

Passwortsicherheit

Cryptoparty Gotha

Prof. Dr. Christian Forler



BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

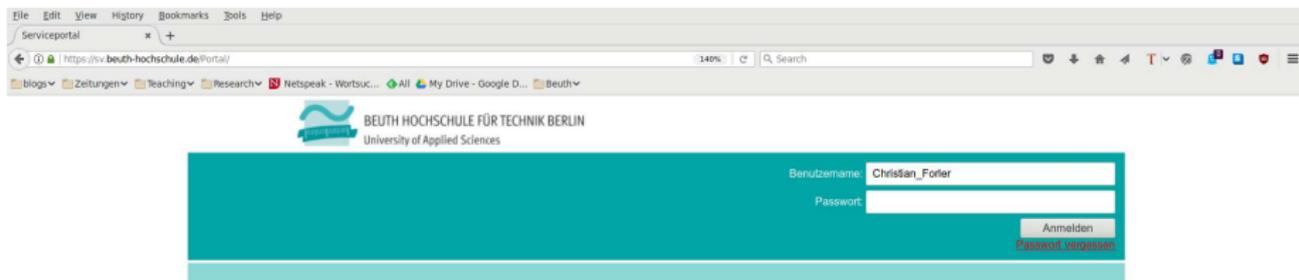
Februar 2018

Agenda

Worum soll es in diesem Vortrag gehen?

- Wie werden Passwörter verwendet
- Wie arbeiten Angreifer typischerweise
- Tipps und Tricks mit den Umgang mit Passwörtern

Passwörter



- Passwörter sind Geheimnisse
- Sind Teil des Alltags geworden
 - Nutzerauthentisierung (Anmeldung)
 - Generierung eines kryptographischen Schlüssels
- Leider sind Passwörter nicht unproblematisch

Erstes Passwortproblem: Mehrfachbenutzung

Die meisten Nutzer haben **5-8** Passworte die sie wiederverwenden

Erstes Passwortproblem: Mehrfachbenutzung

Die meisten Nutzer haben **5-8** Passworte die sie wiederverwenden

- Immer wieder werden die **Nutzerdatenbank** von (unzureichend gesicherten) Webservices *stehlen*

Erstes Passwortproblem: Mehrfachbenutzung

Die meisten Nutzer haben **5-8** Passworte die sie wiederverwenden

- Immer wieder werden die **Nutzerdatenbank** von (unzureichend gesicherten) Webservices *stehlen*
- Passwort-Wiederherstellungsrate liegt in solchen Fällen meist über 60%

Erstes Passwortproblem: Mehrfachbenutzung

Die meisten Nutzer haben **5-8** Passworte die sie wiederverwenden

- Immer wieder werden die **Nutzerdatenbank** von (unzureichend gesicherten) Webservices *stehlen*
- Passwort-Wiederherstellungsrate liegt in solchen Fällen meist über 60%
- **Mehrfach verwendete** Passwörter ermöglichen Angreifern Zugriff auf weitere Services (Email, Webshop, Soziales Netzwerk, ...)

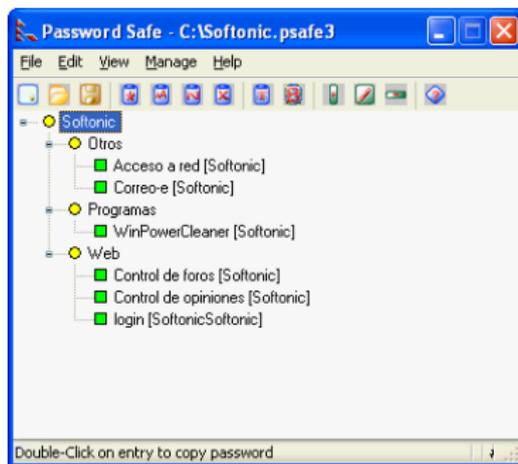
Erstes Passwortproblem: Mehrfachbenutzung

Die meisten Nutzer haben **5-8** Passworte die sie wiederverwenden

- Immer wieder werden die **Nutzerdatenbank** von (unzureichend gesicherten) Webservices *stehlen*
- Passwort-Wiederherstellungsrate liegt in solchen Fällen meist über 60%
- **Mehrfach verwendete** Passwörter ermöglichen Angreifern Zugriff auf weitere Services (Email, Webshop, Soziales Netzwerk, ...)
- Alternative zum Stehlen einer Nutzerdatenbank ist das Betreiben eines (Pseudo-)dienstes

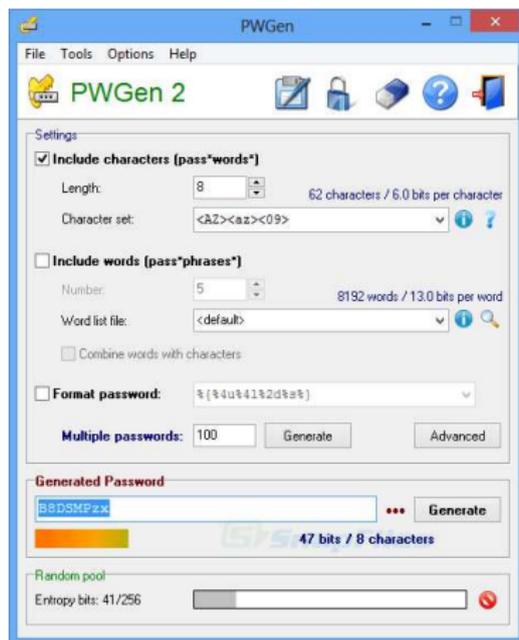
Lösungsvorschlag

Benutzung eines **lokalen** Passwortmanagers (z.B. Password Safe)



Lösungsvorschlag

Benutzung eines **lokalen** Passwortgenerators (z.B. PWGen)



Fazit

Umgang mit Passwörtern

- Benutzen Sie einen lokalen Passwortgenerator

Fazit

Umgang mit Passwörtern

- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager

Fazit

Umgang mit Passwörtern

- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager
- Verwenden Sie keine Passwörter mehrfach

Fazit

Umgang mit Passwörtern

- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager
- Verwenden Sie keine Passwörter mehrfach
- Verwenden Sie mind. 10 (besser 14) Zeichen lange Passwörter

Fazit

Umgang mit Passwörtern

- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager
- Verwenden Sie keine Passwörter mehrfach
- Verwenden Sie mind. 10 (besser 14) Zeichen lange Passwörter
- Verwenden Sie Sätze als Passwörter, falls möglich

Fazit

Umgang mit Passwörtern

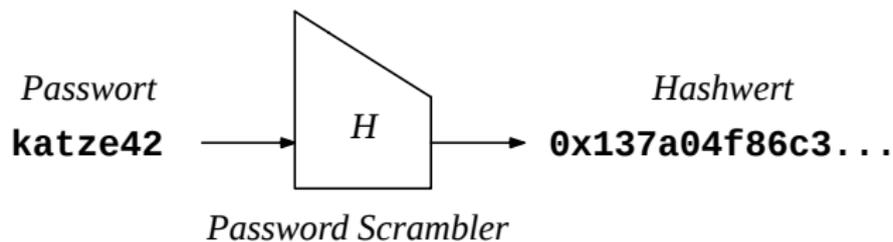
- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager
- Verwenden Sie keine Passwörter mehrfach
- Verwenden Sie mind. 10 (besser 14) Zeichen lange Passwörter
- Verwenden Sie Sätze als Passwörter, falls möglich
- Es ist besser ein gutes Passwort aufzuschreiben als ein schlechtes zu verwenden

Fazit

Umgang mit Passwörtern

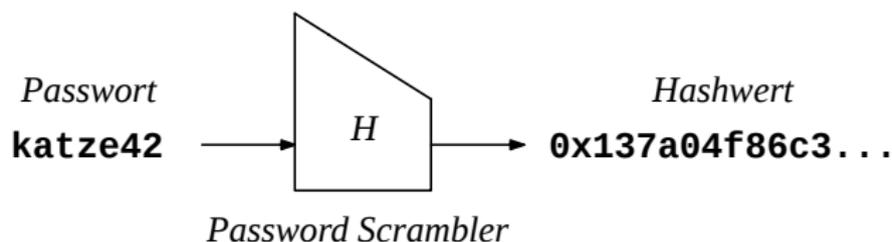
- Benutzen Sie einen lokalen Passwortgenerator
- Benutzen Sie einen lokalen Passwortmanager
- Verwenden Sie keine Passwörter mehrfach
- Verwenden Sie mind. 10 (besser 14) Zeichen lange Passwörter
- Verwenden Sie Sätze als Passwörter, falls möglich
- Es ist besser ein gutes Passwort aufzuschreiben als ein schlechtes zu verwenden
Achtung! Der Aufschrieb sollte sicher verwahrt werden

Speicherung von Passwörtern



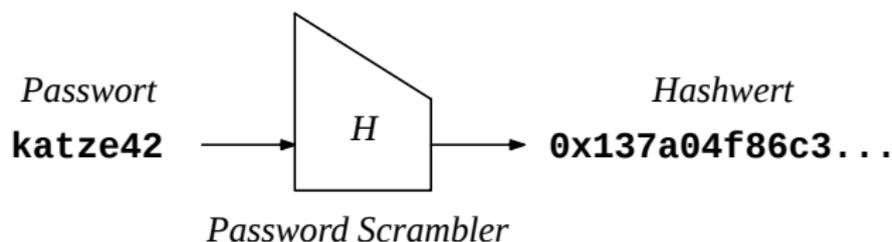
- System speichern normalerweise nur den Fingerabdruck eines Passwortes

Speicherung von Passwörtern



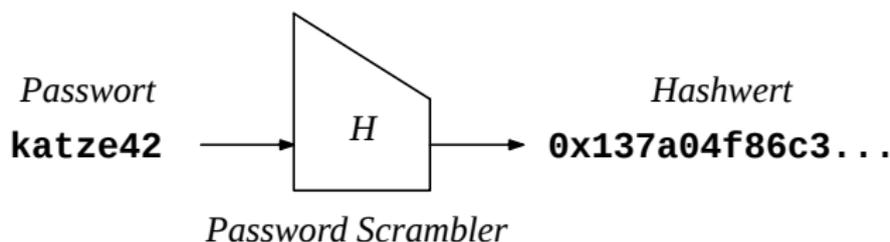
- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdruck eines Passwortes = Hashwert = Passworhash

Speicherung von Passwörtern



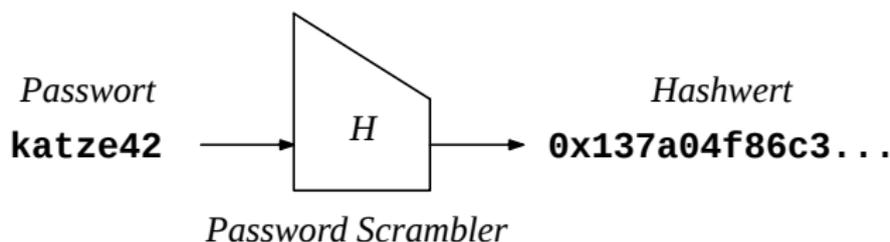
- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdruck eines Passwortes = Hashwert = Passworthash
- Beim Anmelden werden daher nur die Fingerabdrücke verglichen

Speicherung von Passwörtern



- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdruck eines Passwortes = Hashwert = Passworthash
- Beim Anmelden werden daher nur die Fingerabdrücke verglichen
- Eine *Hashfunktion* **H** berechnet den Hashwert eines Passwortes

Speicherung von Passwörtern



- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdruck eines Passwortes = Hashwert = Passworthash
- Beim Anmelden werden daher nur die Fingerabdrücke verglichen
- Eine *Hashfunktion* **H** berechnet den Hashwert eines Passwortes
- Hashfunktionen sind Einwegfunktion, d.h. für gegebenen Hashwert **h** ist es schwer ein Passwort **x** mit $H(x) = h$ zu finden

Preisfrage

Warum ist das mit der Einwegfunktion eine gute Idee?

- Datei mit den Fingerabdrücken kann *verloren* gehen.
 - Adobe (verliert ca. 150 Millionen Passworthashes)
 - LinkedIn (verliert ca. 6.5 Millionen Passworthashes)
 - Yahoo (verliert ca. 0.5 Millionen Klartextpasswörter)
 - ...

Preisfrage

Warum ist das mit der Einwegfunktion eine gute Idee?

- Datei mit den Fingerabdrücken kann *verloren* gehen.
 - Adobe (verliert ca. 150 Millionen Passworthashes)
 - LinkedIn (verliert ca. 6.5 Millionen Passworthashes)
 - Yahoo (verliert ca. 0.5 Millionen Klartextpasswörter)
 - ...
- Angreifer wäre dann in der Lage die dazugehörigen Passwörter zu berechnen

Preisfrage

Warum ist das mit der Einwegfunktion eine gute Idee?

- Datei mit den Fingerabdrücken kann *verloren* gehen.
 - Adobe (verliert ca. 150 Millionen Passworthashes)
 - LinkedIn (verliert ca. 6.5 Millionen Passworthashes)
 - Yahoo (verliert ca. 0.5 Millionen Klartextpasswörter)
 - ...
- Angreifer wäre dann in der Lage die dazugehörigen Passwörter zu berechnen

Was bleibt dem Angreifer noch übrig?

Preisfrage

Warum ist das mit der Einwegfunktion eine gute Idee?

- Datei mit den Fingerabdrücken kann *verloren* gehen.
 - Adobe (verliert ca. 150 Millionen Passworthashes)
 - LinkedIn (verliert ca. 6.5 Millionen Passworthashes)
 - Yahoo (verliert ca. 0.5 Millionen Klartextpasswörter)
 - ...
- Angreifer wäre dann in der Lage die dazugehörigen Passwörter zu berechnen

Was bleibt dem Angreifer noch übrig?

Angreifer probieren alle möglichen Passworte durch

Wie arbeiten Angreifer

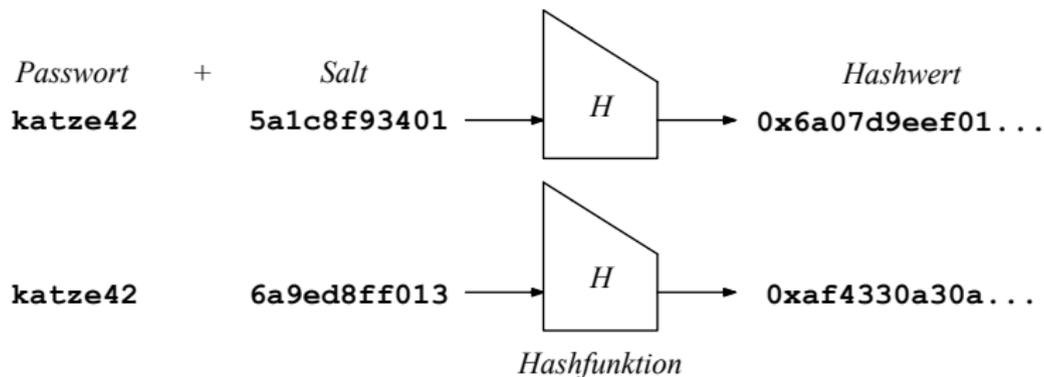
123456	CHARLIE	NELLO	FEDDER	GOLF	DONALD	PUFFIN	GIANTS	ROCKBND	CALVIN
12345678	SUPERMAN	SCOOTER	RENNER	BLAUME	BIGDADDY	REDSOX	BOOTY	JAGUAR	SHRED
123456789	ASHOLE	PLEASE	FERRARI	BEAR	BRUNCO	STAR	BRONDE	GREAT	SWEET
1234	FUCKYOU	POSSONE	CONIE	TIGER	MINI	TESTING	FUCKED	COOL	KELLY
POSSY	DALLAS	OUTAR	CHICKEN	DOCTOR	VANIGER	SHANNON	GOLDEN	COOPER	PAUL
12345	PRATIE	CHELSEA	CORAGO	GATORS	RANGER	MURPHY	ODD	1315	MIKE
JAGGER	PEPPER	BLACK	JACKIE	ANGEL	TRUBLE	FRANK	SANDRA	SCORPIO	KING
9WERTY	JUSTIN	ROCKAR	SEXTEK	JUNIOR	WHITE	HARUNAH	PAKIE	MADISON	RACING
1234567890	WILLIAM	JACKSON	BRUCKE	TWINER	TOPGUN	DRIVE	PRICKER	1234567	5555
MUSTANG	BRITEL	CAMERON	W44444	PARNO	BIGTITS	ERGLE1	EINSTEIN	BRAZIL	ERGLE
INTERNET	SUMMER	GALFER	659321	WIDE	BOBBY	BIESES	TULL	DOLPHIN	00000
BOCEBA	HEATNE	COMPUTER	CAROL	DEBBIE	GREEN	NATHAN	CHRY	LUREN	JAPAN
MURKIN	YANKEE	WILLARD	PANDBA	SPIDER	MELISSA	SUPER	RIDERS	WINSTON	ALFRED
MICHAEL	JASON	XXXXXXXXXX	JUSTIN	BOODGER	BOODGER	ON TMSX	STEV	WARRIOR	SQUAT
FANTASY	MUSCLE	MURD	BALANCO	1212	LAKERS	MAGIC	FOREVER	SAMMY	STARS
SHADOW	PHONE	POKEX	DRIVER	FLYERS	RACHEL	ANGELA	SLV	ALEXIS	APPLE
MONKEY	ENTER	PIKAT	DANAR	FISH	SLAYER	IFER	8WTS309	ABAD	animal
ARIZO	SMILEY	SMILEY	SMILEY	SMILEY	SMILEY	SMILEY	SMILEY	SMILEY	SMILEY
PASS	THUNDER	ICEMAN	DAVID	MATRIX	FORUM	SCOTT	JARKE	NIPPLES	PERCHES
FUCKME	CONWAY	TIGERS	MADRID	TEKINS	ADP	2122	LOVERS	POWER	JARMIN
6789	SILVER	ARAB	WILSON	SCOOPY	VIGOR	GREGORY	SWEET	VICTORIA	KEVIN
JORDAN	RICHARD	HUNT	BUTHEAD	JASON	LONDON	BUDDY	VIRGINIA	ADRIAN	MATT
HARLEY	FUCKER	DEAR	DEAN'S	WALTER	7777	WHATEVER	TOJITA	9WERTY	ENNY
RANGER	ORANGE	PIKAT	FUCKING	CUNSHOT	MARLBORO	YOUNG	TRAVIS	DAWELLE	GIRL
DONALD	MERLIN	MURD	CAPTAIN	BOSTON	SBRIVAS	NICHOLAS	HARDAG	BEAVER	APOLLO
JANUARY	RACHELLE	STARWARS	bigdick	BRAVES	INTERNET	LUCKY	PARIS	4321	PERKER
HUNTER	BIGDOG	EDWARD	SMOKEY	YANKEE	ACTION	HELPME	ROCK	402	9WERT
FUCK	CHEESE	CARLOS	XAVIER	BARNEY	LOVER	CARTER	JACKIE	XXXX	SMITHING
2000	MATTHEW	ERIS	STEVEN	VICTOR	TUCKER	TERESA	MADONNA	EXTREME	DOLPHIN
TEST	HAIR	JACKIE	SMOKEY	PRINCESS	MERCEDES	5150	BILL	BRAN	FREDDY
TRAVIS	ANDREW	WILLIAM	ERIS	WIKING	DOGGIE	CRYSTAL	MARK	ARSENAL	GEMINI
THOMAS	GINGER	TABBI	WINNER	222222	PETER	STARTREK	ACCESS	TV	ARMES
ROBERT	NICOLE	JANAI	JILLER	GUNNER	PUSSIES	SILVERA	WOLF	AUGUST	MAXWELL
ACCESS	SPARKY	JEREMY	FLOWER	HORNEY	COCK	LATHER	232323	NIPPLE	PHYSIC
LOVE	YELLOW	GANDOLF	JACK	BUBBA	BEER	14144	LOVEYOU	ALEX	3333
WATER	CAMPBELL	SPARKY	FIREBIRD	212	ROCKET	BERVIS	FLORIDA	ERIC	CRAB
1234567	SECRET	WINTER	BUTTER	FRED	JOHANSON	OLIVER	HAPPY	LEGEND	BULLER
SOCCER	DICK	BRANDY	UNITED	TURTLE	JOHANSON	OLIVER	HAPPY	LEGEND	CUMMING
HOCKEY	FALCON	COMPAG	STEELERS	KILLER	TRUCK	CARLOS	TEAROSE	TIFFANY	SCORPIO
GEORGE	1123	MICKE	2XCVBM	ANDREW	BIFF	BRAGON	TOMCAT	123456789	ARTHUR
SEXY	12345	MICKE	2XCVBM	ANDREW	BIFF	BRAGON	TOMCAT	123456789	ALBERT
ANDREW	BIFF	BRAGON	TOMCAT	123456789	ALBERT	4444			

100 worst passwords

TIMEA Files Project: Passwords structure, protection, performance of password

Salz (Salt)

Beim Hashen von Passwörtern sollte Salt (zusätzlicher zufälliger Input) verwendet werden. (**Warum?**)



Server speichert sich den Salt und den Hashwert

Password Cracker



Quelle: <http://hashcat.net/>

- Problem: Hashfunktionen sind viel zu effizient

Password Cracker



Quelle: <http://hashcat.net/>

- Problem: Hashfunktionen sind viel zu effizient
- Passwörter lassen sich sehr schnell durchprobieren (z.B. 11 Mrd./s für Windows-XP-Passworthashes)

Password Cracker



Quelle: <http://hashcat.net/>

- Problem: Hashfunktionen sind viel zu effizient
- Passwörter lassen sich sehr schnell durchprobieren (z.B. 11 Mrd./s für Windows-XP-Passworthashes)
- Derzeit nutzen Angreifer oftmals mehrere Grafikkarten

Passwort-Crack-Programme

- Freie gute Software um Passwörter zu *rekonstruieren*:
 - John the Ripper (für CPUs)
<http://www.openwall.com/john/>
 - DaveGrohl (für CPUs)
<http://davegrohl.org/>
 - oclHashcat (für Grafikkarten)
<http://hashcat.net/oclhashcat-plus/>

Passwort-Crack-Programme

- Freie gute Software um Passwörter zu *rekonstruieren*:
 - John the Ripper (für CPUs)
<http://www.openwall.com/john/>
 - DaveGrohl (für CPUs)
<http://davegrohl.org/>
 - oclHashcat (für Grafikkarten)
<http://hashcat.net/oclhashcat-plus/>
- Werden immer besser:
 - Testen erst Wörterbücher
 - Testen auch beliebte Verfremdungen
 - Sortieren Passworte nach Wahrscheinlichkeit

Passwort-Crack-Programme

- Freie gute Software um Passwörter zu *rekonstruieren*:

- John the Ripper (für CPUs)
<http://www.openwall.com/john/>
- DaveGrohl (für CPUs)
<http://davegrohl.org/>
- oclHashcat (für Grafikkarten)
<http://hashcat.net/oclhashcat-plus/>

- Werden immer besser:

- Testen erst Wörterbücher
- Testen auch beliebte Verfremdungen
- Sortieren Passworte nach Wahrscheinlichkeit

⇒ Nur ausreichend lange und zufällige Passwörter sind sicher!

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen
Eine (!) Grafikkarte in wenigen Minuten bis Stunden

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen
Eine (!) Grafikkarte in wenigen Minuten bis Stunden
- 8 zufällig gewählte Zeichen
Tausende mietbare Rechner (z.B. bei Amazon EC2) in wenigen Stunden

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen
Eine (!) Grafikkarte in wenigen Minuten bis Stunden
- 8 zufällig gewählte Zeichen
Tausende mietbare Rechner (z.B. bei Amazon EC2) in wenigen Stunden
- 10 und mehr zufällig gewählte Zeichen
Das dauert. . .

Aber...

- Die Sicherheit reduziert sich drastisch wenn Passwörter keine Zufallskombinationen sind!
 - “A0!94%1+5_” = mehrere Wochen auf Tausenden Rechnern
 - “G3h31m007!” = wenige Minuten auf einer (!) Grafikkarte

Aber...

- Die Sicherheit reduziert sich drastisch wenn Passwörter keine Zufallskombinationen sind!
 - “A0!94%1+5_” = mehrere Wochen auf Tausenden Rechnern
 - “G3h31m007!” = wenige Minuten auf einer (!) Grafikkarte
- **Problem : MenschensindschlechtePasswortgeneratoren**

Schlechte Passwort-Regeln

- Erratbare Begriffe:
 - “Gotha”, “TIF-IT”

Schlechte Passwort-Regeln

- Erratbare Begriffe:
 - “Gotha”, “TIF-IT”
- Namen oder Stichtage:
 - “Helga”, “20sep1993”

Schlechte Passwort-Regeln

- Erratbare Begriffe:
 - “Gotha”, “TIF-IT”
- Namen oder Stichtage:
 - “Helga”, “20sep1993”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
 - “Lichtgeschwindigkeit”, “Sh3ttl4nd-TerrIer”, “Tr0ub4dour”

Schlechte Passwort-Regeln

- Erratbare Begriffe:
 - “Gotha”, “TIF-IT”
- Namen oder Stichtage:
 - “Helga”, “20sep1993”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
 - “Lichtgeschwindigkeit”, “Sh3ttl4nd-TerrIer”, “Tr0ub4dour”
- Wortkombinationen:
 - “Adam2+7Eva”

Schlechte Passwort-Regeln

- Erratbare Begriffe:
 - “Gotha”, “TIF-IT”
- Namen oder Stichtage:
 - “Helga”, “20sep1993”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
 - “Lichtgeschwindigkeit”, “Sh3ttl4nd-TerrIer”, “Tr0ub4dour”
- Wortkombinationen:
 - “Adam2+7Eva”
- Bekannte Begriffe:
 - “supercalifragilisto5” (aus dem Musical Mary Poppins)

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
 - “as8%4,&xn9?14oqj . 1!”
 - **Problem: Wie merke ich mir eine solche Kombination?**

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
 - “as8%4,&xn9?14oqj.1!”
 - **Problem: Wie merke ich mir eine solche Kombination?**
- Einfacher: Kombination aus mind. fünf seltenen zufällig gewählten Wörtern
“korrekt Pferd Batterie Büroklammer Magnet”

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
 - “as8%4,&xn9?14oqj.1!”
 - **Problem: Wie merke ich mir eine solche Kombination?**
- Einfacher: Kombination aus mind. fünf seltenen zufällig gewählten Wörtern
“korrekt Pferd Batterie Büroklammer Magnet”
- Besser: Merksätze mit mind. 19, besser 22 und mehr Zeichen
“IbhdCdTIF-ITeViGulsvNüP” = “Ich besuche heute die Cryptoparty des TIF-IT e.V.s in Gotha und lerne sehr viel Neues über Passwortsicherheit.”

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
 - “as8%4,&xn9?14oqj.1!”
 - **Problem: Wie merke ich mir eine solche Kombination?**
- Einfacher: Kombination aus mind. fünf seltenen zufällig gewählten Wörtern
“korrekt Pferd Batterie Büroklammer Magnet”
- Besser: Merksätze mit mind. 19, besser 22 und mehr Zeichen
“IbhdCdTIF-ITeViGuIsvNüP” = “Ich besuche heute die Cryptoparty des TIF-IT e.V.s in Gotha und lerne sehr viel Neues über Passwortsicherheit.”

Gemeine Frage

Warum ist “IbhdCdTIF-ITeViGuIsvNüP” jetzt kein gutes Passwort mehr?

Das Ende des Vortrags

Fragen?