Passwortmanager für persönliche Sicherheit & Datenschutz

Kieler Linux Tage
2021Sep18 @ 10:00
Big Blue Button

der.hans (https://floss.social/@FLOX_advocate)
CDE
Object Rocket, a rackspace company
https://www.ObjectRocket.com/

Wir suchen gerade Elasticsearch und MongoDB DBA

ObjectRocket
https://www.objectrocket.com/careers/

Rackspace Technologies
https://rackspace.jobs/

kommende Veranstaltungen

- RaiseMe career counseling
  - bei ShellCon, 2021Okt08-09
- Fediverse: Decentralized Social Networking and Services
  - bei GeekBeaconFest, 2021Okt16
- Introduction to Nextcloud
  - bei SeaGL, 2021Nov05-06
- Intro to jq: grep for JSON
  - bei SeaGL, 2021Nov05-06
- Weitere Infos
  - https://www.LuftHans.com/talks

Zuerst

IBKR

Und

ausdrücklich…

Noch wichtiger!

IBNDR

Wenn Du irgendwelche Rechtsberatung brauchst, setz' Dich mit Deinem eigenen Rechtswanwalt in Verbindung

GDPR

mit GDPR ist unser Begriff auf unsere eigene Dataien erweitert

es soll auch weniger persönlicher Infos von Firmen gespeichert werden

Firmen haben aber nicht Plötzlich bessere Sicherheit

Wieso brauchen wir eigene Sicherheit?

Spectre/Meltdown (schon wieder)

— FRITZed — Heartbleed — Apple SSL — Apple iCloud — Yahoo! x 2 — LinkedIn x 3 — Eharmony — Last.FM — Adobe

— Mat Honan — Jennifer Lawrence — Kate Upton — Rhianna

Das wahre Risiko

> "They could have used my e-mail accounts to gain access to my online banking, or financial services. They could have used them to contact other people, and socially engineer them as well." – Mat Honan

Was ist eigentlich zu verlieren?

> "more than a year’s worth of photos, covering the entire lifespan of my daughter" – Mat Honan

> "including those irreplaceable pictures of my family, of my child’s first year and relatives who have now passed from this life" – Mat Honan

Dateien Saugen

- 90% alle bekannte Dateien wurden in der letzte 2 Jahren gesammelt
    - aus einer 2019 Freakanomics Podcast

Ganz Wichtig!

- Patchen!
- Nur von vertraulichen Softwarequellen!

Verschlüsselungsbeispiel

- Postkarte v. Briefumschlag

Wann soll man Verschlüsselung benutzen?

- Immer :)
- Jedes Mal
- HTTPS Everywhere vom EFF

Was soll man verschlüsseln?

- Beschienigungen
- Persönliche (identifizeriende) Infos
    - Name
    - Anschrift
    - Telefonnummer
    - EC Karte Infos
    - Gesundheitsinformation
    - Privatfotos
    - Schuhgroße

Passwortüberschneidung

- Gleiche Passwort bei viele Domänen?
- Einbruch bei einer kann schnell Einbruch bei allen werden
- Benutze einmalige Passwörte bei jedem Dienstanbieter

Bescheinigung für Zugang

- Bescheinigungen sind nich nur Benutzernamen u Kennwörter

Bist Du Du?

- Benutzername, oft Emailanschrift
- Passwort
- Sicherheitsfragen und -antworten
- Multifakter Authentizierung (MFA)
- Körperteil

Einzigartige Beschienigungen

- jeder Teil soll einzigartig für jede Webseite
- jeder Teil, nicht nur als Ganzes
- gewisse Einschränkungen gelten

Random String / zufallsbedingte Zeichenkette

- unerkennbarer Zeichensalat
- je längere und zufälligere Ketten desto besser
- benutze
    - alphabetische Buchstaben
    - Nummern
    - Satzzeichen (`!@#$%^&*.,/:\;`)
- Acht auf
    - gleichaussehenede Zeichen Falls man es tippen oder aussprechen muss
    - Unterstreichen und Ergänzungsstrich
    - Leertasten und Tabulator
- Kettenbeispiel: `fnYV@tki4M’jj;iTW]21`

Passsätze / Wortsalat

- unsinnige Wortsequenz
- je längere und zufälligere Wortketten desto besser
- Wörter aus mehreren Sprachen
- Deklination und Konjugation
- großbuchStaben iM woRt
- zufällige Satzzeichen
- Beispiel: purplish Leche verFaehrt singing liberte
- bekanntes XKCD Beispiel: correct battery horse staple

Hilfe, da spinne ich …

Aber, Hans, es ist viel zu viel um auswendig zu lernen und nicht Mal so Interessant wie kernel debug logs …

Passwortmanager

- Beschienigungsinfos sicher speichern
- sehr einfach zu nutzen

Passwortmanager Anforderungen

- freie Software
- verborgene Passwörter
- lokal Verschlüßelt
- Operating System unabhängige Datei
- Dateien Freisetzung
- Zwischenspiecher automatisch löschen
- einfache kopieren und einfügen
- konfigurbare Passwortgenerator
- Notizen

Passwortmanager Bonusrunde

- lesbare und sprechbare Passworterstellung
- zufallsbedingte Wortgeneration
- Sprachhinweise
- zufallsbedingte Zeichenskettegenerator immer zugreifbar
- Daten exportieren mit Sync

meine Empfehlungen

- GNU/Linux or BSD Device
  - KeePassXC (keepassxc-cli)
  - KeePassX, version 2.x (kpcli)
- Web
  - Nextcloud
    - WebAppPassword
    - Passman
    - Passwords
  - BitWarden
- Android
  - KeePassDroid u viele andere bei FDroid
- andere Betriebssysteme
  - KeePass

Ein Passwort um die Alle zu behalten

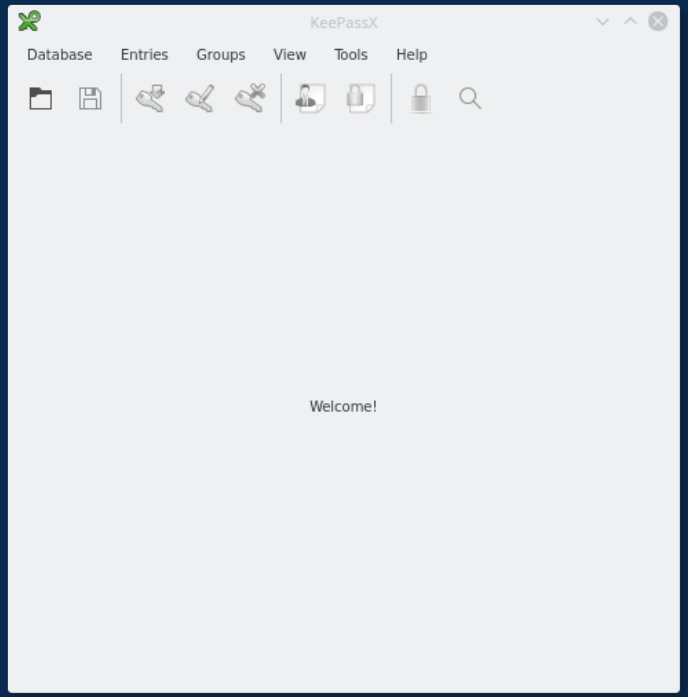
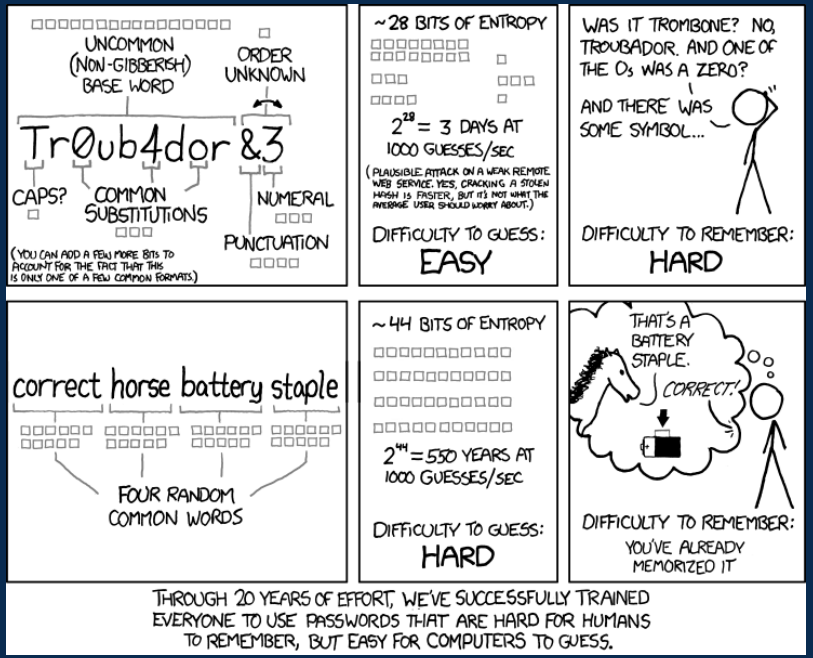


Figure 1. KeePassX

Ein Passwort um die Alle zu schützen

Passsätze / Passphrases



XKCD: Password Strength - https://xkcd.com/936/

aussprechende Zeichenketten

- nutzbar fürs Telefonieren
- Vorsicht vor gleichaussehenden Zeichen
  - 1 l
  - 0 O
- Sprachhinweise
  - werecbyivofejmu (wer-ec-byiv-of-ej-mu)

Ich bin Ich!

Authentifikation stellt sicher, daß Du Du bist

Wie kann man es beweisen?

- 3 Arten Beschienigungsinfos
    - Was weißt Du?
        - Benutzername, Passwort, PIN
    - Was hast Du?
        - Ausweis, Handy, Token
    - Was bist Du?
        - Fingerabdruck, DNA, Gesichtserkennung
            - https://reclaimyourface.eu/

4. Art: Token

- Browser Cookies
- Handy Device ID

ID: Benutzername

- Womöglich, zufällige Zeichenketten benutzen
  - zB: Bank, Einkaufen, usw
  - Ex: `eddyityoz`
- zufällige Zeichenketten sind für Social Network nicht geeignet
- erkennbare Namen: öffentliche und gesellschäftliche Sites
  - Es: `FLOX_advocate`

ID: Emailanschrift

- Subaddressing
  - `benutzername@gmail.com`
  - `benutzername+randomstring@gmail.com`
- Super bei Mailfiltern
  - `benutzername+3qkrl-ebay@gmail.com`
- beschränkte Nutzligkeit bei Socialmedia
  - Freunde und Kollegen
    - `benutzername@gmail.com ist Bekannte von Mir`
  - Socialmedia Benachrichtungen
    - `benutzername+mastodon@pm.me`

ID: Verwendung von Subaddressing

- zufällige Emailanschrift bie jeder Dienstanbieter
- benutze zufällige Zeichenketten für Subaddressing
    - mit Sitename nach der Zeichensalat
        - `benutzername+3qkrl-ebay@gmail.com`
            - Benutzername: `benutzername`
            - Token: `3qkrl`
            - Site: `ebay`
- Bonus
    - Filter Email für die Anschrift
    - Spamerkennung

ID: Browser Cookies

- Dritte Partei Cookies verfolgen uns auf mehreren Domänen
- Lightbeam 3.0 Add-on
- uMatrix Add-on (uBlock Origin)

ID: Sicherheitsfragen und -antworten

Das wichtigste dabei ist…

Unsinn ist sicherer

IBKR

Noch eine kurze Errinerung dran, IBNDR

In den USA können wir schon um Sicherheitsantworten und zum Teil auch bei Geburtsdatum lügen

In der EU bin ich mir nicht sicher …

ID: Sicherheitsfragen und -antworten

- zufällige Antworten
- zufällige Wortsalat als Fragen
- aussprechbare Wort- und Zeichenketten

ID: Multifakter Authentizieren (MFA)

- TOTP - Time-Based Tokens
- HOTP - HMAC
- Message - SMS
- Message - Push-Benachrichtigung
- Telefonanruf
- Email
- Körperteil

MFA: TOTP (Applikation oder Token)

- Zeitbasierte Tokens
- Dientsanbieter brauchen Deine Telefonnummer nicht
- Handy oder Tablet wie Token benutzen
- meine Empfehlung

MFA: HOTP

- Jede Ziffer kann nur ein Mal benutzt werden

MFA: braucht Handynummer

- SMS
  - MitM
  - verlorene Handy
- Message - Push-Benachrichtigung
- Anrufe
  - Siehe SMS :)

MFA: Email

- Siehe SMS :)
  - Lieber Spam als Verkaufsanrufe

MFA: Körperteil

- schwer zu ändern (bis wir Cyborgs werden)

ID: Geburtsdatum

- Lüg wenn möglich
- 31. February funktioniert nimmer :)
- One-liner für zufälliges Datum zwischen 1954 und 1999

```
- date -d @$RANDOM*24*3600/2-500000000 +%Y%b%d
```

Backups

- regelmäßige Backups
- offsite Backups
- Löschen
    - Clouds are forever / Datenwolkenanbieter sind für immer

Nicht Vergessen!

Eindeutige Beschienigungsinfos für jeden Dienstanbieter!

soziale Medien und Fediverse

- FLOX_advocate auf Mastodon
  - https://floss.social/@FLOX_advocate
- LuftHans auf Libera.chat IRC
  - #SeaGL, #LOPSA und #PLUGaz

Quellen

- Linux Journal (2017Jan): Online Privacy and Security Using a Password Manager
  - https://www.LuftHans.com/LinuxJournal/Online_Privacy_and_Security_Using_a_Password_Manager
- Subaddressing list at Wikipedia
  - http://en.wikipedia.org/wiki/Email_address#Address_tags
- XKCD "Password Strength" explained
  - https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength
- Sicherheit beginnt mit starken Passwörtern bei digitalcourage
  - https://digitalcourage.de/digitale-selbstverteidigung/sicherheit-beginnt-mit-starken-passwoertern
- Passwörter Einfach Erklärt von Alexander Lehmann
  - https://digitalcourage.video/w/911cfa32-4365-46db-b30c-71ee52628d3c
- Nextcloud Video Verification
  - https://nextcloud.com/blog/unique-sharing-security-video-verification/
- None of Your Business (noyb)
  - https://noyb.eu/de

Privacy Enhancing Firefox Add-ons

- uMatrix from Raymond Hill
- NoScript from Giorgio Maone
- Lightbeam 3.0 from Princiya
    - forked from Mozilla by former Outreachy intern in Berlin
- uBlock Origin from Raymond Hill
- uBO-Scope from Raymond Hill

Glossary

- Credentials
  - Anything used to identify you for authentication
- Passphrases vs passwords
  - Essentially the same
  - passphrases implies they are longer and the ability to use special characters and spaces
- Subaddressing delimiters
  - Often a '+', but doesn’t have to be. Depends on your mail provider.

Obtaining Software

- KeePassXC
  - https://KeePassXC.org/
- KeePassX
  - https://www.KeePassX.org/
- FDroid - FLOSS Android Apps
  - https://f-droid.net/
- Nextcloud
  - https://Nextcloud.com/
    - WebAppPassword
    - Passman
    - Passwords
- BitWarden
  - https://bitwarden.com/

Credits

- Riesen grossen Dank an Dierk für die grammatische Korrektur!
- Mat Honan Wired article
  - http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- XKCD by Randall Munroe
  - http://XKCD.com
  - Password Strength - https://xkcd.com/936/
- Freakonomics Radio
  - America’s Math Curriculum Doesn’t Add Up (Ep. 391)

Bonus Rounds

Data Escrow

- Use a KeePassXC file to store other important information
  - Bank account info
  - Life insurance info
  - Government citizen numbers
  - Passphrases for GPG keys
  - PDF copies of contracts and other documents
  - Use multiple different files

Tips

- Don’t use links in email to login
- Use application-specific passwords
- Don’t use Internet Explorer
- Don’t use Outlook

Getting Help

- Tech Support Fastlane - http://xkcd.com/806/
- Free Software Conferences (KLT, Privacy Week, CLT, FOSDEM, CCC, Tübix, FOSSASIA, SeaGL)
- Local user groups