Schütze deine digitale Identität!

Zweifaktor-Authentifizierung

Sylvia

Stadtbücherei Tübingen, 20.7.2024

Fragen?

- Nur Verständnisfragen bitte direkt.
- Alle anderen Fragen im Anschluss an den Vortrag.
- Folien: `https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf`

Sylvia Lange

- Informatik-Lehrerin am Beruflichen Gymnasium
- Beschäftigung mit Datenschutzthemen in der Freizeit, z.B. Mitwirkung bei Cryptoparties

Gliederung

Woraus besteht die digitale Identität?

- Aus den vielen Accounts, die man hat, z.B.
  - Mail-Accounts
  - Accounts bei Online-Shops, z.B. Amazon
  - Online-Banking, Paypal
  - Soziale Netzwerke wie Facebook, Instagram
  - Video-Hosting Peertube und Youtube
  - Foren
  - Cloud-Dienste, z.B. Dropbox
- Überblick verschaffen ist aufwendig, zeitraubend.
- Aber: Ein Passwortmanager hilft!

Was man mit einer gestohlenen Identität tun kann

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen**!

Was man mit einer gestohlenen Identität tun kann

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen**!

Was man mit einer gestohlenen Identität tun kann

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen**!

Was man mit einer gestohlenen Identität tun kann

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen**!

Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen

Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen

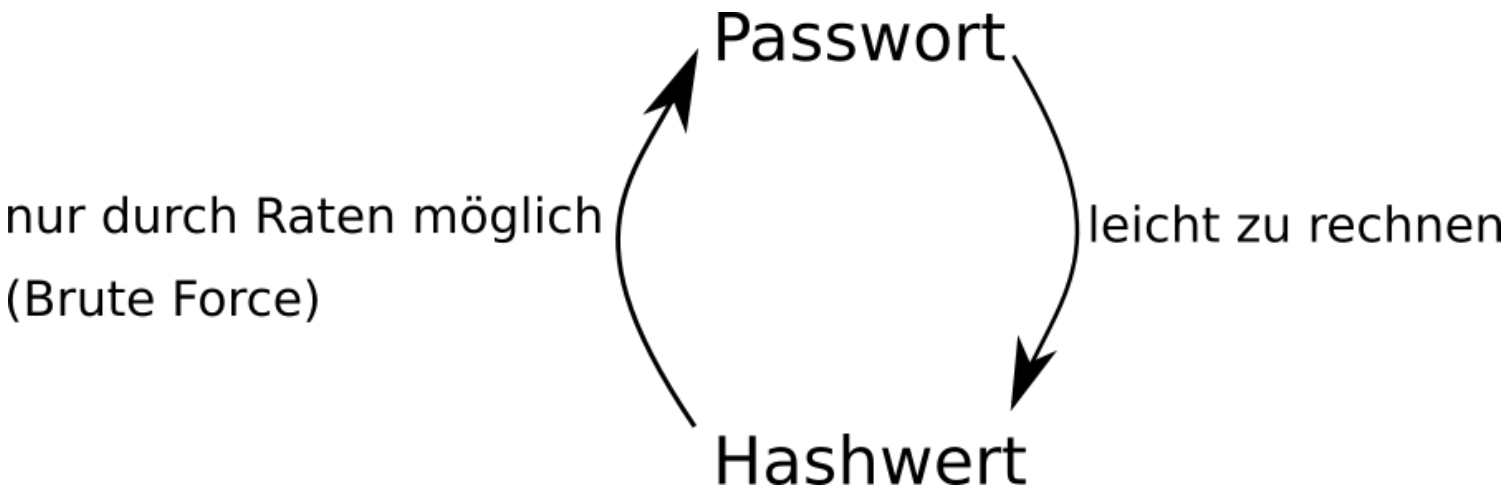
Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen
- Datenpanne beim Dienst. Datenbank mit Useraccounts gestohlen. https://sec.hpi.uni-potsdam.de/ilc/search?lang=de

Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen
- Datenpanne beim Dienst. Datenbank mit Useraccounts gestohlen. `https://sec.hpi.uni-potsdam.de/ilc/search?lang=de`

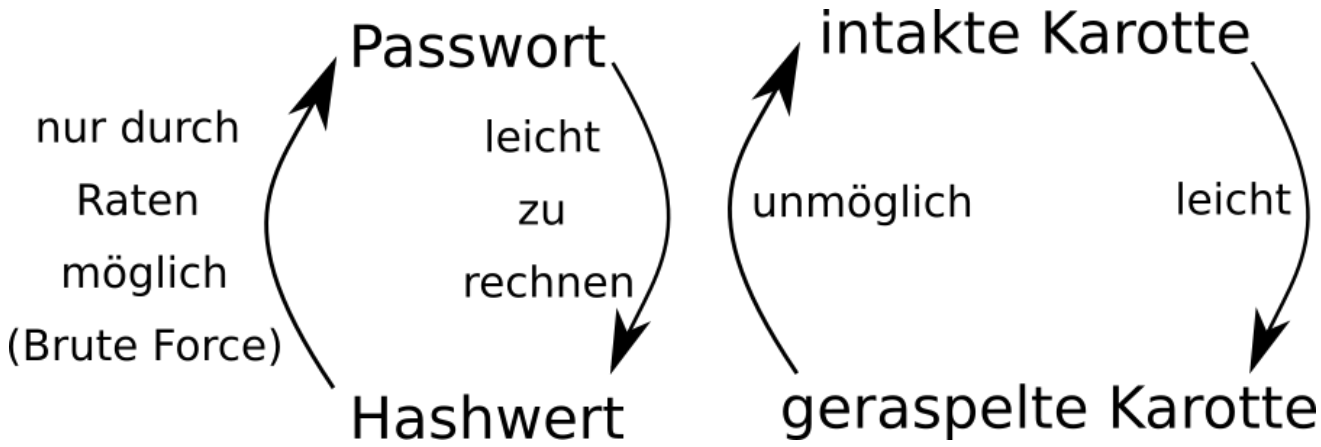
Exkurs: Hashfunktion



Wie eine Falltüre:

- Eine Richtung leicht, . . .
- die andere schwer . . .

Ein anschaulicher Vergleich



- Genau wie mit einer Karotte:
  - raspeln leicht,
  - wieder zusammen setzen unmöglich.
- Sicher ist aber, ob das Geraspelte von einer Karotte kommt.

Hashwerte in Datenbanken

usernr	name	password
100	Annika	072b030ba126b2f4b2374f342be9ed44
101	Denise	d82c8d1619ad8176d665453cfb2e55f0
102	Kathrin	7f39f8317fbdb1988ef4c628eba02591
103	Sarah	9a1158154dfa42caddbd0694a4e9bdc8
104	Jana	b53b3a3d6ab90ce0268229151c9bde11

- In einer Datenbank werden i.d.R. Hashwerte statt des Passwortes im Klartext gespeichert.
- Gibt Nutzer sein Passwort ein, wird dieses gehasht und mit Hashwert in der Datenbank verglichen.
- Bei Übereinstimmung Zugang zur Webseite.

Brute-Force-Angriff

- Hat ein Angreifer eine Datenbank mit Hashwerten, kann er Milliarden von Passwörtern ausprobieren (=Brute Force).
- Ohne eine Zeitverzögerung durch den Dienst. - Denn dieser ist nicht mehr zwischengeschaltet.
- Millionen Versuche pro Sekunde möglich.
- Abfrage möglich: Hat IRGENDEINE Nutzer:in den Hashwert von passwort123?
- Die billigsten Passwörter werden zuerst geknackt.

Phishing – Was ist das?

- Angreifer „fischt “ nach Daten des Opfers
- Z.B. per Mail wird das Opfer unter einem Vorwand aufgefordert sich einzuloggen - Opfer klickt einen Link in der Mail an `https://spakrasse.de/verify`
- auf einem täuschend echt aussehenden Imitat der echten Webseite gibt das Opfer Nutzernamen und Passwort ein.
- Angreifer hat dann die Logindaten und kann diese missbrauchen.

Domains – der Wer-Bereich

https://www.youtube.com/watch?v=4xIU1lPJs_4

Domains – Der Wer-Bereich

- Domain zeigt an, wer für die Inhalte verantwortlich ist.
- Siehe Impressum!
- Hinter `https://paypa1.com` steckt nicht `https://paypal.com`
- Teil vor dem dritten Slash rückwärts lesen
- `https://postbank.de.login.xy.ru/login`
- Hat NICHTS mit `postbank.de` zu tun! Sondern xy.ru ist die Domain!

Domains – Der Wer-Bereich

- Domain zeigt an, wer für die Inhalte verantwortlich ist.
- Siehe Impressum!
- Hinter `https://paypa1.com` steckt nicht `https://paypal.com`
- Teil vor dem dritten Slash rückwärts lesen
- `https://postbank.de.login.xy.ru/login`
- Hat NICHTS mit `postbank.de` zu tun! Sondern xy.ru ist die Domain!

Schutz gegen Phishing

- Keine Links klicken, sondern SELBST die Adresse in die Adressleiste eingeben oder Lesezeichen.
- Nur in seltenen Fällen ist es nötig auf den Link in einer Mail zu klicken, z.B. um ein Passwort zurückzusetzen. Dann weiß man aber, warum genau in diesem Moment eine Mail kommt.
- In anderen Fällen **nicht auf Links klicken!** Vor allem nicht, wenn du müde oder hungrig bist!

Tückische Zufälle

- Mach dir klar: Phishing-Mails werden milliardenfach verschickt, dadurch können die absurdesten Zufälle entstehen:
  Du hast dich bei t-online über eine Störung beschwert. Eine Woche später kommt eine Mail mit einer Entschuldigung und einem Link zum Einlösen eines Gutscheins.
- Das passt und könnte trotzdem Phishing sein!

Mailpostfach = Generalschlüssel

- Angreifer:in hat Zugriff auf xyz@posteo.de
- Opfer hat bei Amazon xyz@posteo.de angegeben.
- Passwort-vergessen-Code auf diese Adresse schicken lassen.
- Angreifer:in hat Zugriff.
- Angreifer:in ändert auch noch Mail-Passwort. → Eigentümer:in des Accounts bekommt keinen Zugriff mehr . . .

Multifaktor-Authentifizierung

Authentifizierung = „Ich beweise, dass ich es bin.“
Multi-Faktor = Ich zeige es auf **mehrere** Arten

1. Wissen	Passwörter
2. Haben	Security-Token, z.B. Nitrokey, Yubikey; One-Time-Passwort (OTP); Passkey, Fido
3. Sein	Biometrische Daten wie Iris, Fingerabdruck, Venenmuster

Arten von Faktoren

1. Wissen — Passwörter üblich $\Rightarrow$ weiter verwenden!
2. Haben — Verbreitet sich zunehmend, z.B. Chipkarten, Security Token
3. Sein — Wird kritisch gesehen: Revoke (=Ungültig- Erklären) und Wechsel nicht möglich

- Übliche Kombination: **sicheres** Passwort (Wissen) + Security Token oder OTP (Haben)
- Denkfehler vermeiden: „Das Passwort ist nicht mehr so wichtig ...“

Passwörter

- Sollen nach wie vor stark sein!
- Inzwischen gilt Faustformel:
  „Länge schlägt Komplexität.“
- Studien zeigen: Sonderzeichen und Zahlen ohnehin sehr vorhersehbar benutzt: 4ufw4ch3n!
- Empfehlung: Dice-Methode

Dice-Methode

- 5 Mal würfeln $\rightarrow$ 63412
- Zufallszahl in Wortliste nachschauen $\rightarrow$ „Verbot “
- 4 solche zufällig entstandenen Wörter aneinander hängen: "VerbotRusseKalbteStatut"
- Geschichte zusammenreimen $\rightarrow$ leicht zu merkendes, sehr langes Passwort (jedoch ohne Zahlen, Sonderzeichen)
- deutsche Wortliste, z.B. `http://world.std.com/~reinhold/diceware_german.txt`

Passwörter im Browser

Passwörter **niemals** im Browser speichern ohne ein Masterpasswort zu setzen!
Falls man vergisst sich abzumelden, kann eine andere Person die Passwörter z.B. im Firefox einfach anzeigen lassen und sogar exportieren!

Haben: Time Based One Time Passwort (TOTP)

- 6-stelliges Passwort
- von einer App aus aktueller Uhrzeit und einem Schlüssel generiert
- nur 30 Sekunden lang gültig

TOTP: Berechnung

Server (z.B. posteo.de):

geheimer Schlüssel:

`facaeb6e8da2d3dcce16cf8245ed982b`

Uhrzeit:

`2020-02-15 14:40:30`

↓

Hashwert von Uhrzeit + Schlüssel

`d28918231340789 45ca1db3d53b`

Client / Token:

geheimer Schlüssel:

`facaeb6e8da2d3dcce16cf8245ed982b`

Uhrzeit:

`2020-02-15 14:40:30`

↓

Hashwert von Uhrzeit + Schlüssel

`d28918231340789 45ca1db3d53b`

TOTP: Token versus App

Yubikey und Nitrokey:

- geheimer Schlüssel auf Key gespeichert
- dort nicht auslesbar, Key spuckt nur TOTP aus, niemals den geheimen Schlüssel

Authentificator Apps:

- Geheimnis auf Gerät gespeichert
- somit unsicherer als Security-Token

Kritik an TOTP

- symmetrische Verschlüsselung (Server arbeitet mit gleichem Schlüssel wie Client)
- Verschleierung durch Hashen wie bei Passwörtern **nicht** möglich
- Somit **KEIN** Schutz gegen Angriff auf Server (wenn Angreifer:in die Datenbank stiehlt)
- Hier hätte TOTP nicht geholfen: `https://monitor.firefox.com/breaches`
- ABER: Gerät das Passwort durch den Nutzer in falsche Hände (z.B. Phishing), ist Account durch zweiten Faktor geschützt.

Wo TOTP schützt ..

- Trojaner, Keylogger
- Phishing
- Shoulder-Surfing
- Geräte-Verlust (zumindest, wenn Token nicht auch verloren oder durch PIN gesichert)
- **Nicht bei** Datenpanne beim Dienst.

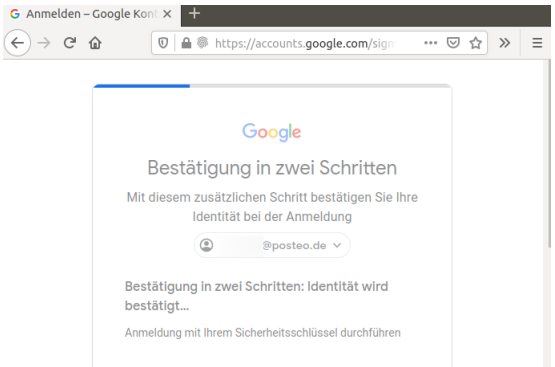
TOTP: Praxis

- z.B. Login bei Posteo zeigen: Webseite aufrufen, Mailadresse + Passwort eingeben, TOTP wird abgefragt, Yubico Authentificator öffnen, TOTP kopieren, in Webseite einfügen

Haben: FIDO, Passkeys

- FIDO-Standard
- z.B. bei Google, Tutanota möglich, sonst bisher wenige Anbieter

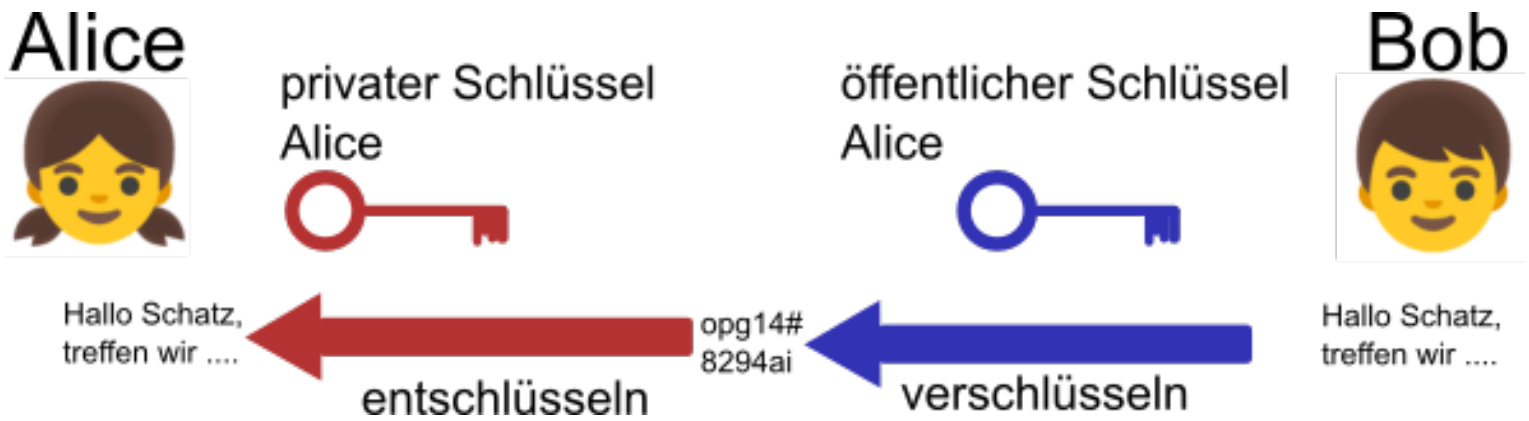
  Siehe `https://passkeys.directory/`
- Easy: einfach Stick bei Anmeldung einstecken
- keine zusätzliche Software nötig
- Sicherer als TOTP, denn basierend auf **asymmetrischer** Verschlüsselung,
- Bei Diensten nachfragen, wann FIDO kommt



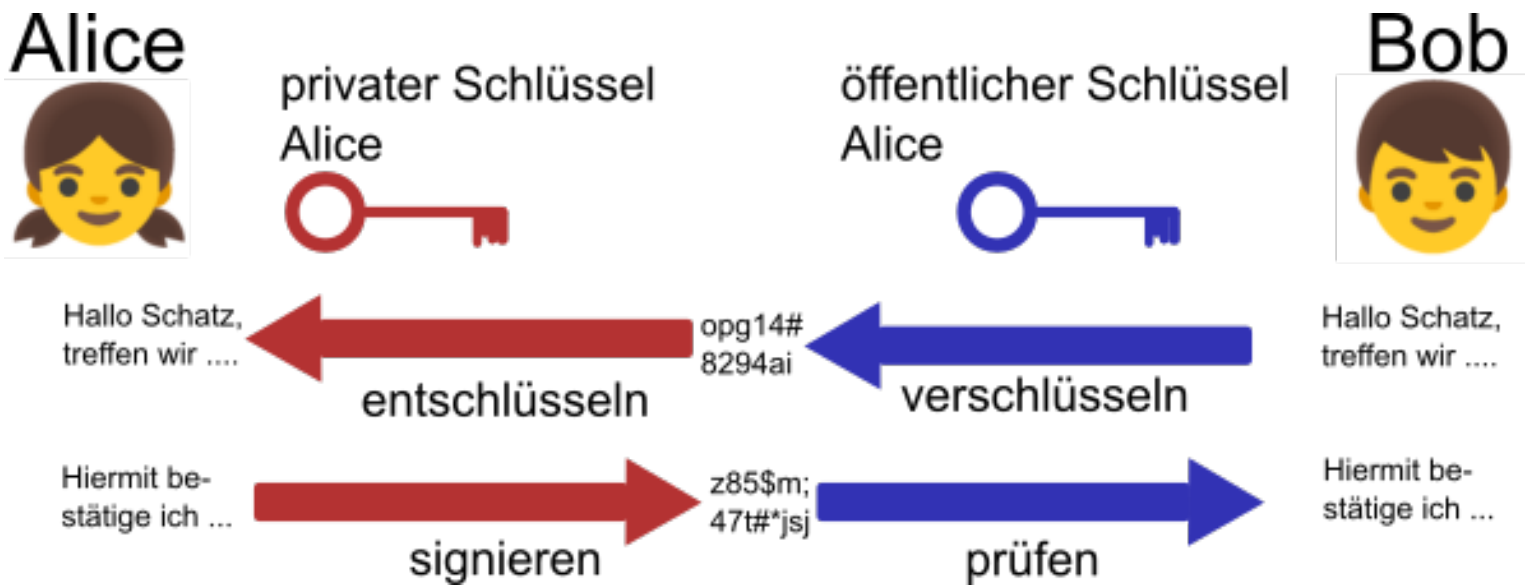
U2F - FIDO: Praxis

- z.B. Login in Github-Konto, Nutzername + Passwort, dann verlangt Browser den Stick, einstecken, antippen, fertig.

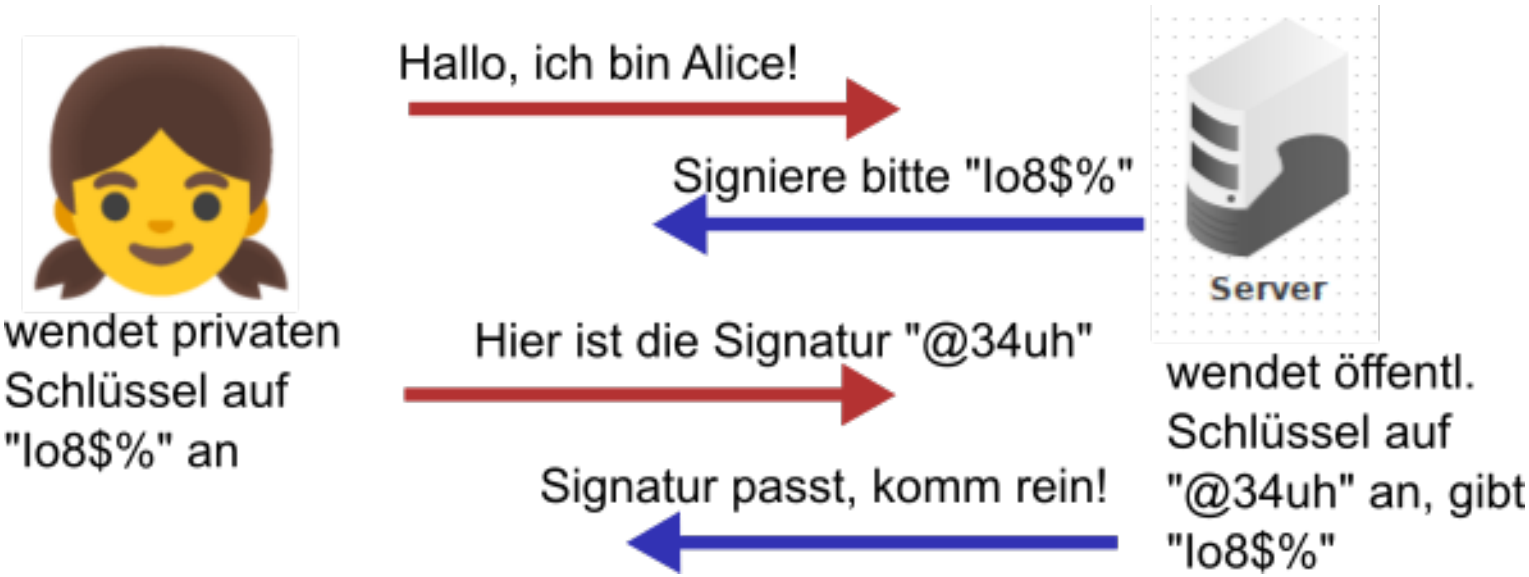
Public-Key-Verfahren



Public-Key-Verfahren



Funktionsweise bei FIDO und Passkeys



Vorteile von Public-Key-Verfahren

hat ihren
privaten Key

hat die öffentlichen
Keys der Nutzer:innen

- öffentlicher Schlüssel kann Signaturen prüfen (nicht erstellen), kann verschlüsseln (nicht entschlüsseln)
- bei Angriff auf Server entsteht in Bezug auf das Public-Key-Verfahren kein Problem
- der öffentliche Key darf gestohlen werden!
- Das ist so bei Fido und Passkeys.

FIDO vs. Passkeys

FIDO

- Schlüssel verlässt das Gerät nicht
- weniger Komfort
- hohes Sicherheitsniveau

Passkeys

- genau wie FIDO
- aber privater Key in Cloud
- viel Komfort, weniger Sicherheit
- trotzdem viel besser als schlechtes Passwort!

Mehr Infos zum Thema Passkeys:
`https://media.ccc.de/v/gpn22-303-passkeys-login-ohne-passwort`

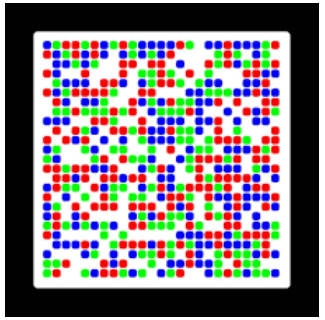
Meine Einschätzung zu Passkeys

- aktueller Hype, passwortloses Zeitalter wird versprochen
- ist sicherer als Absicherung allein mit Passwort
- komfortabel, einfach in der Bedienung
- Schutz vor Phishing
- Problem von Vendor-Lock-In, weil Passkeys aus Google-, Apple-, Windows-Universum jeweils nicht exportierbar
- Ich empfehle es **nicht** für wirklich schützenswerte Accounts wie z.B. Mailadresse!

Faktor Haben beim Online-Banking

- 2. Faktor laut Gesetz vorgeschrieben
- SMS, TOTP-App, chipTAN, Sm@rt-TAN
- nicht empfohlen SMS!

  `https://www.ccc.de/de/updates/2024/2fa-sms`
- empfohlen: Sm@rt-TAN
- privater Schlüssel auf Chipkarte + Daten der Transaktion →TAN
- Gerät nicht mit Internet verbunden



Risiken mit dem Faktor „Haben“

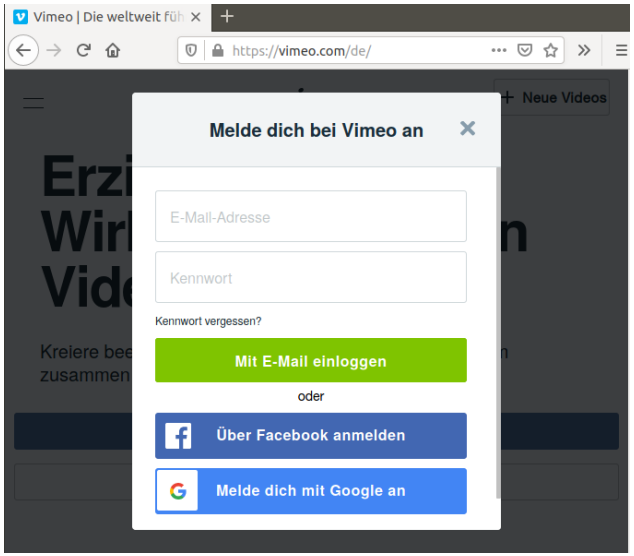
- TOTP könnte durch Phishing gestohlen werden (dann allerdings nur 1 Login möglich)
- Security Token könnte gestohlen werden / verloren gehen
- PIN des Security-Tokens 3 mal falsch eingegeben / vergessen
- Man kann sich aus dem Account aussperren, z.B. Security Token defekt
- Deshalb **Ausweichmethoden** einrichten!

Ausweichmethoden installieren!

- zweiten Key einrichten und sicher verwahren
- RecoveryCodes
- Oder geheimen Schlüssel notieren und sicher aufbewahren

Föderierte Authentifizierung

- z.B. mit Google / Facebook einloggen
- Nachteil: Datenfluss zum Identity-Provider
- eventueller Vorteil: Der Identity-Provider ist besser gesichert als ein kleines Start-up



Was zum Nachdenken ...

- Digitaler Nachlass?
- Sollen meine Erben Zugang zu bestimmten Accounts haben?
- Wie bekommen sie diesen Zugang?

Wo beginnen?

- Recovery-Mail-Adressen
- überall, wo Geld fließt
- Mit Passwortmanager Überblick behalten
- Tipp: Alle Einträge auf ungültig und erst auf gültig stellen, wenn 2FA eingerichtet
- Für normale Foren nicht nötig

Wie sehr das Mail-Postfach abdichten?

Gratwanderung zwischen Sicherheit und Komfort ...

Komfort	**Sicherheit**
Webmailer mit TOTP gesichert, **IMAP aktiviert** (nur Passwort)	Webmailer per TOTP gesichert, **IMAP deaktiviert**
Angriffe per IMAP ohne zweiten Faktor möglich	Niemand kommt ohne zweiten Faktor an Mails ran
Mails per Thunderbird, Handy-App abrufbar	Komfortabler Abruf per App / Thunderbird nicht möglich

Meine Lösung:

1. Mailadresse
für Kontakt mit Freund:innen, Kolleg:innen u.ä.

IMAP-Abruf aktiviert, 2FA im Webmailer

2. Mailadresse
Kontakt mit Diensten (Google, Amazon, Ebay ...)

2FA im Webmailer und **Eingangsverschlüsselung**
Angreifer kann nichts mit erbeuteten Mails anfangen

Falls zu kompliziert: IMAP-Zugriff sperren

Zusammenfassung

- hoher zusätzlicher Schutz durch 2. Faktor
- 2. Faktor ist nur dann ein zweiter Faktor, wenn nicht in Cloud gespeichert!
- erster Faktor immer noch wichtig!
- Ausweichmethoden einrichten
- Recovery-Mail-Adressen und Accounts mit Kontodaten besonders schützenswert

Download der Folien:

https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf

Quellen

- Kuketz-Blog `https://www.kuketz-blog.de/gnupg-e-mail-verschluesselung-unter-android-nitrokey-teil4/`
- `https://shop.nitrokey.com/de_DE/shop`
- `https://posteo.de/hilfe?tag=passwort-und-sicherheit`
- `https://www.security-insider.de/fido2-bringt-den-passwortfreien-login-a-753106/`
  zum Datenschutz bei FIDO
- Deutsche Dice-Wortliste: `http://world.std.com/~reinhold/diceware_german.txt`

Download der Folien:

- `https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf`

Praktischer Teil

- Eigenes Sicherheitskonzept entwickeln und hinterfragen
- Programme für Yubikey / Nitrokey installieren
- ... andere Anliegen?

Mein eigenes Sicherheitskonzept

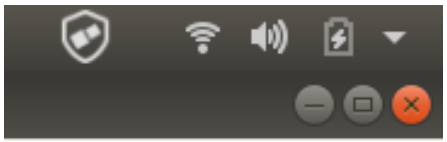
- Welches sind Ihre wichtigsten Accounts?
- Notieren Sie tabellarisch die Accounts und wie diese derzeit geschützt sind, welche Recovery-Möglichkeiten es gibt u.ä.
- Bei Bedarf erstellen Sie eine weitere Tabelle, wie Sie diese Accounts aus der ersten Tabelle künftig schützen wollen. Z.B. Recovery-Mailadresse ändern, zweiten Faktor hinzufügen, stärkeres Passwort usw.
- Beispiel einer solchen Tabelle:
  `https://raw.githubusercontent.com/sylvialange/vortraege/main/auth.pdf`

Sicherheitskonzept hinterfragen

- Sind die Passwörter von wichtigen Konten unique?
- Wie oft gibt es „Passwort auswendig, Passwort unique“? Realistisch?
- Wie gut sind die Konten gegen Aussperren geschützt?
- Sind Konten leicht über Recovery-Möglichkeiten zu übernehmen?
- ...

Nitrokey mit Linux

- `https://www.nitrokey.com/documentation/installation`
- Dort verwendetes Modell und Betriebsystem wählen.
- In der Regel genügt: sudo apt-get update && sudo apt-get install libccid nitrokey-app
- Im Dash nach Nitrokey-App suchen und starten.
- Oben rechts neben Akkusymbol erscheint das Nitrokey-App-Symbol.



Nitrokey mit Windows

- `https://www.nitrokey.com/download/windows`
- Dort gibt es einen Link auf Github: `https://github.com/Nitrokey/nitrokey-app/releases/latest`
- In der Rubrik Assets die exe-Datei herunterladen und als Administrator ausführen.

Yubikey mit Linux

- Terminal: sudo apt-add-repository ppa:yubico/stable
- sudo apt update && sudo apt install yubioath-desktop yubikey-personalization-gui
- Im Dash nach Yubico Authentificator suchen und starten
- Erklärvideo:
  `https://www.youtube.com/watch?v=mdQzbng4B7o`

Yubikey mit Windows

- auf `https://yubico.com` →Support →Downloads
- die Authentificator-App herunterladen
- Erklärvideo:
  `https://www.youtube.com/watch?v=mdQzbng4B7o`

Yubikey mit Android

- Im Playstore Yubico Authentificator herunterladen oder
- auf `https://github.com/Yubico/yubioath-android/releases` APK herunterladen und installieren