Y(Monica) Hung, u22561154

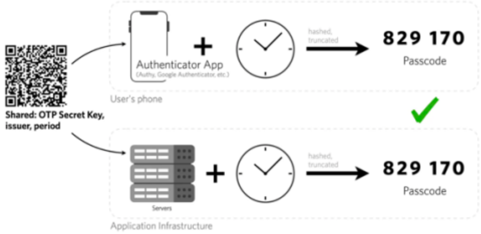
TIME-BASED ONE-TIME PASSWORD (TOTP)

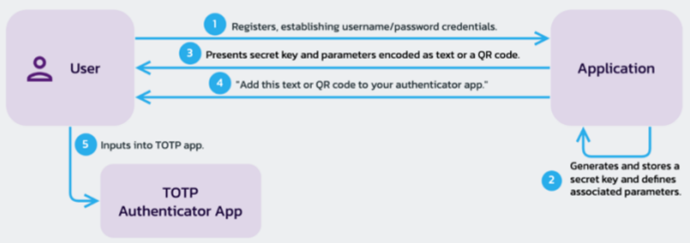
What is used for identification: The user identifies themselves using a unique name or ID. The username will help the authentication scheme determine which user is requesting access to the account.

What is used for authorization: The user generates a time-sensitive one-time password (TOTP) using a shared secret key and system time. The algorithm uses a form of symmetric key cryptography: the same key is used by both parties to generate and validate the token.

Brief description of scheme, how it works, and perhaps showing a picture/ diagram etc.: TOTP is a widely used for two-factor authentication schemes to prove ownership of a particular device or account. It combines a shared secret key (stored on both the user's device and the server) with the current timestamp to generate a unique, temporary password.

Firstly, TOTP requires the system to generate the code and the one that receives it both have a shared key (user scan a QR code containing the shared secret key) and have their clocks synchronized. Then, they each calculate a matched pair of one-time code that are only valid for 30-60 seconds. The user is then asked to type in the code from the authenticator app into the system they wish to log into. The system then compares the code then if they match the user is allowed to proceed.




User
Application
1 Registers, establishing username/password credentials.
2 Generates and stores a secret key and defines associated parameters.
3 Presents secret key and parameters encoded as text or a QR code.
4 "Add this text or QR code to your authenticator app."
5 Inputs into TOTP app.
TOTP Authenticator App

How can it be attacked: Man-in-the-middle attacks during the initial setup or shared secret exchange. It can also be phished and stolen. Uses a shared secret, which means that the service providers hold the secrets for all TOTP generators and if it is stolen, the attacker can generate code for users.

What countermeasures could be put in place: No internet connection is needed, so the device that generate and accept TOTP codes can be completely offline. You can use a secure communication channel during secret key exchange, e.g. HTTPS.

Reference:

"Time-Based One-Time Passwords (TOTP)". www.transmitsecurity.com. 25 June 2020. Retrieved 2 May 2022. https://transmitsecurity.com/blog/totp-the-good-the-bad-and-the-ugly

(Hoagland, 2024) https://pangea.cloud/securebydesign/authn-using-totp/