Technical Articles

Carsten Olt

April 11, 2019 4 minute read

SSO vs. MFA

Some IT security managers are concerned about the fact, that a badly implemented Single Sign-On (SSO) will weaken overall security and may grant unauthorized access to every system tied into it. SSO provides access to many resources once the user is initially authenticated ("keys to the castle"), which increases the negative impact in case the credentials are available to other people and misused.

In fact, that's true, but thankfully, it's easy to add extra security. SSO must use strong encryption and authentication methods to prevent this from happening. As a basic principle, the SSO mechanism must not be weaker than the authentication method itself. Since this blog is all about SAP Security, I'd like to explain to you what options exist to mitigate this potential risk when using SAP's Single Sign-On solution in your landscape.

In today's IT, passwords can be seen as the key to our information and therefore, should be selected safely and handled with care. They accompany us in everyday life and are often used when accessing the operating system or logging on to enterprise applications. SAP is one of them. Because of its multi-system-landscape and terrible decentralized password management, an SAP landscape is an optimal candidate for using single sign-on (SSO) to obviously reduce the overall number of passwords required for multiple applications and systems.

The simple combination of a user ID and password is no longer good enough to protect our most vulnerable information, examples are your bank account, your Bitcoin wallet, your iCloud account or other sensitive systems. In many cases, here you have to provide a second kind of authentication, in addition to something you "know" to secure your accounts against phishing. That is when we start talking about multi-factor authentication (MFA).

SSO and MFA both deal with authentication. While the first is easy to use and mostly transparent to the user, the latter is certainly uncomfortable but more secure. How to reconcile both in a way that makes it possible to

achieve the required security and confidence?

What is multi-factor authentication (MFA)

MFA uses several different factors to verify your identity. Often it requires:

- Something you know (password, personal identification number or login name)

- Something you have (security token, a smartphone app that generates one-time passcodes, an SMS or some other authenticator)

- Something you are (biometric security factors such as fingerprint or face detection)

Furthermore, depending on your IP-Geolocation some services also send e-mails requiring your additional confirmation to sign-in (double opt-in). The advantage is, MFA is very secure. The combination of something you know with something you are or have, significantly reduces the risk of compromised accounts. The most important drawback is its inconvenience, you have to do something which takes time and often this creates a negative user experience.

What is Single Sign-On (SSO)

First of all, you have to know, SSO is not equal to SSO. There are different flavors and the terminology is not clearly settled.

- Enterprise Single Sign-On (E-SSO):To be seen as a client software which automatically populates appearing login screens with the correct user name and password, so a user no longer has to type in the password. Examples include the “password manager” integrated with many modern browsers, as well as many commercial products. Credentials are stored either on the PC or a smart card as well as servers, directory services or databases on the network. E-SSO solutions are often used in cases where the applications do not support real SSO mechanisms. ?? *Weak security and often involved with usability issues.*

- Single Password/Single Credential:Here always the same password will be used to authenticate against many services. This is often combined with E-SSO. Usually, a central password is distributed to all services by means of synchronization (in SAP this requires connectors), while the logon method remains unchanged. ?? *It is not very secure and has many disadvantages.*

- Single Sign-On:The concept of real SSO is based on the idea of enabling the user to access all applications through a first sign-on, mostly during the Windows login. This is considered as the primary authentication. It utilizes industry standards like Kerberos, X.509 or SAML 2.0 and replaces passwords with security tokens. It reduces the number of passwords required by the user to the absolute minimum. Conceptually, the application server only validates the trusted security token instead of authenticating the user. SSO does not mean having the same password on all systems, but in the best case, no longer having a password at all. It is

a simplification, but high-security requirements and restrictions should be considered. ?? A user only has to remember one password at all times and extra security can be added when combined with strong authentication or MFA. SSO is quick and convenient for the end user and as a result, there are fewer calls to the service desk for password resets, reducing IT support costs. Technically no passwords will be retransmitted several times as it is the case with the first two approaches.

Using SSO in high-security environments and enforcing strong authentication

High-security environments, such as the US government, require compliance with FIPS 140-2 standards and the use of smart card authentication as the primary method of accessing their IT systems. The smart card contains a private key protected with a PIN. Thus, two-factor security is achieved. Removing the smart card from the reader will lock the computer immediately. This type of primary authentication (strong authentication) is considered highly secure and is used by some companies that have such requirements.

Usually the combination with building access, time-recording or payment systems makes the most sense. In this case, the (company)-card does not remain in the card reader if the employee is enjoying the lunch ?. Of course, it is possible to combine this with your SAP access controls and even enforce this method of strong authentication for all (or some) SAP users/systems in your organization.

However, if you do not own smart cards, readers and a PKI with a connected card management system, it makes little sense to think about this method. Again, this is considered a high-security requirement.

Using MFA for secure authentication to your most critical systems

According to our experience, most organizations have only a few SAP systems or applications with higher security requirements. It is recommended to categorize your SAP systems into security zones and define the desired authentication procedure on this basis.

It is possible to enforce an additional authentication against a central authentication server (like a central LDAP) for systems where you don't want (or not allowed) to use Single Sign-On. For example, when accessing your SAP Employee Self-Services (ESS) Portal you need to log in with your Active Directory credentials or even provide a one-time passcode.

Or you even may want to require secure MFA at the start of the day, granting continued access to authenticated users throughout their workday. Whichever approach you choose, always ensure transmission of authentication data is done via encrypted communication channels. And ultimately the user is the last bastion. Constantly raise user awareness, educate them in terms of safe handling of IT systems. Introduce clean-desk and lock-screen policies. These non-technical approaches will help to increase security as well.

Conclusion

SSO and MFA can be perfectly combined, especially in your SAP environment using SAP Single Sign-On 3.0

(Cross Posted Content | Original Source: https://xiting.us/blog/sso-vs-mfa/)

Alert Moderator

Assigned tags

SAP Single Sign-On | Security |

Similar Blog Posts

SSO operational documentation with Kerberos
By **Former Member** , Sep 16, 2015

A simple solution to enabling SSO on email links
By **Former Member** , Mar 24, 2015

Helpful SSO links!
By **Former Member** , Jun 26, 2015

Related Questions

SSO/MFA cannot be bypass due saml2=disabled option has been deactivated
By **Mark Jhamil Versoza** , Nov 29, 2019

How to configure Multi Factor Authentication(MFA) in ABAP stack
By **Victor Sevilla** , Feb 19, 2021

SNC questions
By **Former Member** , Jun 18, 2015

Be the first to leave a comment

You must be Logged on to comment or reply to a post.

Find us on

Legal Disclosure	Copyright
Trademark	Cookie Preferences
Newsletter	Support