okta

How Adaptive MFA Helps Mitigate Brute Force Attacks

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

How Adaptive MFA Helps Mitigate Brute Force Attacks

Before public cloud services, large-scale computing infrastructure was expensive, hosted on-premises, and reserved for big enterprises, governments, and universities. Now, anyone with a credit card can access an unlimited supply of cloud apps and computing power.

While cloud computing offers many benefits, its accessibility has also made identity attacks targeting passwords much more popular. The frequency of these attacks has increased sharply over the last few years. As more services move online and the value of data grows, identity attacks will become even more popular.

How are hackers targeting passwords?

Hackers have a variety of techniques at their disposal. Exploiting vulnerabilities in software or deceiving users through social engineering are two common tactics, but brute-force attacks are gaining ground through the use of automated bots. A recent report from Akamai indicates that "more than 40% of global login attempts are malicious, thanks to bot-driven credential stuffing attacks".[1] This increases the likelihood of attacks affecting your organization.

Two types of brute force attacks that target passwords have recently gained ground:

Credential stuffing: This attack takes advantage of users sharing credentials across multiple accounts. Most people have had account credentials compromised as part of a data breach. Attackers acquire credentials from a website breach and use bots to enter these credentials into a variety of sites in the hope that they will grant access.

Password spraying: This attack takes advantage of our tendency to rely on common passwords such as "password1" (which, according to the password checking site HaveIBeenPwned, has appeared in a data breach over 2.3 million times).[2] Attackers use a dictionary of commonly-used passwords across many different accounts, which helps avoid detection.

Once attackers encounter a successful login, they either harvest sensitive data or execute the next stage of their breach.

How can Okta mitigate identity attacks?

Given the popularity of these attacks, knowing how to prevent them has become more important. Although there's no silver bullet to block brute-force attacks, here are two approaches that can help:

[1] "Q4 2017 State of the Internet Security Report | Akamai." Accessed January 11, 2019. https://www.akamai.com/it/it/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf.
[2] "Have I Been Pwned: Pwned Passwords." Accessed January 11, 2019. https://haveibeenpwned.com/Passwords.

Account lockouts

A common approach involves locking users out of accounts after several incorrect password attempts. While this approach is useful, it still relies on password authentication, only slightly reducing the likelihood of account compromise. Hackers could also use this feature to affect your service availability by locking out legitimate users.

Multi-factor authentication (MFA)

Multi-factor authentication offers a better way to secure the login process. By requiring users to submit more than one authentication factor before gaining access, it mitigates the inherent risks of using a single password and is an effective defense against automated attacks.

These authentication factors typically fall into one of three categories: knowledge, possession, and inherence.

Knowledge. A knowledge factor relies on something you know. Passwords are the most obvious example, but personal identification numbers (PINs) and answers to security questions also count. Knowledge factors must be remembered, giving them the same weaknesses as passwords. People deliberately use PINs that are easily remembered and share them across multiple accounts.

Knowledge factors are also often found in the public domain. You can easily use social media or public records to discover answers to typical security questions such as a person’s first school or mother’s maiden name.

Possession. This factor is something you must physically carry during the login process. It is an effective defense against automated password attacks because an intruder would need the physical device for access. The banking industry has combined knowledge and possession factors for years in the form of PINs and ATM cards. Other possession factors include U2F tokens, One-Time PIN (OTP) codes, and push notification technologies like the Okta Verify app.

While possession factors do improve authentication security, they can also be lost or stolen. In that case, an attacker could compromise the user’s account and lock them out.

Inherence. An inherence factor uses traits that are unique to each individual. Biometric identifiers, like fingerprints, retina scans, and facial recognition fall under this category. Requiring users to submit this unique information during the login process offers an effective defense against brute-force attacks.

Like knowledge factors, inherence has a potential downside because biometric information can be found in the public domain. We leave our fingerprints on every surface that we touch, and our faces are in images on social media. While it would take a much more determined hacker to gather this information and use it to impersonate a user during authentication, biometric factors are still not absolutely bulletproof.

It’s vital to consider which MFA verification factors are right for your organization when you use MFA. Each has its own pros and cons. Security is critical, but there are other issues to bear in mind. These include the impact of a verification method on the user experience, and the overhead involved in managing it. Some verification technologies are easier to apply than others and offer a better user experience, but do not provide the same level of security as complex MFA deployments.

For example, it is easier to manage a password or PIN-based solution than it is to issue each user with a hardware token. Simple PIN entry is also more convenient for users than carrying a physical device with them. On the other hand, a knowledge-based factor alone does not offer the same level of assurance as a possession factor.

There are other issues to consider too, such as the accessibility of the technology involved. For example, using certain devices or smartphone apps to deploy MFA may not always be feasible in every scenario. Smartphones are less available in some regions than others, and they would not be a practical authentication device for users in every market.

Adaptive multi-factor authentication (AMFA)

In some instances, you may only want to implement MFA when you need a higher level of assurance. Understanding the context of the user, device, and network can help organizations apply the right level of authentication for the risk involved. A bank may allow customers to access applications with a single password but ask for OTP submissions to approve money transfers. Organizations may let employees log in using passwords on the company network while requiring a hardware token to sign in from an unverified location.

Adaptive multi-factor authentication applies this context to help organizations defend against brute-force attacks without compromising usability. AMFA extends the login process with additional security controls beyond just password validation. It validates the request context by examining geolocation, IP reputation, device, and login behaviors. Based on this context, it might ask users to submit an additional verification factor. These factors might include something the user owns, like a security token, or something unique to the user, like a fingerprint.

By tweaking your security policies with AMFA, you can give customers an effective balance of usability and security. Instead of relying on blanket policies that frustrate users, you can base the login process (deny, MFA, or allow) directly on the associated risk.

Okta has used AMFA as the basis for several specific prevention strategies that customers can employ to suit their business needs. These include:

- Implementing MFA for employees and partners. This mitigates the risk of account compromise due to password attacks. Since Okta is able to implement MFA on top of federated authentication, you can also extend the MFA to partners, regardless of which identity solution they currently use.
- Blacklisting malicious networks and malformed/unknown user agents reduces login attempts from unexpected locations and requests that contain suspicious header agents.
- Rate-limiting suspicious IP addresses reduces suspicious activity by isolating and blocking IP addresses that have a low rate of login success.
- Denying login attempts and locking out users based on behavior complements blacklisting by using context to spot suspicious behavior. An example would involve locking out access attempts from Brazil for an employee in the USA group.

You can even use AMFA to go passwordless. Okta's factor sequencing feature (coming soon) allows you to set any combination of strong authentication factors. For example, you could use Okta Verify as the primary factor that enables users to log in with a single tap on their smartphone. If AMFA detects a high risk level associated with the login request, it can prompt the user to submit a second factor, such as a hardware token or biometric identifier.

Configuring AMFA in this way helps to prevent brute-force attacks. It also provides users with a frictionless authentication experience that gives them easy access to the data they need.

Interested in these options? Contact us for help on implementing the right strategy for your organization to protect your users against identity attacks. You can also learn more about Adaptive MFA by downloading our Multi-factor Authentication Deployment Guide.

To learn more visit us at:
https://www.okta.com/contact-sales/

okta