Passwortsicherheit

Lehrstuhl für Mediensicherheit

Eik List

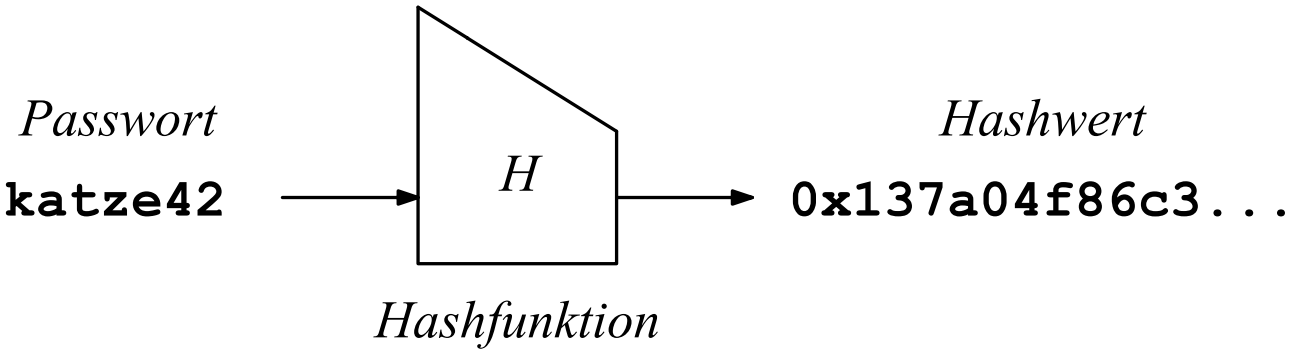
Bauhaus-Universität Weimar

Cryptoparty Weimar
20.09.2013

Agenda

- Passwörter benötigt man ständig
  - Computer-Login, Internet-Dienste, Smartphone-Login, ...
- Worum soll es in diesem Vortrag gehen?
  - Wie werden Passwörter verwendet
  - Wie arbeiten Angreifer typischerweise
  - Welche Regeln gibt es für eine bessere Passwortwahl

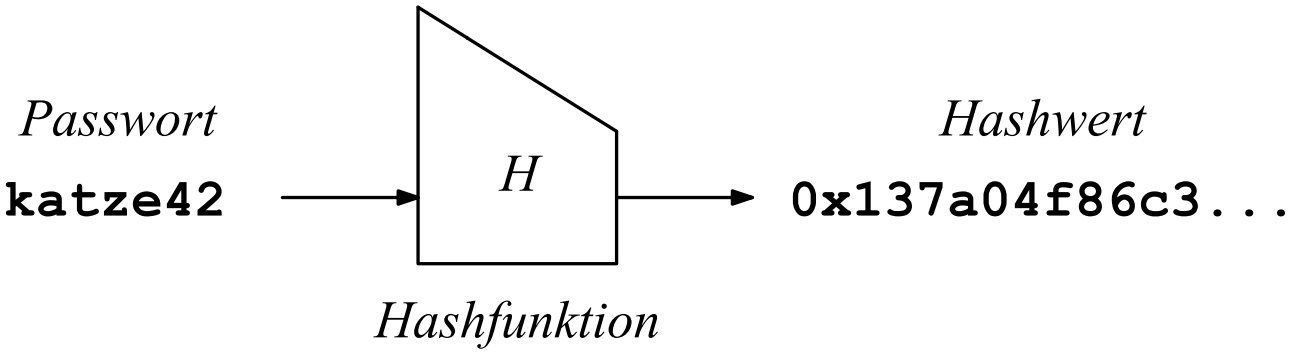
Wie werden Passworte verwendet?



- Meist als Eingabe in kryptographische Hashfunktionen:
  - Kryptographisch stark = nicht umkehrbar
  - Nur der Hash wird gespeichert
    Wird Datenbank publiziert, weiß der Dieb trotzdem noch nicht die Passwörter

⇒ Angreifer probieren alle mögl. Passworte durch

Wie werden Passworte verwendet?



- Meist als Eingabe in kryptographische Hashfunktionen:
  - Kryptographisch stark = nicht umkehrbar
  - Nur der Hash wird gespeichert
    Wird Datenbank publiziert, weiß der Dieb trotzdem noch nicht die Passwörter

$\Rightarrow$ Angreifer probieren alle mögl. Passworte durch

Wie arbeiten Angreifer typischerweise?

- Wir unterscheiden zwischen Online- und Offline-Angreifern
- Online-Angreifer:
  - Benötigt Interaktion mit einem Webserver oder Gerät (z.B. Smartphone)
  - Nur Server/Gerät kann Passworthash berechnen
  - Gut: Nur so viele Versuche wie Server/Gerät zulässt
  - Gut: Potentiell hohe Wartezeit nach einigen Versuchen
- Offline-Angreifer:
  - Kann Passworthashes selbst testen
  - Wird nicht gedrosselt!
  - Hat beliebig viele Versuche!

Wie arbeiten Angreifer typischerweise?

- Wir unterscheiden zwischen Online- und Offline-Angreifern
- Online-Angreifer:
  - Benötigt Interaktion mit einem Webserver oder Gerät (z.B. Smartphone)
  - Nur Server/Gerät kann Passworthash berechnen
  - Gut: Nur so viele Versuche wie Server/Gerät zulässt
  - Gut: Potentiell hohe Wartezeit nach einigen Versuchen
- Offline-Angreifer:
  - Kann Passworthashes selbst testen
  - Wird nicht gedrosselt!
  - Hat beliebig viele Versuche!

Wie arbeiten Angreifer typischerweise?

- Wir unterscheiden zwischen Online- und Offline-Angreifern
- Online-Angreifer:
  - Benötigt Interaktion mit einem Webserver oder Gerät (z.B. Smartphone)
  - Nur Server/Gerät kann Passworthash berechnen
  - Gut: Nur so viele Versuche wie Server/Gerät zulässt
  - Gut: Potentiell hohe Wartezeit nach einigen Versuchen
- Offline-Angreifer:
  - Kann Passworthashes selbst testen
  - Wird nicht gedrosselt!
  - Hat beliebig viele Versuche!

Offline-Angreifer

- Problem: Hashfunktionen sind viel zu effizient
  (nicht für Passwörter entwickelt)
- Passwörter lassen sich sehr schnell durchprobieren, z.B.:
  - ca. 1,2 Mrd./s für aktuelle Hashfunktionen (SHA2)
  - ca. 11 Mrd./s für Windows-XP-Passworthashes
- Derzeit nutzen Angreifer i.d.R. viele Grafikkarten

[Quelle: `http://hashcat.net/`]

Offline-Angreifer

- Problem: Hashfunktionen sind viel zu effizient
  (nicht für Passwörter entwickelt)
- Passwörter lassen sich sehr schnell durchprobieren, z.B.:
  - ca. 1,2 Mrd./s für aktuelle Hashfunktionen (SHA2)
  - ca. 11 Mrd./s für Windows-XP-Passworthashes
- Derzeit nutzen Angreifer i.d.R. viele Grafikkarten

[Quelle: `http://hashcat.net/`]

Offline-Angreifer

- Problem: Hashfunktionen sind viel zu effizient
  (nicht für Passwörter entwickelt)
- Passwörter lassen sich sehr schnell durchprobieren, z.B.:
  - ca. 1,2 Mrd./s für aktuelle Hashfunktionen (SHA2)
  - ca. 11 Mrd./s für Windows-XP-Passworthashes
- Derzeit nutzen Angreifer i.d.R. viele Grafikkarten

[Quelle: `http://hashcat.net/`]

Passwort-Crack-Programme

- Freie gute Software für diverse Hashfunktionen:
  - 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

$\Rightarrow$ Nur ausreichend lange und zufällige Passwörter sind sicher!

Passwort-Crack-Programme

- Freie gute Software für diverse Hashfunktionen:
  - 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

$\Rightarrow$ Nur ausreichend lange und zufällige Passwörter sind sicher!

Passwort-Crack-Programme

- Freie gute Software für diverse Hashfunktionen:
  - 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

$\Rightarrow$ Nur ausreichend lange und zufällige Passwörter sind sicher!

Was sind ausreichend lange Passwörter?

- 95 druckbare Zeichen
  - Klein-/Großbuchstaben, Ziffern, Satz- und Sonderzeichen
- Beispiel: Passwort aus 6 Zeichen
  - Eine von 95^6 Möglichkeiten
  - Informatik rechnet in 2er-Potenzen: $95^6 \approx 2^{40}$ Möglichkeiten

  $\Rightarrow$ 40 Bit **Entropie**

Was sind ausreichend lange Passwörter?

- 95 druckbare Zeichen
  - Klein-/Großbuchstaben, Ziffern, Satz- und Sonderzeichen
- Beispiel: Passwort aus 6 Zeichen
  - Eine von 95^6 Möglichkeiten
  - Informatik rechnet in 2er-Potenzen: $95^6 \approx 2^{40}$ Möglichkeiten

  $\Rightarrow$ 40 Bit **Entropie**

Was sind ausreichend lange Passwörter?

- Wir wissen:
  Eine aktuelle Grafikkarte kann 1,2 Mrd. $= 2^{30}$ Passwörter/s testen

$$\frac{2^{40}\ \text{Möglichkeiten}}{2^{30}\ \text{Möglichkeiten}/s} = 2^{10}\ \text{s} = 1024\ \text{s} \approx 17\ \text{min}$$

- Wie lange benötigen Angreifer für Passwörter mit höherer Entropie?
  - 50 Bit Entropie: $\approx$ 12 Tage
  - 60 Bit Entropie: $\approx$ 34 Jahre
  - 80 Bit Entropie: $\approx$ 35 Mio. Jahre
  - ...

Was sind ausreichend lange Passwörter?

- Wir wissen:
  Eine aktuelle Grafikkarte kann 1,2 Mrd. $= 2^{30}$ Passwörter/s testen

$$\frac{2^{40}\ \text{Möglichkeiten}}{2^{30}\ \text{Möglichkeiten}/s} = 2^{10}\ \text{s} = 1024\ \text{s} \approx 17\ \text{min}$$

- Wie lange benötigen Angreifer für Passwörter mit höherer Entropie?
  - 50 Bit Entropie: $\approx$ 12 Tage
  - 60 Bit Entropie: $\approx$ 34 Jahre
  - 80 Bit Entropie: $\approx$ 35 Mio. Jahre
  - ...

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen: $\approx$ 40 Bit Entropie
  - Eine (!) Grafikkarte in wenigen Minuten bis Stunden
- 8 zufällig gewählte Zeichen: $\approx$ 52 Bit Entropie:
  - Tausende mietbare Rechner (z.B. bei Amazon EC2) in wenigen Stunden
- 10 und mehr zufällig gewählte Zeichen: $>$ 65 Bit Entropie
  - Das dauert...

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen: $\approx$ 40 Bit Entropie
  - Eine (!) Grafikkarte in wenigen Minuten bis Stunden
- 8 zufällig gewählte Zeichen: $\approx$ 52 Bit Entropie:
  - Tausende mietbare Rechner (z.B. bei Amazon EC2) in wenigen Stunden
- 10 und mehr zufällig gewählte Zeichen: $>$ 65 Bit Entropie
  - Das dauert...

Was sind ausreichend lange Passwörter?

- 6 zufällig gewählte Zeichen: $\approx$ 40 Bit Entropie
  - Eine (!) Grafikkarte in wenigen Minuten bis Stunden
- 8 zufällig gewählte Zeichen: $\approx$ 52 Bit Entropie:
  - Tausende mietbare Rechner (z.B. bei Amazon EC2) in wenigen Stunden
- 10 und mehr zufällig gewählte Zeichen: $>$ 65 Bit Entropie
  - 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

- Menschen sind nie zufällig...

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
- Menschen sind nie zufällig...

Schlechte Passwort-Regeln

- Erratbare Begriffe:
  - “Weimar”, “monami”
- Namen oder Stichtage:
  - “Helga”, “20sep1993”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
  - “Lichtgeschwindigkeit”, “Sh3ttl4nd-TerrIer”, “Tr0ub4dour”
- Wortkombinationen:
  - “Adam.2+%;7Eva”
- Bekannte Begriffe:
  - “supercalifragilisto5287” (aus dem Musical Mary Poppins)

Schlechte Passwort-Regeln

- Erratbare Begriffe:
  - “`Weimar`”, “`monami`”
- Namen oder Stichtage:
  - “`Helga`”, “`20sep1993`”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
  - “`Lichtgeschwindigkeit`”, “`Sh3ttl4nd-TerrIer`”, “`Tr0ub4dour`”
- Wortkombinationen:
  - “`Adam.2+%;7Eva`”
- Bekannte Begriffe:
  - “`supercalifragilisto5287`” (aus dem Musical Mary Poppins)

Schlechte Passwort-Regeln

- Erratbare Begriffe:
  - “`Weimar`”, “`monami`”
- Namen oder Stichtage:
  - “`Helga`”, “`20sep1993`”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
  - “`Lichtgeschwindigkeit`”, “`Sh3ttl4nd-TerrIer`”, “`Tr0ub4dour`”
- Wortkombinationen:
  - “`Adam.2+%;7Eva`”
- Bekannte Begriffe:
  - “`supercalifragilisto5287`” (aus dem Musical Mary Poppins)

Schlechte Passwort-Regeln

- Erratbare Begriffe:
  - “`Weimar`”, “`monami`”
- Namen oder Stichtage:
  - “`Helga`”, “`20sep1993`”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
  - “`Lichtgeschwindigkeit`”, “`Sh3ttl4nd-TerrIer`”, “`Tr0ub4dour`”
- Wortkombinationen:
  - “`Adam.2+%;7Eva`”
- Bekannte Begriffe:
  - “`supercalifragilisto5287`” (aus dem Musical Mary Poppins)

Schlechte Passwort-Regeln

- Erratbare Begriffe:
  - “`Weimar`”, “`monami`”
- Namen oder Stichtage:
  - “`Helga`”, “`20sep1993`”
- Wort aus dem Wörterbuch, auch Verfremdung hilft nicht:
  - “`Lichtgeschwindigkeit`”, “`Sh3ttl4nd-TerrIer`”, “`Tr0ub4dour`”
- Wortkombinationen:
  - “`Adam.2+%;7Eva`”
- Bekannte Begriffe:
  - “`supercalifragilisto5287`” (aus dem Musical Mary Poppins)

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
  - "`as8%4,&xn9?14oqj.1!`"
  - $>$ 65 Bit Entropie
  - Problem: Wie merke ich mir eine solche Kombination?
- Einfacher: Kombination aus mind. fünf seltenen zufällig gewählten Wörtern
  - "`korrekt Pferd Batterie Büroklammer Magnet`"
  - $>$ 60 Bit Entropie

Gute Passwort-Regeln

- Zufällig (maschinell generierte) Passwörtern mit 10 und mehr Zeichen
  - "`as8%4,&xn9?14oqj.1!`"
  - $>$ 65 Bit Entropie
  - Problem: Wie merke ich mir eine solche Kombination?
- Einfacher: Kombination aus mind. fünf seltenen zufällig gewählten Wörtern
  - "`korrekt Pferd Batterie Büroklammer Magnet`"
  - $>$ 60 Bit Entropie

Gute Passwort-Regeln (ff.)

- Besser: Merksätze mit mind. 19, besser 22 und mehr Zeichen
  - "`IbhaCBUimiWulvüEMVTuP`" = Ich besuche heute abend die Cryptoparty der Bauhaus-Uni im monami in Weimar und lerne viel über E-Mail-Verschlüsselung, TOR und Passwortsicherheit.
  - 19 Zeichen: $>$ 60 Bit Entropie
  - 22 Zeichen: $>$ 70 Bit Entropie

- Noch besser: Ebenso lange Merksätze ohne der/die/das (weniger vorhersagbar)

  Kurzer Check: Warum ist "`IbhaCBUimiWulvüEMVTuP`" jetzt kein gutes Passwort mehr?

Gute Passwort-Regeln (ff.)

- Besser: Merksätze mit mind. 19, besser 22 und mehr Zeichen
  - "`IbhaCBUimiWulvüEMVTuP`" = Ich besuche heute abend die Cryptoparty der Bauhaus-Uni im monami in Weimar und lerne viel über E-Mail-Verschlüsselung, TOR und Passwortsicherheit.
  - 19 Zeichen: $>$ 60 Bit Entropie
  - 22 Zeichen: $>$ 70 Bit Entropie
- Noch besser: Ebenso lange Merksätze ohne der/die/das (weniger vorhersagbar)

Kurzer Check: Warum ist "`IbhaCBUimiWulvüEMVTuP`" jetzt kein gutes Passwort mehr?

Gute Passwort-Regeln (ff.)

- Besser: Merksätze mit mind. 19, besser 22 und mehr Zeichen
  - "`IbhaCBUimiWulvüEMVTuP`" = Ich besuche heute abend die Cryptoparty der Bauhaus-Uni im monami in Weimar und lerne viel über E-Mail-Verschlüsselung, TOR und Passwortsicherheit.
  - 19 Zeichen: $>$ 60 Bit Entropie
  - 22 Zeichen: $>$ 70 Bit Entropie
- Noch besser: Ebenso lange Merksätze ohne der/die/das (weniger vorhersagbar)

  Kurzer Check: Warum ist "`IbhaCBUimiWulvüEMVTuP`" jetzt kein gutes Passwort mehr?

Guter Umgang mit Passwörtern

- Nutzen Sie ruhig Passwortgeneratoren für zufällig gewählte Passwörter
  - Z.B. PWGen: `http://pwgen-win.sourceforge.net/`
  - Vertrauen Sie Online-Programmen nicht!
- Passworte aufschreiben?
  - Ja, wenn man sie sicher verwahrt
- Alternative: Passwortsafe-Programme
  - KeyPass: `http://keepass.info/`
  - Password Safe: `http://passwordsafe.sourceforge.net/`
  - Problem: Synchronisierung zwischen mehreren Geräten

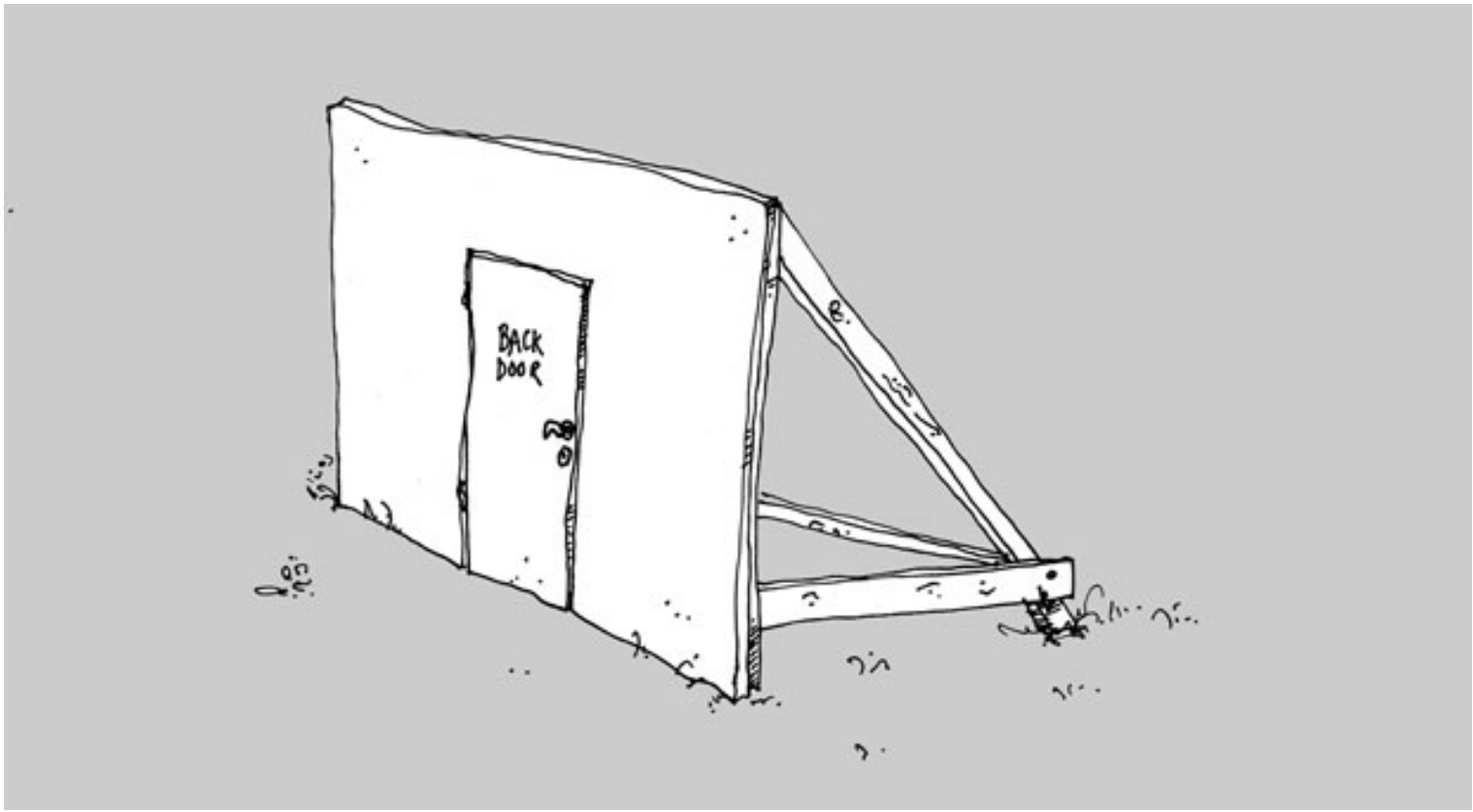
Guter Umgang mit Passwörtern

- Nutzen Sie ruhig Passwortgeneratoren für zufällig gewählte Passwörter
  - Z.B. PWGen: `http://pwgen-win.sourceforge.net/`
  - Vertrauen Sie Online-Programmen nicht!
- Passworte aufschreiben?
  - Ja, wenn man sie sicher verwahrt
- Alternative: Passwortsafe-Programme
  - KeyPass: `http://keepass.info/`
  - Password Safe: `http://passwordsafe.sourceforge.net/`
  - Problem: Synchronisierung zwischen mehreren Geräten

Guter Umgang mit Passwörtern

- Nutzen Sie ruhig Passwortgeneratoren für zufällig gewählte Passwörter
  - Z.B. PWGen: `http://pwgen-win.sourceforge.net/`
  - Vertrauen Sie Online-Programmen nicht!
- Passworte aufschreiben?
  - Ja, wenn man sie sicher verwahrt
- Alternative: Passwortsafe-Programme
  - KeyPass: `http://keepass.info/`
  - Password Safe: `http://passwordsafe.sourceforge.net/`
  - Problem: Synchronisierung zwischen mehreren Geräten

Gute Passwörter alleine reichen nicht



[Quelle: http://www.raumlabor.net/?p=502]

- Auch das beste Passwort nützt nichts, wenn man den Schutz einfach umgehen kann

Gute Passwörter alleine reichen nicht (ff.)

- Schließen Sie potentielle Hintertüren
  - Lügen Sie bei PW-Wiederherstellungsfragen (“erstes Auto”, “Mädchenname der Mutter”)
- Verwenden Sie Passwörter nicht mehrfach
  - Wegwerf-Passwörter für Unwichtige Seiten
  - Master-Passwort für versch. Dienste variieren, solange nicht nachvollziehbar für Andere
- Speichern Sie Passwörter niemals online
  - Dropbox und co. lesen Ihre Dateien (ja, wirklich!)

Gute Passwörter alleine reichen nicht (ff.)

- Schließen Sie potentielle Hintertüren
  - Lügen Sie bei PW-Wiederherstellungsfragen ("erstes Auto", "Mädchenname der Mutter")
- Verwenden Sie Passwörter nicht mehrfach
  - Wegwerf-Passwörter für Unwichtige Seiten
  - Master-Passwort für versch. Dienste variieren, solange nicht nachvollziehbar für Andere
- Speichern Sie Passwörter niemals online
  - Dropbox und co. lesen Ihre Dateien (ja, wirklich!)

Gute Passwörter alleine reichen nicht (ff.)

- Schließen Sie potentielle Hintertüren
  - Lügen Sie bei PW-Wiederherstellungsfragen ("erstes Auto", "Mädchenname der Mutter")
- Verwenden Sie Passwörter nicht mehrfach
  - Wegwerf-Passwörter für Unwichtige Seiten
  - Master-Passwort für versch. Dienste variieren, solange nicht nachvollziehbar für Andere
- Speichern Sie Passwörter niemals online
  - Dropbox und co. lesen Ihre Dateien (ja, wirklich!)

PS: Es gibt auch bessere Passwort-Verfahren

- Verlangsamte Berechnung
  - Rufen Hashfunktion intern Tausende Male auf
  - Stört den Nutzer nicht (0.1 Sekunden)
  - Bremst aber Angriffe aus
- Einsatz
  - Aktuelle Betriebssystem-Logins, GnuPG/PGP, ...
- Hier reichen schon Passwörter mit 50 Bit Entropie
- Hauptziel von Angreifern sind aber Webdienste

PS: Es gibt auch bessere Passwort-Verfahren

- Verlangsamte Berechnung
  - Rufen Hashfunktion intern Tausende Male auf
  - Stört den Nutzer nicht (0.1 Sekunden)
  - Bremst aber Angriffe aus
- Einsatz
  - Aktuelle Betriebssystem-Logins, GnuPG/PGP, ...
- Hier reichen schon Passwörter mit 50 Bit Entropie
- Hauptziel von Angreifern sind aber Webdienste

PS: Es gibt auch bessere Passwort-Verfahren

- Verlangsamte Berechnung
  - Rufen Hashfunktion intern Tausende Male auf
  - Stört den Nutzer nicht (0.1 Sekunden)
  - Bremst aber Angriffe aus
- Einsatz
  - Aktuelle Betriebssystem-Logins, GnuPG/PGP, ...
- Hier reichen schon Passwörter mit 50 Bit Entropie
- Hauptziel von Angreifern sind aber Webdienste

PS: Es gibt auch bessere Passwort-Verfahren

- Verlangsamte Berechnung
  - Rufen Hashfunktion intern Tausende Male auf
  - Stört den Nutzer nicht (0.1 Sekunden)
  - Bremst aber Angriffe aus
- Einsatz
  - Aktuelle Betriebssystem-Logins, GnuPG/PGP, ...
- Hier reichen schon Passwörter mit 50 Bit Entropie
- Hauptziel von Angreifern sind aber Webdienste

Fragen?