CERT-EU Security Whitepaper 16-003

Authentication Methods

D.Antoniou, K.Socha

ver. **1.0**
20/12/2016

TLP: WHITE

1 Authentication

Lately, protecting data has become increasingly difficult task. Cyber-attacks have become one of the most serious threats to any organization. Companies and organizations are taking measures in order to defend their assets, and the authentication methods are an increasingly important security measure.

Authentication is the security term for verifying that the user is indeed who he claims to be. The procedure of confirming a user's authenticity, is the action of comparing the provided credentials of the user against an existing database of validated identities.

However, since depending only on the use of simple credentials – or a single method of authentication in general – have lately proven to be highly unreliable, the use of multiple factors for the authentication process is highly recommended. Traditionally, authentication mechanisms have been categorized as either:

- Based on a **knowledge** factor. These methods are vulnerable to obtaining something the user knows (e.g. phishing): password, PIN code, etc.
- Based on a **possession** factor. These methods are vulnerable to obtaining something the user has (e.g. stealing): ID card, token, etc.
- Based on an **inherence** factor. These methods are vulnerable to replicating something the user is (e.g. impersonating): fingerprint, iris scan, etc.

2 Multi-Factor Authentication

Multi-factor authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism. In practice however, there is still value in multiple methods of the same type, as long as compromising one method does not mean compromising the other as well. Generally, confirming a user's claimed identity by utilizing a combination of multiple components results in a higher level of assurance. This is the case since even if one of the factors has been compromised, the chances of the other factor also being compromised are low. Two-factor authentication for instance, is a method of confirming a user's identity by utilizing a combination of two methods of authentication.

User experience is critical for successful MFA. Organizations and companies need to strike a balance between user convenience, risk, usability and cost. A global approach for combining authentication methods does not give companies the flexibility required to apply a MFA solution that fits the needs of different user groups in today's complex IT and security world.

There exists a wide variety of authentication methods, each having its own set of strengths and weaknesses in terms of both security and user experience. In the following subsections we discuss the most popular ones.

2.1 Passwords (*Knowledge* Factor)

The password authentication method is based on a username and a password:

- The user identifies the account he wants to use by means of a username and demonstrates that he or she is the legitimate owner by means of a secret password.

- Authentication is successful if the provided elements are valid by comparing them against an existing database of authorized identities.

2.2 Single Sign-On with Windows (*Knowledge* Factor)

NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials [1].

2.3 Hardware Tokens (*Possession* Factor)

Hardware tokens are small devices that a user uses to authorize access to a system or application. They come in different forms, including key fobs, USBs, Wallet-cards. The hardware device generates one-time passwords (OTP) that the user provides when requested. In general, hardware tokens are widely used in two-factor authentication, since they provide strong security and they are easily integrated. On the other hand, some of the disadvantages that has to be taken into consideration is the high cost of implementing the authentication procedure, the fact that the hardware tokens can be inconvenient for the user (extra item to carry and keep safe), and the fact that their use creates questions about the chain-of-custody. This last point is related to their life cycle, as a token goes from manufacturer to vendor, to distributor, to customer, and the chain-of-custody involves person-to-person delivery and identification-checking and signing.

2.4 Soft Tokens (*Possession* Factor)

Soft tokens are software-based tokens or applications which operate as a type of second-factor authentication security device, and that may be used to authorize the use of computer services by generating an OTP. Software tokens are stored on a general-purpose electronic device such as a desktop computer, a laptop, a PDA, or a mobile phone, and can take advantage of push notifications for improved user convenience. The widespread use of mobile devices have made soft tokens a popular and convenient option. Soft tokens have two main advantages over hardware tokens. First, there is no additional physical token to carry around, and second, they are less expensive to distribute. In addition, they do not require a cell phone signal to use. On the other hand, in contrast with hardware tokens, software tokens can be duplicated, because a user cannot physically possess them. The soft token has to be duplicated on all workstations the user logs on. Therefore, the token may be copied or *stolen* from any of these machines. Another threat is the malicious software, which may infect any machine, read the stored soft token and send it over the Internet to an attacker.

The variations of software tokens that may be used are the following:

- Based on a username, a password, and a one-time-password generated by an application installed on a mobile device.
- Based on a username, a password, and a challenge/response exchange between the server and the application installed on a mobile device.
- Based on a PIN code and a challenge/response exchange between the server and the application installed on the mobile device.

2.5 Certificate-Based (*Possession* Factor and *Knowledge* Factor)

Certificate-based authentication is the use of digital certificates (X.509) to identify a user before granting access to systems, web services or applications. Usually, it is used in combination with traditional methods such as username and password authentication, in order to employ a two-factor authentication mechanism. Certificate-based authentication relies on what the user has, which is the user's private key, and what the user knows, which the password that protects the private key.

Using a cloud-based certificate management platform makes it easy for administrators to issue, renew, or revoke certificates. The most important advantage is the ease-of-use, especially in the case of external users, because no additional software is required and no training needs to be provided. In addition, integration with Active Directory allows certificates to be automatically installed and thus minimal involvement is needed from end-users. As far as cost is concerned, there is no additional hardware required, since the certificate is stored locally on the machine of the user.

Most important drawback of certificate-based authentication is that it cannot handle issues related to the physical access of individual workstations or passwords. Therefore, it is up to the user to physically protect his machine and the password.

2.6 SMS/Text Message (*Possession* Factor)

This authentication method is based on a username, a password, and a one-time password sent to the user's mobile phone using Short Message Service (SMS). One major advantage of this authentication method is that no additional hardware or infrastructure is required to implement this method. On the other hand, text messages require a reliable cell phone signal and sufficient battery life, and may result in occasional SMS delivery failures.

However, SMS-based two-factor authentication is now considered insecure. NIST argues [2] that SMS-based two-factor authentication is an insecure process because it is too easy for anyone to obtain a phone, and the website operator has no way to verify whether the person who receives the code is even the correct recipient. In fact, SMS-based two-factor authentication is also vulnerable to hijacking, if the individual uses a voice-over-internet protocol (VoIP) service, which provides phone call service via a broadband Internet connection instead of a traditional network. Since some VoIP services allow the hijacking of SMS messages, hackers could still gain access to your accounts protected with SMS-based two-factor authentication. Also, the design flaws in SS7 or Signaling System Number 7 protocol also allow an attacker to divert the SMS containing the one-time password (OTP) to their own device. This lets the attacker hijack any service, including Twitter, Facebook, or Gmail that uses SMS to send the secret code to reset account password.

2.7 Biometric (*Inherence* Factor)

Biometrics can be very valuable as a part of multi-factor authentication and is the most technologicaly advanced solution today. There is a number of different types of biometric authentication currently in use or being developed, such as fingerprint, retina scans, facial recognition, and more.

Most mobile devices now-a-days contain a fingerprint scanner and since companies no longer have to invest on developing any hardware component, the cost is not only affordable but even smaller than other authentication methods. Of course, an important drawback is that, depending on the method, false positives and false negatives can be expected. In addition, the most serious drawback is that if a biometric authentication factor is compromised, this situation is not reversible. For example, a password can be reset, while a user's fingerprints cannot. Specifically in the second case, the fingerprints of a user can be easily copied, since a fingerprint can be left on any surface.

2.8 Device Identification (*Knowledge* Factor)

Device identification is a method that establishes a device fingerprint considered unique to that device. This fingerprint allows to recognize the device, and when the user associated with it attempts to authenticate from a different one, this could indicate suspicious activity. For device identification characteristics such as geolocation, OS version, and browser version may be used, but the simplest solution would be a cookie that is downloaded on the device browser by the authentication server. Device identification applications are suitable for organizations that have large populations of users accessing sensitive information from the Internet and prevents the user from verifying his identity from the same device again.

Device identification allows the user to use the relatively inexpensive username/password authentication without any additional tokens required. However, it can be proven to be ineffective if it is configured incorrectly, which means that the characteristics used to identify the device are not unique. This situation could result to false negatives, meaning that the previously identified may not be recognized as known, or false positives, where a device is recognized as a previously known device, while it has never been used by the user for validating credentials before.

3 Suggestions and Conclusions

Organizations need to ensure that access to all sensitive information is authenticated, wherever the information resides and whatever means are used to access it. Besides employing a secure enough authentication mechanism, authentication environments have to offer convenience and transparency for users and administrators as well. To do so, organizations have to be able to manage efficiently all users across all devices and resources, while the procedure of authenticating keeps a user friendly profile and guarantees security.

It is clear that a single method of authentication is not enough. For example, a password or a token can be stolen and fingerprints can be copied from any surface. In order to achieve a safer authentication mechanism, two challenges should be chosen in combination for validating a user access. The use of multiple factor authentication raises safety, cost, and complexity at the same time. In addition, some methods have now been proven to be vulnerable, such as SMS, and hence organizations and companies must constantly adapt to these threats. For the moment, it is safe to say that the username/password days for authentication are far from over.

As a general recommendation, a strategy of combining at least two authentication methods that are mutually independent is advised. Ideally, one is non-replicable and the other non-reusable, exchanging credentials through different communication channels or devices. It is also important that users are continuously trained, in order to improve their perception of the actual risks involved in authentication mechanisms, keeping in mind the last threat patterns discovered by criminals [3].

4 References

[1] https://msdn.microsoft.com/en-us/library/windows/desktop/aa378749(v=vs.85).aspx

[2] https://pages.nist.gov/800-63-3/sp800-63b.html

[3] https://www.enisa.europa.eu/publications/eIDA-in-e-finance-and-e-payment-services