# Schütze deine digitale Identität!

## Multifaktor-Authentifizierung

Sylvia Lange

Cryptoparty Tübingen, 15.2.2020

# Fragen?

- Es gibt keine dummen Fragen!
- Verständnisfragen bitte direkt.
- Alle anderen Fragen im Anschluss an den Vortrag.

# Sylvia Lange

- Lehrerin für Informatik (Oberstufe am Beruflichen Gymnasium)
- Mitglied des Chaos Computer Club
- Beschäftigung mit Datenschutzthemen in der Freizeit, z.B. bei Events des C3

# 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!

# 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**!

# Passwörter reichten nicht: Doxingskandal 2018

- Weihnachten 2018: Jugendlicher „Hacker“ **ohne besondere Hacker-Künste** gelangte an Daten von Politikern.
- Nutzt Passwort-Zurücksetzen-Funktion.
- Veröffentlicht intime Chatverläufe von Politikern.

# 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

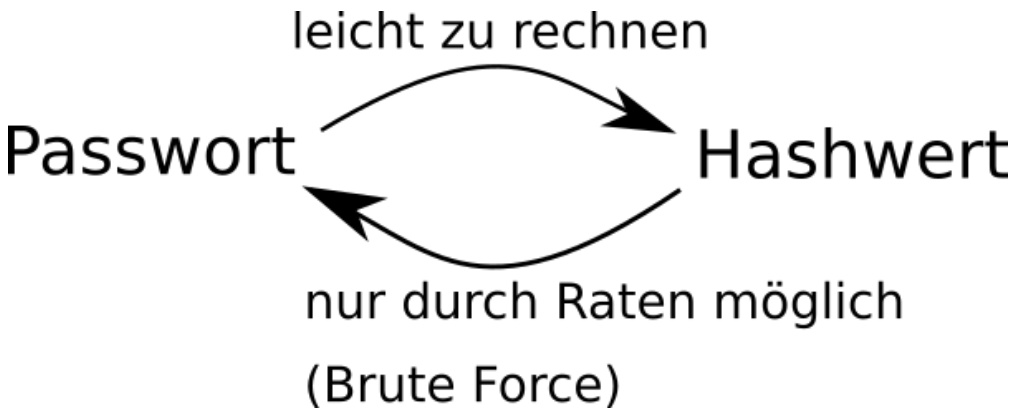
# Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen
- Die „Berta“ hat’s gehört, wie Uli sein Passwort murmelt ...
- 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
- Die „Berta“ hat’s gehört, wie Uli sein Passwort murmelt ...
- Datenpanne beim Dienst. Datenbank mit Useraccounts gestohlen. `https://sec.hpi.uni-potsdam.de/ilc/search?lang=de`

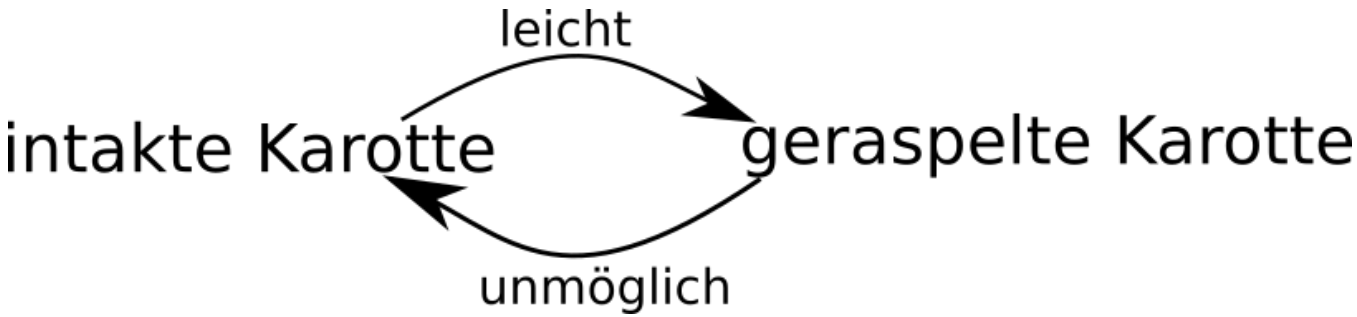
# Exkurs: Hashfunktion




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.

# Der Generalschlüssel zur digitalen Idenität

- Angreifer hat Zugriff auf xyz@posteo.de
- Z.B. bei Amazon xyz@posteo.de angegeben.
- Passwort-vergessen-Code auf diese Adresse schicken lassen.
- Der Angreifer hat Zugriff.
- Angreifer ändert auch noch Mail-Passwort. ➔Eigentümer 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) |
| 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 → 63412
- Zufallszahl in Wortliste nachschauen → „Verbot “
- 4 solche zufällig entstandenen Wörter aneinander hängen: "VerbotRusseKalbteStatut"
- Geschichte zusammenreimen → leicht zu merkendes, sehr langes Passwort (jedoch ohne Zahlen, Sonderzeichen)
- deutsche Wortliste, z.B. `http://world.std.com/~reinhold/diceware_german.txt`

# Haben: Time Based One Time Passwort (TOTP)

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

# TOTP: Berechnung

Server (z.B. tutanota.com):

geheimer Schlüssel:

facaeb6e8da2d3dcce16cf8245ed982b

Uhrzeit:

2020-02-15 14:40:30

↓

Hashwert von Uhrzeit + Schlüssel

d2891823134078945ca1db3d53b

?=

Client / FIDO-Stick:

geheimer Schlüssel:

facaeb6e8da2d3dcce16cf8245ed982b

Uhrzeit:

2020-02-15 14:40:30

↓

Hashwert von Uhrzeit + Schlüssel

d2891823134078945ca1db3d53b

# TOTP: Token versus App

Yubikey und Nitrokey:

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

Authentificator Apps:

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

# Kritik an TOTP

- symmetrische Verschlüsselung
- Verschleierung durch Hashen wie bei Passwörtern **nicht** möglich
- Somit **KEIN** Schutz gegen Angriff auf Server.
- Hier hätte TOTP nicht geholfen: `https://monitor.firefox.com/breaches`
- ABER: Gerät das Passwort durch den Nutzer in falsche Hände, ist Account durch zweiten Faktor geschützt.

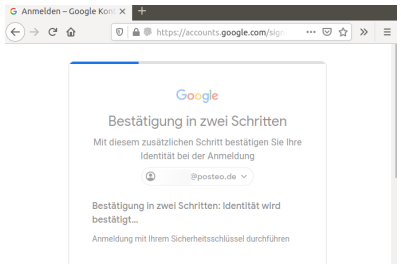
# Wo TOTP schützt ..

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

# TOTP: Praxis

# Haben: Universal 2 Factor Authentification (U2F)

- FIDO-Standard
- z.B. bei Google, Tutanota möglich, sonst bisher wenige Anbieter
- Easy: einfach Stick bei Anmeldung einstecken
- keine zusätzliche Software nötig
- Sicherer als TOTP, denn basierend auf **asymmetrischer** Verschlüsselung, geheimer Schlüssel sicher auf Security-Token verwahrt.
- Bei benutzten Diensten nachfragen, wann FIDO implementiert wird.



# U2F - FIDO: Praxis

# Faktor Haben beim Online-Banking

- 2. Faktor laut Gesetz vorgeschrieben
- SMS, TOTP-App, chipTAN
- Mike Kuketz empfiehlt chipTAN
- geheimer Schlüssel auf Chipkarte + Daten der Transaktion →TAN
- Gerät nicht mit Internet verbunden


# Risiken mit dem Faktor „Haben“

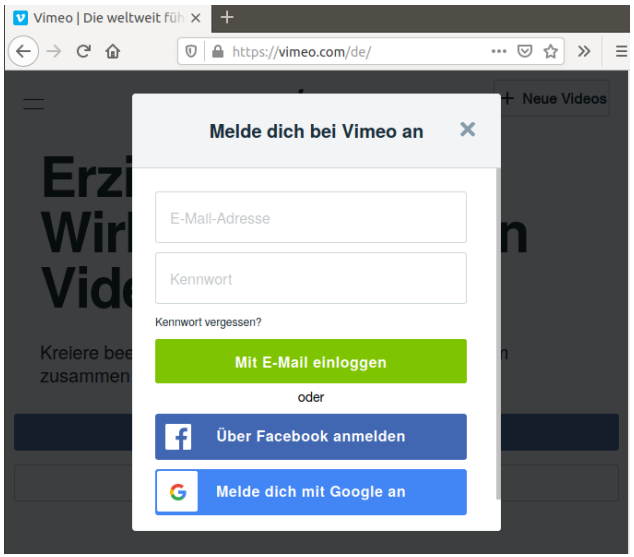
- TOTP könnte durch Phishing gestohlen werden (dann allerdings nur 1 Login möglich)
- Security Token könnte gestohlen werden / verloren gehen
- PIN des Tokens 3 mal falsch eingegeben / vergessen
- Man kann sich aus dem Account aussperren, z.B. Security Token defekt
- Deshalb **Ausweichmethoden** einrichten!

# 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?

# Praktische Umsetzung: Entscheidung für einen Key

| **Nitrokey** | **Yubikey** |
| --- | --- |
| offene Software, offene Hardware | proprietäre Software |
| etwas teurer (29€ + 49€), schlechteres Design | sehr hübsch, 49€ |
| Berliner Firma | us-amerikanische Firma |
| saubere Webseite (nur 4 Cookies) | verwanzte Webseite mit vielen Dritt-Domains (hat mit Key an sich nichts zu tun, zeigt aber etwas über die Firma) |
| nur bei `https://shop.nitrokey.com` verfügbar | zwar nicht im Elektromarkt aber immerhin bei Amazon verfügbar. |

# Yubikey

- Blaues Modell für 25€ bietet nur FIDO, z.B. Absichern des Posteo-Postfaches nicht möglich.
- Yubikeys der 5er-Serie für ca. 50€ haben alle Funktionen, die man braucht: FIDO, TOTP, statisches Passwort, OpenPGP
- TOTP auch am Handy möglich

# Nitrokey


**Nitrokey FIDO2**

- Kinderleichter Schutz Ihrer Benutzerkonten
- Passwortloses Login (FIDO2)
- Zwei-Faktor-Authentisierung (2FA, FIDO U2F)

**29,00 €**


**Nitrokey Pro 2**

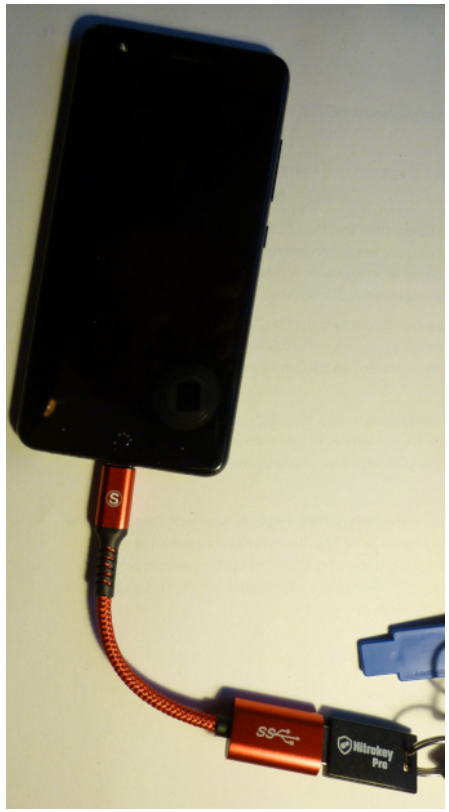
- Sicheres Login mit Einmalpasswörtern
- E-Mail-Verschlüsselung
- Festplatten- und Dateiverschlüsselung
- Manipulationssichere Chipkarte
- Open Source & Open Hardware

**49,00 €**

- FIDO-Stick kann nur FIDO
- Nitrokey Pro 2 für ca. 50€ kann: TOTP, statisches Passwort, OpenPGP, KEIN FIDO
- 29€ mehr Invest als bei Yubikey, TOTP am Handy nicht möglich

# NFC = Near Field Contact

- Yubikey hat NFC
- Komfortable Benutzung am Handy möglich
- unnötige Sicherheitslücke?
- Statt NFC auch USB OTG („on the go“) möglich.




Nitrokey über USB OTG verbunden

# 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 Freunden, Kollegen 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

# Bonus: OpenPGP

- Security-Token als Smartcard
- RSA-Keys für Mailverschlüsselung sicher auf Smartcard speichern
- Schlüssel verlässt die Smartcard nicht. Alle Operationen finden auf der Smartcard statt.
- Funktioniert z.B. mit Thunderbird und Openkeychain.

# Zusammenfassung

- hoher zusätzlicher Schutz durch 2. Faktor
- erster Faktor immer noch wichtig!
- Ausweichmethoden
- Recovery-Mail-Adressen und Accounts mit Kontodaten besonders schützenswert

Download der Folien:
`https://walz-lange.de/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://walz-lange.de/2fa.pdf

# Praktischer Teil

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

# Mein eigenes Sicherheitskonzept

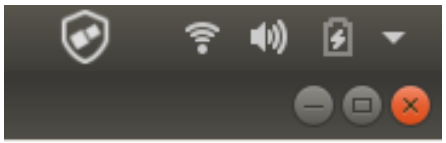
- Welches sind Ihre wichtigsten Accounts?
- Notieren Sie tabellarisch die Accounts und wie diese derzeit geschützt sind, welche Recovery-Möglichkeiten es gibt u.ä.
- Bei Bedarf erstellen Sie eine weitere Tabelle, wie Sie diese Accounts aus der ersten Tabelle künftig schützen wollen. Z.B. Recovery-Mailadresse ändern, zweiten Faktor hinzufügen, stärkeres Passwort usw.
- Beispiel einer solchen Tabelle:
  `https://walz-lange.de/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/tag/v1.4
- 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.invidio.us/watch?v=mdQzbng4B7o`

# Yubikey mit Windows

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

# Yubikey mit Android

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