Passwortsicherheit

Cryptoparty Gotha

Prof. Dr. Christian Forler

BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

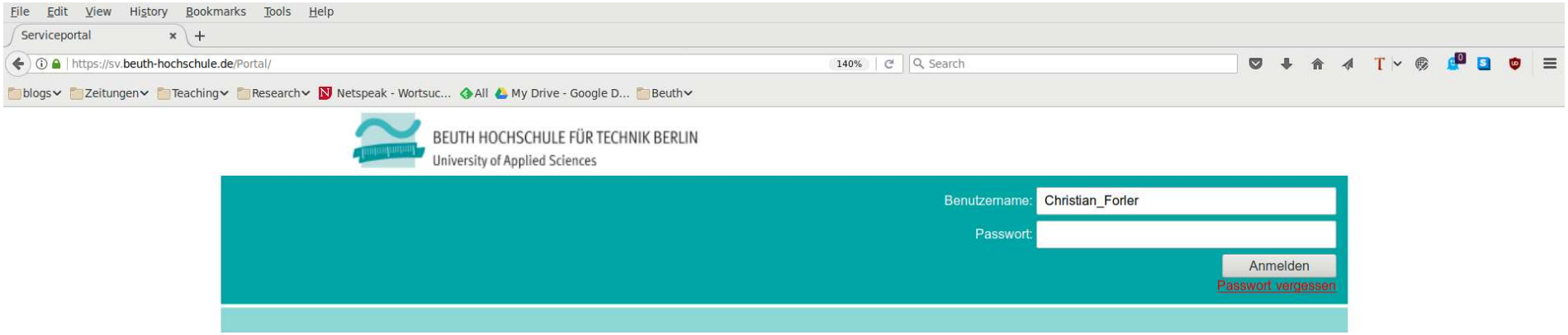
Februar 2018

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, . . .)

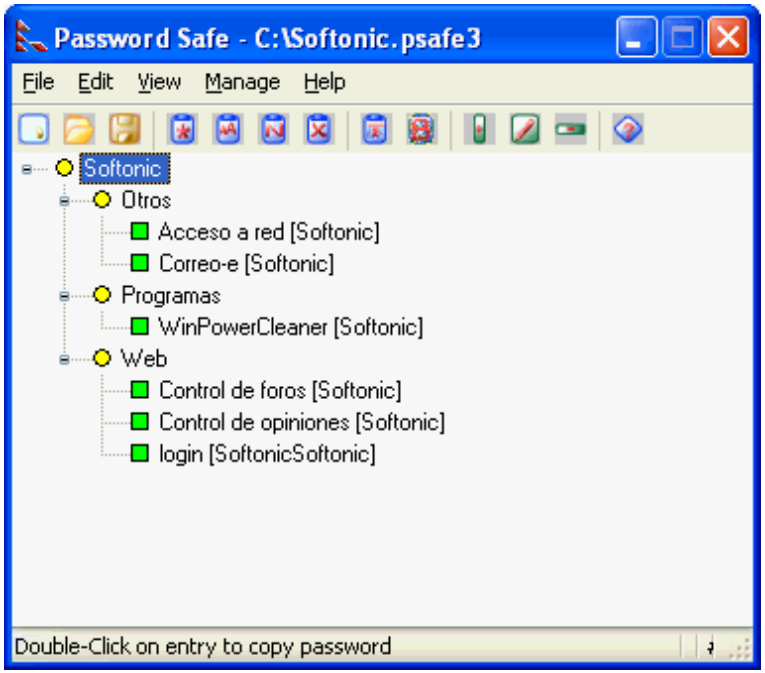
Erstes Passwortproblem: Mehrfachbenutzung

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

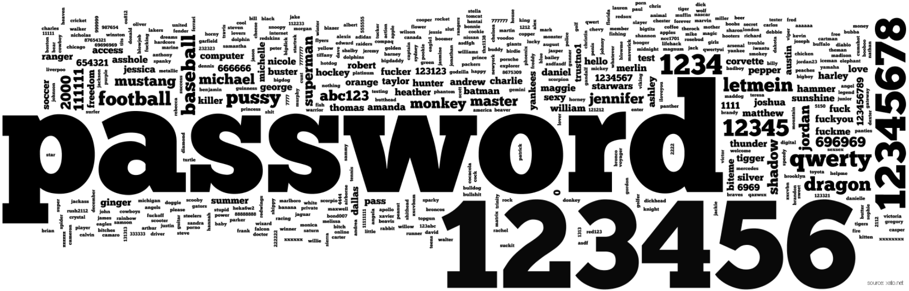
- Immer wieder werden die **Nutzerdatenbank** von (unzureichend gesicherten) Webservices *stehlen*
- Passwort-Wiederherstellungsrate liegt in solchen Fällen meist über 60%
- **Mehrfach verwendete** Passwörter ermöglichen Angreifern Zugriff auf weitere Services (Email, Webshop, Soziales Netzwerk, . .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

Lösungsvorschlag

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



Top 1000 Passwörter



(Quelle: `http://xato.net`)

Top 1000 Passwörter

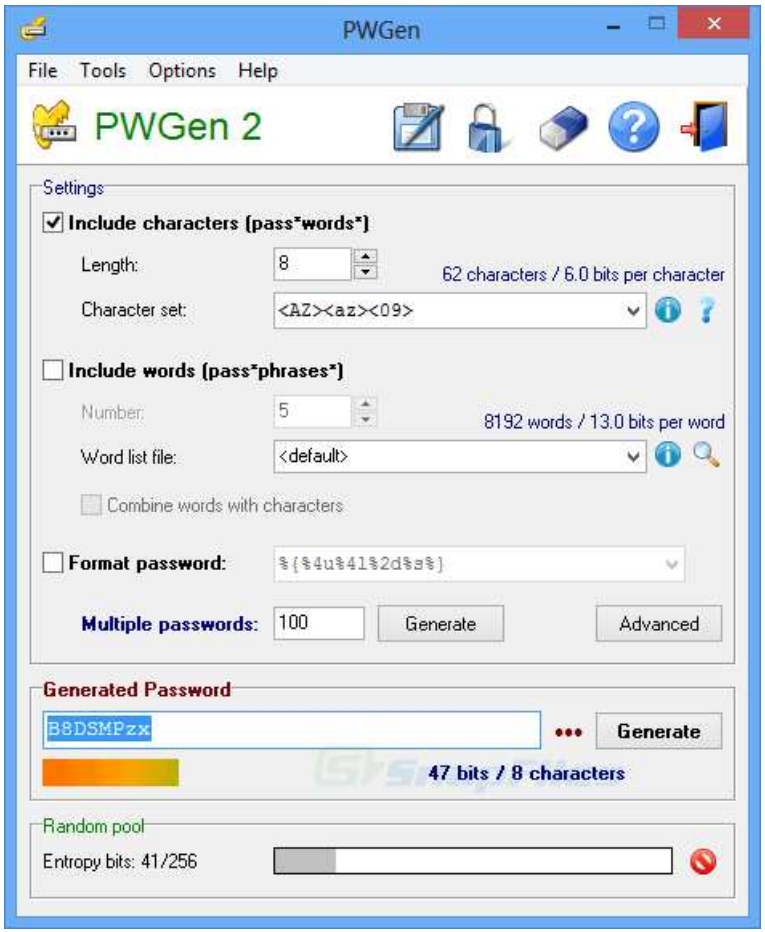
(Quelle: `http://xato.net`)

Passwort Dilemma

- *Schlechtes* Passwort (einfach zu *erraten*)
- *Gutes* Passwort (schwer zu merken)

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

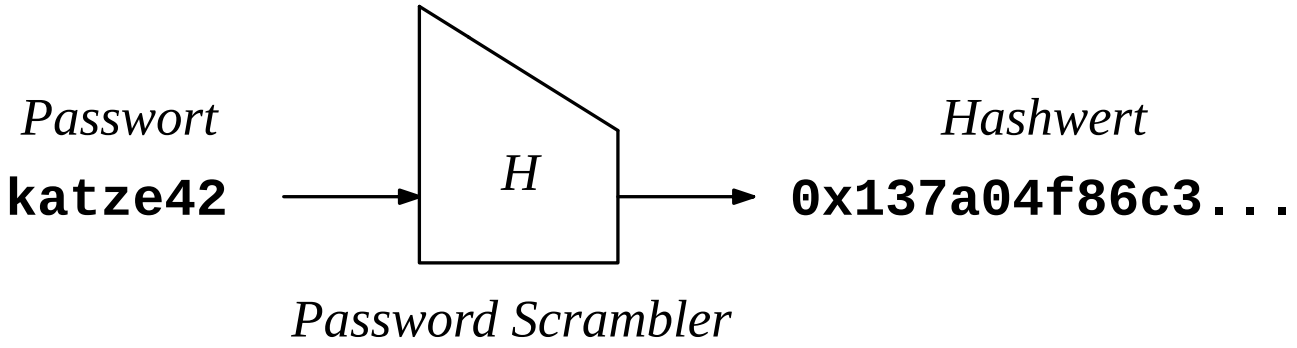
Fazit

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

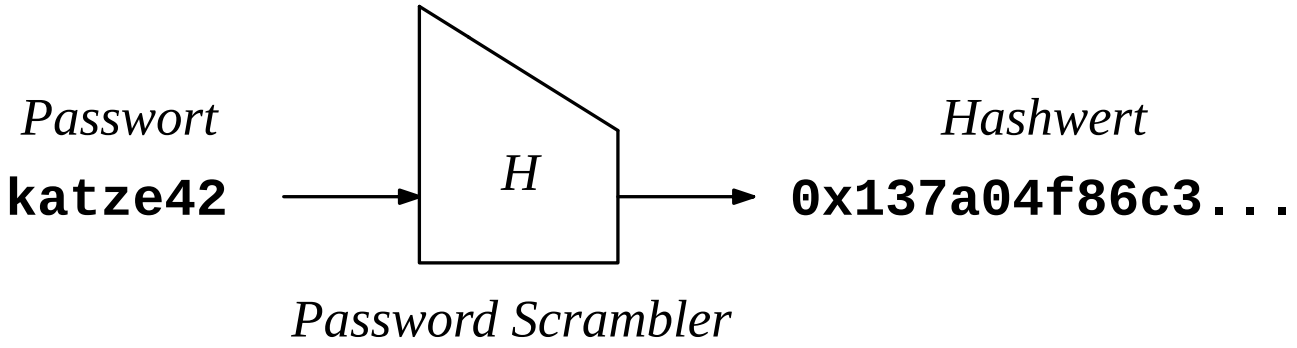
  Achtung! Der Aufschrieb sollte sicher verwahrt werden

Speicherung von Passwörtern



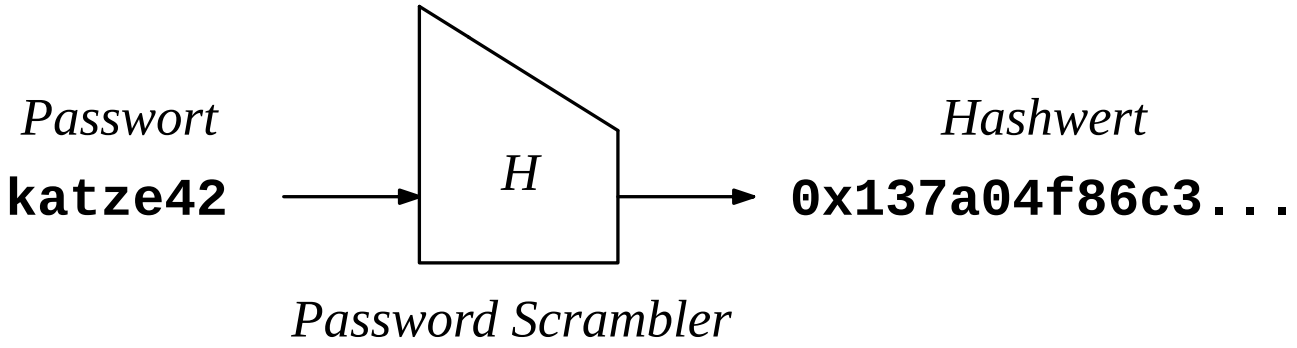
- System speichern normalerweise nur den Fingerabdruck eines Passwortes

Speicherung von Passwörtern



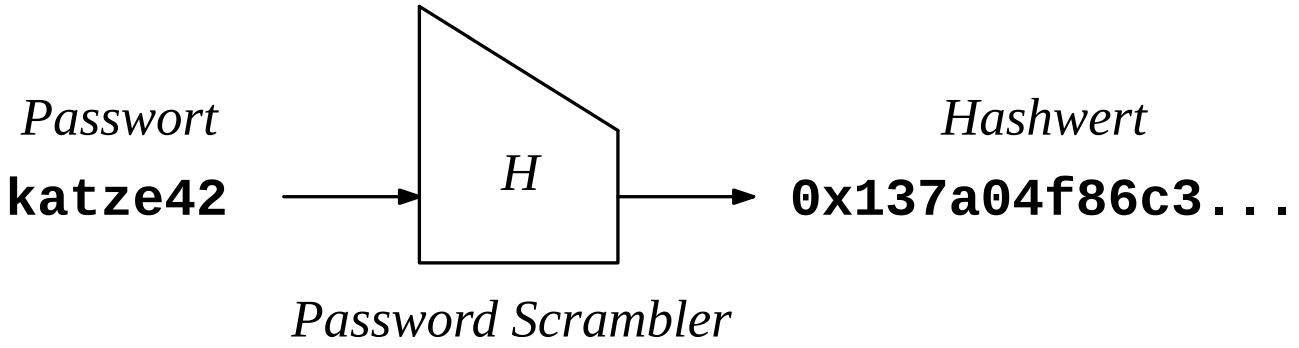
- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdurck eines Passworts = Hashwert = Passworthash

Speicherung von Passwörtern



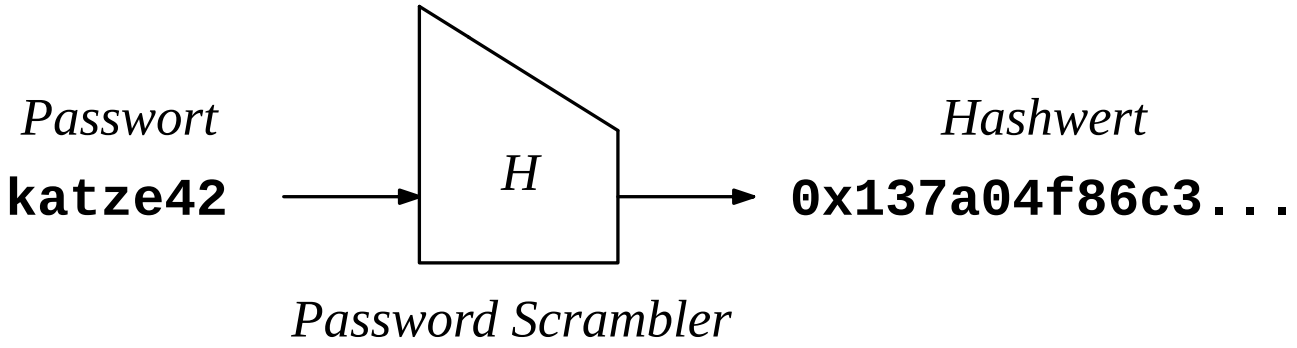
- System speichern normalerweise nur den Fingerabdruck eines Passwortes
- Fingerabdurck eines Passworts = Hashwert = Passworthash
- Beim Anmelden werden daher nur die Fingerabdrücke verglichen

Speicherung von Passwörtern



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

Speicherung von Passwörtern



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

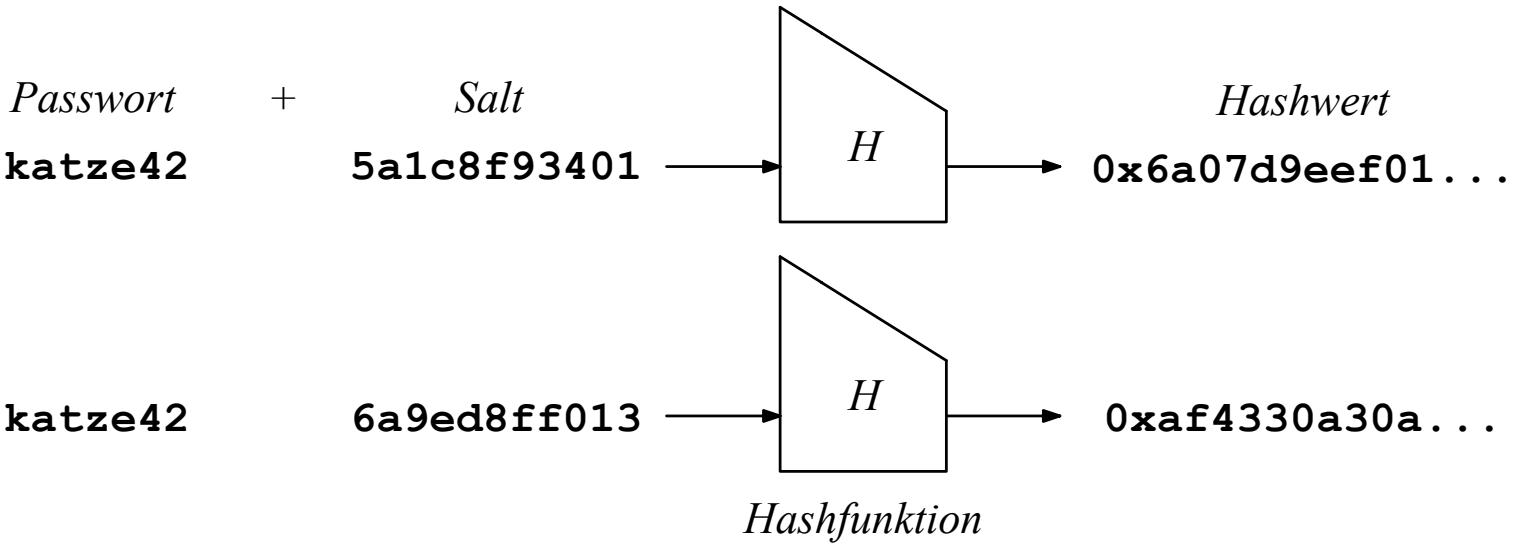
Was bleibt dem Angreifer noch übrig?

Angreifer probieren alle möglichen Passworte durch

Wie arbeiten Angreifer

Salz (Salt)

Beim Hashen von Passwörten 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%l+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%l+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-ITeViGulsvNüP`” = “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-ITeViGulsvNüP`” jetzt kein gutes Passwort mehr?

Das Ende des Vortrags

Fragen?