Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Implementing Multi-Factor Authentication

JANUARY 2019

Introduction

Multi-factor authentication is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to a device or network and accessing sensitive information. When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network. Due to its effectiveness, multi-factor authentication is one of the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents***.

This document has been developed to provide guidance on what multi-factor authentication is, different multi-factor authentication methods that exist and why some multi-factor authentication methods are more secure, and therefore more effective, than others. It also discusses how multi-factor authentication is different to multi-step authentication.

The Australian Cyber Security Centre (ACSC) recommends that multi-factor authentication is implemented for remote access solutions, users performing privileged actions and users accessing important (sensitive or high-availability) data repositories. Using multi-factor authentication provides a secure authentication mechanism that is not as susceptible to brute force attacks as traditional single-factor authentication methods using passwords or passphrases.

Why multi-factor authentication is important?

Adversaries frequently attempt to steal legitimate user or administrative credentials when they compromise a network. These credentials allow them to easily propagate on a network and conduct malicious activities without additional exploits, thereby reducing the likelihood of detection. Adversaries will also try to gain credentials for remote access solutions, including Virtual Private Networks (VPNs), as these accesses can further mask their activities and reduce the likelihood of being detected.

When multi-factor authentication is implemented correctly, it is significantly more difficult for an adversary to steal a complete set of credentials as the user has to prove they have physical access to a second factor that either they have (e.g. a physical token, smartcard or software certificate) or are (e.g. a fingerprint or iris scan).

When implementing multi-factor authentication, it is essential that it is done so correctly to minimise security vulnerabilities and to avoid a false sense of security that could leave a network vulnerable. For example, when multi-factor authentication is used for remote access solutions in an organisation, but not for corporate workstations, an adversary could compromise the username/passphrase from a device used for remote access and then use it to authenticate either locally to a corporate workstation or to propagate within a network after compromising an initial workstation on the network via spear phishing techniques. In such a scenario, multi-factor authentication for remote access is significantly better than single-factor authentication but does not negate the requirement for appropriately hardened devices to be used as part of a comprehensive remote access solution.

What is multi-factor authentication?

The ACSC defines multi-factor authentication as 'a method of authentication that uses two or more authentication factors to authenticate a single claimant to a single authentication verifier'.

The authentication factors that make up a multi-factor authentication request must come from two or more of the following:

- something the claimant knows (e.g. a personal identification number (PIN), password or response to a challenge)
- something the claimant has (e.g. a physical token, smartcard or software certificate)
- something the claimant is (e.g. a fingerprint or iris scan).

The claimant being authenticated may be a person, device, service, application or any other security principal that can be authenticated within the system.

An authentication verifier is an entry point to a confined sub-system where a single technical authentication policy is enforced.

Multi-factor authentication often involves the use of passphrases in addition to one or more of the following multi-factor authentication methods:

- Universal 2nd Factor (U2F) security keys
- physical one-time PIN (OTP) tokens
- biometrics
- smartcards
- mobile apps
- Short Message Service (SMS) messages, emails or voice calls
- software certificates.

If an authentication method at any time offers a user the ability to reduce the number of authentication factors to a single factor it is by definition no longer a multi-factor authentication method. A common example of this is when a user is offered the ability to 'remember this computer' for a public web resource. In such a scenario, a user may be authenticated initially using multi-factor authentication but a token is then set on their device such that subsequent authentications use a single factor (usually a passphrase) as long as the token on their device is accessible and valid. In this scenario, the claimant verified by the token is the user's web browser rather than the user. As such, it violates the requirement for two or more authentication factors to authenticate a single claimant to a single authentication verifier. Furthermore, the token has characteristics more akin to a session token than an authentication factor, which makes it unsuitable for the purposes of authentication.

Multi-factor authentication versus multi-step authentication

A common authentication approach often confused with multi-factor authentication is multi-step authentication. Multi-step authentication is an architectural approach to accessing resources sequentially through multiple authentication verifiers. Each authentication verifier grants access to increasingly privileged areas of the system until access to the desired resources is achieved. Authentication verifiers may be single-factor or multi-factor in nature.

While multi-step authentication may significantly improve the security of a system, it is easier for an adversary to bypass than multi-factor authentication as there is no single point within the system that uses two or more authentication factors to authenticate a single claimant to a single authentication verifier. As a result, an adversary can incrementally compromise a system, gaining ever increasing access while never having to overcome the requirement for multi-factor authentication. For this reason, the ACSC does not recognise multi-step authentication as being a suitable substitute for multi-factor authentication.

Consider a remote access solution. In this scenario (figure 1), a computer has an Internet Protocol Security (IPsec) certificate that authenticates the computer to the VPN concentrator, a user has a passphrase that authenticates them to the VPN concentrator and then a passphrase that authenticates them to the Active Directory (AD) domain.

This scenario demonstrates multi-step authentication; however, there is no multi-factor authentication implemented in this scenario. When authenticating to the VPN concentrator, the user and computer are considered separate claimants, therefore the computer's IPsec certificate and the user's passphrase are not a form of multi-factor authentication. Furthermore, the user authenticates separately to the VPN concentrator and to the AD domain. These authentications take place on different authentication verifiers and fail to use different types of authentication factors; therefore, this approach is also not multi-factor authentication.

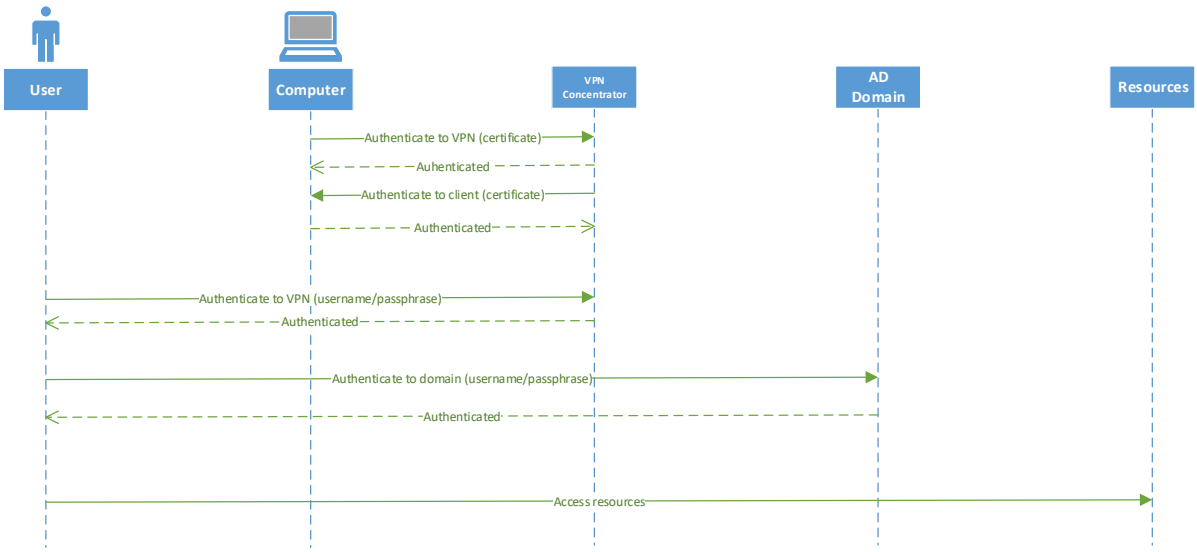

Figure 1: Multi-step authentication used within a multi-step architecture

The risk associated with this scenario is that an adversary may be able to compromise the computer's IPsec certificate at one point in time, compromise the passphrase the user uses to authenticate to the VPN concentrator at another point in time and, finally, compromise the user's AD credentials at yet another point in time. In this way the adversary is able to increase their access over time, which increases the level of risk associated with this approach.

Consider a second remote access solution. In this scenario (figure 2), the user is authenticated to the VPN concentrator using a passphrase and one-time PIN from a physical token. All other authentication steps are the same as in the previous scenario (figure 1).

This scenario demonstrates a relatively secure remote authentication architecture with a multi-factor authentication method used to authenticate the user to the VPN concentrator. In this case, the computer is authenticated with single-factor authentication in the form of the computer's IPsec certificate. The multi-factor authentication takes place on entry into the remote access environment (using the user's passphrase and one-time PIN), which verifies access through to the corporate environment, which remains protected by single-factor authentication in the form of the user's passphrase.

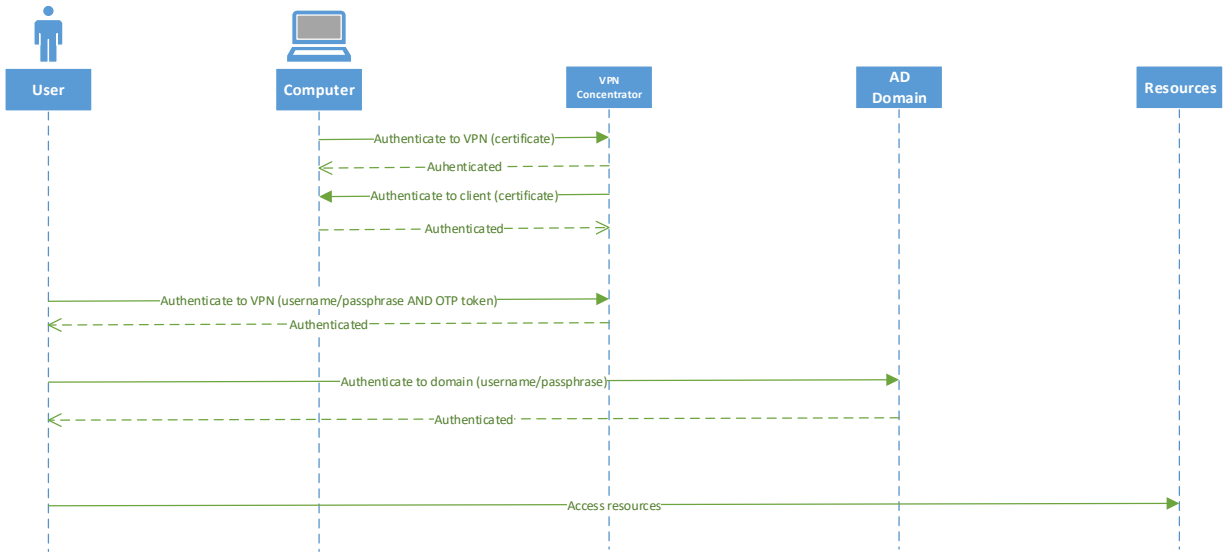

Figure 2: Multi-factor authentication used within a multi-step architecture

Are all multi-factor authentication methods equally effective?

While all forms of multi-factor authentication listed in this document provide significant advantages over single-factor authentication, some methods are more effective than others. Notably, multi-factor authentication is most effective when one of the authentication factors is physically separate from the device from which the user is accessing the system or resource, such as using a physical token rather than a software certificate.

To maximise the security effectiveness of any multi-factor authentication method chosen, the authentication service (if a dedicated authentication server) should be hardened and isolated from the rest of the network as much as possible. This can be achieved by (at a minimum):

- implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (where applicable)
- implementing appropriate network segmentation and segregation to limit the types of network traffic to and from the authentication service to only traffic required for its proper operation, with particular care paid to which devices and users on the network can access the authentication service directly
- applying any specific hardening advice provided by vendors.

Multi-factor authentication methods

U2F security keys

This multi-factor authentication method uses a physical token or card (referred to as either a U2F security key or U2F authenticator) as a second factor. Software on the user's device prompts the user to either press a button on the U2F security key or tap it using Near Field Communication (NFC). In doing so, the U2F security key uses public key cryptography to verify the user's identity by signing a challenge-response request from a service which had been passed

through via a web browser or mobile app. The service then verifies that the response is signed by the valid and correct private key for that service, and grants or denies access to resources.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure users do not store U2F security keys with their devices, especially those with NFC capabilities
- ensure users receive a visual notification each time an authentication request is generated that requires them to authenticate using their U2F security key
- use U2F security keys that have been certified[1] to the latest U2F specification version
- instruct users to report any lost or missing U2F security keys as soon as practical.

Physical one-time PIN tokens

This multi-factor authentication method uses a physical token that displays a time-limited one-time PIN on its screen as a second factor. Alternatively, the user may be required to press a button on a physical token, which is connected to their device, to submit the one-time PIN on their behalf. The time on both the physical token and the authentication service are synchronised and the authentication service knows what one-time PIN should be used by all physical tokens that it services at a particular time. When the user authenticates with a passphrase and one-time PIN, the authentication service verifies that all details are correct for that user and grants or denies access to resources.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure users do not store physical tokens with their devices
- set the expiry time of the one-time PIN generated by physical tokens to the lowest value practical
- instruct users to report any lost or missing physical tokens as soon as practical
- ensure users know that they should never provide details (such as the serial number) of their physical token unless they are certain it is being requested by their ICT support staff.

Biometrics

This multi-factor authentication method uses biometrics, such as a fingerprint or iris scan, as a second factor. When the user enrols they provide a scan of the appropriate biometric as a reference point for the authentication service to compare to. When the user authenticates they provide a passphrase along with their biometric data, the authentication service verifies both the passphrase and the biometric data with those provided at enrolment, and grants or denies access to resources. It should be noted though, that for every biometric mechanism, due to the wide range of differences between individuals, some of the potential users will not be able to successfully enrol.

[1] https://fidoalliance.org/certification/fido-certified-products/

There are, however, potential security vulnerabilities in this multi-factor authentication method caused by the fact that biometric characteristics are not secrets (especially if the biometric reader converts biometric data into a hashed form), biometric matching is probabilistic rather than deterministic, and there is a reliance on the biometric capture software installed on the user's device. If an adversary compromises the user's device and gains elevated privileges, then it is possible for the adversary to use the services provided by the biometric capture software to intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf – within the limitations of any anti-replay measures. Furthermore, the effectiveness of biometrics is reliant on the quality of the biometric readers and capture software to ensure that false negatives (denying access when it should be allowed) and, more importantly, false positives (granting access when it should have been denied) provide an appropriate trade-off.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure users receive a visual notification each time an authentication request is generated that requires them to provide their biometric data
- ensure an alternative authentication method, including supplementary security measures, is implemented for cases where users cannot successfully enrol using biometrics.

Smartcards

This multi-factor authentication method uses a private key stored on a smartcard as a second factor. Software on the user's device prompts the user to unlock the smartcard by entering a PIN or password. When the smartcard is successfully unlocked, the software on the device verifies the user's identity by signing an authentication request with the user's private key. The authentication service then verifies that the authentication request is signed by the valid and correct private key, and grants or denies access to resources.

Like biometrics, this multi-factor authentication method has a potential security vulnerability due to the software involved in interacting with the smartcard. If the user's device is compromised and an adversary gains elevated privileges, they can potentially intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf – within the limitations of any anti-replay measures.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure users do not store smartcards with their devices
- ensure users receive a visual notification each time an authentication request is generated that requires them to unlock their smartcard
- instruct users to not leave their smartcard inserted into their device and unlocked
- instruct users to report any lost or missing smartcards as soon as practical.

Mobile apps

This multi-factor authentication method uses a time-limited one-time PIN or password provided via a mobile app as a second factor. When the user enrols they either scan a QR code or provide a phone number or an email address so that a one-time PIN or password can be provided to them to register the mobile app. During the logon process the user requests the mobile app to provide them with a one-time PIN or password in order to complete the authentication process. The user then provides this information to the authentication service, which verifies that all details are correct for that user and grants or denies access to resources.

The advantage of this multi-factor authentication method is that it uses a second factor that the user already has and therefore minimises the cost to the system owner; however, there are also a number of disadvantages, namely:

- use of devices for web browsing or reading emails may mean that the device running the mobile app may no longer be secure
- many devices are not secure and a device can be compromised by motivated and competent adversaries, particularly when travelling overseas.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure the expiry time of the one-time PIN or password generated via the mobile app is set to the lowest value practical
- instruct users to report the theft or loss of a device running the mobile app, even if it is a personal device, as soon as practical.

SMS messages, emails or voice calls

This multi-factor authentication method uses a time-limited one-time PIN or password provided via an SMS message, email or voice call to a device as a second factor. When the user enrols they provide a phone number or an email address so that a one-time PIN or password can be provided to them to register. During the logon process the user requests that the authentication service provide them with a one-time PIN or password in order to complete the authentication process. The user then provides this information to the authentication service, which verifies that all details are correct for that user and grants or denies access to resources.

The advantage of this multi-factor authentication method is that it uses a second factor that the user already has and therefore minimises the cost to the system owner; however, there are also a number of disadvantages, namely:

- depending on the user's location, telecommunication networks may have degraded service or no service at all, which may affect the availability to receive a one-time PIN or password
- use of devices for web browsing or reading emails may mean that an SMS message, email or voice call containing the one-time PIN or password may no longer be secure, particularly when SMS messages are delivered via VoIP or internet messaging platforms
- many devices are not secure and a device can be compromised by motivated and competent adversaries, particularly when travelling overseas
- telecommunication networks do not provide end-to-end security and an SMS message, email or voice call may be intercepted by motivated and competent adversaries, particularly when travelling overseas.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used, as well as those receiving second factors, as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- set the expiry time of the one-time PIN or password provided via an SMS message, email or voice call to the lowest value practical
- instruct users to report the theft or loss of their device, even if it is a personal device, as soon as practical.

Software certificates

This multi-factor authentication method uses a software certificate stored on a device as a second factor. When the user wishes to authenticate, the system attempts to access the user's software certificate, which is stored in a file, in the registry or in the Trusted Platform Module (TPM) of their device. If successful, the software installed on their device assists the user to verify their identity by signing an authentication request with the user's private key. The authentication service then verifies that the authentication request is signed by the valid and correct private key, and grants or denies access to resources.

The security vulnerability in this multi-factor authentication method is due to a reliance on the software and the operating system installed on the user's device. If an adversary compromises the user's device, then it is possible for the adversary to use the services provided by the software in order to intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf – within the limitations of any anti-replay measures. By compromising the user's device, an adversary can gain access to both authentication factors easily with a low likelihood of detection. There is also the additional risk that if an adversary can gain elevated privileges, the user's keys and certificates can be stolen from their device and used by the adversary from their own devices or infrastructure to enable prolonged and difficult to detect remote access to a network. For this reason, it is recommended that organisations only use software certificates for low risk transactions or systems.

For maximum security and effectiveness, the following security measures should be implemented when using this multi-factor authentication method:

- harden the devices being used as much as possible, this can be achieved by (at a minimum)
  - implementing the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** (if applicable)
  - applying any specific hardening advice provided by vendors
- ensure users receive a visual notification each time an authentication request is generated that requires them to enter their PIN or password to access their software certificate
- store the software certificate in the device's TPM (if present), otherwise store it in the device's certificate store rather than in a regular file on the device's local storage
- instruct users to report the theft or loss of their device, even if it is a personal device, as soon as practical.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).