SECMON1

Information Security Guideline

Multi Factor Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

Multi-Factor Authentication requires end users to provide multiple methods of identification to confirm their identity in order to gain access to corporate resources and applications, as well as perform online transactions. By requiring an additional factor beyond a simple password, multi-factor authentication technology makes it far more difficult to exploit the login process and wreak havoc by stealing corporate, customer or partner data.

The authentication factors that make up a multi-factor authentication request must come from two or more of the following (Claimant being authenticated may be a person, device, service, application or any other security principal that can be authenticated within the system):

a. Something a claimant knows (e.g., a personal identification number (PIN)/passphrase or response to a challenge question)
b. Something a claimant has (eg, physical token, smartcard or software-based certificate)
c. Something a claimant is (e.g., a fingerprint or iris scan)

Before investing in a multi-factor authentication solution, organisations need to take several things into account. A guide to criteria for evaluating and procuring multi-factor authentication products can be found here. That way, when it is time to select the right solution, the organisation will know what multi-factor authentication product features best match the use cases (e.g., Active Directory augmentation, strong identity verification and/or the strengthening of Web server logons) that apply to its environment and authentication needs.

Here are some examples of multi-factor authentication products:

- CA Strong Authentication
- Okta Verify
- Quest Software Defender
- RSA Authentication Manager and RSA SecurID
- SafeNet Authentication Service
- SecureAuth IdP
- Symantec Validation and ID Protection Service
- Vasco IDENTIKEY Server and DIGIPASS

A comparison of the above products can be found here.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what multi-factor authentication is and why it is an essential security measure. In this document we are going to provide some multi-factor authentication information as well as provide you with interesting and important links where you can educate yourself further on this topic and discuss available options.

Implementation Guidance

Currently the available multi-factor authentication methods are provided by external companies and not freely available (at least not at actual secure solutions).

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.

Ensure mandatory multi-factor authentication for all administrative service accounts; other accounts unable to use multi-factor authentication should use strong passwords or passphrases that contain a minimum of four random words, numeric and special characters.

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-based certificate.

To maximise the security effectiveness of any multi-factor authentication method chosen, the following security measures should be implemented:

a. The authentication services (if a dedicated authentication server) is hardened and isolated from the rest of the network as much as possible
b. The passphrase used for remote access is different to the user's standard passphrase for the network
c. Ensuring users do not store a physical token or smartcard with the device used for remote access
d. Devices used to receive or generate the second factor are hardened as much as possible

Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

Common Multi-Factor Authentication Methods

Token-Based Multi-Factor Authentication

This method uses a physical token that displays a time-limited one-time PIN/passphrase on its screen as a second factor. The time on both the physical token and the authentication service are synched and the authentication service knows what PIN/passphrase should be displayed on all physical tokens that it services at a particular time. When the user authenticates with a passphrase and the PIN/passphrase displayed by the physical token, 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 method:

a. The expiry time of the PIN/passphrase displayed on the physical token is set to the lowest value practical
b. Users are instructed to report any lost or missing physical tokens
c. Users know that they should never provide details (eg, serial number and PIN/passphrase displayed) about their physical token unless they are certain it is being requested by their IT support staff.

Biometric-Based Multi-Factor Authentication

This 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 scan, the authentication service verifies both the passphrase and the biometric 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.

There are potential vulnerabilities in this method in that biometric characteristics are not secrets, biometric matching is probabilistic rather than deterministic, and there is a reliance on the biometric capture software and the operating system installed on a user's device.

For maximum security effectiveness, the following security measures should be implemented when using biometrics:

a. Users receive a visual notification each time an authentication request is generated that requires the user to enter their PIN/passphrase. This will enable them to potentially detect fraudulent authentication requests.

b. An alternative authentication method, including supplementary security measures, is implemented for cases where a user cannot successfully enrol using the biometric mechanism.

Certificate-Based Smartcard Multi-Factor Authentication

This method uses a private key stored on a smartcard as a second factor. Software installed on a user's device prompts the user to also provide a PIN/passphrase to unlock the smartcard, and then verifies their identity using the private key stored on that smartcard. When the smartcard is successfully unlocked, 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.

This method has a potential security vulnerability due to a reliance on the smartcard software and the operating system installed on a user's device. If the user's device is compromised and an adversary gains elevated privileges, they can use services provided by smartcard software to intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf.

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

a. Users receive a visual notification each time an authentication request is generated that requires the user to enter their PIN/passphrase. This will enable them to potentially detect fraudulent authentication requests.
b. The Certification Authority's keys are adequately protected (e.g., stored in a Hardware Security Module (HSM)) and backups of keys are physically secured and stored offline.
c. Users do not leave their smartcards inserted and unlocked in the reader. Contactless smartcard readers can be used to enforce this control.
d. Storage and functionality on the smartcard is minimised as much as possible.
e. Users are instructed to report any lost or missing smartcards as soon as practical.

App-Based Multi-Factor Authentication

This method uses a time-limited one-time PIN/passphrase provided via an app as a second factor. When the user enrols they provide a phone number, instant message identity or an email address so that a time-limited one-time PIN/passphrase can be provided to them via an

SMS message, instant message, voice call or email to register the app. During the logon process the user requests the app to provide them with a PIN/passphrase 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 advantages of this method are that it uses a second factor the user already has and thus minimises cost to the system owner; however, there are also some disadvantages:

a. Use of devices for Web browsing may mean the device running the app may no longer be secure
b. Many devices are not secure and a device can be compromised by motivated and competent adversaries, particularly when traveling overseas.

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

a. The expiry time of PIN/passphrase provided via app is set to the lowest value practical.
b. Users are instructed to report theft or loss of any device running the app, even if it is a personal device, as soon as practical.

SMS, Instant Message or Voice Call-Based Multi-Factor Authentication

This method uses a time-limited one-time PIN/passphrase provided via SMS, instant message or voice call to a device as a second factor. When the user enrols they provide the phone number or instant message identity of their device so a time-limited one-time PIN/passphrase can be provided to them to register. During the logon process the user requests that the authentication service provide them with a PIN/passphrase 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 advantages of this method are that it uses a second factor the user already has and thus minimises the cost to the system owner; however, there are some disadvantages:

a. Telecommunication networks can have degraded service or no service at all, which may affect the availability of the system
b. Use of devices for web browsing may mean an SMS, instant message or voice call containing the PIN/passphrase may no longer be secure, particularly when SMS are delivered vis VoIP or internet messaging platforms
c. Many devices are not secure and a device can be compromised by motivated and competent adversaries, particularly when traveling overseas

d. Telecommunication networks do not provide end-to-end security and an SMS message, instant message or voice call may be intercepted by motivated and competent adversaries, particularly when traveling overseas.

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

a. The expiry method of the PIN/passphrase provided via SMS message, instant message or voice call is set to the lowest value practical
b. Users are instructed to report the theft or loss of their device, even if it is a personal device, as soon as practical.

Software-Based Multi-Factor Authentication

This method uses a software-based certificate stored on a device as a second factor. When the user wishes to authenticate, the system attempts to access the user's 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 method is due to a reliance on the software and the operating system installed on a user's device. 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-based certificates for low-risk transactions or systems, and never for authentication via a remote access solution

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

a. Users receive a visual notification each time an authentication request is generated that requires the user to enter their PIN/passphrase. This will enable them to potentially detect fraudulent authentication requests.

b. Store the certificate/keys in the device's TPM (if present), otherwise the certificate/keys should be stored in the device's certificate store rather than in a regular file on the device's local storage.
c. Users are instructed to report the theft or loss of their device, even if it is a personal device, as soon as practical.

Final Note

We at SECMON1 are available to review your multi-factor authentication needs and strategies with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement multi-factor authentication for your company.

Please feel free to visit our website at www.secmon1.com.

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com.