Multi-Factor Authentication is Becoming a Fundamental Security Necessity

Summary
Authentication is a cornerstone of cybersecurity; it is the means of verifying and individual is who they claim to be. However, attacks on traditional authentication methods like usernames and passwords have ramped up significantly in recent years. This sad reality is a direct result of the growing number of data breaches that have taken place, leaking entire databases of user credentials into the wild for hackers to use at their leisure. As a result, additional authentication practices have begun to be implemented that provide additional challenges for hackers. These methods combine multiple forms of authentication, hence the moniker Multi-Factor Authentication (MFA). Unfortunately, as these solutions have become more popular, they’ve entered the crosshairs of data thieves. While not an enterprise authentication panacea, MFA is an essential component for any organization’s security strategy.

The War for Authentication

There is a holy trinity that comprises cybersecurity, known as the CIA triad. Confidentiality, integrity, and availability provide the foundations of information security as we know it. Confidentiality is the act of ensuring only authorized individuals can view protected data. Integrity prevents data from being altered in any way by unauthorized individuals, ensuring the information remains legitimate. Lastly, availability ensures that authorized users have uninterrupted access to the respective data at all times. While copious research has been written on all three areas, in brief, effective cybersecurity demands that all three of these factors work together in unison to ensure comprehensive data protection.

One subcategory of confidentiality is user identification. In the digital world, identification traditionally takes the form of a username or email address that tells the respective service who the user claims to be. However, in the digital world (as well as the physical world) identities are regularly shared through various interactions. The frequency of identity sharing, as well as the propensity for adversaries to employ fraudulent identities, introduces the need for additional steps to validate the identity being offered by a user. Authentication is the means by which an individual’s identity is effectively verified and validated.

Authentication mechanisms have traditionally surrounded four primary factors: knowledge (something you know), possession (something you have), inherence (something you are), and location (somewhere you are). One of the most widely used methods of knowledge authentication would be a password, created by the user, that is ultimately tied to the given username. Unfortunately, due to countless information breaches over the last decade, entire databases of these paired credentials have been stolen and shared by data thieves. With both the username (identity) and password (knowledge authentication) for a user in hand, the hackers can now access a user’s respective accounts uninhibited.
Multi-Factor Authentication (MFA) Solutions

In response to the frequency by which credentials are stolen by data thieves, more robust authentication measures have been introduced in recent years, including Multi-Factor Authentication (MFA). MFA is an additional form of authentication that requires more than one validation method be used before an identity is verified. This means that a user will not be granted access by simply providing his or her identity and knowledge authentication information; the user must also verify possession, inherence, or location in addition to knowledge.

Inherent authentication is being utilized with greater frequency, as it provides additional security while placing the fewest requirements on the user. Some of the most prevalent examples of inherent authentication solutions are biometric in nature. These technologies allow users to authenticate themselves through unique physical characteristics like fingerprints, facial scans, voice recognition, eye scans, etc. While these technologies are not without their own challenges (such as accommodating physical changes in the users), when used in conjunction with another authentication factor, information security is significantly bolstered.

Like all other authentication methods, possession authentication can take several forms, including both digital and physical. Physical devices such as RFID cards and security tokens can be used to limit access to only those individuals who have these devices in their possession. Digital examples can include software applications that generate a one-time-password (OTP) that expire and change in mere seconds. Additionally, text messages with a OTP can be sent to a user’s mobile phone; the user then has a limited time to provide it for authentication.

Location authentication is a relatively new method that seeks to validate an individual’s identity through his or her physical whereabouts. For example, access to certain areas of a file system might be limited to only those individuals who are directly connected to the internal network, as this provides additional evidence that the user is physically onsite. As with all forms of MFA, location authentication is not a foolproof solution. However, when used in conjunction with other methods, location authentication can help cultivate a more robust information security environment.

MFA Methods Being Targeted

The growing adoption of MFA has resulted in a proportionate rise in cyberattacks targeting MFA technologies. In a recent Private Industry Notification (PIN), the Federal Bureau of Investigation (FBI) recognized how different cyberattack campaigns have taken place in recent years that focus directly on circumventing MFA. The FBI outlined three specific and comprehensive tactics that hackers have been developing in order to bypass MFA.

One of the first MFA notifications mentioned by the FBI PIN outlined the growing number of Subscriber Identity Module (SIM) card-swapping attacks that have taken place in recent years. Each telephony-capable mobile device has an onboard SIM card, programmed with the customer’s phone number, and tied to his or her respective account with the carrier. A SIM swap attack involves switching a victim’s phone number over to a different SIM card on a device controlled by a hacker. This is often accomplished by conducting social engineering on customer service representatives of cellular phone carriers who are often unprepared to handle these savvy adversaries.

To social engineer such an attack, an adversary tries to take advantage of a person’s naturally trusting tendencies. For example, the attacker might call the victim’s carrier posing as the victim in an emergency situation, demanding that the target phone number be transferred to a different SIM card on new device immediately. In an effort to help the struggling “customer” reach a resolution quickly, many representatives end up processing the hacker’s request. As a result, the adversary now has a device with the victim’s phone number programmed to it, while cellular service to the victim’s actual device is disconnected.
The damage that can be wrought by a successful SIM swap can be catastrophic. If the perpetrator knows the victim’s credentials for a website, any text message MFA OTPs will be sent to the victim’s number, which now arrive on the attacker's device. Even if the adversary doesn’t know the victim’s credentials, it becomes possible to use the “forgot password” service on many websites to receive an MFA OTP text message that can be used to reset the victim’s password. The attacker can even call services posing as the victim, using the victim’s actual number. This number will be recognized by the service in question as legitimate, possibly allowing the attacker to bypass any additional security checks. With this level of control, it becomes possible to alter all credentials to lock the victim out of his or her own accounts. All the while, the victim remains unaware of these events, unable to make or receive calls or text messages on their own device.

Another MFA circumvention method outlined by the FBI is derived from poorly designed and insecure websites. The FBI highlighted how a competent attacker had previously managed to manipulate a vulnerable bank website into bypassing MFA. The adversary managed to accomplish this by inserting a custom command string into the web address once it presents an MFA request. The command string not only resulted in the MFA request being bypassed, but the bank also officially recognized the attacker's computer as a trusted device on the victim’s account, resulting in unrestricted access to the account in question.

The final method outlined by the FBI PIN includes phishing attacks, which still remain tried and true methods used by data thieves to trick a victim into revealing their information. In one example, an attacker can send a fake message purporting to be from the victim's financial institution, demanding he or she open a link in the message or risk an account being shut down as a security precaution. The link takes the victim to a fraudulent website designed by the attacker that serves as a proxy to (and also resembling) the legitimate website, capturing and forwarding all interactions between the victim and the legitimate website in real time. This is referred to as a Real-Time Phishing attack. Once the user is authenticated by the genuine website, the adversary can capture the browser “session cookie” that the legitimate website associates with the authenticated user. Using that captured session cookie, the result is unrestricted access to the victim’s account; this type of attack is referred to as Channel-Jacking.

While these attacks can be quite effective at bypassing MFA, Channel-Jacking in particular requires advanced technical skills, including knowledge in reverse-proxy web server configuration. Various tools have been developed to streamline the overall phishing and response processes. One pair of tools the FBI highlighted was Muraena and NecroBrowser, which work in concert to automate the attack procedure. Unfortunately, by automating the complex processes involved in such campaigns, these tools allow attacks to be carried out with greater frequency, and on a much larger scale.

Defensive Strategies

While each of these attacks can be devastating to a potential victim, there are multiple strategies that can be implemented to safeguard an account from MFA compromise. A user can take several precautions to protect themselves from a SIM swapping attack. As more carriers are becoming aware of this type of attack, they are offering additional password functions that must now be provided before a representative is able to take any action on an account. This password can likely be reset, but a great deal of user information needs to be verified before this can take place. Additionally, users can request that all SIM-related changes on an account are required to be conducted in person at a physical store location. As this will require photo identification and additional account details be verified, it greatly reduces the chances of an “over-the-phone” request from going through.
Another response to the growing SIM swap threat is the adoption of a secondary, internet-based phone service such as Google Voice. Google Voice allows its users to set up a second phone number tied to their Google Account that will forward all communications to any additional numbers associated with the account. By using a Google Voice number as a primary contact number for any important service, an individual can help circumvent threats introduced by SIM swapping. As a Google Voice service is tied to an online account and not a SIM card in a physical device, there is nothing for a hacker to attempt to swap through a social engineering effort. A hacker would have to compromise an entire Google Account first, in order to access the Google Voice service. However, Google offers an MFA service of its own that is tied to a software application on the user’s device, not their phone number. With this MFA application active, anytime anyone attempts to login to a user’s account, the user is notified through the application and can choose whether to accept or deny access.

As previously mentioned, a successful SIM swap results in the carrier’s cellular service being disconnected from the victim’s device. However, Google Voice allows its users to make phone calls over Wi-Fi, instead of relying on their cellular carrier. This means that even if a victim suffers from a successful SIM swap attack on his or her carrier number, the victim is not powerless. The victim can connect to a Wi-Fi signal and then contact the applicable carrier to reverse the swap. Furthermore, the victim can also login to the Google Voice account and turn off any active communication forwarding options, or simply forward all communication to a friend or family member’s device until the swap can be reversed. By taking these steps, even following a successful SIM swap of a victim’s carrier number to an adversary’s device, the attacker will not receive any MFA OTPs if the victim quickly takes action.

When it comes to choosing a possession authentication method, each one has its own pros and cons. Physical possession authentication devices provide the strongest overall security, but are also vulnerable to being lost or stolen. MFA OTPs sent to physical devices through text messages are vulnerable to interception through attacks such as SIM swapping or social engineering. However, digital possession authentication applications such as Microsoft Authenticator, Google Authenticator, Authy, and others provide a happy medium between these options. Once initially configured on a device, these applications generate MFA OTPs that expire within seconds, and are tied to an online account instead of a phone number. As a result, these applications are not vulnerable to SIM swapping, and most devices provide additional security options that prevent access if the equipment is ever lost or stolen.

Users Need to be Proactive

Be it clicking a malicious link, visiting a fraudulent website, or downloading an infected file, the vast majority of cyberattacks rely on a victim taking some form of action to be effective. Phishing attacks rely on the naivety and trusting nature of their victims to engage in just such actions. Unfortunately, there is no easy solution when it comes to phishing attacks. The only true defense against such hacking efforts is to apply a healthy degree of skepticism to every message received, especially from individuals or organizations you don’t recognize. A potential victim that receives a worrisome message demanding immediate action should never click any links in the message or open any attached files. The concern, if genuine, will be available to address by logging in to the official website of the respective service.
Lastly, users can help to mitigate any threats posed through authentication attacks by using password managers. Unfortunately, most users have only a few passwords that they use throughout their countless online accounts. Even worse, these passwords are often far from complex, making the accounts that use them more vulnerable to compromise. However, when user credentials are leaked through data breaches on such services, those credentials are immediately used by hackers to try and access other popular services with the same leaked credentials. If the user has the same credentials for multiple services, the hacker now has access to every account that uses them. While remembering a unique password for each account you have might seem exhausting, there are solutions that can do this for you. Password managers can help to generate complex passwords that are far more robust and harder for hackers to compromise, and don’t require you remember them on your own. By using unique passwords on every service, the only account compromised is the one associated with the breach. Of course, users should protect their password managers with either MFA or a highly complex password that would be impossible for an attacker to guess or steal.

Bottom Line

The FBI has recognized that while attacks on MFA solutions have increased in recent years, they still remain extremely rare in comparison to other forms of cyberattacks. In fact, during a recent announcement, Microsoft stated that attacks that seek to bypass MFA are so infrequent that the company doesn’t even have statistics on these specific efforts. Microsoft noted in its tech community blog that “the rate of compromise of accounts using any type of MFA is less than 0.1% of the general population.”

While MFA is not a catch-all solution, it is a fundamental step toward comprehensive account security. By implementing another form of authentication, users can protect themselves against the dreaded single-point-of-failure that comes from relying on just their password. Sadly, the number of individuals who utilize some form of MFA are in the minority. Microsoft argued that less than 10% of their monthly enterprise accounts implement MFA. This means that the majority of users rely on just a username and password for account access. As a result of the vulnerabilities present in a limited username and password security strategy, MFA is the most effective measure individuals can engage in to help significantly reduce the chances of account compromise.

Analyst contact

Tanner Johnson
Senior Analyst
Cybersecurity Technology, IoT
+1 417.343.9980
tanner.johnson@ihsmarkit.com
@IHSMarkitTech
@cybersec_tanner