P4sswort! Hacking

10.06.2023 - Inflac

Ablauf

Passwörter [

- Wofür Passwörter?
- Wie funktioniert ein Login?
- Wie werden Passwörter gespeichert
- Was für Anforderungen gibt es an Passwörter?
- Wie kommen Angreifer an Passwörter?

]

Demo [...]

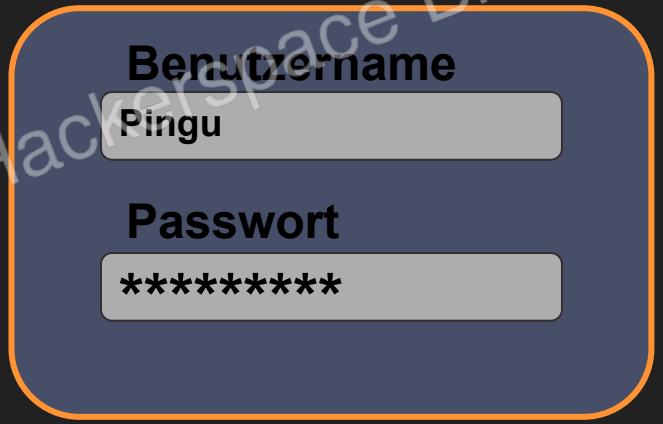
Schutz [...]

Wofür Passwörter?

Offline

VS.

Online



Wo nutze ich Passwörter wie?

Online Shopping

Unterhaltung

Banking

Gesundheit

Ich habe doch nichts zu verbergen

SELBSTHILFE KONTAKTSTELLE

Erweiterte Informationen: https://youtu.be/Kjxfhb-2hRg

Wie funktioniert ein Login?

Server

E-Mail Adresse	Benutzername	Passwort
guenther@gmx.de	guenni50	abcdefg

Wie funktioniert ein Login?

- Datenbank (Tabelle)

E-Mail Adresse	Benutzername	Passwort
guenther@gmx.de	guenni50	abcdefg
naiver@nutzer.de	freddi_faulig	moinmeister
kuschelbär@hotmail.de	haeckseHD	liebe

Wie funktioniert ein Login?

Benutzername	Passwort
guenni50 ?	abcdefg ?
freddi_faulig	moinmeister
haeckseHD	liebe

Server

guenni50

abcdefg

Datenbank leak

Datenbank wird veröffentlicht

- Benutzernamen
- Passwörter
- E-Mail Adressen
- ...

Wie funktioniert ein Login?

Server

Hashfunktion

E-Mail Adresse	Benutzername	Passwort
guenther@gmx.de	guenni50	7ac66c0f148de9519 b8bd264312c4d64

Wie werden Passwörter gespeichert?

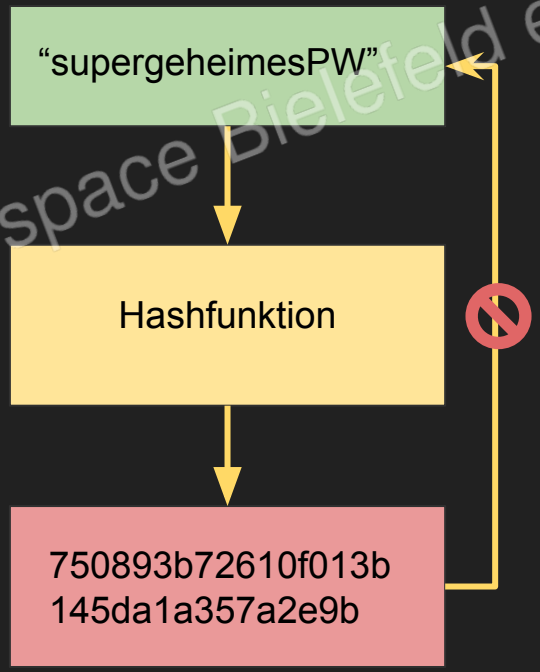
- Datenbank (Tabelle)
- Passwort wird gehasht (im besten Fall)
- Hashing: Kryptografische Einwegfunktion

E-Mail Adresse	Benutzername	Passwort
guenther@gmx.de	guenni50	7ac66c0f148de9519b8bd264312c4d64
naiver@nutzer.de	freddi_faulig	20b44c69af56f3fb3f9ecb4753a32dca
kuschelbär@hotmail.de	haeckseHD	eb755ccf2e8fa968a9db849abef02038

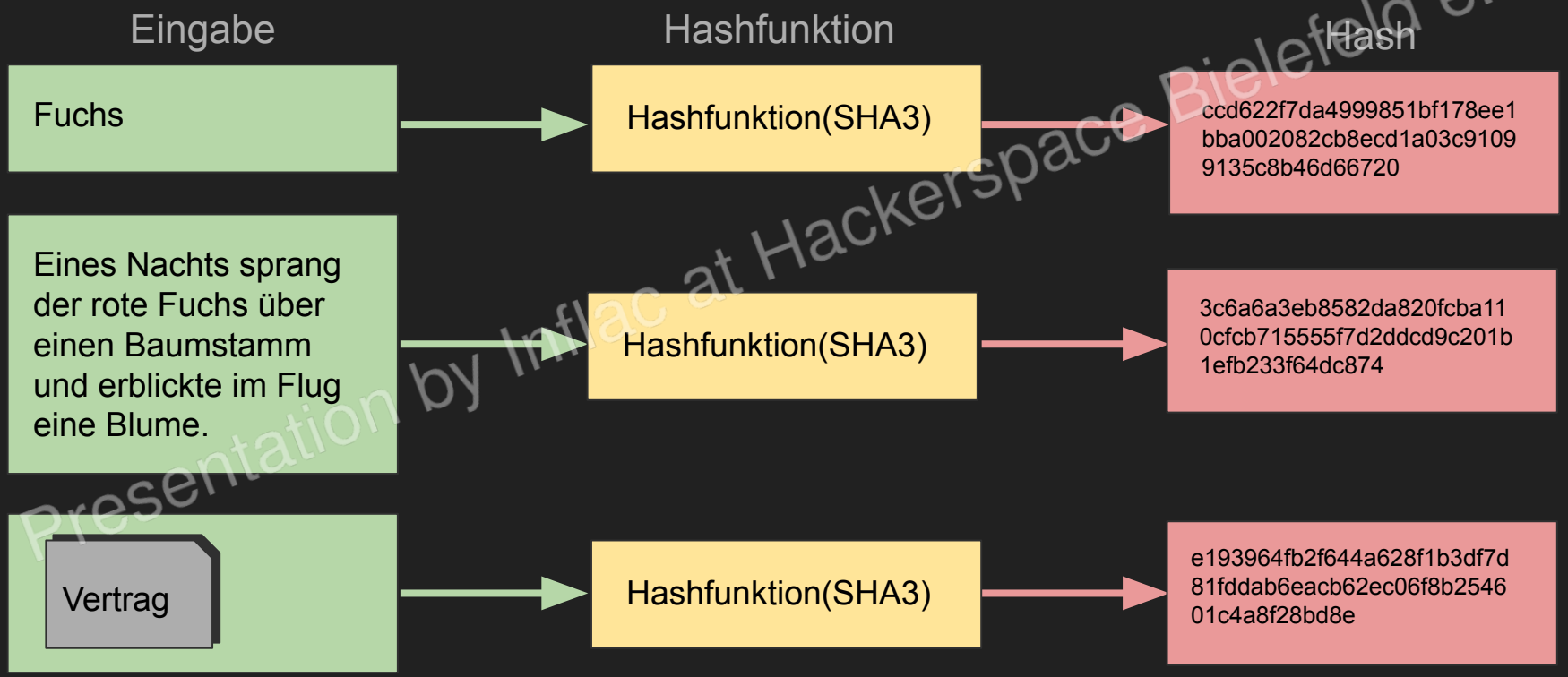
Exkurs: Hashing

Exkurs: Hashing

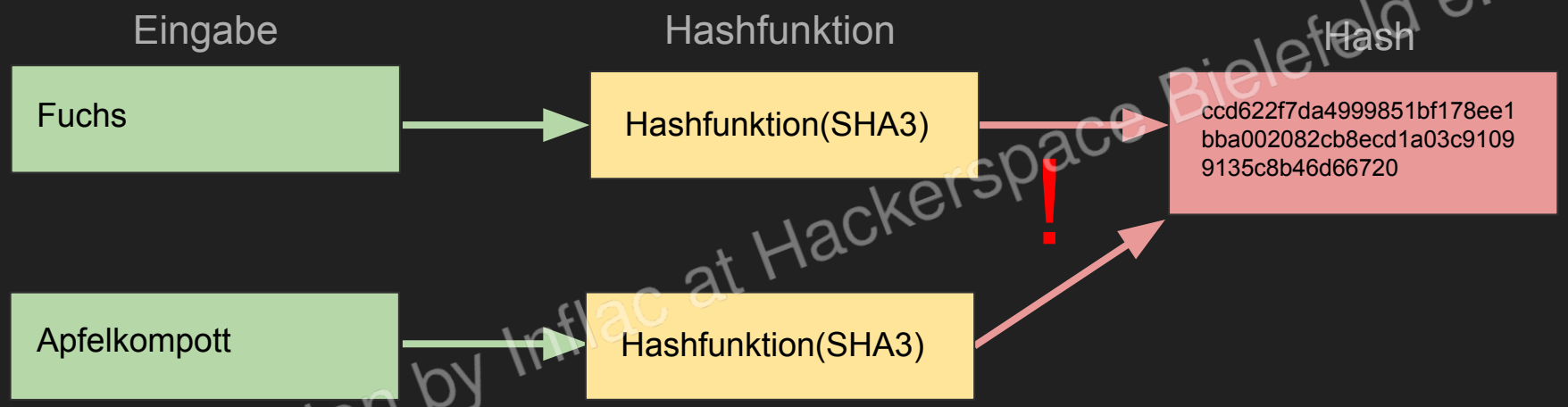
- Kryptografische Einwegfunktion
- Beliebige Eingabelänge
- Feste Ausgabelänge
- Aus dem Hash kann die Eingabe nicht wiederhergestellt werden.
- Es ist sehr schwierig, Eingaben zu finden, die den gleichen Hash haben.



Exkurs: Hashing

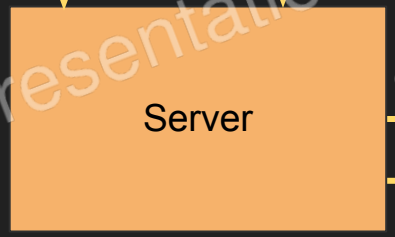


Exkurs: Hashing



Wie funktioniert ein Login?

Benutzername	Passwort
guenni50	7ac66c0f148de9519b8bd264312c4d64
freddi_faulig	20b44c69af56f3fb3f9ecb4753a32dca
haeckseHD	eb755ccf2e8fa968a9db849abef02038



guenni50

abcdefg

7ac66c0...

Was für Anforderungen gibt es an Passwörter?

- Mindestens 12 Zeichen [**********]
- Groß- und Kleinschreibung [a-Z]
- Zahlen [0123456789]
- Sonderzeichen [#!*~”§$%/()&/`[]{}\<>|€…]

ok: A7$p=2’%1J super: 0dE%t:,#9OLFv6Q1,Ziq

schlecht: Apfel1203! schlecht: Reispfanne123456#*

Erweiterte Informationen: https://www.youtube.com/watch?v=3NjQ9b3pgIg

Was für Anforderungen gibt es an Passwörter?

Passwort: Kraftwerk 2 5 *

Struktur: WORT || ZAHL || ZAHL || ZEICHEN

Wörterbuch [00-99] [!,#,*,?,§,$,%,&,/]

1.000.000 ✖ 100 ✖ 9

= 900.000.000

Wie kommen Angreifer an Passwörter?

- Bruteforce = Alle Kombinationen ausprobieren
- Wörterbuchangriff = Ausgewählte Kombinationen
- Phishing, Social Engineering
- Datenbank breach
- Shoulder Surfing
- Rainbowtables
- …

Ablauf

Passwörter […]

Demo [

- Wörterbuchangriff
- Datenbank breach
- ~~Phishing~~

]

Schutz […]

Bruteforce

Ziel: Alle Kombinationen ausprobieren und richtige finden

Erweiterte Informationen: https://youtu.be/7U-RbOKanYs

Bruteforce

Annahme: 8 Zeichen aus [A-Z]

Anzahl Kombinationen:

= 26 * 26 * 26 * 26 * 26 * 26 * 26 * 26

= 26^8 = 208.827.064.576

Warum sind 8 Zeichen dann nicht ausreichend?

Bruteforce

Rechner: 10.000.000.000 Passwörter pro Sekunde

Passwort Komplexität: 208.827.064.576

$$\frac{208.827.064.576}{10.000.000.000} \approx 97.24 \text{ Sekunden}$$

Bruteforce

Annahme: 12 Zeichen aus [a-Z] und [0-9] und [!,#,*,?,§,$,%,&,/]

Passwort Komplexität: $(26+26+10+9)^{12}$ = 16.409.682.740.640.811.134.241

Rechner: 10.000.000.000 Passwörter pro Sekunde

Passwort Komplexität: 16.409.682.740.640.811.134.241

$$\frac{16.409.682.740.640.811.134.241}{10.000.000.000} \approx 52034.762 \text{ Jahre}$$

Wörterbuchangriff

Ziel: Viele Kombinationen ausprobieren und richtige finden

Wortlisten um häufige Kombinationen abzudecken

1234
12345
passwort
januar
kaffee
rockyou
…

Erweiterte Informationen: https://youtu.be/7U-RbOKanYs

Wordlist: https://github.com/Edd13Mora/MoroccanRockyou/blob/main/MoroccanRockyou.txt

Datenbank breach

- Twitter (2023)
  235-400 Millionen Daten

- Plex (2022)
  20 Millionen Benutzernamen

- LinkedIn (2021)
  700 Millionen Benutzer

- Facebook (2019)
  533 Millionen Benutzer


```
"full_name":"charlie [redacted]","gender":"male",
"linkedin.com/[redacted]5",
"linkedin_username":"charlie-[redacted]5","linkedin_id":"2[redacted]3",
"facebook_url":"facebook.com/v[redacted]",
"facebook_username":"v[redacted]",
"facebook_id":"1[redacted]5",
"work_email":"c[redacted]com",
"mobile_phone":"+15[redacted]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts"
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01",
"linkedin_connections":120,"inferred_salary":"[redacted]",
"inferred_years_experience":5,
"summary":"I am a motivated researcher with a [redacted]
"full_name":"mehari [redacted]"
"linkedin_url":"linkedin.com/[redacted]",
"linkedin_username":"mehari-[redacted]5",
```

Datenbank breach

https://haveibeenpwned.com/

Ablauf

Passwörter […]

Demo […]

Schutz [

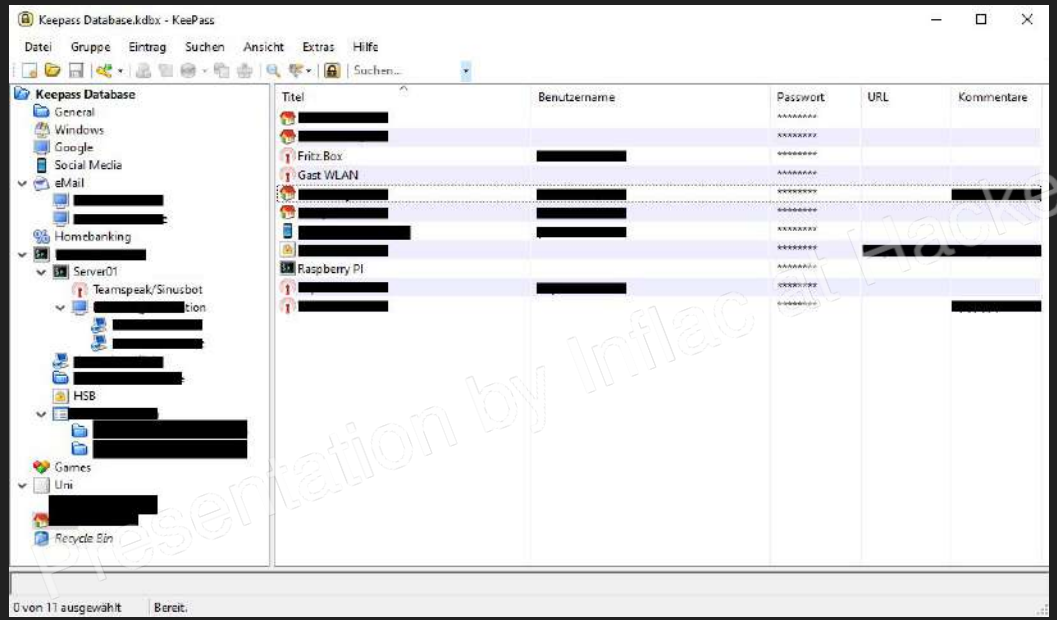
- Passwort Manager
- MFA
- Geheim Trick :)

]

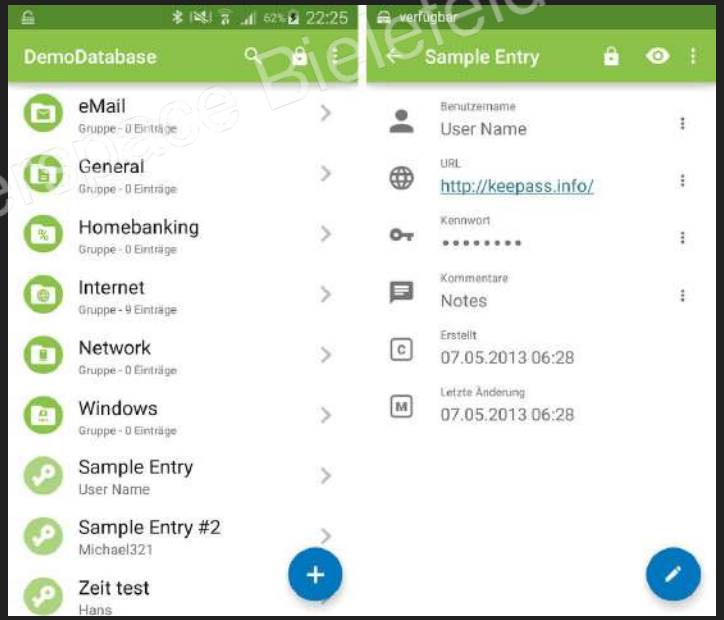
Passwortmanager

Erweiterte Informationen:
Passwortmanager Vergleich: https://www.youtube.com/results?search_query=passwort+manager+vergleich
Laspass Hack: https://www.heise.de/news/Passwort-Manager-LastPass-meldet-Sicherheitsvorfall-Bitwarden-streitet-ab-7362705.html, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/
Keepass CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32784

KeePass

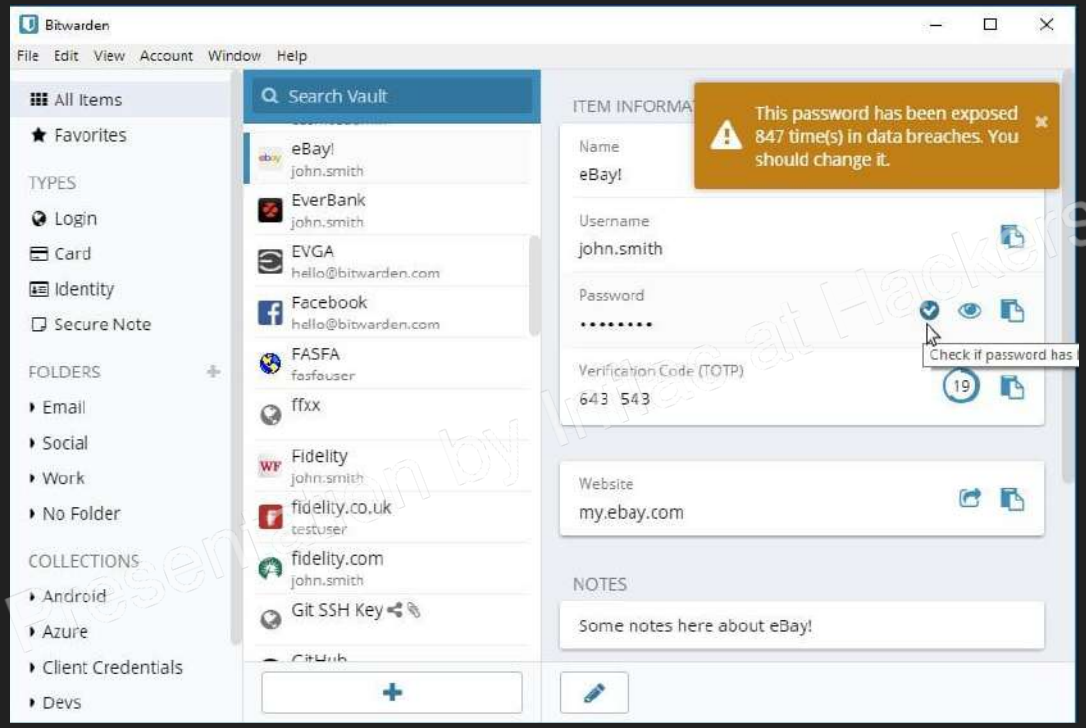


Desktop Client

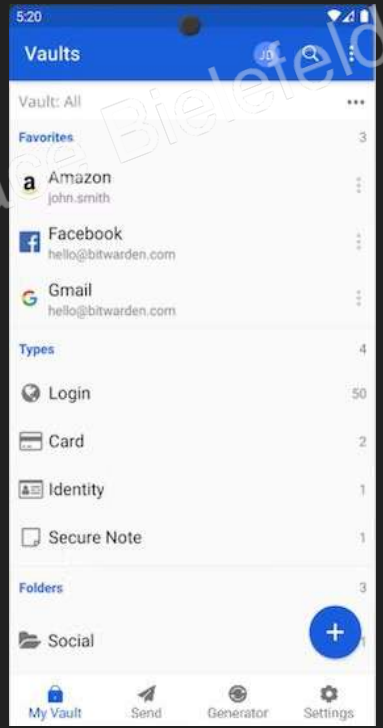


Mobile Client

Bitwarden



Desktop Client



Mobile Client

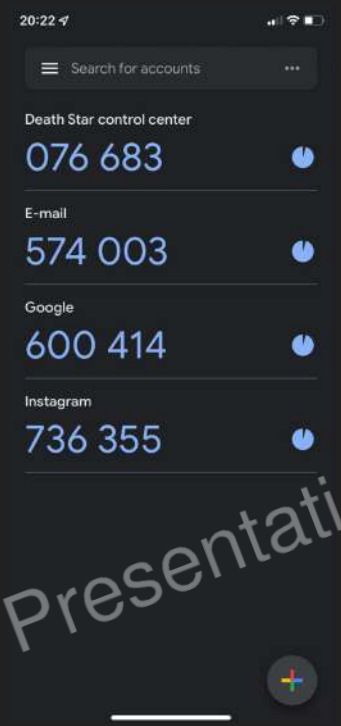
Bitwarden vs KeePass

Bitwarden	KeePass
Speichert in der Cloud ● Einfacher Zugriff ● Immer Synchronisiert	Speichert lokal auf eurem Gerät ● Einfacher Zugriff ● Man muss die Datenbank selber Synchronisieren
Hat einige Zusatzfunktionen	Es gibt Plugins für Erweiterungen
Man kann Daten als Datei Exportieren	Daten direkt in Datei verfügbar
Sichere Verschlüsselung	Sichere Verschlüsselung
Passwortgenerator	Passwortgenerator

Multi Faktor Authentifizierung(MFA)

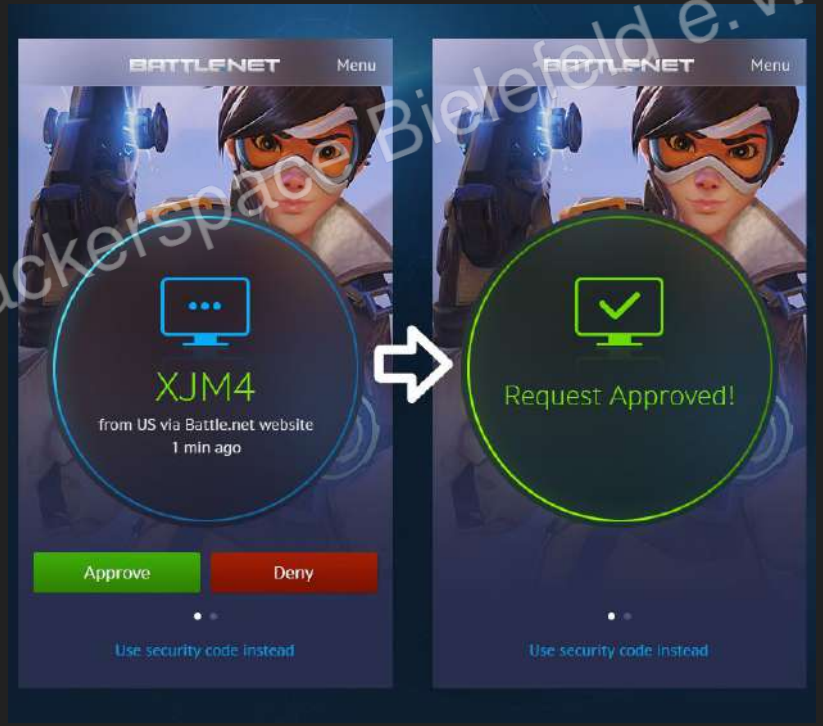
Wissen	Besitzen	Inhärenz(Sein)	Standort, etc.
- Passwort	- Smartphone	- Fingerabdruck	- IP-Adresse
- Pin	- Tan Generator	- Gesicht	- Zugriffszeiten
- “Sicherheits”-Frage	- Chipkarte	- Iris	- …
	- USB Token	- Stimme	

Besitzen



Google Authenticator

SMS



Blizzard Mobile Authentication

Erstell nicht überall
einen Account

Weitere Interessante Materialien

- Hashfunktionen: https://www.youtube.com/watch?v=evx8gptqoro
- Passwörter aus dem Browser klauen: https://youtu.be/uYJTt8vZ9f4
- Password cracking: https://youtu.be/z4_oqTZJqCo
- WLan WPA/WPA2 hacking: https://www.youtube.com/watch?v=GLmpLeghM2Y
- Passwort Salt/Pepper: https://www.youtube.com/watch?v=KiypYcB6NZ8
- Die sicherste Verschlüsselung: https://www.youtube.com/watch?v=nKEKDS0epKw
- Ich habe doch nichts zu verbergen: https://youtu.be/Kjxfhb-2hRg
- Sicherheitslücken in E-Mail: https://efail.de/
- Sicherheit im Internet: https://www.youtube.com/@networkanddatasecurityruhr6966/videos

Danke

Mail: inflac@inflacsan.de Matrix: @inflac:matrix.space.bi

Danke

https://inflacsan.de/presentation/rand_and0jsdjah9w82z498z19bsuadi1z91/SicheresP4sswort!.pdf

Mail: inflac@inflacsan.de Matrix: @inflac:matrix.space.bi