HMAC One Time Password

HMAC OTP, or Hash-based Message Authentication Code One-Time Password, is a secure method for generating one-time passwords in two-factor authentication systems. It combines the strength of both HMAC (Hash-Based Message Authentication Code) and OTP (One-Time Password) to ensure secure authentication processes.

In HMAC OTP, a client and the authentication server share a secret key. This key generates a unique hash value for each password attempt, which is combined with a counter or timestamp (in TOTP) to create a one-time password. The password is then sent to the user's device, typically a smartphone or hardware token, where it is verified against the server's expected value.

One of the main advantages of HMAC OTP is its resistance to common password attacks such as rainbow table attacks and brute force attacks. Using a secret key ensures that an attacker cannot use the OTP without knowledge of the key, even if it is intercepted. Additionally, the one-time nature of the passwords makes them useless for subsequent login attempts.

HMAC OTP not only provides a high level of security for online authentication but also does so with remarkable efficiency. This makes it an indispensable tool for safeguarding sensitive information and thwarting unauthorized access, instilling confidence in its effectiveness.

The versatility of HMAC OTP is a key aspect that empowers its users. The core concept of HMAC OTP is the counter, which increments with each authentication attempt. This counter value, combined with a secret key shared between the authentication server and client, is then hashed with a cryptographic hash function, such as SHA-1 or SHA-256, to generate the OTP. This flexibility allows HMAC OTP to be used in scenarios where connectivity is unreliable, and it is often found in hardware tokens like the Yubico Security YubiKey and DUO Mobile Authenticator. This feature enables the 2FA token to remain valid until it is used in a logon attempt, without imposing any time restrictions on the user's authentication process.

TOTP (Time-Based One-Time Password) is an extension of HMAC OTP and is also used in many mobile authenticators for 2FA/MFA. TOTP generates OTPs by hashing a time counter, typically in 30 to 60-second intervals, along with a secret key. It is commonly used in mobile authenticator applications such as Google Authenticator, Authy, and Microsoft Authenticator.

Despite their advantages, HOTP and TOTP are still susceptible to various attacks and weaknesses. When HOTP was created, brute force attacks were the most concerning since the HOTP value would remain the same until a successful login attempt. However, brute force attacks are easily dealt with by limiting the number of failed authentications. Some other common attacks include man-in-the-middle attacks and phishing attacks. One of the most significant weaknesses of HOTP and TOTP is synchronization. Since the algorithms for generating the OTPs rely on client and server synchronization, desynchronization can render the process useless. Some countermeasures are in place to correct desync but are imperfect and may require manual resynchronization.

In summary, HOTP is an event-based, one-time password algorithm that combines HMAC and OTP to create a secure 2FA method that offers increased security over standard passwords. A client and a server share a secret key and a synchronized counter; with these two values, the client and server calculate the HOTP independently. If the calculation is the same on both ends, authentication is achieved. While HOTP is not without its flaws, it is far more secure than using static passwords on their own.

References

https://www.rfc-editor.org/rfc/pdfrfc/rfc4226.txt.pdf

https://www.descope.com/blog/post/totp-vs-hotp

https://www.professormesser.com/security-plus/sy0-401/one-time-password-algorithms/#google\_vignette

https://www.onelogin.com/learn/otp-totp-hotp#:~:text=Put%20in%20layman's%20terms%2C%20HMAC,incremented%20based%20on%20a%20counter.

https://www.youtube.com/watch?v=XvQ7iOGjEsA

One-time password - Wikipedia

One-Time Password (OTP) - Guide For ISVs 2023 (10duke.com)

One-Time Password vs. One-Time Pad: What’s the Difference? - Rublon

https://www.youtube.com/watch?v=MKn3cxFNN1I

https://www.youtube.com/watch?v=46AKWNOJ3-Y