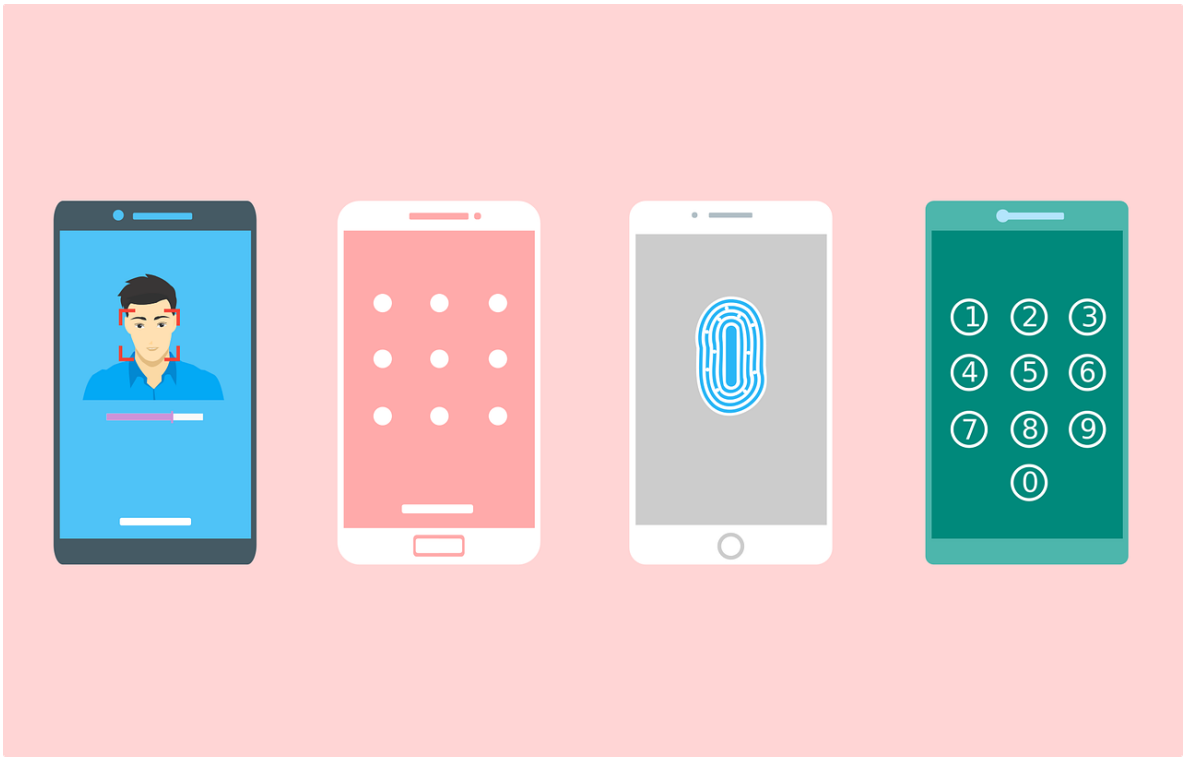
GUIDANCE

Multi-factor authentication for online services

Advice for organisations on implementing multi-factor authentication (or two-factor authentication) to protect against password guessing and theft on online services.

28 November 2019



This guidance describes how to use multi-factor authentication (MFA) to mitigate against password guessing and theft, including brute force attacks. MFA can also be called two-step verification or 2-factor authentication (2FA).

- This guidance is primarily for senior decision makers in larger organisations, and administrators responsible for configuring access to online and enterprise services that requires users to authenticate to the service.
- Information about implementing 2FA on personal accounts is covered in separate guidance.
- This guidance does not cover authentication to devices, which can be found in the End User Devices Guidance.

Introduction

Enterprise services have historically used a password to authenticate a user to services hosted on the enterprise's internal network. Enterprises are now using more services that are directly connected to the Internet, to enable collaboration, to make remote working easier, or to benefit from shared services. The services themselves are commonly hosted in the cloud, or may allow remote connectivity to on-premise services that would previously have only been accessible from an organisation's internal network. In both cases, authentication becomes the main decision point for whether a user or attacker can gain access to a service.

In recent attacks, adversaries have logged in to services using guessed or stolen passwords, thus granting that attacker the same permissions (sometimes privileged access) as the legitimate user. This is prevalent when there is no way to differentiate between the actual user and an attacker pretending to be them. These attacks work in a number of ways including:

- Trying passwords from leaked datasets in case a user has reused a password on other services.
- Socially engineering account details from users using techniques such as phishing.
- Attempting to log into multiple user accounts using one of the passwords on the commonly used password lists. This is known as password spraying and works on the assumption that some users will have chosen passwords on those lists. Even if an account automatically locks after a number of failed attempts, by trying multiple user accounts, statistically an attacker will still be able to break into a few. It has the advantage of being less obvious to monitoring than a brute force attack ,where multiple passwords are tried against a single account.

The NCSC password guidance describes these issues in more detail and gives advice for users and administrators needing to cope with an ever-increasing number of passwords.

When to use an extra factor

As long as passwords are used for authentication, there will always be a chance that users and administrators will choose machine-guessable passwords and be susceptible to social engineering. Therefore:

- Organisations should choose Cloud and Internet-connected services that offer a form of multi-factor authentication.
- All users, including administrators, should use multi-factor authentication when using Cloud and Internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data.
- Administrators should, wherever possible, be required to use multi-factor authentication.
- Organisations should consider carefully the use of services which only allow for single-factor authentication.

The service will need to check the extra factor whenever there is a need to authenticate a user. The exact implementation will vary per-service. Common implementations include:

- The user needs an extra authentication factor when they are logging on to a service using a device that they have not used before. The service tracks devices previously used and so will not need the extra factor every time. It may be necessary to opt in to the service remembering the device by selecting a 'remember my device' option.
- The user needs an extra authentication factor every time they log on to a service. This is more usual for services that have a higher impact if they're compromised, such as an email account or online

banking.

- The user needs to re-verify themselves using an extra factor when performing high risk actions - such as changing a password or transferring money.
- The user is prompted to use their extra authentication factor when the authentication has been determined to be high risk, such as the connection coming from a different part of the world than is normal for that user.

Choosing extra authentication factors

Your choice of extra factor will vary depending on the service you are using, because the service might not support your first choice. Enterprises should consider a single sign-on (SSO) solution to give the best user experience. A multi-factor token will then usually only be needed to register a new device. On personal devices, or in bring your own device (BYOD) scenarios where SSO is unavailable, you should consider using the techniques that have the best user experience.

Using a managed/enterprise device as an extra factor +

Using an app on a trusted device as an extra factor +

Using a physically separate extra factor +

Using a known or trusted account as an extra factor +

Using another piece of knowledge as an extra factor +

Additional considerations

The introduction of multi-factor authentication to online services may require your IT helpdesk to offer extra services to support users. If users lose their extra factor, they will need a way of reporting and replacing it. This could be offered directly by the service or via an enterprise portal. You will need to consider how your account reset and multi-factor token replacement processes verify that the user is who they say they are. You will need to ensure that an attacker cannot use these processes to bypass multi-factor authentication.
You will need to consider how administrators can gain access to the service if multi-factor authentication is unavailable. This could be caused by a service configuration or the loss of an authentication token. Accounts such as an emergency or 'break glass' account that use a single authentication factor should be the subject of increased protective monitoring so that its misuse can be easily detected.

Defence in depth

Authentication requests should report successful and unsuccessful authentication requests to enterprise audit and monitoring systems. This allows the monitoring system to highlight unusual activity and contribute to a log of malicious activity post-breach. Services that email the user when they log in

are an effective way of detecting unauthorised authentications, but only if the user has a route to report unexpected emails.

Some online services adjust authentication requirements based on things such as the physical location associated with the connecting IP address, whether a connection comes from a higher risk network such as Tor or deviations from a user's normal usage patterns. A service may choose to force multi-factor authentication when the risk is deemed too high, or block authentication entirely. These approaches can reduce the success rate of brute force attacks however are most effective when used alongside multi-factor authentication.

PUBLISHED
14 June 2018

REVIEWED
3 December 2018

VERSION
1.0

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector