Sie und Ihr Passwort

„Mathematik schützt!“

Sie und Ihr Passwort

Warnung:

Die nachfolgenden Zahlenkolonnen können Ihre geistige Gesundheit langfristig im Guten, wie im Schlechten, beeinflussen.

Sie und Ihr Passwort

Der Zeichenumfang

Großbuchstaben-Umlaute = 26 verschiedene Zeichen

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Kleinbuchstaben-Umlaute = 26 verschiedene Zeichen

abcdefghijklmnopqrstuvwxyz

Ziffern = 10 verschiedene Zeichen

0123456789

Sie und Ihr Passwort

Der Zahlenraum

	Anzahl(Großbuchstaben)	= 26
+	Anzahl(Kleinbuchstaben)	= 26
+	Anzahl(Ziffern)	= 10
	verschiedene Zeichen	= 62

Sie und Ihr Passwort

Potenzen

Beispiel: für 3 Stellen nur Ziffern

10^3 = 10 * 10 * 10 = 1.000 Möglichkeiten

Sie und Ihr Passwort

Potenzen

Beispiel: für 3 Stellen nur Ziffern

10^3 = 10 * 10 * 10 = 1.000 Möglichkeiten

000 … 999 => 1.000

Sie und Ihr Passwort

Potenzen

Beispiel: für 3 Stellen Ziffern+Groß+Kleinbuchstaben

62^3 = 62 * 62 * 62 = 238.328 Möglichkeiten

Sie und Ihr Passwort

Potenzen

Beispiel: für 6 Stellen nur Ziffern

10^6 = 10 * 10 * 10 * 10 * 10 * 10 = 1.000.000 Möglichkeiten

Beispiel: für 6 Stellen nur Ziffern+Groß+Kleinbuchstaben

62^6 = 56.800.235.584

Beispiel: für 20 Stellen nur Ziffern+Groß+Kleinbuchstaben

62^20 = 70.442.342.554.699.802.296.833.026.461.637.000

Sie und Ihr Passwort

Potenzen

Beispiel: für 20 Stellen nur Ziffern+Groß+Kleinbuchstaben

62^20 = 70.442.342.554.699.802.296.833.026.461.637.000

70,4 Quintilliarden Möglichkeiten

Sie und Ihr Passwort

Passwortcracking

„John – The Ripper“ bei der Arbeit :

```
Tasks: 279 total,   2 running, 247 sleeping,   0 stopped,   1 zombie
%Cpu(s):  3,0 us,  1,7 sy, 93,9 ni,  0,0 id,  0,0 wa,  1,0 hi,  0,3 si,  0,0 st
KiB Mem :  4088688 total,   403624 free,  1677128 used,  2007936 buff/cache
KiB Swap:  1048572 total,   902396 free,   146176 used.  2300112 avail Mem

  PID  USER  PR  NI   VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
15423 root    39  19  16164   3020   2384 R   93,2  0,1     27:13.78 john /tmp/test.file
```

Nach 26 Minuten hatten wir diesen Zwischenstand:

```
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08   7% 1/3 0g/s 188.2p/s 188.2c/s 188.2C/s xt999996..morgade0
0g 0:00:01:30 38% 1/3 0g/s 175.8p/s 175.8c/s 175.8C/s "nettohaus..]99999
0g 0:00:26:42 21% 2/3 0g/s 51.35p/s 180.7c/s 180.7C/s bullet3..hannah3
```

Sie und Ihr Passwort

Passwortcracking

Beispiel: für 6 Stellen nur Ziffern+Groß+Kleinbuchstaben

62^6 = 56.800.235.584

Bei 180 Crackversuchen pro Sekunde würde das …

315.556.864,35 Sekunden
oder 3652,28 Tage
oder 9,99 Jahre

dauern.

Sie und Ihr Passwort

Eleminierung

„Bei 180 Crackversuchen pro Sekunde würde das 10 Jahre dauern...“

… wenn man wirklich alle Kombinationen testen müßte.

Muß man aber nicht.

Sie und Ihr Passwort

Eleminierung

Kombinationen wie …

aaaaaa
zzzzzz
000000
usw.

kann man weglassen, da diese so trivial sind,
daß angenommen werden kann,
das Crackprogramme oder Angreifer diese zuerst ausprobieren.

Sie und Ihr Passwort

Eleminierung

Kombinationen wie …

aaaaaa
ababab
...
000001

sind in Ihrer binären Schreibweisen für Passwörter ungeeignet,
da die resultierenden Bitmuster zu wenig Zufall für einen
Verschlüsselungsalgorithmus aufweisen.

Sie und Ihr Passwort

Eleminierung

Diese Annahmen reduziert den Testumfang um fast 20% .

In unserem Fall wären das 2 Jahre.

Sie und Ihr Passwort

GPU - Einsatz

GPU's

Die Prozessoren von Grafikkarten können die Berechnung deutlich schneller durchführen, als die Haupt-CPU das kann.

Sie und Ihr Passwort

GPU - Einsatz

Statt 180 Cracks/s , erlaubt eine Laptop GPU bereits 5 Millionen/s.

Sie und Ihr Passwort

GPU - Einsatz

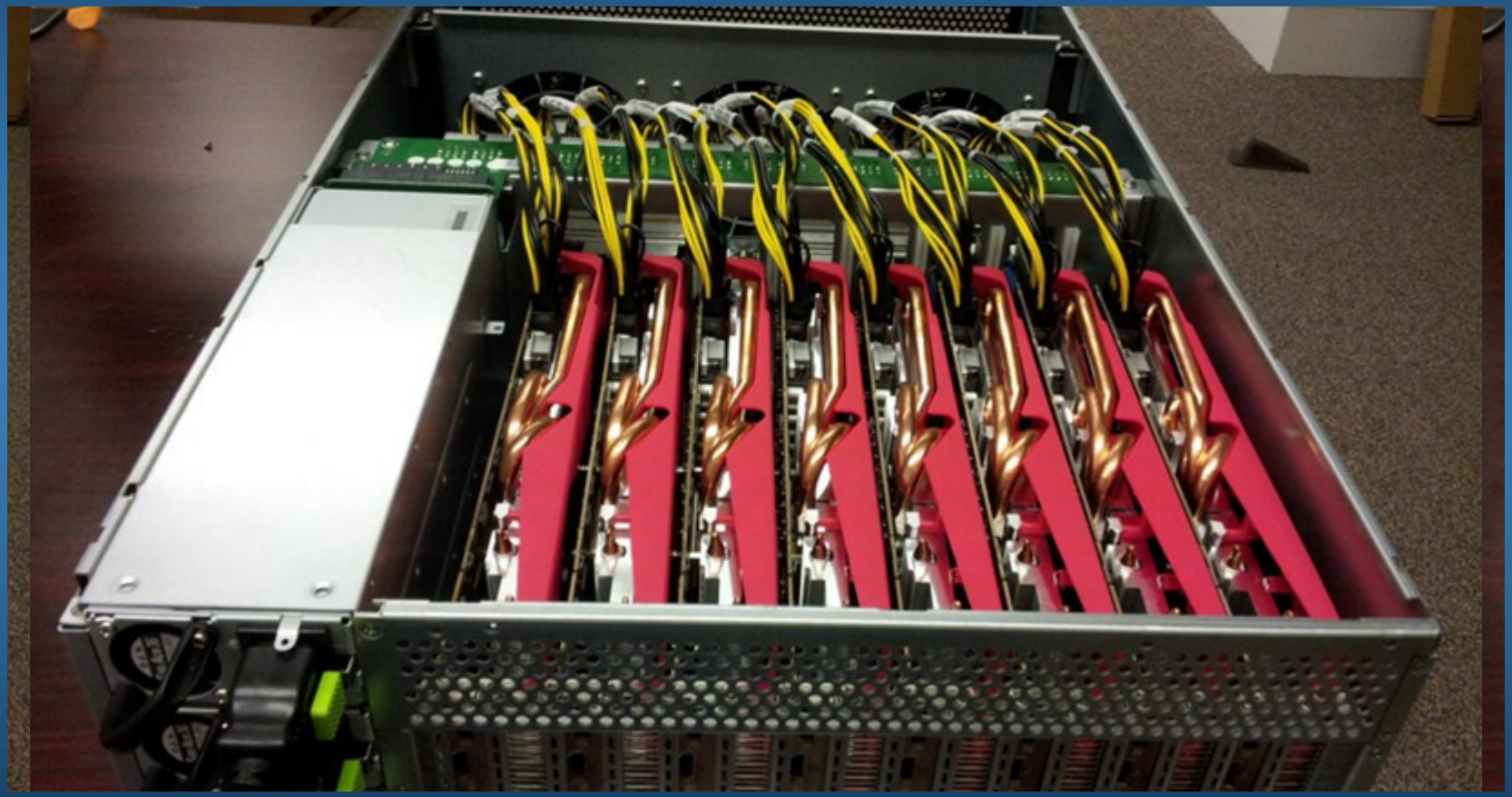
Statt 180 Cracks/s , erlaubt eine Laptop GPU bereits 5 Millionen/s.

Statt 10 Jahren dauert der Crack von 6 Stellen jetzt nur noch 3,1 Stunden

auf einem LAPTOP !

Sie und Ihr Passwort

25x GPU – 348 Milliarden Hashes pro Sekunde



© 2012 hackaday.com Mike Szczys

Sie und Ihr Passwort

25x GPU – 348 Milliarden Hashes pro Sekunde

Beispiel: für 20 Stellen nur Ziffern+Groß+Kleinbuchstaben

62^20 = 70.442.342.554.699.802.296.833.026.461.637.000

2.024.205.246.000.000.000.000 Sekunden

64.143.193.580.000.000 Jahre

64 Billiarden Jahre

Sie und Ihr Passwort

64 Billiarden Jahre
zum Vergleich, **das** hier ….

… ist grade mal 13,8 Milliarden Jahre alt.

Sie und Ihr Passwort

Zeit ist Sicherheit

Merke:

Alles was sicherstellt, daß

ein reines „Durchprobieren“ über 100 Jahre dauert,

gilt als sicher.

Sie und Ihr Passwort

Warum?

Weil es so etwas gibt.

Sie und Ihr Passwort

„Wie kann ich mich schützen?“

- Verschiedene Passwörter für verschiedene Dienste benutzen.
- Passwörter müssen eine Mindestlänge von 12 Zeichen haben
- Groß- und Kleinbuchstaben und Zahlen müssen gemischt vorkommen
- Für verschlüsselte Datenträger sollten mindestens 20 Zeichen, besser 30 benutzt werden.
- Gedankenstützen sind bei der Länge erlaubt, z.B. das (gedankliche) Aufsagen eines Satzes aus dem Wortanfänge und Satzzeichen benutzt werden. Der Satz sollte nicht erratbar sein!

  Beispiel: Ich möchte etwas lernen, deswegen bin ich heute hier und höre auf Platz 33 zu.
- Methode 1: „Ichmöchteetwaslernen,deswegenbinichheutehierundhöreaufPlatz33zu.“
  Methode 2: Imel,dbihhuhaP33z

Sie und Ihr Passwort

„Verbale Hashfunktion“

Beispiel:

„Ich möchte etwas lernen, deswegen bin ich heute hier und höre auf Platz 33 zu.“

Hashalgoritmus:

Entferne Leerzeichen & Entferne alle Zeichen nach der ersten Stelle.

Hashwert: Imel,dbihhuhaP33z.

Sie und Ihr Passwort

„Verbale Hashfunktion“

Ein Hashwert kann durch ein Geheimnis und einen Hashalgoritmus ermittelt werden,

aber

aus dem Hashwert kann das Geheimnis nicht direkt zurück gerechnet werden.

Sie und Ihr Passwort

„Verbale Hashfunktion“

Zum guten Schluß

Dies war natürlich nur ein ganz simples Beispiel für einen Hashalgorithmus.

In der Realität sind deutlich komplexere Algorithmen im Einsatz.

Sie und Ihr Passwort

„Verbale Hashfunktion“

Danke fürs Zuhören.