Passwortmanager. Böse Programme, die Passwörter fressen und oft gestohlen werden? Oder doch nicht?

Mathias Lindt

digitalcourage
Hochschulgruppe
Bayreuth

Juni 2020

Vorstellung

Über mich

- Mathias Lindt
- Systemadministrator und Softwareentwickler
- Studierte an der TH-Wildau (Telematik)

Schwerpunkte

- Systemadministration im Unix/Linux-Umfeld
- IT-Security
- Netzwerktechnik

Digitalcourage e.V.

digitalcourage
Hochschulgruppe
Bayreuth

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - ≫Für eine lebenswerte Welt im digitalen Zeitalter≪
  - BigBrotherAwards
  - Aktionen zu aktuellen Themen
- Digitalcourage Hochschulgruppe
  (`www.digitalcourage.de/hsg-bt`)
  - Vorträge
  - Workshops
  - Lesungen gegen Überwachung
  - BigBrotherAwards Live Stream (in der Black Box am RW21)

Digitalcourage: Weitere Termine

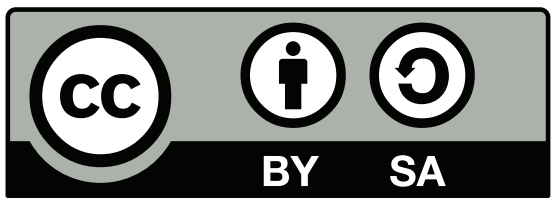
digitalcourage
Hochschulgruppe
Bayreuth

Weitere Termine:

- ~~16. Juni~~: Verschoben: Digitale Selbstbestimmung und Personale Identität
- ~~19. Juni~~: Theorie & Praxis von Festplatten- und Stick-Verschlüsselung
- **20. Juni: Passwortmanager. Böse Programme, die Passwörter fressen und oft gestohlen werden? Oder doch nicht?**
- 26. Juni: Spurenarm surfen Teil 1
- 18. September: BigBrotherAwards

Copyrights und Lizenzen

- Die in dieser Arbeit benannten Produktnamen, Firmennamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.
- Dieser Vortrag ist privater Natur und verfolgt keine gewerblichen Absichten.
- Quellenangaben zu den verwendeten Bildern, Darstellungen etc. finden sich am Ende der Foliensammlung.
- Dieses Werk ist lizenziert unter einer “CC BY-SA 4.0” Lizenz.



Passwörter

Kombination = Zeichenanzahl * Passwortlänge

28 bits = Very Weak; might keep out family members
28 - 35 bits = Weak; should keep out most people, often good for desktop login passwords
36 - 59 bits = Reasonable; fairly secure passwords for network and company passwords
60 - 127 bits = Strong; can be good for guarding financial information
128+ bits = Very Strong; often overkill

Grenzen der Passwortsicherheit

- Erraten
- Phishing
- Stehlen
- Knacken:

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0–9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a–z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A–Z; a–z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A–Z; a–z; 0–9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Bedrohungen – Passwörter knacken

- Hashcat
- Rainbow-Tables
- Pure Rechenpower (SRAM)
- Cluster

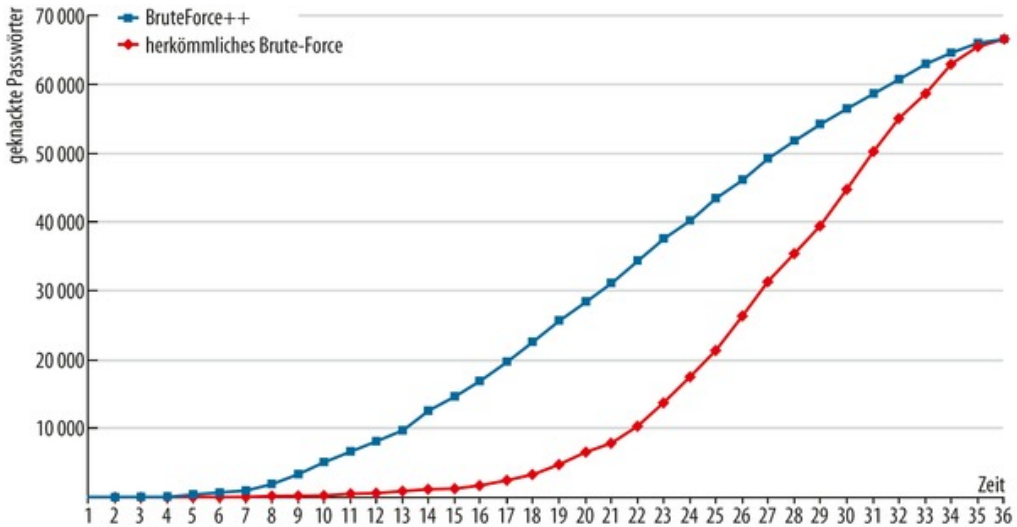


Abbildung: Netcat knackt effizient Passwörter.

Bedrohungen – Wie Profis da rangehen

- Hashcat
- Rainbow-Tables
- Pure Rechenpower (SRAM)
- Cluster

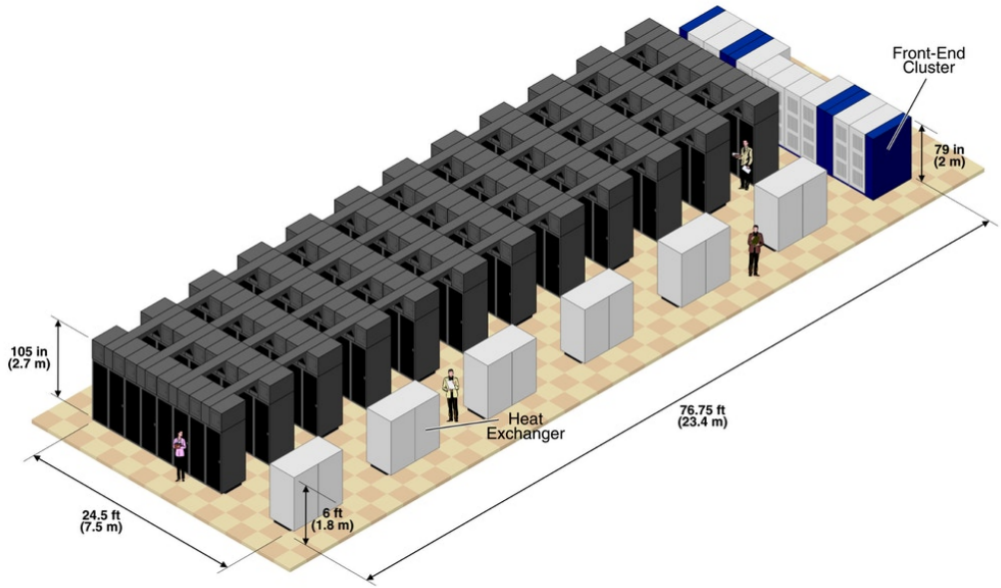


Abbildung: Among the Windsor documents on the NYU hard drive was an illustration of an IBM computer codenamed ≫Cyclops≪

Vorfälle, die geschehen sind

`https://haveibeenpwned.com/`

Passwörter und ihre Probleme

- Sich Passwörter merken macht keinen Spass.
- Passwörter werden beiläuftig behandelt - sie nerven.
- Sicherheit. Naja. Kann man das Essen?

Wozu bedarf es Passwortmanager?

- In Zeiten, als das Passwort erfunden wurde, gab es ≫nur≪ 1-3 Passwörter.
- Die Passwort-Komplexität spielt kaum eine Rolle.
- Heute haben sich die Situationen geändert und Passworte kommen an ihre Leistungsgrenzen.
- Kaum wer versteht heute, was ein gutes Passwort ausmacht.

Sind Passwortmanager nicht unsicher? Schließlich sind sie an zentraler Stelle gesichert.

- Ja
- Nein

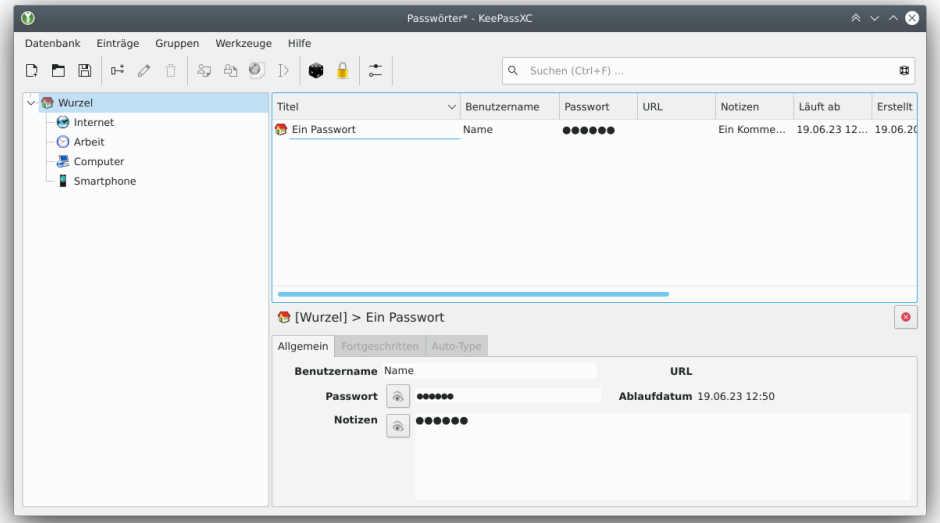
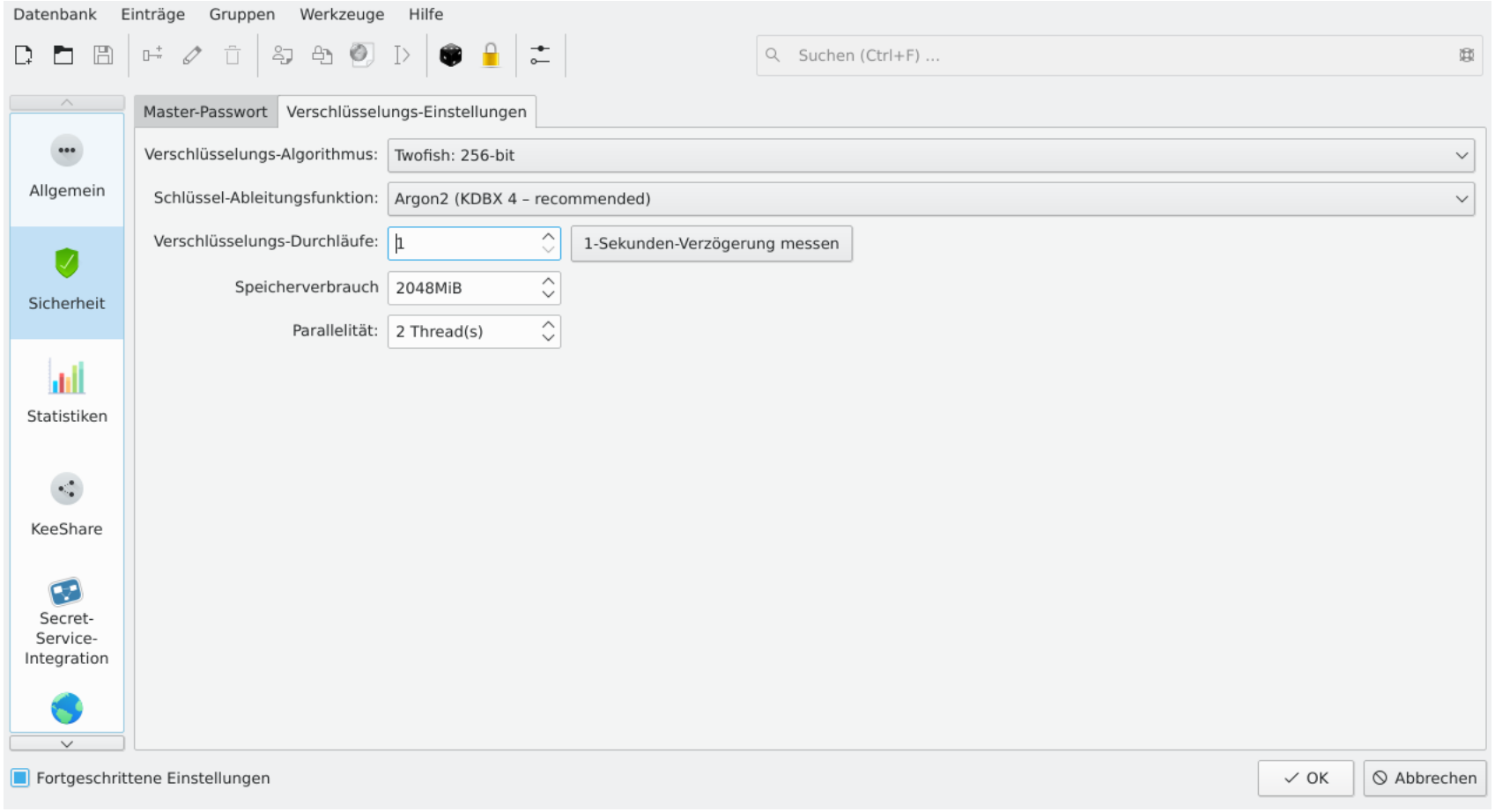


Abbildung: Passwortdatenbank: KeepassXC

Können mir nicht alle Passwörter auf einen Schlag wegkommen?

- Ja
- Nein

Was macht Passwortmanager sicher?



Wie funktioniert die Handhabung?

- Via Drag & Drop
- Via Browser-Plugin
- Klassisch: Dient nur zur Aufzeichnung

Welches der vielen Passwortmanager sollte ich benutzen? Gibt es Empfehlungen?

Nein, **tl;dr**

- Würden alle den selben Passwortmanager verwenden, gäbe es eine Monokultur.
  - Dies ist schlecht für die Sicherheit.
- Jeder hat andere Anforderungen an einen Passwortmanager.

Zusammenfassung

- Ein Passwortmanager benutzen ist besser als keinen Passwortmanager zu benutzen.
- Passwortmanager bieten digitale Souveränität.

Quellenangaben

- Brute-Force-Übersicht, https://de.wikipedia.org/wiki/Passwort
- Netcat-Diagramm: https://www.heise.de/ct/ausgabe/2013-3-Die-Tools-und-Techniken-der-Passwortknacker-2330451.html
- Cyber-Bild, https://www.securitymagazine.com/articles/88338-cyber-crime-costs-117-million-per-business-annually
- FotoTan: https://www.commerzbank.de/portal/de/help/verwaltung-weiteres/phototan/phototannutzen.html
- Der NSA-Computer Cyclops, https://theintercept.com/2017/05/11/nyu-accidentally-exposed-military-code-breaking-computer-project-to-entire-internet/
- Meldung zu Cyclops im Fefe-Blog, https://blog.fefe.de/?q=nyu-accidentally-exposed-military-code-breaking-computer-project-to-entire-internet
- Netcat-Diagramm https://www.heise.de/ct/ausgabe/2013-3-Die-Tools-und-Techniken-der-Passwortknacker-2330451.html