Cos'è un OTP (One-Time Password)

Guida tecnica e pratica al codice di sicurezza monouso per l'autenticazione informatica.

1. Definizione e Concetto Base

Un **OTP (One-Time Password)** è una password monouso, ovvero un codice segreto di cifre (solitamente da 4 a 8 caratteri) valido esclusivamente per una singola sessione di accesso o per una specifica transazione.

> **Caratteristica fondamentale:** Una volta utilizzato o scaduto il tempo limite (spesso 30-60 secondi), il codice diventa istantaneamente obsoleto e inutilizzabile, anche se intercettato da malintenzionati.

2. Perché si usa l'OTP? (I Vantaggi di Sicurezza)

Le password tradizionali statiche presentano forti vulnerabilità (furto di credenziali, attacchi di forza bruta, riutilizzo della stessa password su più siti). L'OTP risolve questi problemi introducendo i seguenti vantaggi:

Vantaggio	Descrizione dettagliata
Protezione da Replay Attack	Anche se un hacker intercetta il codice durante la trasmissione, non potrà riutilizzarlo perché sarà già scaduto o consumato.
Autenticazione a Due Fattori (2FA)	Si affianca alla password fissa: anche se la password viene rubata, l'intruso non possiede il dispositivo fisico che genera l'OTP.
Nessun rischio di riciclo	Non richiede di memorizzare codici complessi a lungo termine, riducendo la cattiva abitudine di annotare le password.

3. Principali Ambiti di Applicazione

L'OTP è ampiamente diffuso nella vita digitale quotidiana: transazioni bancarie online (bonifici e pagamenti con carta), accesso ai servizi della Pubblica Amministrazione (come lo SPID), login su piattaforme Cloud, social media e VPN aziendali.

4. Le Tipologie di Generazione OTP

Esistono diverse tecnologie e standard con cui i codici monouso vengono generati e recapitati all'utente:

Tipologia	Come funziona	Esempi comuni
SMS / Email	Il codice viene inviato in tempo reale tramite messaggio di testo o posta elettronica al momento della richiesta.	Home Banking, notifiche di accesso
App Authenticator (TOTP)	App basate su algoritmi temporali che generano codici offline sincronizzati (es. Google Authenticator, Microsoft Authenticator).	Google, GitHub, SPID, account di gioco
Token Hardware	Dispositivi fisici tascabili con un piccolo display che mostrano un nuovo codice a intervalli regolari.	Token bancari aziendali o dispositivi token RSA

5. Come avviene il processo di verifica

Il meccanismo si basa sulla condivisione di un segreto iniziale (chiave segreta) tra il server del servizio e il dispositivo dell'utente:

- **1. Sincronizzazione:** Dispositivo e server condividono un algoritmo matematico e un seme iniziale.
- **2. Generazione:** In base all'orario corrente (TOTP) o a un contatore incrementale (HOTP), il dispositivo calcola la sequenza numerica.
- **3. Controllo:** Quando inserisci il codice, il server esegue lo stesso calcolo: se il risultato coincide, l'accesso viene autorizzato.

> **Buone pratiche di sicurezza:** Non comunicare mai il tuo codice OTP a nessuno, neanche a chi finge di essere un operatore della banca o dell'assistenza tecnica. I sistemi automatici non richiedono mai l'OTP a voce o via chat.

6. Considerazioni finali

L'adozione dell'OTP rappresenta oggi uno standard imprescindibile per la sicurezza informatica personale e aziendale, riducendo drasticamente le intrusioni non autorizzate derivanti da violazioni di password tradizionali.