National Cyber Security Centre
Ministry of Justice and Security

Mature authentication

Use of secure authentication tools

Factsheet FS-2022-01 | Version 1.1 | 20 April 2022

Authentication is the technology a system uses to verify a user's identity. Following successful authentication, the user is granted access to accounts and systems within an organisation. The best known example of authentication is logging in with a username and password. This is also, however, the least secure authentication method.

If a malicious party obtains the login details for a legitimate user, that party can also penetrate the organisation's accounts and systems. There are many ways these details can be obtained with very little effort.

Stronger authentication methods provide more protection against such attacks. Examples of this include two-factor authentication and the FIDO Alliance's FIDO2 standard. This factsheet includes information about things to consider when determining the most suitable authentication method for the accounts and systems in your organisation.

Target group

CISOs, identity managers, access managers and security managers

This factsheet was compiled in consultation with:

FI-ISAC, Rabobank, de Volksbank

Background

Authentication is the technology a system uses to verify the identity of a user. This grants a user access to data or systems. Authentication is part of identity and access management and is supplemented by authorisation in applications. The relationship between those two is that

authentication makes the identity of a user known. This is not the case for authorisation. Authorisation concerns assigning the user certain privileges within the system after this user has successfully been authenticated.

Accounts and systems can be protected by various types of authentication tools. They are usually categorised as follows:

- something you know (username and password, for example);
- something you are (biometric data, such as an iris scan, for example);
- something you have (a telephone or a token, for example).

Ease of use and security

Ease of use plays a major role in protecting accounts and systems. An authentication tool that is not user friendly results in the end users looking for alternatives and circumventing the security if possible. This reduces the effectiveness of the security measures that have been implemented. Example: an employee should change their password regularly. This outdated rule was often recommended in the past but never worked well in practice. Users choose easy passwords and often only change a single letter or symbol in the password. In many cases, a password is used for several systems.

The issue at hand

Malicious parties seeking to gain access to systems can focus on cracking the authentication mechanism. The attack techniques that are used are becoming increasingly accessible and easier to use. This increases the possibility of unauthorised login attempts. Common attack techniques relating to unauthorised login attempts are described in Table 1.

Accounts with higher privileges within a system, such as administrator accounts, are increasingly the target of attacks. They often have access (authorisation) to sensitive information and are therefore an interesting target for financial and information-motivated reasons. A malicious party can, for example, install ransomware on the data and systems that are accessible to the administrator. The impact of such an attack is significant.

Given these developments, it is even more important to suitably protect accounts. The Cyber Security Assessment Netherlands 2021 emphasises the importance of sound authentication and shows that the threat level for weak authentication is high.[1]

Table 1 **Threats**.

Threat	**Description of threat in relation to authentication**

[1] National Coordinator for Counterterrorism and Security - Cyber Security Assessment Netherlands 2021

Credential phishing	An attack where the malicious party represents himself/herself as a reliable source to acquire login details. A type of social engineering.
Brute-force attacks	The cracking of login details by attempting all possibilities.
Theft from data leaks	If information is leaked, these data can be used to facilitate automatic login attempts.
Dictionary attacks	A brute-force method for acquiring login details by automatically or otherwise entering commonly used passwords and variations of them.
Social engineering	The acquisition of login details through social relationships or manipulation.
Key logging	Malware that records key presses on the keyboard and thereby acquires login details.

Differences in authentication

Not all types of authentication are equally resistant to the threats mentioned above. For instance, authentication with only a username and password is the least secure of the authentication methods mentioned. This type of authentication is highly susceptible to all threats shown in Table 1. Authentication where a second layer of security is implemented in addition to the traditional username and password significantly increases the security of accounts and systems. When two different categories (something you are, have or know) are used for authentication, this is known as two-factor authentication (2FA).

Not all types of 2FA are the same. Generally, 2FA where an SMS or email containing a one-time code is sent after the username and password have been entered is the least secure type of 2FA. This is because this method provides the opportunity for phishing and what are known as man-in-the-middle attacks. In a man-in-the-middle attack, the malicious party intercepts the traffic between the communicating parties. This traffic can therefore also include the password and the code for the second authentication step.

The use of biometric data as a second security layer is less susceptible to the aforementioned threats but is subject to legislation and regulation relating to privacy, such as the General Data Protection Regulation (GDPR). These measures must therefore be suitable for the organisation. In addition to this, tokens are a more secure type of 2FA. A distinction can be made between software tokens (e.g. a one-time-password (OTP) in an app) and hardware tokens (e.g. a smart card or USB security key). Despite the high level of protection, not all tokens protect against phishing. A standard from the FIDO Alliance, known as FIDO2, is resistant to phishing.[2] Therefore, tokens that implement this standard provide the most comprehensive protection for authentication at this time.

[2] In this factsheet, phishing refers to large-scale bulk phishing. Spear-phishing in combination with DNS hijacking is not considered within the context of this factsheet.

Other factor

Another factor that influences the security of authentication is ease-of-use. Table 2 contains a summary of the various types of authentication, their advantages and disadvantages and an assessment of the user friendliness of the measure.

Table 2 **Type of authentication**

Authentication	**Advantages**	**Disadvantages**
Username and password	Popular with developers.	Susceptible to all threats in Table 1. Not user friendly.
Two-factor authentication with SMS or email	More secure than username and password alone.	Susceptible to man-in-the-middle attacks, phishing and social engineering. Not user friendly.
Biometrics	Strong type of security.	Privacy and ethical issues and/or regulations.
Software tokens	Easy and secure type of authentication, therefore user friendly.	Not totally resistant to phishing. Software tokens can be compromised more easily than hardware tokens.
Hardware tokens	Easy and secure type of authentication, therefore user friendly.	Not totally resistant to phishing. Hardware tokens can be lost.
Phishing-resistant authentication (WebAuthn)	Most secure type of authentication, phishing resistant and user friendly.	If browsers are not up to date, they may not yet support FIDO2. Hardware tokens can be lost.

WebAuthn

FIDO2 is an open standard from the FIDO (Fast Identity Online) alliance. The standard comprises WebAuthn, a WebAPI and the Client to Authenticator Protocol (CTAP). FIDO2 is based on public key cryptography and provides a high level of protection. This is because the login details are unique to each system and can only be used there. This makes the reuse of an intercepted authentication between the user and the legitimate system by a malicious party impossible. The private key does not leave the registered device and is not stored on a server. Private keys can only be leaked individually; this makes possible attacks less scalable. Moreover, because only public keys are leaked in a traditional data leak, there is no danger of misuse. Finally, the stored public key is unique, which means it is untraceable.

The risks

A malicious party can gain access to your accounts and systems through the threats mentioned in Table 1. The risk of unwanted access is higher when less-secure authentication methods are used. The impact of an attack is greater when a legitimate user has authorisation for sensitive information. This is because a malicious party, following a successful attack, has full access to systems with all of the access privileges granted to the account that has been cracked. Some examples of impact are:

- The attacker can steal confidential information.
- The attacker can disrupt your business operations if data are cryptographically encoded and a sum of money has to be paid to regain access. This is known as ransomware. If there are no recent backups that can be restored, there is a high risk of the data being lost forever.
- Even an attack on an account with few access privileges can be used by a malicious party to access sensitive information. After all, the malicious party can use the account with few access privileges to scan for vulnerabilities within a network once again. If this is not detected, they can use these vulnerabilities to get to the desired information.

Advice

Protect your accounts in a manner suitable for the sensitivity of the data and resources they have access to. When doing so, distinguish between different accounts based on the corresponding risk. High-impact accounts (administrator accounts, for example) require a different level of protection to low-impact accounts (guest accounts, for example). Determine the risk to the accounts within your organisation and protect them in a suitable manner. The authentication maturity model can help you determine suitable protection. In general, Level 0 provides insufficient protection.

Mitigating measures

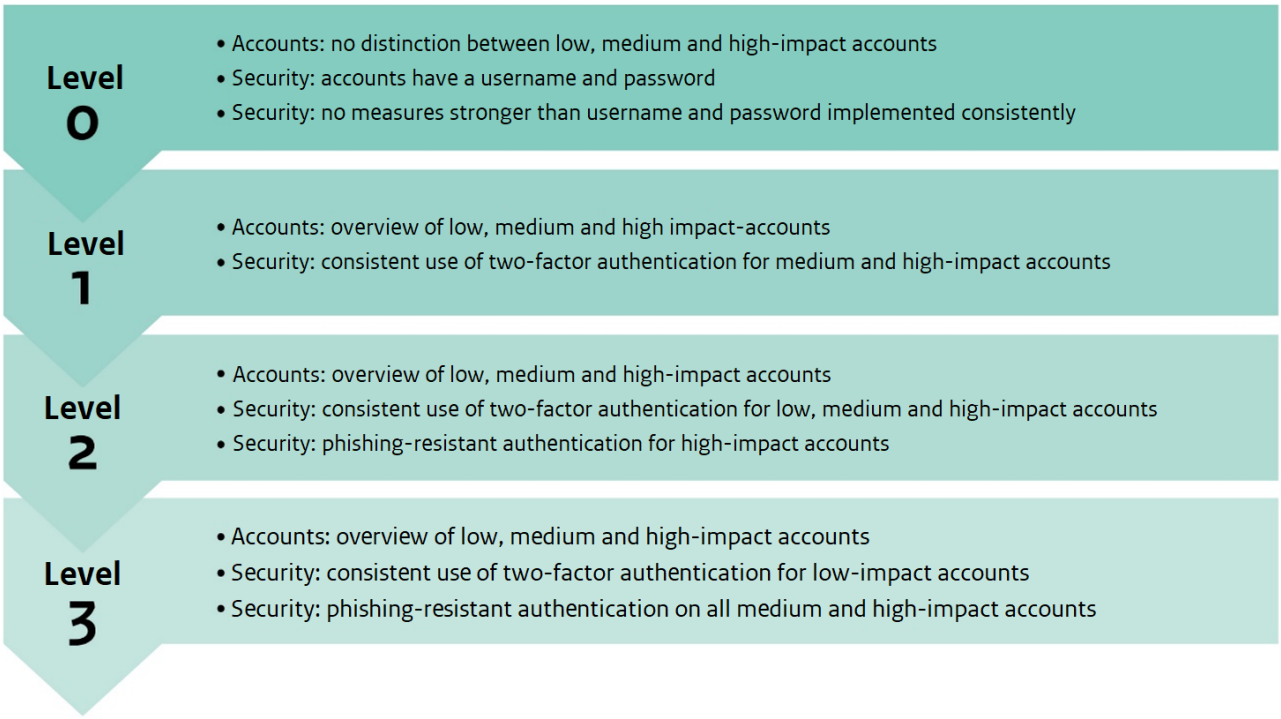
In addition to suitable protection, there are also mitigating measures that you can implement to reduce the risk of unauthorised login attempts. These measures can ensure that an organisation that does not meet all the requirements for a specific maturity level can still temporarily or otherwise obtain a suitable level of resilience.

- Position of your internal and external access points on the network: the position of accounts and systems on the network can change the risk of unauthorised login attempts, so the risk of unauthorised login attempts on the internal network is smaller, for example.
- Monitoring access systems: monitoring access systems means actively seeking out suspicious login attempts. This reduces the risk of an unauthorised login attempt not being detected.[3]
- A maximum permitted number of login attempts per time unit: setting a maximum number of login attempts per time unit reduces the risk of a successful attack; this means there is no need for interaction with the legitimate user (brute-force) and reduces the risk of a Denial-of-Service (DoS) attack. Limit the login attempts for the specific client, not based on the account.

[3] Monitoring is a detection method and therefore does not provide the same degree of protection as implementing the correct authentication method.

The NCSC recommends setting up a suitable level of authentication within your organisation using the authentication maturity model. In addition, mitigating measures reduce the risk and provide additional protection.

Authentication maturity model



Action framework

The NCSC recommends classifying your accounts as low, medium and high-impact accounts based on a risk assessment. You can then start protecting the accounts in a suitable manner using the authentication maturity model. When doing so, a distinction can be made between the implementation of two-factor authentication (2FA) and phishing-resistant authentication. Finally, the NCSC recommends the implementation of supplementary mitigating measures.

Implement two-factor authentication

The precise way in which 2FA can be set up differs per application and system. Ask your administrator if and how 2FA could be implemented. For example, many cloud services such as Google, Outlook and Dropbox provide 2FA. There could also be legal requirements or standards frameworks that make 2FA obligatory for your organisation.

There are a number of other matters that must be taken into account when implementing 2FA. It must be possible to reset 2FA, when a telephone or token is lost, for example. Recovery keys must be stored in a different location to the password.

If your organisation is a public organisation, where DigiD can be used to log in, you must comply with the eIDAS regulation. Finally, your organisation must abide by privacy regulations when implementing a security measure for which personal data are processed.

Implement phishing-resistant authentication

Despite the standard not yet being widespread, the number of FIDO-compatible platforms and browsers is growing quickly. An overview of the browsers and platforms that support FIDO2 can be found on the FIDO Alliance website.[4] You can use FIDO2 in applications in Google Chrome, Microsoft Edge and Windows 10, among others. You can check how to get FIDO2 up and running on the FIDO Alliance website.[5]

Implement supplementary measures

Set up monitoring and logging. Monitoring and logging are used to detect unusual activity. See our factsheet 'Building a SOC, start small'.[6]

Draw up an overview of the internal and external access points on your network, so that you know where the risk of unauthorised login attempts is highest. This is generally the external access points in your network. Nevertheless, there is always a risk on your internal network, from disaffected employees, for example.

Moreover, set a maximum number of permitted login attempts per time unit for all clients. In addition, it is also desirable for employees to have insight into their log-in history. This allows suspicious activities to be detected and reported more quickly.

[4] FIDO2: Web Authentication (WebAuthn) – FIDO Alliance

[5] Implementation & Deployment – Getting FIDO up & running (fidoalliance.org)

[6] Factsheet Building a SOC: start small | Factsheet | National Cyber Security Centre (ncsc.nl)

Publication
National Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague, The Netherlands
Turfmarkt 147, 2511 DP The Hague, The Netherlands
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

April 2022