

openHPI-Kurs „Digitale Identitäten“
Sichere Authentifizierung
mit Einmalpasswörtern

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Idee der **Einmalpasswörter (OTP – One-Time Passwords)**:

- Jedes Passwort kann nur einmal zur Authentifikation verwendet werden. Ein Passwort verliert nach erstem Gebrauch sofort seine Gültigkeit
 - Abfangen und Ausspähen nutzlos
- Einmalpasswörter sind **automatisch** und **zufällig generierte Zeichenketten**, die dem Nutzer über einen zweiten, unabhängigen Übermittlungskanal bereitgestellt werden



Bereitstellung von Einmalpasswörtern

Herausforderung

- Sowohl Nutzer, als auch Authentifizierungsstelle müssen darüber Bescheid wissen, welche Einmalpasswörter gültig sind und welche verbraucht

2 mögliche **Lösungsansätze**

- Passwortlisten
 - Liste mit gültigen Einmalpasswörtern wird von der Authentifizierungsstelle generiert und dem Nutzer über zweiten sicheren Transportweg übermittelt, z.B.
 - TAN-Listen, mTAN, ...
- Passwortgeneratoren
 - Generieren dynamisch Einmalpasswörter, die nur für bestimmten Zeitraum gültig sind

Passwortgeneratoren ...

... sind kleine Geräte – **Token** – oder Applikationen

- Passwortgeneratoren produzieren Einmalpasswörter auf Grundlage spezieller Algorithmen
- Können drei Generierungsverfahren unterscheiden:
 - **zeitgesteuerte** Generierung
 - **ereignisgesteuerte** Generierung
 - **Challenge-Response-gesteuerte** Generierung

Token und Authentifizierungsstelle arbeiten zeitlich synchron

- Beide Seiten berechnen im selben zeitlichen Intervall Einmalpasswörter, die bis zur Verwendung oder zur nächsten Berechnungsiteration gültig sind
- Authentifizierungsstelle erlaubt einen zeitlichen Toleranzbereich, da die Uhr im Token nicht immer 100%ig exakt arbeitet
- Beispiele:
 - Google Authenticator
 - SecurID



SecurID



Google Authenticator

Generierung eines Einmalpassworts wird durch den Nutzer getriggert, z.B. durch Drücken einer Taste auf einem Token

- Token und Authentifizierungsstelle merken sich Anzahl der bisher generierten Passwörter
- Berechnung des Einmalpassworts erfolgt unter Einbeziehung zuvor generierter Passwörter
- Authentifizierungsstelle erlaubt Toleranzbereich, für den Fall, dass der Nutzer ein generiertes Passwort nicht verwendet hat

Nutzer möchte sich authentifizieren und fragt bei der Authentifizierungsstelle an

Ablauf:

1. Authentifizierungsstelle übersendet zufälligen Wert an Token
 2. Token wendet Berechnungsalgorithmus auf empfangenen Wert an und gibt Ergebnis (Einmalpasswort) aus
 3. Nutzer sendet generiertes Einmalpasswort an Authentifizierungsstelle
 4. Authentifizierungsstelle kennt den Berechnungsalgorithmus und überprüft den vom Token berechneten Wert
- Bei Korrektheit ist der Nutzer authentifiziert

Einmalpasswörter

- Jedes Passwort kann nur 1x genutzt werden
- Bereitstellung mithilfe von Passwortlisten und Passwortgeneratoren
- Passwortgeneratoren lassen sich in drei Kategorien unterteilt:
 - zeitgesteuerte Generierung
 - ereignisgesteuerte Generierung
 - Challenge-Response-gesteuerte Generierung