Contraseña de un solo uso basada en el tiempo (Time-based one-time password, TOTP)

Una contraseña de un solo uso basada en el tiempo (TOTP) es un código temporal y único generado por un algoritmo que utiliza el tiempo actual como un factor clave.

- ¿Qué es TOTP?

¿Qué es TOTP?

Una Contraseña de un Solo Uso Basada en el Tiempo (TOTP) es un código temporal y único generado por un algoritmo que utiliza el tiempo actual como un factor clave. Similar a un Contraseña de un solo uso (One-time password, OTP) genérico, un TOTP se usa solo una vez, pero tiene una vida útil fija, que generalmente varía entre 30 y 60 segundos. Al expirar, se genera automáticamente un nuevo código.

El estándar TOTP está definido por el Internet Engineering Task Force (IETF) bajo RFC 6238 y es ampliamente adoptado en varios sistemas de autenticación de dos factores (2FA) y autenticación multifactor (MFA). Debido a que los TOTP dependen de una sincronización temporal entre el cliente (dispositivo del usuario) y el servidor, ofrecen un alto nivel de seguridad y son difíciles de predecir o reutilizar.

Cómo funciona TOTP

La generación de un TOTP involucra los siguientes pasos:

1. Clave secreta compartida: Durante la configuración inicial, se genera una clave secreta compartida que se almacena de manera segura tanto en el cliente como en el servidor. Esta clave suele estar codificada como un código QR que los usuarios escanean utilizando una aplicación de autenticación.
2. Intervalos de tiempo: El tiempo actual se divide en intervalos fijos, usualmente de 30 segundos.
3. Aplicación de algoritmo: La clave secreta compartida y la marca de tiempo actual se introducen en un algoritmo basado en hash (a menudo HMAC-SHA1) para producir un código numérico único.
4. Sincronización: Tanto el cliente como el servidor generan el código de manera independiente utilizando la misma clave secreta compartida y la marca de tiempo actual. Los códigos coinciden solo si ambos están sincronizados.
5. Verificación: Cuando el usuario inicia sesión o realiza una transacción crítica, ingresa el TOTP mostrado en su aplicación de autenticación. El servidor luego lo compara con su TOTP generado internamente para validación.

Cuándo usar TOTP

En la mayoría de los casos, se recomienda un OTP normal, pero en los casos donde no se puede “activar” un código nuevo, entonces se recomienda TOTP.

- Ejemplo de TOTP: App Authenticator
- Ejemplo de OTP: Email, SMS

¿Cuál es la diferencia entre OTP y TOTP?

La principal diferencia es que TOTP está basado en el tiempo, por lo que es adecuado cuando el dispositivo no está conectado al servidor. El servidor puede fácilmente enviar un nuevo código a una dirección de correo electrónico o a un número de teléfono, pero eso requiere que el correo o teléfono esté en línea. Sin embargo, la App Authenticator puede permanecer desconectada y usar el “tiempo” para verificar el código.