attackers exploit the victim's frustration or confusion, leading them to inadvertently approve the login request. A prominent case involved the Uber attack in 2022, where attackers used MFA fatigue to gain access to internal systems. This technique was also linked to the Lapsus$ group, which targeted companies like NVIDIA, Okta, and Microsoft.

2 SIM Swapping

SIM swapping is a method where attackers transfer a victim's phone number to a new SIM card under their control, allowing them to intercept SMS-based MFA codes. This technique was notably used in a case involving cryptocurrency theft, where fraudsters in San Antonio stole over $250,000 from victims' accounts. The perpetrators impersonated the victims by using their phone numbers to bypass MFA and access sensitive accounts.

3 Man-in-the-Middle (MitM) Attacks

MitM attacks, also known as Adversary-in-the-Middle attacks, involve intercepting the communication between a user and a legitimate service. Attackers use a malicious proxy to capture login credentials and session cookies, thereby bypassing MFA. This method is particularly effective when combined with phishing tactics, where the victim is tricked into entering their credentials on a fake login page. These attacks have been observed across various sectors, including government and corporate systems.

4 SIM Swapping Fraud in Korea

In Korea, a notable case of SIM swapping fraud involved a gang exploiting the identity of mobile phone users to gain unauthorized access to financial accounts. The scammers gathered personal information about their victims through phishing attacks or by purchasing the information from the dark web. Once they had sufficient data, they contacted the mobile carrier, impersonating the victim, and requested a SIM swap, transferring the victim's phone number to a new SIM card under the fraudster's control.

This unauthorized access allowed the scammers to intercept SMS-based two-factor authentication (2FA) codes and perform illegal transactions, such as transferring money from the victim's bank accounts or stealing cryptocurrency. The fraudsters exploited the mobile carrier's verification process, which sometimes lacked rigorous identity checks, allowing the scam to be executed smoothly.

These incidents highlight the vulnerabilities of relying on SMS-based 2FA for security. Even with strong passwords and additional security measures, the use of mobile numbers for authentication can still be compromised through SIM swapping. It's crucial for both users and service providers to adopt stronger security protocols, such as app-based authentication or hardware tokens, and to remain vigilant against potential social engineering attacks.

Mitigating MFA Bypass Risks

To mitigate these risks, organizations and users can adopt several best practices:

- Limit Push Notifications: Implementing rate limits on push notifications can reduce the effectiveness of MFA fatigue attacks.
- Switch to More Secure MFA Methods: Avoiding SMS-based MFA and adopting more secure methods such as hardware tokens or app-based authenticators can enhance security.
- User Education and Awareness: Training users to recognize phishing attempts and the importance of not approving unexpected MFA requests is crucial.

While MFA significantly enhances security, it is not a panacea. It is vital to implement MFA correctly, choose the most secure methods available, and educate users about potential threats. Combining MFA with other security measures, such as digital certificates and strong password policies, can further strengthen an organization's defenses.

Understanding the limitations of MFA helps in making informed decisions about security strategies and ensures that organizations do not rely solely on MFA but integrate it as part of a comprehensive security framework.

Conclusion

While MFA significantly enhances security by adding additional layers of protection, it is not a comprehensive solution. It is crucial to implement MFA correctly, select the most secure methods, and educate users about potential threats. Complementing MFA with other security measures, such as digital certificates and robust password policies, can further strengthen an organization's defense against unauthorized access.

Understanding the limitations of MFA helps organizations make informed decisions about their security strategies and ensures that MFA is integrated as part of a broader, more comprehensive security framework.

Therefore, Aircuve's V-FRONT v7 can be used to control the safe access of in-house employees when accessing the internal business network within the enterprise, and to support complete AAA radius security and encryption of transmitted data for the connected network. In other words, it is a user authentication enhancement solution that can easily build MFA(multiple factor authentication) such as SMS, E-mail, mobile OTP, HW Token (Card Type), QR Code, App push, YubiKey, Fingerprint, Facial recognition, etc.

NPCore
New Paradigm Core

T. +82-2-1544-5317
M. marketing@npcore.com
Geumgang Penterium IT Tower 701, 171,
Dangsan-ro, Yeongdeungpo-gu, Seoul, R.Korea, 07217