TRENDING TOPICS

ASIA PACIFIC

PROFESSIONAL & FINANCIAL RISKS //
CYBER // RISK MANAGEMENT // ASIA PACIFIC

Summary: Multi-factor Authentication Cyber security series

JUNE 2023

This is a summary of a comprehensive Liberty Trending Topics paper.

To access the full version, please contact your Liberty Professional & Financial Risks Underwriter.

The following paper is the first in a series of topics on common cyber security challenges organisations are facing, alongside regulatory changes for which organisations require awareness. In this paper we explore the increasingly used control of multi-factor authentication; why it is used, some of the techniques used by adversaries to bypass it, and recommendations that organisations can adopt to enhance their cyber defence strategy.

Multi-factor Authentication (MFA) is an essential cyber security control to prevent trivial account compromise, and something that many organisations rely upon to help secure access to critical systems. Liberty Specialty Markets (Liberty) along with cyber security advisers NCC Group, aims to provide an overview of MFA and discuss common pitfalls and challenges that an organisation should be aware of when choosing to implement an MFA strategy.

This paper provides an insight into the different methods of MFA, highlighting those that have proven resistant to attack and those which have proven less resistant, in order to guide on best practice implementation.

Whilst MFA is undoubtedly superior to single-factor authentication, it is not a “silver bullet”, and not all methods of MFA can be considered equal. Organisations should consider MFA an essential control, but always as a single component of their broader defensive strategy.

What is MFA?

When implemented in accordance with best practice, MFA is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to its systems and information.

MFA is an authentication mechanism that requires two or more different proofs of identity to grant access to a resource. It’s also commonly referred to as two-factor authentication (2FA), where a second factor of authentication is required. However, in contrast to 2FA, whilst MFA requires at least two it is not limited to this number.

Governing bodies such as ACSC and the National Institute of Standards and Technology (NIST) identify MFA as requiring two or more different factors to achieve authentication – as such, using two of the same factors to access a system, would not be considered MFA. Authentication factors that make up a multi-factor authentication request must come from two or more of the following:

- Something a user **knows**
  Example: a PIN code or password
- Something a user **has**
  Example: physical hardware, physical smartcard or a digital certificate stored on their device
- Something a user **is**
  Example: their fingerprint or facial recognition scan

The Australian Cyber Security Centre (ACSC) identify MFA as one of the eight essential strategies to mitigate a cyber security incident.

How does MFA help?

In the event of a password compromise, MFA can safeguard access and prevent an adversary from using the stolen password to gain access to the user's account. The adversary may know the user's password, however they would also need access to the second authentication factor, such as the person's fingerprint or one-time code to obtain access. Whilst the adversary has access to credentials, they may not have access, or the capability to access the other factor(s).

A common occurrence is that an organisation storing a large set of credentials experiences a data breach, and the adversary uses the obtained credentials to perform "credential stuffing" attacks against other services and organisations.

If a user has reused the same set of credentials for another service – that is the same email address, same password and has not enabled MFA, then the stolen credentials will grant the adversary access to that service as the user.

When an account or system is protected using only a single factor of authentication, most commonly a password, all an adversary needs to obtain is the username and associated password to access the resource.

Common forms of MFA implementation

MFA can be implemented using a variety of options, including but not limited to:

- PIN codes or a string of characters, often sent to the user via SMS, email, or voice "call-back"
- An app on a trusted device (such as those provided by Microsoft or Google)
- A software certificate installed on a device
- Biometric details (such as a fingerprint scan, or facial recognition)
- A physical security device that the user must physically connect to their device (such as via USB)

Are all MFA methods equally effective?

While any form of MFA provides advantages over single-factor authentication, some methods are more effective than others. Notably, MFA is most effective when one of the authentication factors is physically separate from the device initiating the access request. For example, using a physical hardware device provides a higher level of security than using a software certificate, or a "soft" token stored on the same device. Additionally, some methods of MFA are more resilient to sophisticated phishing techniques designed to bypass MFA controls such as adversary-in-the-middle (AiTM) phishing and Open Authorisation (OAuth) consent phishing (more about those later).

When implementing MFA, it is essential that it does not create a false sense of security.

It is important to remain aware and vigilant in the face of potential threats.

In the event of MFA being implemented at the perimeter of an organisation, it may not be in place on local workstations or internal web applications and systems. A well-resourced and motivated adversary may seek to target users with malware to obtain a "reverse connection" and bypass perimeter defences.

In such a scenario, MFA for remote access is significantly better than SFA but does not negate the requirement for additional security controls such as monitoring and logging, and appropriately hardening systems in accordance with industry best practice.

MFA methods

SMS messages, emails or voice calls

A password is sent to the user using a pre-established communication channel, such as phone numbers and email addresses which may have been provided during the registration and setup of the user account.

The password is usually a time-based one-time password (TOTP), meaning it expires if not used and works only once, preventing an attacker that finds the password from reusing it.

Mobile apps

Multiple mobile applications, each with varying approaches, exist to provide a secure MFA solution. All rely on the principle of using a secure channel, for example a Transport Layer Security (TLS), to communicate the MFA proof to the user.

Users download the application – for example, Google Authenticator or Microsoft Authenticator – from a trusted application store and configure them on a mobile device. Configuration commonly involves account setup, where the user enrols the application using a QR code or other means.

The following are examples of three common solutions. Although more secure than SMS, email and voice calls, it should be noted that they are not without vulnerability.

1. Push notification TOTP

A TOTP is sent to the user using the pre-established mobile application channel in the form of a push notification.

2. Push notification approval

Like the above, but in place of a TOTP, a push notification provides the user the option to approve or decline the login attempt.

3. Push notification approval challenge

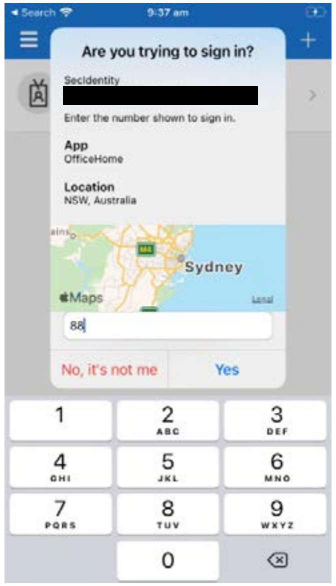
Following a rise in “MFA bombing” attacks, push notification approval challenge requires the user to not only approve an MFA request, but also confirm a further piece of information, for instance a random number generated by the resource the user is attempting to access.

What is MFA bombing?

In the event of an adversary obtaining a set of credentials but lacking the sophistication to perform an adversary-in-the-middle attack, they may resort to a technique known as “MFA bombing”.

This involves repeatedly authenticating a service, causing the legitimate user’s device enrolled for MFA to continuously request login confirmation.

The user may assume there is an error with the application and confirm the login. There also exist many plausible scenarios within which the user mistakes the alert for a legitimate request or accidentally confirms the login while distracted by another task. Although the technique is crude, it has been seen to be effective and leveraged by real-world adversaries to breach high-profile organisations.



Are you trying to sign in?

SecIdentity

[redacted]

Enter the number shown to sign in.

App
OfficeHome

Location
NSW, Australia

88

Source: https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

Software certificates

A software certificate is installed locally on a device as a second factor, and when a user performs an authorisation request, the system presents the certificate. The certificate may be stored within a file on the system, within the system registry or within system hardware, for example, on a Trusted Platform Module (TPM), which is the more secure option. Although this method removes the need for a user to provide a time-bound pin, if an adversary can compromise the device storing the certificate and private key, the adversary can likely replay legitimate requests to gain access, or depending on the level of access required, extract the certificate and install this on a device they control.

Biometrics

A fingerprint, facial recognition pattern or iris scan are examples of biometrics that can be used as a second factor and would be enrolled during account setup. Due to the technical limitations of some biometric technology, some users may not be able to successfully enrol, and it is likely an alternative form of MFA may also be required.

Physical hardware devices

Physical hardware-based MFA, can be implemented in several ways including the use of:

- PIN-generating key FOB: PIN codes generated by a physical device
  Example: RSA SecurID
- A physical device that contains a mechanism to secure storage of a private key
  Example: smartcard, FIDO U2F - now renamed to Client to Authentication Protocol version 1 (CTAP1)

In the case of a hardware device that generates a time-bound code, a separate physical device is used which is already pre-synced to the code generation mechanism. As a result of this pre-synchronisation, a significant vulnerability remains in that if the code is intercepted, it provides the capacity for an MFA bypass such as AiTM phishing to occur.

An alternative approach to physical hardware-based MFA is that of a smartcard or other USB-style hardware providing secure storage of a private key that, when combined with a password, authenticates a request for access.

Common techniques used to bypass MFA

In addition to the individual weaknesses outlined against particular MFA methods, there exists a number of techniques used by adversaries to bypass MFA. These are usually as a result of poorly implemented controls associated to MFA registration, or logic flaws in associated processes. The following are some important considerations to be mindful of.

New users

When a new user is onboarded into an organisation, they are frequently required to set up MFA upon joining. Given modern ways of remote working, users may never physically visit an office and have their device(s) shipped directly to their home.

Under such a circumstance, if an adversary were able to obtain the user's credentials ahead of them, it would be feasible that they could register a device they control and bypass MFA. Combined with weak and common passwords for all users (e.g. all new users have a password of "Welcome1" that requires changing on first use), and password spraying attacks, this scenario is easily exploited.

MFA rollout not choreographed

When an organisation has "turned on MFA" and required existing users to enrol when prompted, opportunities for exploitation emerge.

For example, an organisation requires MFA to access corporate resources from home, but not the office. An employee who only works full-time from the office has credentials stolen, with the adversary registering a mobile number to receive MFA code. The likely outcome is the office-based user would not be aware of the MFA enrolment, and unless the organisation had the appropriate logging and monitoring controls may be unaware of the unauthorised access.

Self-service password reset (SSPR)

Due to flawed logic in the process flow of an authentication service, it may be possible to reset a password by answering easy-to-guess security questions.

Weak conditional access policy

An organisation may have configured a conditional access policy to require MFA for users "not accessing resources via a trusted IP address" (the office IP address).

Where guest Wi-Fi is available, an adversary with access to credentials may be able to use the stolen credentials to authenticate to services from the guest Wi-Fi and bypass MFA requirements.

Under the right conditions, or through the use of specialised antennas, the adversary could even gain access to a guest Wi-Fi remotely. Provided they are able to send and receive traffic on the network, it would be feasible to obtain an external IP within the allow list of the conditional access policy.

MFA bypass attack (adversary-in-the-middle)

Due to the increased prevalence of MFA usage, competent adversaries have developed techniques and tooling to bypass MFA controls, most notably AiTM tooling.

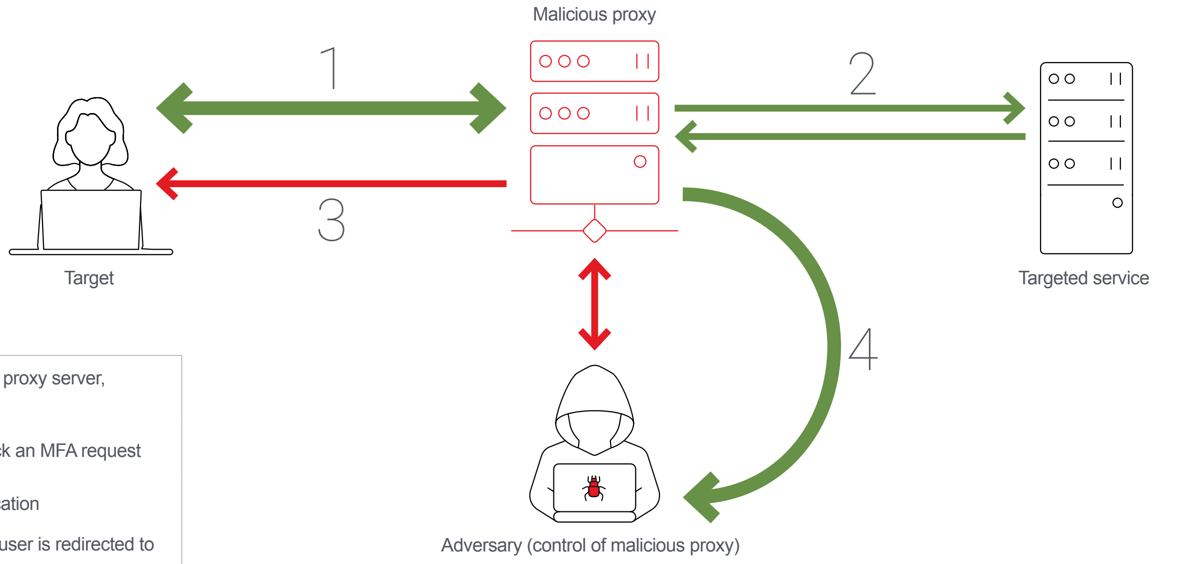
Such tooling enables an adversary to deploy a proxy between the target user and the legitimate service they wish to access. A common means of deploying the access would be traditional phishing techniques and requesting the user visit a URL and perform an action – for example "log in to a Microsoft 365 account to access a time-sensitive email or voicemail" or other appropriate lures.

An example of this technique is featured below.

OAuth consent phishing

As a result of the continual arms race between those tasked with designing MFA methods and those tasked with identifying weaknesses and bypasses and exploiting them, a new class of attack has been developed.

Consent phishing is designed to be capable of bypassing the use of passwords, MFA, and even passwordless solutions. This attack exploits services that support OAuth 2.0 authorisation – for example, Microsoft and Google – and through the use of a malicious application masquerading as an alternative service, attackers send phishing emails to targets and request that they provide consent for the malicious app to make API requests on their behalf.



1 Adversary supplies user with a request to login to a targeted service via a proxy server, into which they enter their account username and password

2 This information is relayed to the targeted service which in turn sends back an MFA request

3 MFA request is forwarded to the user via the malicious proxy for authentication

4 Upon authentication the adversary is granted access to the service while user is redirected to a failed login page, giving the appearance that the password or code was entered incorrectly

In summary: MFA implementation best practices

MFA is an essential complement of any business's approach to cyber security, and it is essential that it's implemented and managed in a strategic and well-thought-out way. Whilst any form of MFA provides advantages over single-factor authentication, with evolving threats some methods have proven less effective than others. Notably, MFA is most effective when one of the authentication factors is physically separate from the device, and resistant to communicating to illegitimate authenticators.

The following guidance is offered to enhance the MFA strategy of an organisation

Choreograph the rollout of MFA in a planned fashion and consider process requirements and weaknesses

For example, enabling users to enrol in MFA from anywhere globally may be a requirement for a geographically dispersed workforce, but if additional controls are not in place an adversary may be able to enrol a device for MFA usage with the user unaware.

- The onboarding process could involve the user providing a mobile number to the helpdesk, who restricts enrolment to that number.
- Where a corporate mobile device is provided for use as the second factor, ensure that the provided device is the device used and not a device owned by the employee. The corporate mobile device should be managed and hardened in accordance with industry best practice.

Harden all devices involved in the authentication process
This includes laptops and mobiles, in accordance with industry best practice, and could be informed by:

- Vendor-specific guidance.
- Australian Cyber Security Centre (ACSC) guidance.
- Other regionally appropriate cyber security centres. For example, National Cyber Security Centre (NCSC), Cyber security and Infrastructure Security Agency (CISA).

Set the expiry times of time-bound PINs to the lowest practical values
Ensure they are configured for single use only and only communicated over secure encrypted protocols.

Educate users on the importance of protecting MFA hardware
Example: users know that they should never provide details (such as the serial number) of their physical hardware, unless they have initiated a call to the IT helpdesk.

Require access controls to access authentication applications on mobile devices
Example: require use of the device password or a user biometric to open the device.

Instruct users to report lost or missing hardware involved in any MFA process as soon as possible
Example: lost mobile device with authenticator app, lost smartcard etc.

Implement logging and monitoring with detection rules to detect and respond to stolen authentication factors
Example: turn on "impossible travel" anomaly detection that alerts when authentication/simultaneous sessions occur from geographically impossible locations that a user could not travel between or exist in at the same time.

Ensure all users have been provided with a basic level of incident response training
Example: know how to report a suspicious email or suspicious request and ensure the security team or incident response team knows how to respond in the event of MFA compromise.

Plan for the capability to revoke MFA hardware
Example: remotely wipe a lost device, and revoke a private key.

MFA is not a ''silver bullet'' and should rather form a component of an organisation's broader cyber defence strategy. In addition to MFA, it is important that organisations have an ability to patch security vulnerabilities, deploy and use hardened applications and operating systems, have a tested incident response plan and perform regular backups of key and critical systems, with backup and restoration capabilities regularly tested and proven.

Liberty Specialty Markets

nccgroup

Global reach. Financial strength. Local authority.

Distinct, complex and constantly evolving – every business is as unique as its insurance needs. To confidently progress in the face of risk and uncertainty requires a level of security you can only achieve through working with specialists.

Liberty Specialty Markets offers a breadth of world-class insurance and reinsurance services to brokers and insured clients. We bring value and solutions to more than 25,000 of Asia Pacific's most significant business and government organisations – helping protect what they earn, build and own.

We're part of the global Liberty Mutual Group, a Fortune 100 company that's been in business since 1912 with a Standard and Poor's 'A' (strong) rating.

About NCC Group

Liberty Specialty Markets engages NCC Group as a cyber security adviser to support clients underwriting Professional and Financial Risk policies.

NCC Group is trusted by more than 15,000 clients to protect their most critical assets from cyber threats. With NCC's knowledge, experience and global footprint, they are well placed to help clients identify, assess and treat risks. NCC continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

NCC has more than 1,800 colleagues in 12 countries. NCC's Technical and Risk Consulting, Incident Response and Managed Services have significant market presence in North America, Europe and Asia Pacific.

This is a summary of a comprehensive Liberty Trending Topic. To learn about this topic in greater detail and access the full version, please contact your Liberty Professional & Financial Risks underwriter.

⊞ View our office locations

⊞ Meet our Cyber team members

in Follow

Connect and join the
Liberty conversation

Liberty is not authorised to provide financial product advice. The information in this document does not take into account your objectives, financial situation or needs. Always consider the applicable policy wording and other relevant documents before deciding to acquire a financial product. © Liberty Mutual Insurance Company 2023. This information is current as at June 2023. Liberty means Liberty Specialty Markets, a trading name of Liberty Mutual Insurance Company, Australia Branch (ABN 61 086 083 605) incorporated in Massachusetts, USA (the liability of members is limited); Liberty Specialty Markets Hong Kong Limited (No. 2400200); Liberty Specialty Markets Singapore Pte Limited (UEN 201538069C); and Liberty Specialty Markets Singapore Pte Limited, Labuan Branch (Company No. LF12903), a licensed insurer under the Labuan Financial Services and Securities Act 2010 (Licence No. IS2016162).