International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 08 | Aug - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Strengthening Security: Implementation of Multi-Factor Authentication (MFA) in Data Center Environment

Vijaya Saradhi Nanduri[1]

Solution Architect, DXC Technology
Building # 4, Mindspace IT Park,
Madhapur, Hyderabad, Telangana 500081, India
Email: vnanduri@dxc.com

Executive Summary - Today's digital landscape needs robust security measures to safeguard sensitive information and maintain trust with users. Multi-Factor Authentication (MFA) stands as a critical technology in this journey, by offering an additional layer of defense beyond the traditional single-layer security.

This white paper explores what is MFA, MFA Architecture, MFA Methods, Benefits of using MFA, current MFA Market providers and future trends. It outlines how MFA addresses the vulnerabilities of single-factor authentication by requiring users to verify their identity through multiple independent credentials. These factors typically include something the user knows (like a password), something they have (such as a smartphone or hardware token), and something they are (like biometric data).

This white paper addresses key aspects of MFA as mentioned below:

- **Enhanced Security** - MFA significantly reduces the risk of unauthorized access, protecting against common threats such as phishing, credential theft, and brute-force attacks.
- **User Experience** - The MFA solution can be designed to streamline user interactions while maintaining security standards.

Compliance requirements - Industries mandate the use of MFA to comply with data protection regulations. Implementing MFA ensures adherence to legal requirements..

Key Words: Authentication, Multi-Factor Authentication, security journals

1. INTRODUCTION

Business improvement leads to growth in sensitive data and essential to invest in data security systems. Traditional passwords to secure the data are not enough anymore. Hackers have developed multiple tools and methods like spear-phishing and pharming to steal and gain unauthorized access to private accounts. Organizations need an effective and cost-efficient way to address identity theft exploitation.

Traditional password authentication to check email, bank accounts, and other services are considered a single-factor authentication. Authentication happens using what you know, what you have, and what you are. There are multiple categories of authentication factors: Knowledge, Possession, Inherence, and Location. Modern knowledge factors include identification, passwords, PINs, and answers to security questions. ID cards, security tokens, one-time passwords (OTP), and smartphones are considerable possession factors. Biometric authentication including scanning fingerprints, facial and voice recognition, and retina scans are considered part of Inherence factors. Users' physical location at the time of authentication using a physical IP address is considered a location factor.

Single-factor authentication has multiple limitations like forgetting passwords, being easily stolen, and being easily hacked. Hence, it is required to adopt two-factor authentication in short 2FA is a subset of multi-factor authentication in simple it is MFA.

Multi-Factor Authentication (MFA) is the method this document focuses on and provides guidance on what MFA is, MFA architecture, various methods of MFA, benefits of MFA, and various MFA market providers.

2. Multi-Factor Authentication Definition

MFA is defined as a method of authentication that uses two or more authentication factors to authenticate a single user to a single verifier. It is the technique for the end user to prove the identity by providing at least two factors.

The factor that makes MFA authentication comes from two or more of the following.

a. Something the end-user knows
b. Something the end-user has
c. Something the end-user is

Here, the end user may be a person, a device, a service, an application, or any other source that can authenticate into the system.

Authentication verification is by the verifier and a single authentication policy is enforced.

MFA involves using passcodes in addition to one or more of the following MFA methods.

a. Biometrics
b. Physical tokens (One-time PIN)
c. Smartcards
d. Mobile applications
e. Software certificates
f. Voice calls, SMS messages, email verification

3. MFA ARCHITECTURE

Multi-Factor Authentication is mainly built on four pillars, such as Requester, first-factor authentication, second-factor authentication and accessing the resource. The requester requests first and second-factor authentication to authenticate the use of the resource. Once the first and second-factor authentication are passed the Requester can access the resource.

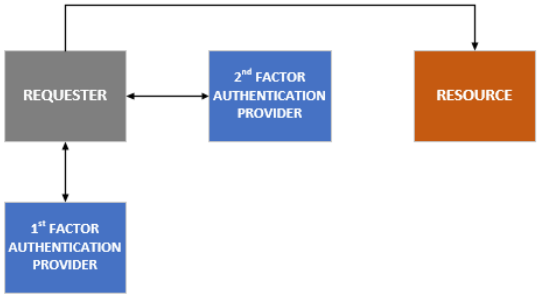

Figure 1: Four Pillers of MFA

Multiple solution components support this solution to operate around these four pillars. The requester uses an authentication method that is internal to the organization and passes through the first-factor authentication. Once the 1st factor is successful and the requester is enabled can use multiple tools and methods to work with the second-factor authentication.

Second-factor authentication is generally through the 3rd party security providers which prefer to use multiple MFA methods. Once 2nd-factor authentication is also successful then the requester can use the resource.

Following is the stepwise verification and network path that the authentication requests pass through multiple solution components.

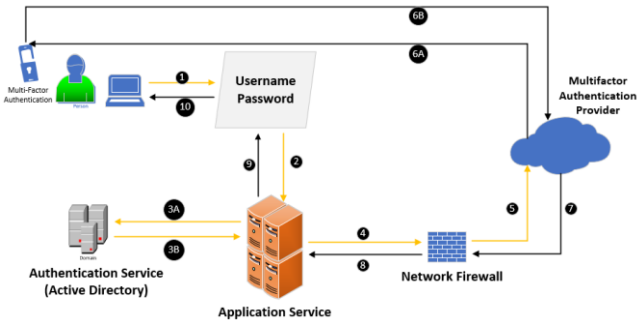

Figure 2: MFA Stepwise Verification

Point 1: Requester (User) initiates resource access by providing the username and passcode.

Point 2: This username and passcode are passed to the application service and the application service should verify these details with internal authentication.

Points 3A and 3B: The details passed on by the application service to the authentication service are verified by the authentication service. Once the details are verified, then the token will be generated by the authentication service and then passed to the application services to allow the requester.

This is the first-factor authentication verification that is completed at this stage. If the requester is enabled with multi-factor authentication, then the verification request needs to be passed on through the corresponding MFA provider.

Point 4: The application service passes the second-factor verification to the MFA provider through the network firewalls.

Point 5: After the necessary firewall port allows the IP traffic, the verification request reaches the MFA provider.

Point 6: The MFA provider receives the verification request and passes the verification confirmation to one of the verification methods. The verification method shown in the figure is the PIN push confirmation to the mobile application. The requester verifies the mobile application for the PIN and once allowed, the request confirmation issues the MFA provider to deliver the PIN for the authentication process.

Point 7: The MFA provider passes the verification request to the network firewalls

Point 8: Once the request is allowed through the required ports at the network firewalls, the request passes to the corresponding application service.

Points 9 and 10: The application service allows the requester to use the resource.

4. MFA METHODS

The following are methods used in implementing Multi-Factor Authentication (MFA).

- Biometrics
- Physical Tokens
- Smartcards
- Mobile Applications
- Software Certificates
- Voice calls, SMS, and Email verification

4.1. BIOMETRICS

Biometrics is one of the reliable MFA methods_that uses fingerprints, voice recognition, and iris scan as a second factor. In the beginning, the user must enroll in the authentication service to provide an appropriate biometric scan as a reference to compare. At the time of authentication, the end user provides a passcode to authenticate along with the biometric scan, so that the authentication verifier verifies the provided passcode and biometric data, and grants access to the requested resource.

However, there are multiple security potential vulnerabilities in this MFA method caused by compromised end-user device biometric capture software which replays legitimate authentication requests or initiates fraud authentication requests on the user's behalf. This method's effectiveness depends on the biometric reader and the software to detect false negatives and positives.

4.2. PHYSICAL TOKENS

Physical tokens are also called Physical one-time PIN (OTP) tokens which is one of the other known MFA methods. A physical token displays an OTP on the screen which the user uses as an MFA to authenticate into the service. The time synchronization between the Physical token and the authentication service is synchronized and the service knows the OTP generated by the physical token at a given point in time. When the user uses passcode and OTP to authenticate into the service, then the service verifies the details and grants access to the service.

There should be security hardening, and a few tips must be followed by the end users on the usage of the physical tokens. Users must ensure not to store the physical tokens with their devices and apply specific hardening methods suggested by the vendors. Physical tokens have an expiry time as per the enterprise security guidelines. The main threat of having the physical token with the end users is its serial number. If end users lose the physical tokens, then it must be reported to the concerned security support staff to block the physical token for usage.

4.3. SMART CARDS

Smartcards store a unique private key that will be used by end-user device software while authenticating into the service. The software on the user's device prompts to unlock the smart card using a PIN(Password). Once the smartcard unlocks, the software on the end user device verifies user authentication along with the private key. Once the authentication service verifies the successful authentication and allows the resource service to be used by the end user.

Like biometric authentication, smartcard MFA also has a few security vulnerabilities due to the software on the end user device interacting with the smartcard. If the end-user device is compromised, then hackers can easily intercept the device and initiate fraud authentication requests on behalf of the end user.

To avoid potential threats on the end user devices, users must ensure to harden the devices, and not store smartcards with the devices. Even it is required to notify the user via SMS or any other visual confirmation on each authentication attempt using smartcards. Users must ensure not to leave the smartcards inserted into the device and even report to the security team the loss of the card.

4.4. MOBILE APPLICATIONS

The mobile application provides a time-bounded PIN or password which can be used as a second-factor authentication. The user registers into the provider site using a mobile number or email address or scans a QR code. Once the mobile application is installed on the mobile device, it provides a PIN/Password which can be used at the time of user authentication. During the user login process, users provide the time-bound PIN/Password generated by the mobile application to the authentication service. The authentication service verifies all the provided details and allows the user to use the service.

The advantage of this method is minimizing the cost due to the user already having the authentication factor. Still, there are disadvantages to using this method.

If the mobile device is used for other web browsing and email reading activity, then the mobile device is no longer secure. Specific device hardening makes the mobile device secure and can be utilized for this multi-factor authentication. The device theft and remote wiping must be enabled on the mobile devices which ensures the device is secure.

4.5. SOFTWARE CERTIFICATES

This method uses a software certificate which is stored in the end-user device as a file. Once the user initiates the logon process, the system accesses the software certificate file in the registry or the Trusted Platform Module (TPM) of the device. The software assists the user to enter the credentials for verification and authenticates using the user's private key. Then the authentication service verifies the request is signed by the valid private key and then grants access to the resource service.

The security vulnerability of this authentication method is the usage of the software on the user's device and the device has the operating system. If the end-user device is compromised, then the authentication services are compromised. There is one more risk associated with this type of method which is the elevated privileges gained by the adversary. Hence it is advised that organizations use this type of authentication method only for low-risk systems.

To ensure maximum security by this authentication method, it is required to harden the end-user device, visual notification of each time the authentication request generates a PIN, store the certificate in the proper certificate stored in the device and report to the security team for any device loss.

4.6. VOICE CALLS, SMS MESSAGES, EMAIL VERIFICATION

This method uses a time-bound OTP provided via voice calls, SMS messages, or email verification to a device. At the time of user registration, the user is required to provide a phone number or email address so that the PIN can be provided to register. During the logon process, the user requests the authentication service provide OTP to complete the authentication process. The OTP will be delivered to the user's device using SMS messages, email verification, or Voice calls.

The disadvantage of this authentication method is depending on the user's location and the mobile network provider coverage so the PIN delivery will be affected.

The end-user device can be compromised as the end users' web browsing and email checks on the device are allowed.

Hardening the device and specific time limit on the generated OTP provides security to the authentication method. The user must report to the local security team about the device loss.

5. MFA BENEFITS

The following are the benefits of Multi-Factor Authentication (MFA) implementation.

- Increases security while working with third-party Organizations.
- Controls the access that who can access the internal Organization files.
- Helps to meet security and regulatory requirements.
- Offers a wider variety of methods to meet security needs.
- Compatible with Single Sign-On.
- Adaptable for various enterprise user authentication Use Cases.
- Reduces Fraud and Identity theft.
- Increases customer trust and simplifies the login process.
- Adds a level of security and can operate remotely.

6. MFA MARKET PROVIDERS

There are multiple user Authentication and Access Management platforms available, as mentioned below.

Name of the Platform	MFA	Single Sign-On	Configurable Access Policy	Authentication App	Phone Centric Identity
HID Advanced MFA	Y	Y	Y	Y	N
OKTA MFA	Y	Y	N	Y	N
Prove MFA	Y	N	N	Y	Y
PingIdentity	Y	Y	Y	Y	N
Entrust Identity Guard	Y	Y	Y	Y	N
SecureAuth Identity	Y	Y	Y	Y	N
Thales Safenet	Y	Y	Y	Y	N
Typing DNA	Y	Y	Y	Y	N
ESET Secure Auth	Y	Y	Y	Y	N
DUO ACCESS	Y	Y	Y	Y	N
Authy	Y	Y	Y	Y	N
One Identity	Y	Y	Y	Y	N
LastPass	Y	Y	Y	Y	N
Symantec VIP	Y	Y	Y	Y	N
AuthO	Y	Y	Y	Y	N

Table 1: MFA MARKET PROVIDERS

6.1. FUTURE TRENDS

The future trends in multi-factor authentication (MFA) are dependent on technological advancement, new security threats, and enhanced user experience. The following are some of the emerging trends.

- AI and ML: AI-driven user behavior solutions analyze user behavior patterns. This detects anomalous activities and security threats. The user interactions with the systems and applications are monitored by the AI system which triggers alarms if any identified deviations from normal behavior. Predictive authentication will be triggered based on user authentication historical data.
- Blockchain for Authentication: Each user will be issued with a Decentralized Identifier (DID) for authentication. Each DID will have a private key. Each person will have multiple DIDs. This limits the extent to which the DID can be tracked across multiple activities. The credentials are associated with the DIDs. These DIDs are secured by using cryptography. The access will be granted to services if the match happens between the user-presented identifier in the form of QR code attestation and the service provider

checks the attestation which is associated with the DID having a private key.

- Multi-modal authentication: To enhance security, integrate different types of authentication factors such as biometric authentication, possession-based authentication, and Knowledge-based authentication.
- Biometric authentication advancements: Enhance security by utilizing unique patterns in user behavior such as mouse movements and typing rhythm for authentication. The user behavior will be monitored in real-time and prompt for re-authentication in case any anomalies are detected.
- Integrating with Public Cloud Security Systems**:** Seamless integration of MFA with the public cloud-provided security methods such as IAM (Identity and Access Management). This integration provides centralized control over the Identity and access and will have complete visibility. This also facilitates zero trust architecture which verifies every access request regardless of location and device.

7.0. CONCLUSIONS

Multi-Factor Authentication (MFA) stands as a critical tool in implementing cybersecurity strategies, which extends protection against unauthorized access and mitigates risks associated with compromised credentials. MFA creates multiple layers of defense through the integration of multiple authentication factors—typically something you know, something you have, and something you are.

Throughout this white paper, we have explored various aspects of MFA, including its effectiveness in common attack vectors such as phishing, credential stuffing, and brute-force attacks. By requiring users to present at least two different types of credentials, MFA introduces complexity that makes it exponentially more difficult for malicious sources to gain unauthorized access.

While MFA offers robust security benefits, its successful deployment provides seamless integration with organizational workflows and user acceptance. Looking ahead, the landscape of cybersecurity continues to evolve, with new threats constantly emerging. The adoption of MFA should be viewed as a foundational element of a broader cybersecurity strategy rather than a solution. Organizations must remain vigilant, continually updating their MFA policies and technologies to stay ahead of evolving threats and compliance requirements.

While no single security measure can guarantee complete protection, multi-factor authentication represents a significant advancement in securing digital identities and sensitive information. By leveraging the combination of multiple authentication factors, organizations can enhance their resilience against cyber threats and safeguard the trust of their stakeholders.

8.0. REFERENCES

The following are the articles referred to prepare this white paper.

- Types of Multi-Factor Authentication.

https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/

- What is Multi-Factor Authentication

https://www.loginradius.com/blog/identity/what-is-multi-factor-authentication/

- What are the 3 types of Multi-Factor Authentication

https://expertinsights.com/insights/what-are-the-3-types-of-multi-factor-authentication/

- Future Trends in Multi-Factor Authentication: What to expect

https://www.oloid.ai/blog/future-trends-in-multi-factor-authentication/