

Two-Factor-Authentication






Marc-Niclas Harm | 29.11.2018 | TH-Lübeck

Gliederung

- Was ist **2FA**?
- Wieso überhaupt **2FA**?
- Algorithmus-Beispiel: **TOTP** (anhand von **HOTP**)
- Weitere **2FA** Möglichkeiten
 - SMS, Anruf, E-Mail, Security-Token
- U2F-Standard

Was ist 2FA ?

- Unterkategorie der **Multi-Factor-Authentication (MFA)**
- Dient der Bestätigung der Identität eines Nutzers
- Bestehend aus mind. **zwei** unabhängigen Faktoren

Wissen 	Besitz 	Inhärenz 
---	--	--

Was ist 2FA ?



Wieso überhaupt 2FA ?

- Verlust von persönlichen Daten bei Unternehmen immer zahlreicher
- Internetkriminalität wird anspruchsvoller
- Datenverlust oder Identitätsdiebstahl für Verbraucher verheerend
- Selten unterschiedliche Passwörter
- Passwörter allein **nicht** ausreichend zum Schutz von Daten

➔ 2FA als zusätzlicher Schutz

Algorithmus-Beispiel:

TOTP (anhand von HOTP)

Kurz: Was ist ein Hash ?

- Jeder Input ergibt immer denselben Output (**Determinismus**)
- Aus einem gegebenen Hash (Output) den Input zurückzuerhalten ist rechnerisch "nicht" machbar (**Einwegfunktion**)
- Kleine Änderung im Input, führt zu drastischer Änderung im Output (**keine Korrelation**)

HOTP (RFC 4226 aus dem Jahr 2005)

HMAC-Based One-Time Password

$$HOTP(K, C) = Truncate(HMAC - SHA - 1(K, C))$$

Name	Beschreibung
K	Schlüssel
C	Zähler
HMAC	Keyed-Hash Message Authentication Code
SHA-1	Secure Hash Algorithm 1
Truncate	Konvertiert Hash in HOTP

Nachteile von HOTPs

- Counter muss ggf. synchronisiert werden
- Generiertes HOTP ist solange gültig bis ein neues generiert wird
- Alle möglichen HOTPs mittels **Brute-Force** ausprobieren
 - Zugang muss nach einigen Fehlversuchen für ein bestimmtes Zeitintervall gesperrt werden

TOTP (RFC 6238 aus dem Jahr 2011)

Time-Based One-Time Password Algorithm

$$TOTP = HOTP(K, T)$$

$$T = \text{Floor}((\text{Unixtime}(\text{Now}) - \text{Unixtime}(T_0)) / T_1)$$

Name	Beschreibung
K	Schlüssel
Now	Aktuelles Datum & Zeit
T ₀	1. Januar 1970, 00:00 Uhr UTC (Start der Unixzeit)
T ₁	Gültigkeitsintervall
Unixtime	Konvertiert Datum & Zeit in Unix-Zeitstempel
Floor	Rundet auf die nächste ganze Zahl ab

Vorteile von TOTP

- Jedes generierte TOTP ist nun nur in einem **bestimmten, kurzen** Zeitintervall gültig
- **Aber:** Auch hier **Brute-Force-Methode** möglich, solange die Durchsatzrate an TOTP nicht begrenzt wird

Live-Demo 

Weitere 2FA Möglichkeiten

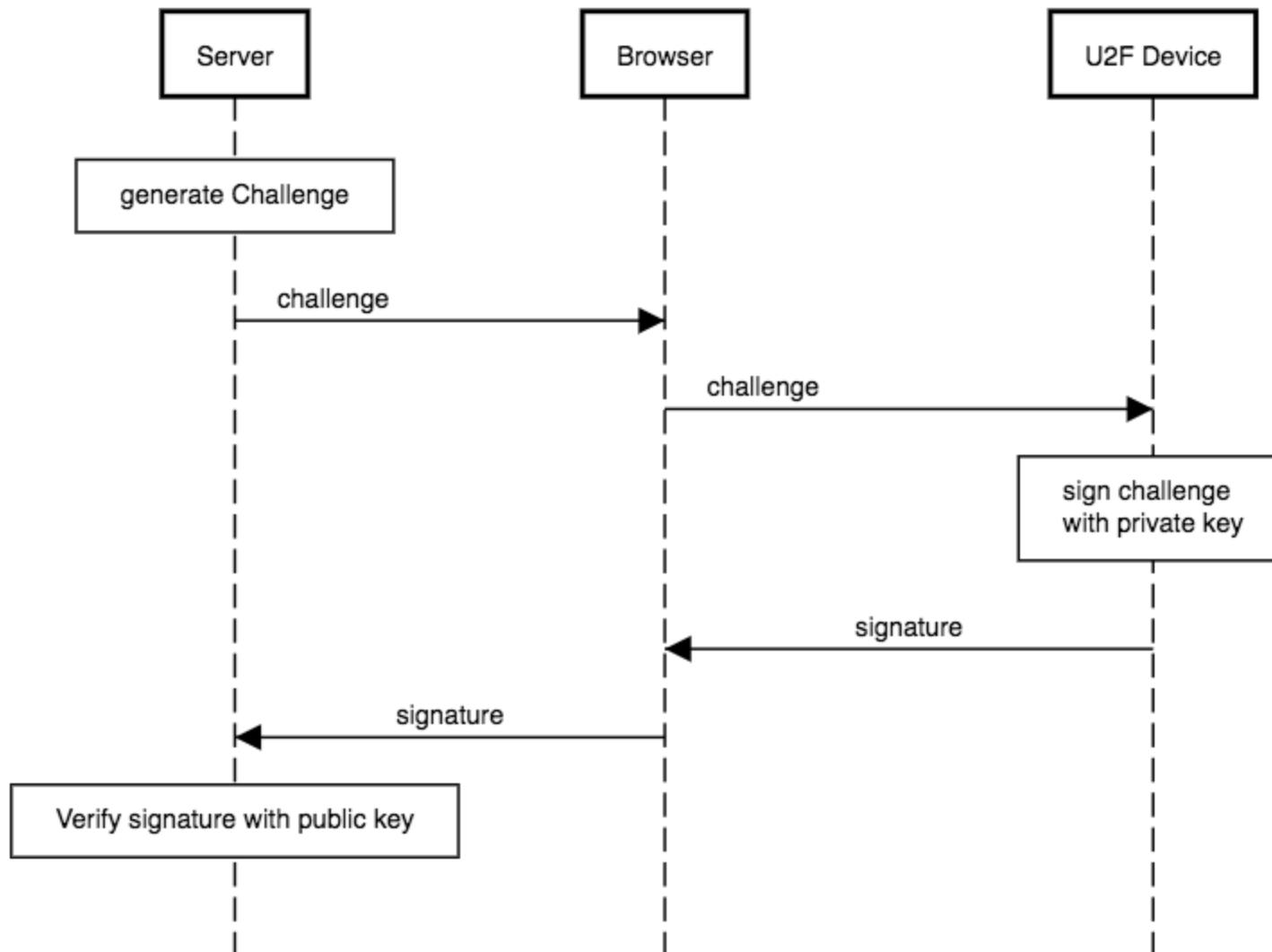
- SMS, Anruf, E-Mail
 - Zusendung des OTPs nach Eingabe der Telefonnummer/E-Mail
- Security-Token
 - Identifizierung und Authentifizierung von Benutzern mittels einer Hardwarekomponente
 - Bekanntes Beispiel: **U2F-Standard der FIDO-Allianz**



U2F-Standard

Universal Second Factor

Public-key cryptography



Welche Mechanismen wählen ?

IT-Grundschutz

M 4.133 Geeignete Auswahl von Authentikationsmechanismen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT

Verantwortlich für Umsetzung: Administrator

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden. Die Identifikation und Authentisierung muss vor jeder anderen Interaktion zwischen IT-System und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben (sie prüfen oder ändern können). Bei jeder Interaktion muss das IT-System die Identität des Benutzers feststellen können.

Vor der Übertragung von Nutzerdaten muss der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentisiert sein. Erst nach der erfolgreichen Identifikation und Authentisierung darf eine Übertragung von Nutzdaten erfolgen. Beim Empfang von Daten muss deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Es gibt verschiedene Techniken, über die die Authentizität eines Benutzers nachgewiesen werden kann. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern)
- Passwörter
- Token wie z. B. Zugangskarten
- Biometrie

IT-Grundschutz-Kataloge

[IT-Grundschutz-Kataloge Downloadarchiv](#)

[IT-Grundschutz International](#)

IT-Grundschutz-Kataloge

Inhalt

Allgemeines

Bausteine

Gefährdungskataloge

Maßnahmenkataloge

M 1 Infrastruktur

M 2 Organisation

M 3 Personal

M 4 Hardware und Software

M 5 Kommunikation

M 6 Notfallvorsorge

Rollendefinitionen

Glossar

Index A-Z


<https://twofactorauth.org>



Two Factor Auth (2FA)

List of websites and whether or not they support [2FA](#).

Add your own favorite site by submitting a pull request on the [GitHub repo](#).

 Search websites



Backup and Sync



Banking



Betting



Cloud Computing



Communication



Cryptocurrencies



Developer









Domains



Education



Email

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
 AOL Mail		✓	✓			
 FastMail		✓			✓	✓
 Freenet	 Tell them to support 2FA on Facebook					

Quellen

Bildquellen

- <https://www.eff.org/files/2016/12/08/2fa-1.png>
- <https://www.safetynet-inc.com/wp-content/uploads/2017/08/Two-Factor-Authentication.jpg>
- <https://steemitimages.com/DQmaVQoXdxoT3oPQd6h6yxnhpAavnhBWvkkzsrMQaj113sS/Public-key cryptography.png>
- <https://www.mtrix.de/wp-content/uploads/2017/09/hardware-yubikeys-2.jpg>

Quellen

Textquellen 1

- <https://authy.com/what-is-2fa/>
- <https://itsecblog.de/2fa-zwei-faktor-authentifizierung-mit-totp/>
- <https://fidoalliance.org/specs/fido-u2f-v1.0-rd-20140209/fido-u2f-overview-v1.0-rd-20140209.pdf>
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html
- <https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic>

Quellen

Textquellen 2

- <https://www.allthingsauth.com/2018/04/20/a-medium-dive-on-the-totp-spec/>
- <https://tools.ietf.org/html/rfc4226>
- <https://tools.ietf.org/html/rfc6238>

Vielen Dank!