The Hacker's Waterloo: Adaptive Authentication

Adaptive Authentication is a new buzzword in cybersecurity today. Various IAM companies are now offering solutions which perform risk-based authentication and authorization. It is a next-generation technology that oozes smartness.

Before we get into what it is, let us first explain what the different possibilities for authorization are. It is important.

There are three broad categories into which an authorization mechanism can fall.

- What You Know
- What You Have
- What You Are

Here's a breakdown on each:

What You Know: These are things you have in your mind and can remember. They consist of information. Your username, password, PINs, secret questions and answers (called challenge-response questions), are all examples of What You Know.

What You Have: These are things that you physically possess. If you own a smartphone, it can be linked to your account in an Identity Management system. SMS or Phone Call based One-Time-Passwords (OTPs) can then be used to check whether the right person is trying to sign in. You may also have received a hardware device from your employer that displays a new access code every time it is needed (Hardware Token).

What You Are: Technology has progressed to this final frontier of access management only very recently. Your retinal scan, thumbprint, facial features, and behavioral

biometrics are all biomarkers of What or Who You Are. These can now be used as the most powerful way to protect your identity within an Identity and Access Management System.

The traditional technology for a higher degree of authentication than simple credentials is called Multi-Factor Authentication (MFA). It uses multiple levels of authentication that include 2 or more authorization mechanisms to authenticate a login attempt. This may be a combination such as a password plus an SMS OTP or any other combination. Over time, the use of this authentication has revealed some shortcomings.

Firstly, one of your physical factors can get lost or be stolen. If you lose your phone or hardware token, you are simply locked out of the systems that you need to access until you get a new phone and sim or hardware token. You may forget one or more of your What You Know credentials such as your PIN or password. Reset and recovery here is a much longer and more complex process than with simple credentials based authentication.

Secondly, MFA provides a certain degree of a false sense of security. Let’s say you lose a factor. Resetting it will utilize some other, perhaps less secure factor. So, the actual level of security at this point is not as tight as it might seem on the surface.

Thirdly, and perhaps the biggest shortcoming of MFA, is that it is not adaptive. It utilizes no intelligence to protect user identities, but instead doubles up on brute-force security. The issue with this is that there is no intuition acting to determine the legitimacy of an access attempt. All that someone needs to log into your account is the information you know or one of your hardware tokens.

Spy movies aside, the truth is that Biometric authentication, at the moment, is very secure. Hackers are never very far behind though, and it is only a matter of time before they devise ways to compromise.

Hackers (called bad actors) are no longer relying on brute force to crack credentials (see our article Identity as the New Attack Surface.) They are utilizing intelligence. The attempts of solutions to protect identities needs to also be intelligent and adaptive.

Adaptive Authentication does just that. It uses authentication mechanisms such as What You Know, What You Have, and Who You are, but does far more than that.

Here, a whole host of intelligent processes determine if a user is actually who he says he is, and blocks or grants accesses based on what it finds. It also increases or decreases the number and type of factors required for a login based on the risk-assessment that it performs for a particular login attempt.

Adaptive Authentication is the organic evolution of intelligence. Since a hacker is only as good as he is smart, it levels the playing field – permanently. New techniques for Adaptive Authentication may be invented, but the playing field will always remain at this level. As such, it is the final frontier in the defense of identities.

Today, Adaptive Authentication from various vendors feature a whole host of intelligent processes.

Here are a few of them:

1) This isn't the correct device: At a simple level, Adaptive Authentication solutions respond to the device that a login is attempted from. A device with a familiar MAC address, or even with familiar OS and software configurations, will be granted access more readily than one that is different or new.

2) The IP address is suspect: The IP address of the user is put through the wringer to reveal anomalies and cross referenced with black-listed IPs to prevent bad actors from stealing an identity.

3) Behavioral biometrics. Now, we can capture and analyze patterns in the keystrokes and mouse gestures of a user, and use it to protect their identity. This is a groundbreaking feature that provides a very high level of biometric protection.

4) This isn't a known location: If an access attempt is made from a location where an organization has no known employees, contractors, partners or customers, login is denied or stepped up far up the ladder in the MFA scheme.

These examples give a good idea of the way in which intelligence can be imparted to our systems and processes to bolster the security of our identities in this hacker-happy world. It is not the specifics of the examples themselves that matter, but the realization that we can use our own intelligence to protect ourselves. With Adaptive Authentication,

hackers are no longer one step ahead of us. The field is finally level, and our protection finally matches and can adapt to the threats issued.