ender informatics

Passwortlose Authentifizierung mit Passkey

Die Zeit, die ein Hacker benötigt, um dein Passwort mittels einer Brute-Force-Attacke zu ermitteln 2023

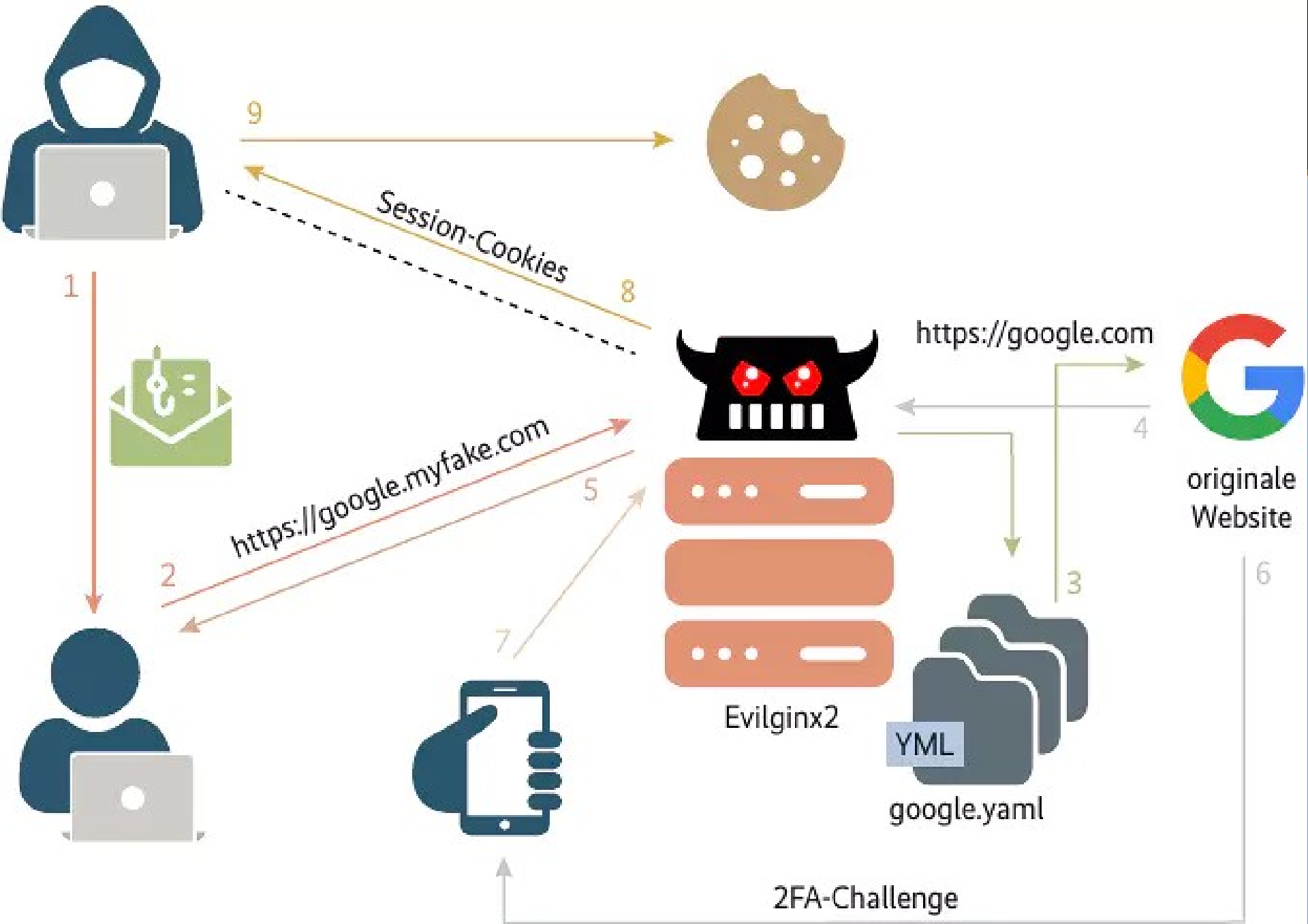
Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein-/Großbuchstaben	Zahlen Klein-/Großbuchstaben, und Symbole
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	Sofort	Sofort	Sofort
6	Sofort	Sofort	Sofort	1 Sekude	5 Sekunden
7	Sofort	Sofort	25 Sekunden	1 Minute	6 Minuten
8	Sofort	5 Sekunden	22 Minuten	1 Stunde	8 Stunden
9	Sofort	2 Minuten	19 Stunden	3 Tage	3 Wochen
10	Sofort	58 Minuten	1 Monat	7 Monate	5 Jahre
11	2 Sekunden	1 Tag	5 Jahre	41 Jahre	400 Jahre
12	25 Sekunden	3 Wochen	300 Jahre	2 Tsd. Jahre	34 Tsd. Jahre
13	4 Minuten	1 Jahr	16 Tsd. Jahre	100 Tsd. Jahre	2 Mio. Jahre
14	41 Minuten	51 Jahre	800 Tsd. Jahre	9 Mio. Jahre	200 Mio. Jahre
15	6 Stunden	1 Tsd. Jahre	43 Mio. Jahre	600 Mio. Jahre	15 Mrd. Jahre
16	2 Tage	34 Tsd. Jahre	2 Mrd. Jahre	37 Mrd. Jahre	1 Bio. Jahre
17	4 Wochen	800 Tsd. Jahre	100 Mrd. Jahre	2 Bio. Jahre	93 Bio. Jahre
18	9 Monate	23 Mio. Jahre	61 Bio. Jahre	100 Bio. Jahre	7 Brd. Jahre

HIVE SYSTEMS

› Lerne, wie wir diese Tabelle erstellt haben: www.hivesystems.com/password

Nachteil Passwort

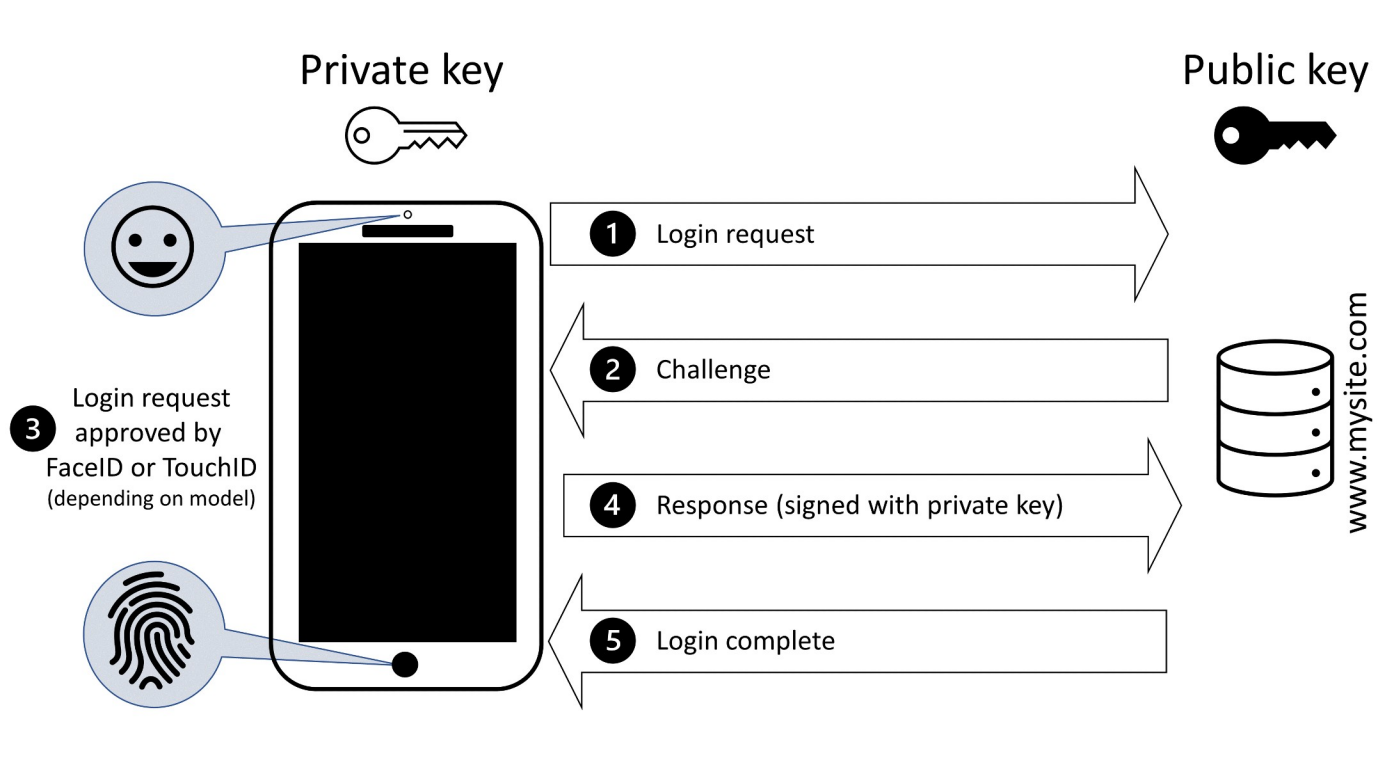
- Geheimnis / Passwort
  - wird bei Server/Anbieter gespeichert
  - muss zum Server gesendet werden
  - verlässt den Hoheitsbereich des Benutzers
  - Kann mehrfach benutzt werden
  - Angreifbar durch Phishing
- Auch Mehr-Faktor-Authentifizierung lässt sich mit Phishing aushebeln


9
Session-Cookies
8
1
https://google.com
4
originale
Website
https://google.myfake.com
2
5
3
6
7
Evilginx2
YML
google.yaml
2FA-Challenge

Wie funktioniert Passkey?

Authenticator generiert für jede Domain einen eigenen geheimen Schlüssel, mit dem er die Antwort auf eine Challenge des Servers signiert.

Diese Antwort authentifiziert den Anwender.



Vorteil Passkey

- Geheimnis / geheimer Schlüssel
  - wird nicht bei Server/Anbieter gespeichert
  - Wird nie gesendet / übertragen
  - verlässt nie Geräte des Benutzers
  - Kann nicht mehrfach benutzt werden
  - Nicht Angreifbar durch Phishing
  - Freischalten des Schlüssels mit Biometrischen Daten

Noch nicht perfekt

- Passkey ist auf das Gerät gebunden
- Hohe Sicherheit kann ausgehebelt werden durch: Passwort vergessen oder «Sicherheitsfragen»
- Bei Diebstahl des Geräts könnten alle Zugänge gestohlen werden
- Gemeinsame Verwendung ist nicht möglich
- Uninteressant für Datensammler: Login kann anonym sein. Es braucht kein Loginname oder E-Mail Adresse

Empfehlung

- Bei Cloud- und online Diensten: 2 Faktor aktivieren
- Passwortmanager verwenden. Z.B. Keepass oder Bitwarden (beides Open-Source)
- Passkey nicht verwechseln mit Keepass :-)