Blog

The Ultimate Authentication Playbook

Jack Shepherd
Manager, Content Marketing

February 5, 2019

With the rise of of credential stuffing and similar attack methods, simple username and password authentication is not enough to deter bad actors. According to the Verizon Data Breach Investigations Report, there were over **55,000 security incidents and 2,200 confirmed data breaches in 2018**, with a whopping **81% of those incidents being tied to stolen or weak passwords.**

With the proliferation of data breaches and loss of consumer trust, enterprises must take a second look at the security posture of their web applications, starting with an exploration of more secure authentication methods.

In this post, I will break down some of the most common authentication methods we see today, as well as some tips on how to best implement them.

Authentication vs Authorization

To be clear, when we talk about authentication, we are talking about the act of verifying an identity —making sure users are who they say they are. The most basic form of authentication is using a username and password to log in to your account.

Very crudely speaking, in terms of web apps, **authentication** is when the system checks login credentials to see if it recognizes a user, and confirm that they should be logged in. Whereas **authorization** is when the system looks up within the access control permissions whether or not to allow the user to view, edit, delete or create content.

	Authentication	Authorization
Meaning	"Are you allowed to *access* X app?"	"What are you allowed to *modify* in X app?"
Methods	Password, 2FA, MFA, X509 Certificates, Biometric authenticators, WebAuthN	Access control for URI, Access control lists etc.

Now that that's cleared up...

What are the different types of authentication methods?

Single Factor Authentication

Also known as primary authentication, this is the simplest and most common form of authentication. Single Factor Authentication requires, of course, only one authentication method such as a password, security pin, PIV card, etc. to grant access to a system or service.

While these methods score high on usability and familiarity, they are typically associated with poor security and can be easily guessed or stolen via data breaches, phishing or using keyloggers.

2nd Factor Authentication

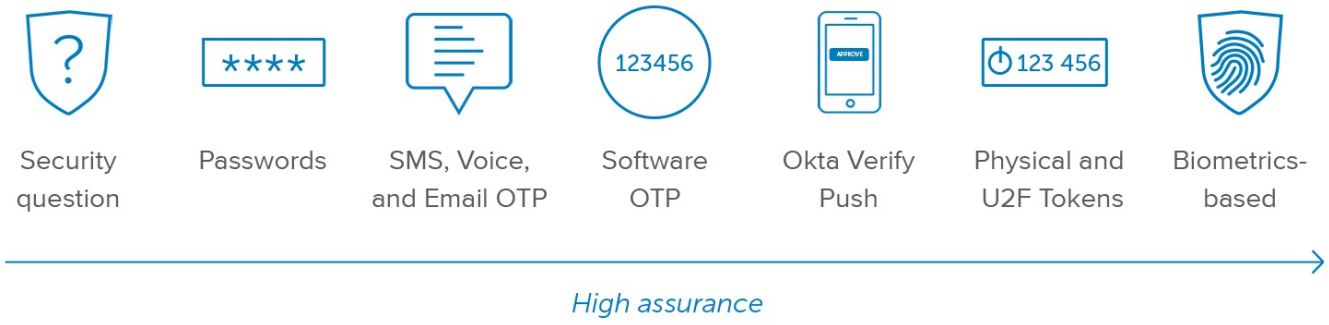
Adding a layer of complexity, 2FA requires a second factor to verify a user's identity. Common examples include tokens generated by a registered device, One Time Passwords, or PIN numbers. The mere presence of two authentication metho i ificantly– in fact, according to research from Symantec, **80% of**

users, noting that >10% of users who tried 2FA, failed to enter the SMS code correctly.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is the most sophisticated authentication method that leverages 2 or more independent factors to grant user access to a system. In typical scenarios, MFA methods leverage at least 2 or 3 of the following categories.

1. **Something you know** - a password or a pin
2. **Something you have** - mobile phone or a security token
3. **Something you are** - fingerprint or FaceID
4. **Something you do** - typing speed, locational information etc.



Authentication Method Protocols

Authentication methods that leverage usernames/passwords and/or multi-factor are generally considered secure. But there are authentication scenarios that break the bidirectional model of authentication.

One common example is when you access a third p e service (either from a mobile device, another website, or desktop app). For example, when linking

surface and makes a user vulnerable to credential breach attacks.

There are several authentication protocols you can implement to prevent yourself from exposing your user data to attackers, including Oauth, OpenID, SAML and FIDO.

What about API Authentication?

In the age of the API economy, API's handle large volumes of data and add a new dimension to the security surface of an online service. While there are many API authentication methods, most of them can be categorized within one of three methods:

HTTP Basic Auth

Using this approach, a user agent simply provides a username and password to prove their authentication. This approach does not require cookies, session ID's, or login pages because it leverages the HTTP header itself. While simple to use, this method of authentication is vulnerable to attacks that could capture the user's credentials in transit.

API Keys

An API key is an identifier meant to identify the origin of web service requests (or similar types of requests). A key is generated the first time a user attempts to gain authorized access to a system through registration. From there, the API key becomes associated with a secret token, and is submitted alongside requests going forward. When the user attempts to re-enter the system, their unique key is used to prove that they're the same user as before. This API Authentication Method is very fast and reliable, but is frequently misused. More importantly, this method of authentication is not a method of authorization.

OAuth

Oauth is one of the most secure methods of API aut
and authorization. OAuth allows the API to authenticate by establishing scope, and can access the

Making authentication more about the user and less about the attacker

The authentication game is changing, big time. Biometric authenticators that are built into user devices such as FaceID, TouchID or Windows Hello will continue to shape how users authenticate into online services.

Forward-looking businesses will look beyond passwords and improve API authentication as a means of enhancing the user experience, reducing the success rates of phishing attacks. Attackers will no longer benefit from the weaknesses of passwords by incorporating more secure authentication methods.

To learn more on how Okta can help you deliver on the promise of better and secure authentication experience authentication page around Customer Identity.

Jack Shepherd

Manager, Content Marketing

Jack Shepherd has worked in multiple roles within the identity space for 3+ years. Now the Content Marketing Manager for all things Security, Jack is responsible for providing unique insight into the latest trends in cybersecurity and access management.

Follow Jack Shepherd

Tags

security, Multi-Factor Authentication, 2FA

JANUARY 4, 2021

Okta for Good's Nonprofit Technology Initiative: Announcing $1M+ Grant Round

By **Erin Baudo Felter**

As we kick off the new year, Okta for Good's mission to strengthen the connections between people, technology, and community has never been more critical. In...

Read now ›

okta

It's time to move on from Active Directory.

Okta Integration Network

Platform Services

Privacy Policy Security FAQ Sitemap Visit our Developer Site

United Kingdom

France

Germany

Japan

Hey there! Back again to check us out? Things must be getting serious!