2 Factor Auth Explained

Author	josh
Date	2021-12-05

Overview

In modern security, we've found that passwords just aren't enough. With the ubiquity of data breaches and terribly insecure passwords, the addition of a second factor has become commonplace. 2 factor authentication adds a second layer to the process of logging into an application, meaning yet another layer an attacker must break in order to compromise a user's account. Let's discuss why 2 factor auth exists, and the different types you may see.

2FA Why and How

What is 2 factor authentication?

The most common type of authentication most of us encounter is the *password*. This is a secret phrase that we're required to type in or copy in when authenticating to some application. But what actually is a password? We call a password (or preferably a passphrase) "*something you know*". This is a phrase that only the user is supposed to be aware of – a *secret*. But with data breaches and password cracking capabilities, the reality is that attackers can often find out your password and use it to masquerade as you – since they now have the secret too!

The second factor we use such as a phone authenticator app or hardware security key becomes "*something you have*", adding an additional layer of security! This isn't another password, but rather a stored secret used to generate one-time-passwords on a rotating basis. This now means that an attacker has to compromise the *something you know* (your password) **and** *something you have* such as your phone or token, which is a much more difficult task. There are ways of compromising 2FA as well, but this additional authentication makes compromise harder for attackers, thus increasing security for end users.

Common Types of 2FA

Most Secure → Least Secure

Hardware Security Key (ex: Yubikey)

The most secure type of 2FA as of this writing is considered to be the hardware security key, such as a Yubikey. This is a USB device that stores a secret for that device that cannot be read of the device. You then plug it into your PC and simply press a button when authenticating to a website.

This is considered the most secure as it requires physically stealing the device to compromise 2FA, as secrets cannot be read by malware from a hardware token. They are also, in my opinion, the easiest to use! No typing in rotating one-time-passwords, simply have the device on hand.

Authenticator App (ex: Microsoft Authenticator, Google Authenticator)

The most common type of 2FA that is also strong and secure is the use of an Authenticator app such as Microsoft Authenticator, Google Authenticator, Duo, etc. For this type of 2FA, the user scans a secret using their phone when applying 2FA with the application. That secret is securely stored, and used to generate rotating one-time-passwords that the user enters when authenticating. For example, you visit your email account, enter your password, then enter a 2FA code from your phone to complete the login.

This type of 2FA is considered secure, as secrets are kept on your phone device encrypted and the one-time-passwords are not sent anywhere in plain text. This is slightly less secure than hardware keys as some form of malware or implementation issue could potentially leak the secret stored on your general-purpose phone, whereas they cannot be read from a hardware key like a Yubikey (only the one-time-passwords generated).

SMS or Email

This is the least secure type of 2 factor auth and should not be used. For this type of 2FA, the application sends you a one-time-password from the server via text message or email, and you enter that code alongside your password. It is similar to authenticator app 2FA in that regard.

However, this implementation has several flaws. First off, the passwords are sent over plain-text insecure mediums such as email or SMS text message. These codes could be intercepted by an attacker. The most common form of intercept (especially in the world of cryptocurrency) is called the *sim swap attack.* For this, the attacker socially engineers the phone company into porting your phone number to their account. Since they now control the phone number, they use the password reset feature on a website to gain access to the account (since they can receive the 2FA text message codes required). Millions of dollars worth of cryptocurrencies have been stolen using this attack – it is a very real threat.

Enable 2FA!

2 factor authentication is simple to set up and use, so use it! This provides an extra layer of security in case your passwords are compromised, and should be enabled for every website and application you can. Using a hardware key especially is secure and easy to use, with authenticator app as a solid option as well. Avoid SMS or email based 2FA unless absolutely required by a website. If you're not already, use 2FA and make sure you're generating strong passphrases and using a password manager. Preventing account takeovers is much, much better than recovering from attacks when it is too late.