16.7. Multi-Factor Authentication

Objective

16.7.1. Multi-Factor Authentication (MFA) mechanisms are adequately implemented to enhance and maintain security.

Context

Scope

16.7.2. This section provides information and guidance on the establishment and operation of MFA. It is a critical component of Identity and Access Management (IAM).

16.7.3. Reference to other chapters and sections in this document is essential. In particular:

- Chapter 7 – Information Security Incidents;
- Section 9.1 – Information Security Awareness and Training;
- Section 16.1 – Identification, Authentication and Authorisation;
- Section 16.2 – System Access;
- Section 16.3 – Privileged User Access;
- Section 16.4 – Privileged Access Management; and
- Chapter 17 - Cryptography.

Background

16.7.4. Authentication is a key element of security that provides confirmation of a returning user to a system when making a transaction. In this context a transaction may include browsing, financial operations, and all types of data access, creation, copying and deletion.

16.7.5. MFA is a security system that verifies a returning user by requiring multiple credentials, which are typically in the form of another factor or type. Initial authentication often requires a username and password followed by a requirement for other (additional) credentials. MFA can enable, for example, valid users' access to permit credential reset, even if they are using a username and password that may have been compromised.

16.7.6. Through adequate implementation, MFA can be a strong defence and deterrent against many credential attacks, including brute-force, credential stuffing, and password spraying attacks. It is also an additional defence against many social engineering attacks seeking user credentials.

16.7.7. MFA requires two or more authentication factors (from a single entity) before authorising system access. MFA requires two elements from any of the three categories of authentication and with the second factor from a different group to the first factor selected.

These factors or groups are:

1. **The possession/ownership factor** - Something you have, preferably NOT the device itself but a SEPARATE authentication device such as a token, RFID card or smartcard;
2. **The knowledge factor** - Something you know such as a passcode, One-Time password (OTP), reusable password, pattern or other component of a standard authentication mechanism;
3. **The inherence factor** - Something you are, biological or behavioural characteristics of various types.

16.7.8. Using MFA increases attack resistance by increasing the difficulty of obtaining all necessary authenticators. It is important to note, however, that the strength of an MFA solution is contingent on how robust any of the authentication factors are.

16.7.9. It is important to use a variety of factors to strengthen attack resistance in order to increase confidence levels in the chosen authentication system. For example, using two factors from the knowledge group is not considered 2FA and is less effective than using factors from two different groups. The knowledge group is the most exposed to attack and compromise through social engineering.

16.7.10. Additional authentication also assists in managing Privileged Access (refer to Section 16.4 – Privileged Access Management).

Phishing resistant MFA

16.7.11. Although the use of MFA provides improved levels of security than the traditional single-factor authentication, it is imperative to recognise that not

all methods provide adequate protection against all attacks.

16.7.12. The majority of credential stealing is obtained through phishing attacks and adversary in the middle attacks (AiTM). Some traditional MFA is vulnerable to interception or AiTM attacks, where an access token is stolen that contains the MFA claim and can be replayed by the attacker. These types of traditional MFA do not provide the adequate security to mitigate against many advanced phishing attacks.

16.7.13. Phishing resistant MFA are types of authentication methods that are designed to mitigate these phishing attacks found in some traditional MFA approaches.

16.7.14. Phishing resistant MFA are methods where attackers cannot replay the stolen access token or manipulate the authentication process. This includes mitigating against social engineering attacks, phishing attacks, and AiTM attacks.

16.7.15. Phishing resistant MFA relies on cryptographic keys which eliminate the risk of interception and phishing attacks. Methods include:

1. FIDO2/WebAuthn.
2. Smartcards.
3. PKI-Based Authentication.

16.7.16. Due to the reliance on cryptographic keys, this typically can involve additional infrastructure and can add additional time and cost to implement across organisations.

16.7.17. Agencies need to understand what systems and data needs to be protected. Not all entities or transactions may need to implement phishing resistant MFA, however it is essential to consider implementing phishing resistant MFA to sensitive information, where entities have elevated privileges within organisations, and consider adding phishing resistant MFA to PAM policies.

16.7.18. **Traditional MFA with known vulnerabilities**

Some methods of MFA are known to be susceptible to phishing threats. Methods, such as SMS based one-time passwords (OTP), email and application-based OTPs have well documented vulnerabilities that can be exploited, particularly through phishing and AiTM attacks.

16.7.19. SMS have several known vulnerabilities which may make it unsuitable and unsafe for authentication purposes; these include:

1. SIM swapping attacks.
2. AiTM attacks.

16.7.20. **Email** based OTPs are vulnerable to email account compromises. If an attacker gains access to email accounts they can intercept OTPs via email.

Adaptive Authentication

16.7.21. **Adaptive Authentication** is a form of MFA which varies the level or degree of authentication required where an unusual authentication request occurs. For example, out of normal hours, from an unusual geolocation, from an unrecognised device, from an unrecognised IP address and so on. When an unusual authentication request is received, Adaptive Authentication may request additional authenticators such as an MFA token. Some **risk factors** that may trigger Adaptive Authentication include:

- The location of the access request such as such as a café, airport or home;
- The time of the access request such as like late at night, over weekends or during normal working hours;
- The type of device, such as a smartphone, tablet, laptop, or unrecognised device;
- The type of connection, for example, a public network such as the internet, or a VPN or some other private network; and
- A request for access to privileged accounts.

16.7.22. Adaptive Authentication includes what is sometimes described as transaction identification where known characteristics are compared to the transaction or access request, for example, a known location or common access request. If known characteristics do not match then additional authentication steps may be indicated or required.

Client-Side Authentication

16.7.23. Client-side authentication originates from the user's device such as laptop, mobile phone, tablet, or home computer. These devices may provide a variety of authentication methods including:

- Inherence factor/Biometric:
    - Fingerprint scans;
    - Facial recognition;
    - Voice command/recognition;
    - Iris scans;
    - Keystroke dynamics;

- Knowledge factor:
    - PIN codes;
    - Pattern codes;

- Possession factor:
    - Geofencing;
    - Bluetooth device proximity/Near field communication (NFC).

16.7.24. It is important to note that some biometric and other measures, for example fingerprints, are susceptible to attacks such as spoofing. To combat these biometric attacks secondary measures are also required, for example pulse-sensing in addition to fingerprint detection in order to ensure the fingerprint presentation is a live person. Clearly not all secondary measures are fully effective by themselves and multiple secondary measures may be required for high risk/high value authorisation requests. FIPS-140 provides guidance to organisations to confirm which hardware meets secure standards.

Single-User and Multi-User Authorisation

16.7.25. **Single-User authorisation** involves prompting the account holder to authorise an action being taken on his behalf. For example, single-user authorisation can even prevent fraud as it occurs in a user-friendly manner. Instead of calling the customer to verify the legitimacy of a purchase, credit card companies could request customer authentication for an on-line purchase by sending an authorisation request to the customer through an alternate channel such as a mobile phone.

16.7.26. **Multi-User authorisation** usually requires multiple and separate authentications (usually by other people) in order to authorise a transaction or event, such as establishing an account. This system supports the "separation of duties" concept common in accounting transactions or other high-risk activities. Multi-user authorisation may also assess risk indicators and context (e.g. time, location) to select the authentication components and requirements.

Multi-Step Authentication

16.7.27. **Multi-step Authentication** is a design and architectural approach to control access to resources by sequentially using multiple authentication verifiers. Each authentication step grants access to increasingly privileged areas of the system until access to the desired resources is reached (refer also to 16.4 – Privileged Access Management). Multi-Step Authentication can be activated by risk-based "triggers" where risk factors are identified.

16.7.28. **Multi-step Authentication** may require only one authentication factor or mechanism, so it is important not to confuse Multi-Step Authentication with Multi-Factor Authentication. Multi-Step Authentication may not be as secure as MFA and cannot be an appropriate substitute for MFA. A key risk is repeated use of a single authentication factor.

16.7.29. It is also worth noting, however, that Multi-Step combined with Multi-Factor Authentication is a strong architectural security construct, particularly when a multi-factor request is triggered for accessing a privileged account.

Perfect Forward Secrecy

16.7.30. In addition to the encryption protocols and algorithms discussed in Chapter 17 - Cryptography, the concept of **Perfect Forward Secrecy (PFS)**, often simplified to Forward Secrecy, should also be incorporated into any authentication mechanism design.

16.7.31. **Forward Secrecy** is a property of secure communication protocols that is intended to prevent a compromised encryption key from being used to decrypt previously encrypted traffic. Clearly a compromised key must be immediately replaced in order to maintain the integrity of communications. This mechanism is described as a **"rolling secrets"** technique and is designed to prevent device spoofing and the cloning of mobile clients.

16.7.32. A **"rolling secret"** key is located on the client device. The client receives two encrypted packages. The first contains another private key and is decrypted by the current private key held on the client device. The new key is used to decrypt the second package and the new private key replaces the existing private key, which is then discarded. The new key is used to encrypt traffic to the authentication server. With each cycle the client replaces the old key with the new key.

Cryptography

16.7.33. The use of encryption is a fundamental component in the security of a Multi-Factor Authentication mechanism. It is essential that only approved cryptographic protocols and algorithms are used, refer to Chapter 17 – Cryptography.

Risk Analysis

16.7.34. The design of Multi-Factor Authentication should start with a risk review in order to identify any existing and new risks from changing environments, user populations and threat landscapes. Some early steps will include:

- Review business drivers, existing identity infrastructure, enterprise applications, core platform infrastructure and development plans for each of these;

- Ensure any plans for cloud and related services are reviewed and incorporated;
- Identify authentication use cases including employees and contractors, consumers, customers, partners, and suppliers. For Digital Government this may also include the General Public for some systems;
- Develop baseline requirements;
- Undertake a threat analysis for each use case; and

Select control mechanisms to manage identified risks.

16.7.35. This risk analysis will inform and direct the development of an authentication architecture to provide robust but usable security for each use case. Some key questions include:

- How will users access the system or application?
- At what stages will users be authenticated?
- What authentication factors will provide the appropriate level of authentication and security?
- Is the level of authentication appropriate to secure and protect the systems, data and other related assets? and
- Is there sufficient capacity to service anticipated workloads?

16.7.36. MFA is an additional way of managing access to systems and data. MFA will only provide additional layers of managing access to systems provided the fundamentals of Identification and Access Management are met. This includes:

- Implementation of least privileged principles.
- Access is removed when not required.
- Administration privileges are limited to only users who require these privileges.
- Enforcing strong passwords through password policies (when passwords are in use).

Governance and Control

16.7.37. Good governance processes assist in identifying potential risks to your systems, data, employees, partners and contractors. This reduces the risk of a breach or failure to comply with legislation and regulation. Good governance processes support the fulfilment of duties of senior and executive management.

16.7.38. Technology governance must demonstrate effective control, security, effectiveness and clear accountability. Identity Access Management and Authentication are fundamental components in protecting agency systems, data and technology assets and underpinning technology governance structures.

16.7.39. There are also several national and international legislative and regulatory requirements and accepted international standards which may influence aspects of governance, particularly in relation to data protection and privacy. While not an exhaustive list, these include:

- New Zealand's Privacy Act;
- New Zealand's Public Records Act;
- The EU's General Data Protection Regulation (GDPR);
- ISO/IEC 27701

References

16.7.40. Additional information relating to event logging is contained in:

Title	Publisher	Source
Identification Standards	NZ Govt	Identification Management Standards | NZ Digital government
ISO/IEC 27001	ISO/IEC/ Standards NZ	ISO - International Organization for Standardization
NIST Digital Identity Guidelines	NIST	NIST Special Publication 800-63 Digital Identity Guidelines | NIST
OAuth 2.0	IETF OAuth Working Group	OAuth 2.0 — OAuth
Cloud security guidance - Identity and authentication	NCSC UK	Principle 10: Identity and authentication - NCSC.GOV.UK
FIDO Specifications Overview	FIDO Alliance	User Authentication Specifications Overview - FIDO Alliance
Microsoft Entra ID - Multi-Factor Authentication	Microsoft	Microsoft Entra multifactor authentication overview - Microsoft Entra ID | Microsoft Learn
Multifactor Authentication Cheat Sheet	OWASP	Multifactor Authentication - OWASP Cheat Sheet Series
Implementing Phishing Resistant MFA	CISA	Implementing Phishing-Resistant MFA

Rationale & Controls

Risk Analysis

16.7.41.R.01. **Rationale**

The requirement for an agency information security policy is discussed and described in Chapter 5 – Information Security Documentation. An essential part of any security policy is the assessment of risk and the inclusion of requirements for securing access to systems, applications and data.

16.7.41.R.02. **Rationale**

A risk analysis is fundamental to the design, implementation and maintenance of Multi-Factor Authentication (MFA) processes and will inform and direct the development of requirements and an authentication architecture to provide robust but usable security.

16.7.41.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6948]

Agencies MUST undertake a risk analysis before designing and implementing MFA.

System Architecture and Security Controls

16.7.42.R.01. **Rationale**

Security controls should support security while enabling authorised user access. The system architecture should be sufficiently comprehensive to support this objective.

16.7.42.R.02. **Rationale**

External facing systems and authenticating to third-party services exposes additional risk to the organisation. MFA provides an additional layer to help an organisation manage risk of systems compromise through authentication attacks.

16.7.42.R.03. **Rationale**

While phishing-resistant MFA methods, such as hardware security keys or biometric authentication, offer stronger protection (compared to non-phishing-resistant MFA), some of these methods may not always be feasible for all users of systems. Therefore, while we strongly encourage the

adoption of phishing resistant MFA wherever possible, any form of MFA is considered an improvement over relying solely on passwords.

16.7.42.R.04. **Rationale**

Where devices or systems do not support MFA, organisations are encouraged to implement appropriate compensating controls. These measures can help mitigate the risks associated with relying solely on passwords.

16.7.42.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7563]

Where an agency has external facing systems, cloud-based services, or is authenticating to third-party services services, they MUST:

- require MFA for all user accounts; and
- implement a secure, multi-factor process to allow entities to reset their standard user credentials.

16.7.42.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6953]

Where an agency has implemented MFA they MUST:

- require MFA for administrative or other high privileged users; and
- implement a secure, multi-factor process to allow entities to reset their standard user credentials.

16.7.42.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7564]

Agencies MUST implement MFA on all user accounts with **remote** access to organisational resources.

16.7.42.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7565]

Agencies SHOULD implement MFA on all user accounts with access to organisational resources.

16.7.42.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7566]

Where agencies have implemented MFA, they SHOULD implement phishing-resistant MFA on administration accounts.

16.7.42.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7567]

Agencies SHOULD use phishing-resistant MFA when authenticating users to systems.

16.7.42.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:6952]

The design of an agency MFA SHOULD include consideration of:

- Risk identification;
- Level of security and access control appropriate for each aspect of an organisation's information systems (data, devices, equipment, storage, cloud, etc.)
- A formal authorisation process for user system access and entitlements;
- Logging, monitoring and reporting of activity;
- Review of logs for orphaned accounts and inappropriate user access including unsuccessful authentication;
- Identification of error and anomalies which may indicate inappropriate or malicious activity;
- Incident response;
- Remediation of errors;
- Suspension and/or revocation of access rights where policy violations occur;
- Capacity planning.

Integration with Policy

16.7.43.R.01. **Rationale**

The requirement for an agency information security policy is discussed and described in Chapter 5 – Information Security Documentation. Privileged Access Management policy is discussed in Section 16.4 - Privileged Access Management.

16.7.43.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:6956]

The design of an organisations MFA system SHOULD be integrated with the agency's Information Security Policy, the agency's Privileged Access Management (PAM) Policy, and any additional agency password policies.

User Training

16.7.44.R.01. **Rationale**

It is important that users understand and have continued awareness of risks and threats to authentication credentials, in order to maintain the integrity of the credentials and to maintain the security of the systems being accessed.

16.7.44.R.02. **Rationale**

MFA introduces some complexity and may require the use of specific devices, hardware or applications. Training is essential to increase user awareness and maintain adequate security practices.

16.7.44.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:6960]**

When agencies' implement MFA they MUST ensure users have an understanding of the risks, and include appropriate usage and safeguards for MFA in the organisation's user training and awareness programmes.