WHITE PAPER

Keep Calm and Authenticate: Why Adaptive is the Next Best Thing

By Tharindu Bandara, Thiyagarajah Abilashini

October 2018

Table of Contents

1. Introduction

Authentication is the process of recognizing a user's identity in order to provide access to any sensitive resource. In the history of identity and access management (IAM), we have come across different authentication mechanisms that have evolved rapidly in terms of security. This white paper will discuss the evolution of authentication mechanisms and the advantages and disadvantages of each, why we need a better mechanism to ensure great user experiences without compromising on security, and how adaptive authentication is a good solution.

2. Evolution of Authentication

At the dawn of authentication systems, single-factor authentication (SFA) was the most widely adopted mechanism because of its simplicity and user-friendliness. However, this meant that it was also the weakest level of authentication. Passwords used by users weren't secure and could easily be hacked. A brute force attack, dictionary attack, man-in-the-middle attack or any other common method of password hijacking can easily impersonate a user and gain access to protected resources or services. In fact, according to Verizon's 2017 Data Breach Investigations Report, about 81% confirmed data breaches involve weaker, default or stolen passwords.

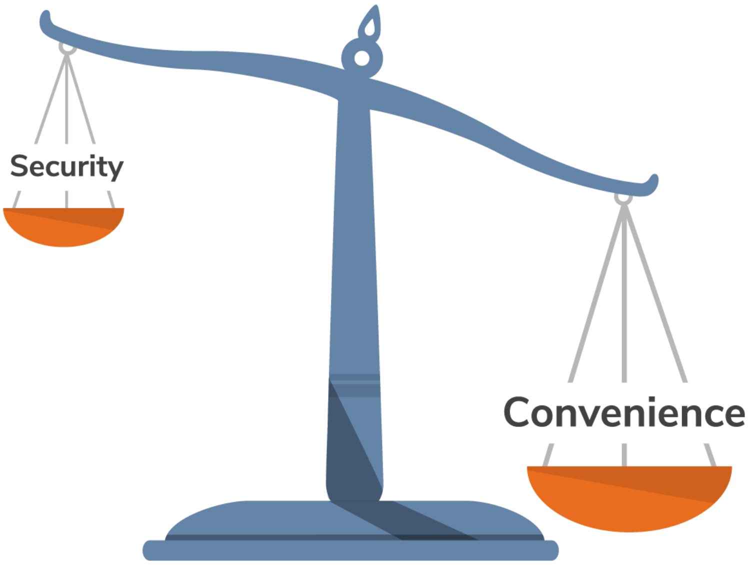

Figure 1

The increased number of such security threats led to the understanding that a single factor for authentication does not provide adequate protection. Hence, multi-factor authentication (MFA) was introduced with three factors of knowledge to bring enhanced security levels in the authentication process.

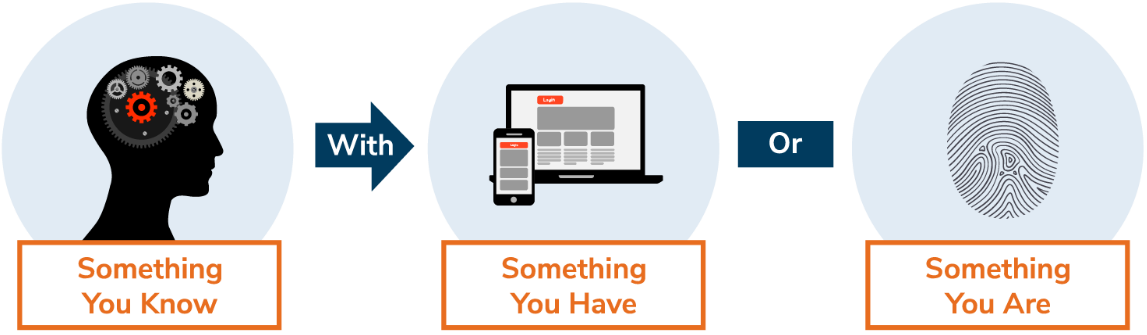

Figure 2

Simply put, the three knowledge factors of MFA are:

- **What you know:** This refers to something that only you would know. Most commonly this factor is the user's password. But it can also be in other forms like a PIN code, as in the case of an ATM transaction.
- **What you have:** This refers to a specific item which is in the possession of the user. In the authentication process, the user will confirm their identity by SMS, typing a unique code generated from a physical token, or inserting a smart card.
- **What you are:** This refers to a biometric confirmation. This usually involves a fingerprint scan, a facial recognition or a retinal scan.

Figure 3

The level of security provided by MFA has made it the best way to authenticate in the modern world. Given that one of the factors is compromised by an attacker, it is highly unlikely that all the other factors are also compromised.

Because of the better identity assurance, organizations quickly adopted MFA into their authentication systems. As of today, MFA appears in digitized organizations in various forms. This includes various combinations of knowledge factors and applying strict conditions for selecting knowledge factors as in the case of strong authentication. However, MFA is a static authentication flow. Even though it provides a strong foundation of security, it is bounded by its static nature.

The entire world is becoming more digitized and the balance between user convenience and security is more important than ever. The nature of modern attack strategies is also becoming more complex. Therefore modern authentication mechanisms can no longer be static.

3. Problems with MFA

Although MFA is a strong way of authenticating users, there are several problems with it. The security level for a specific application should depend on the user type and the resource they are trying to access. But in static authentication mechanisms like MFA, every user needs to go through the same set of authentication steps no matter what resources they are accessing and from where. An average user will find it hard to integrate multiple factors such as a token generator or fingerprint scanner to get authenticated to a simple application. In these cases MFA's high security hinders usability. For example, security for administrators that have privileged access should be strong, but a general user browsing information on a site shouldn't require such strong authentication.

3.1 The Balance Between Security and Convenience

When talking about authentication, we should consider the required security level as well as the convenience of the user who needs to be authenticated. Strong authentication mechanisms compromise the convenience of common users and basic authentication compromises security. So it's always hard to achieve the balance between security and convenience with current authentication mechanisms.

Figure 4

3.2 Vulnerability to Attacks

Security has evolved into newer, stronger mechanisms because attackers find a way to break into systems that use mechanisms that are popular and last for a long period. So having a constrained authentication mechanism such as MFA, which is now popular and has been in use for a long time, will not prevent the system from being attacked even if multiple steps are introduced.

Let’s think about a situation where a user logs into an application with MFA in a public device and forgets to log out. Anyone who gets access to the device later will be able to access the logged in session of the previous user. In this case, we can see that even strong authentication is not enough to secure a resource.

3.3 Security Based on Device Types

Today, users access applications using different device types like desktop, laptop, and mobile devices. Static authentication mechanisms expect the user to go through the same authentication steps despite the device they use. In the perspective of the user, they might feel more secure when accessing an application through their mobile phone, which is rarely or never used by someone else. So the user would prefer not to go through multiple steps when authenticated from his personal device.

3.4 Static Authentication Flow

What happens if a user provides the wrong credentials multiple times during authentication? With a static authentication mechanism, the user will most likely get blocked and asked to reset the password after confirming his identity. But imagine a situation where the identity provider avoids the account from being compromised by linking user behaviors to make authentication decisions. By doing so, the user will be provided with another way to be authenticated without his account getting blocked.

Figure 5

Can we get rid of the above-mentioned problems with a static authentication mechanism? Will it be possible to build an MFA mechanism that changes depending on the user type, context, user behavior or any other factor? With current static authentication mechanisms, this is impossible or highly complex to build and manage.

Then how can we achieve such an authentication mechanism that won't compromise on security or user convenience? That's where adaptive authentication comes in.

4. What is Adaptive Authentication?

Adaptive authentication is the ability to switch the authentication flow based on the context. This shouldn't be misunderstood as a completely different mechanism that replaces MFA. Adaptive authentication orchestrates different authenticators based on the context during the user authentication process. The best part is that most times users won't even know that the authentication process has changed. Adaptive authentication intelligently takes various factors in the current authentication process context and provides the authentication flow to the user.

Therefore adaptive authentication can also be seen as a set of MFA methods where for each authentication context an MFA method is selected from the set and presented to the user to preserve an optimum balance between security and convenience.

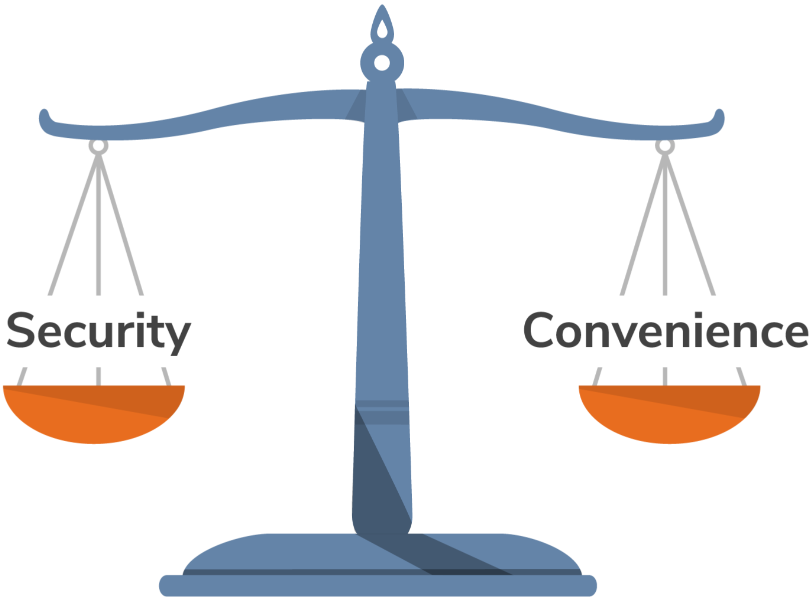

Figure 6

Now we have understood the basic concept behind adaptive authentication and can see that it allows us to overcome all the limitations of static MFA. This is achieved via the authentication context. An authentication context can be based on factors like device type, geolocation, identity attributes, user behavior, and risk.

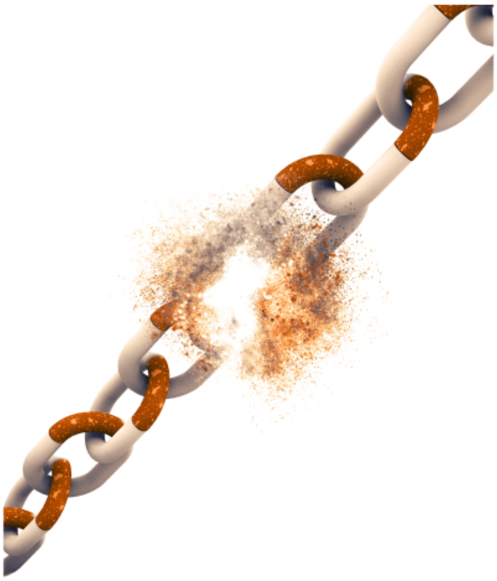

Figure 7

All of the above factors can create a different context for the authentication process. Adaptive authentication can increase or decrease security based on the context. For example, if a user logs in from a risky or unusual context, more authentication steps will be presented. On the other hand, fewer steps like a simple username-password authentication process might be presented to a more trusted context. This achieves the same levels of security that MFA provides with maximum user convenience. This dynamic behavior makes adaptive authentication unbound by any limitation as opposed to static authentication flows, allowing it to move back and forth between security and user convenience as required.

5. Why Adaptive Authentication is the Next Big Thing

Adaptive authentication can replace almost all of the available authentication scenarios without compromising the level of security, making it the most promising replacement for modern authentication scenarios.

Adaptive authentication can be applied to many real-world use cases based on several major categories including environment, device, attribute, behavior, and risk. There are some interesting use cases that exist for adaptive authentication in each of these categories.

5.1 Geolocation

Geolocation based authentication is an important authentication scenario that a typical user faces. For example, a credit card transaction is performed on behalf of a user and requires authentication. Geolocation based adaptive authentication is configured for this specific use case. The location details for the user are collected by either their IP address, GPS coordinates or triangulating cellular signals (collected from the user’s personal mobile phone). This data will be processed against the location provided by the credit card transaction. If a suspicious geolocation comparison is evaluated, adaptive authentication will use the user’s phone for additional authentication to reduce the risk of a potential credit card scam.

Figure 8

5.2 Device Types

In the modern world, a typical user would use several devices for authentication. Therefore a stolen device is a potential security threat in any authentication process based on that device. In this use case, device-based adaptive authentication can be applied in the following manner. Once configured, adaptive authentication will check whether the device is a stolen device using the information given prior to the authentication. The authentication process can be immediately terminated for a stolen device. Device-based authentication can also be applied to tighten the security for a new device that logs in to ensure reduced risk of potential security threats as well.

5.3 Attributes

In a corporation, there are levels of users that are differentiated by attributes. Not all of them are required to have the same authentication flow. This is a good use case where we can apply attribute-based adaptive authentication. During the authentication process, user attributes can be checked and simpler authentication steps can be provided for a general user like a cashier in a shop. For an administrator, authorization levels are higher. In this case, more security steps can be provided.

5.4 Behavior

An important factor in an authentication flow of a user is the behavior pattern. A typical user usually follows a login pattern where they log in at certain times. In use cases like this, behavior-based adaptive authentication can be applied. During the authentication, user login times will be monitored and compared with past login information. If an unusual behavior is detected, the user will be provided with additional authentication steps to increase the security level. Behavior-based adaptive authentication can also be used for geo velocity based scenarios as well. If a user logs in from Sri Lanka at a particular time and another login request occurs from London after a few minutes, the authentication process will monitor this unusual behavior and responds with additional security steps.

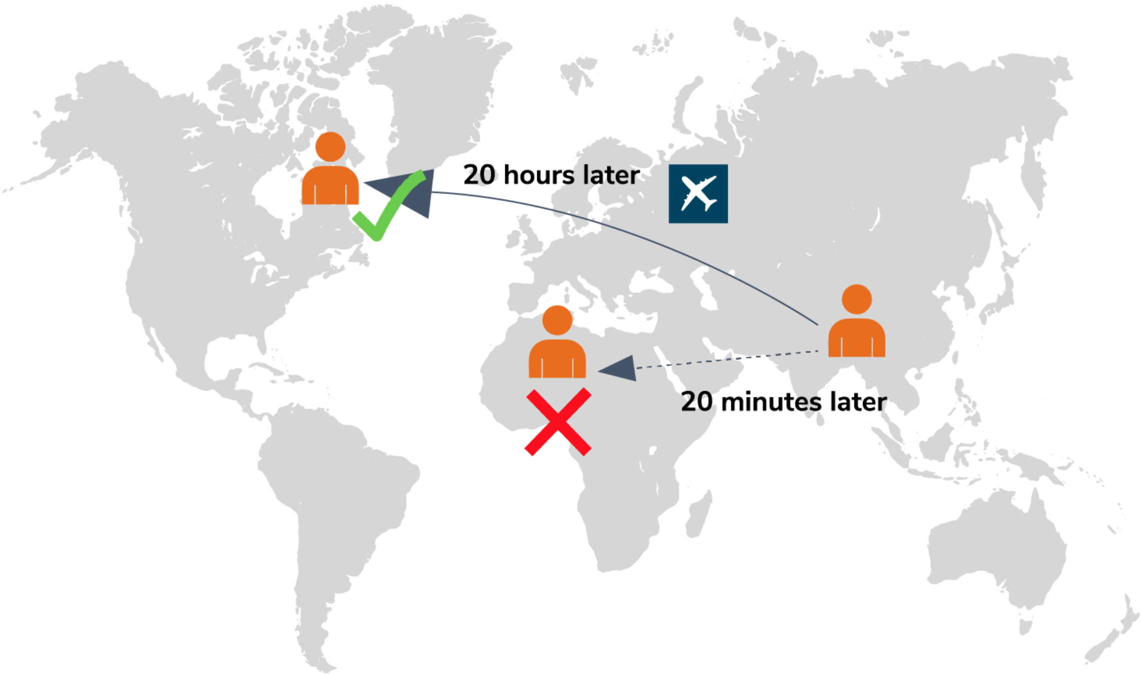

Figure 9

5.5 Risk

There is one more important scenario to look at. The risk of a certain authentication request can be calculated from facts like outputs from risk calculating algorithms, criticality of a system and firewall status of a device. In a case like this, risk-based adaptive authentication can be used with certain methods to calculate a risk score and provide additional security steps based on that value as necessary.

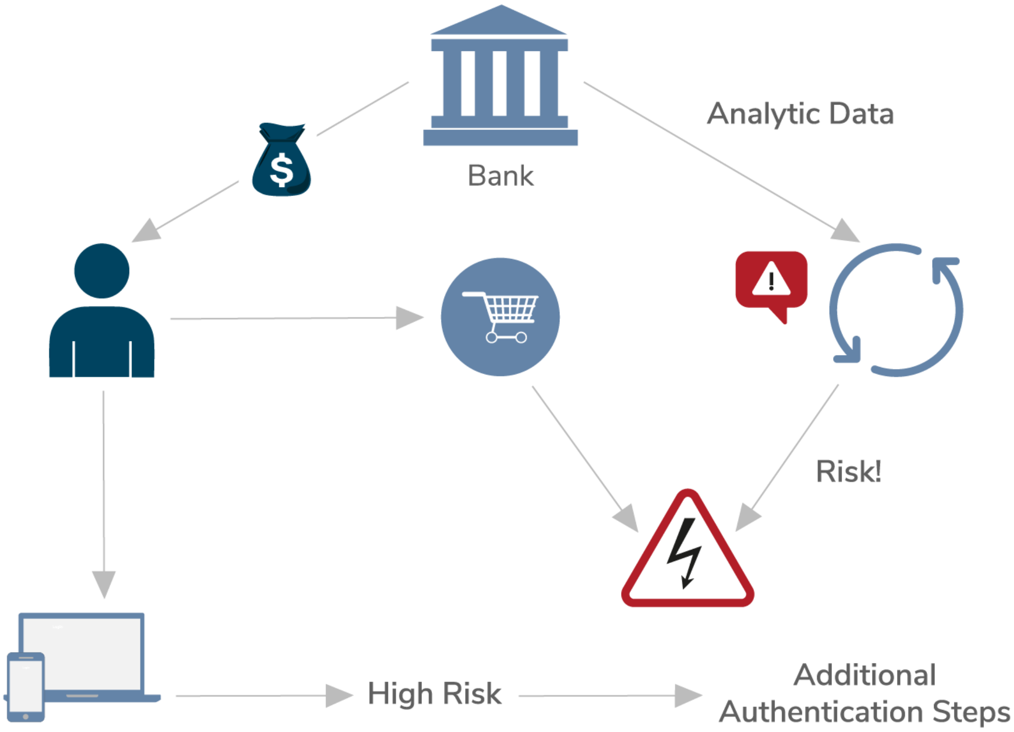

Figure 10

6. Conclusion

Adaptive authentication is a dynamic authentication mechanism that makes changes the level of security using a range of factors such as user behavior, geolocation, device type, and risk. Depending on the resource and user, the complexity of the authentication is adjusted without the knowledge of the user. It resolves all most every problem we face with strong authentication. Adaptive authentication strikes the perfect balance between security and convenience.

The highly extensible and open source WSO2 Identity Server is equipped to provide adaptive authentication. Learn more >