Über die Sicherheit von Passwörtern

Autor: Christoph Zurnieden (*czurnieden@users.sourceforge.net*)
Layout: Matthias Hagedorn (*matthias.hagedorn@selflinux.org*)

Die Sicherheit eines passwortgeschützten Systems hängt entscheidend von der richtigen Auswahl eines Passworts ab. Es können im grobem fünf Sicherheitsstufen unterschieden werden: **Nachlässig**, **Niedrig**, **Mittel**, **Hoch** und **Sehr Hoch**.

Inhaltsverzeichnis

1 Über die Sicherheit von Passwörtern

2 Nachlässig

3 Niedrig

4 Mittel

5 Hoch

6 Sehr hoch

7 Laufzeit

8 Extrem

9 Beruhigung

1 Über die Sicherheit von Passwörtern

Die Sicherheit eines passwortgeschützten Systems hängt entscheidend von der richtigen Auswahl eines Passworts ab. Es können im grobem fünf Sicherheitsstufen unterschieden werden: **Nachlässig**, **Niedrig**, **Mittel**, **Hoch** und **Sehr Hoch**.

Unter dem Punkt **Wahrscheinlichkeit** ist die Wahrscheinlichkeit in Prozent angegeben, daß das Password in einer gegebenen Zeit durch Brute-Force-Methoden erraten werden kann.

Die Berechnung erfolgt nach der Formel des **National Computer Security Centers** [NCSC1985a] (eine Kopie liegt unter http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.html)

$$P(S) = \frac{t_{life} \frac{n_{tries}}{\text{sec}}}{{n_c}^l}$$

Formel NCSC1985a

wobei `tlife` die Lebenszeit des Passwortes in Sekunden ist,

$$\frac{n_{tries}}{\text{sec}}$$

die Anzahl der möglichen Tests pro Sekunde, `nc` die Anzahl der möglichen Zeichen und `l` die Länge des Passwortes.

$$\frac{n_{tries}}{\text{sec}}$$

liegt mit durchschnittlichen Rechnern und normalem Verfahren `(crypt())` bei etwa 250.000 Versuchen/Sekunde.

2 Nachlässig

Als **nachlässig** sind solche Passwörter einzustufen, die aus regulären Wörtern bestehen, die aus einer Wortliste abgearbeitet werden können, wie sie massenhaft im Internet kursieren. Ja, jede Rechtschreibhilfe hat eine solche Wortliste. Unter solche Wörter fallen natürlich auch Namen, insbesondere von Familienangehörigen und Haustieren. Auch Wörter, die auf der Tastatur gebildet werden können ("wert", "asdf" u.s.w.) gehören dazu. Außerdem alle Passwörter, die einfach zu kurz sind, mögen sie auch noch so geschickt gewählt sein.

Wahrscheinlichkeit:
Geht stark gegen 100%.

3 Niedrig

Als **niedrig** gelten solche Passwörter, die folgenden Regeln folgen:

* Das Passwort muß mindestens ein alphanumerisches Zeichen enthalten.
* Es ist nicht länger als 14 Zeichen.
* Es enthält keine Leerzeichen.
* Es kann zudem noch ein Sonderzeichen enthalten, muß aber nicht.
* Es wird zwischen Groß- und Kleinschreibung unterschieden.

* Es hat eine Lebensdauer von maximal einem Jahr.

Beispiele (In Klammern die Beispielaussprache in Englisch):

IcvawyowgIbCic (Ic-vaw-yowg-Ib-Cic)
tunebelk (tun-eb-elk)
itvigumI (it-vig-um-I)
uccywojEgty (uc-cy-woj-Eg-ty)
hiddUlicdift (hidd-Ul-ic-dift)
SudNom (Sud-Nom)

Wahrscheinlichkeit:

10454% bei einer Länge von 6 und einer Auswahl aus 65 Zeichen [a-zA-Z0-9] und ein paar Sonderzeichen.*
161% bei einer Länge von 7 aus gleicher Auswahl.*
2,5% bei einer Länge von 8 aus gleicher Auswahl.
0,0000000000003% bei einer Länge von 14 und gleicher Auswahl.

*)
Die Werte über 100% kommen dadurch zustande, daß die gesamte Gültigkeitsdauer als Zeit für die Versuche zur Verfügung steht. Bei der theoretischen Anzahl von 250.000 Versuchen pro Sekunde sind die einfachen Passwörter nun einmal sehr schnell geknackt, bei sehr einfachen Passwörtern sogar deutlich innerhalb der Gültigkeitsdauer. Solche Passwörter/Gültigkeitsdauer Kombinationen sind demnach eindeutig ungeeignet.

Das Login-Programm benutzt unter anderem auch die Möglichkeit, durch Herabsetzung der Anzahl der Versuche pro Sekunde die Sicherheit der Passwörter zu erhöhen. In den mir bekannten Distributionen ist z.B. eine kleine Pause von einer Sekunde nach Eingabe eines fehlerhaften Passwortes eingestellt. Dadurch reduziert sich die Anzahl der Versuche auf einen pro Sekunde. Dieser Umstand sollte aber unter gar keinen Umständen genutzt werden, da die verschlüsselten Passwörter in einer Datei gehalten werden.
(Eine Datei vor dem Lesen zu schützen ist sehr schwierig, es können immer mal wieder Sicherheitslücken auftreten, die das zulassen könnten, nicht zuletzt direkter Hardwarezugriff) Auf diese Angaben können dann normale Crackprogramme angesetzt werden, die dann wieder auf 250.000 Versuche pro Sekunde und mehr kommen können.

4 Mittel

Als **mittel** gelten solche Passwörter, die diesen Regeln folgen:

* Das Passwort muß mindestens 8 Zeichen enthalten, ist aber nicht länger als 14 Zeichen.
* Es kann Sonderzeichen enthalten.
* Es muß mindestens ein alphabetisches Zeichen enthalten sein.
* Es darf den Benutzernamen nicht enthalten.
* Es enthält keine Leerzeichen.
* Es wird zwischen Groß- und Kleinschreibung unterschieden.
* Es hat eine Lebensdauer von maximal einem halbem Jahr.

Beispiele 1:

!Tvv,+I*k?%
(Sea?{~Cp@
IROKobh`#>d
vobjiWuz> (vob-ji-Wuz-GREATER_THAN)
Wruhaukbot) (Wru-hauk-bot-RIGHT_PARENTHESIS)
ishcichejKev} (ish-cich-ej-Kev-RIGHT_BRACE)

Beispiele 2 (Enthält keine Sonderzeichen, die Ärger in Shellscripten machen könnten, es aber meist trotzdem tun):

;)XbNo#h%]
j~//pdZq<
CnjKdgM(M-n*(
ofNocip} (of-Noc-ip-RIGHT_BRACE)
vafAdyif; (vaf-Ad-yif-SEMICOLON)
pomcotyadoon& (pom-cot-yad-oon-AMPERSAND)

Wahrscheinlichkeit:
0,06% bei einer Länge von 8 und einer Auswahl aus 95 Zeichen [:print:]
0,0006% bei einer Länge von 9 und gleicher Auswahl.
0,0000066% bei einer Länge von 10 und gleicher Auswahl.

5 Hoch

Als **hoch** gelten solche Passwörter, die jenen Regeln folgen:

* Es gelten alle Regeln für **mittel**.
* Es muß mindestens ein numerisches Zeichen enthalten.
* Es muß mindestens ein Sonderzeichen enthalten.
* Die ersten drei Zeichen dürfen nicht gleich sein.
* Die ersten drei Zeichen dürfen nicht im Benutzernamen enthalten sein.
* Es hat eine Lebensdauer von maximal 3 Monaten.

Beispiele 1:

_y@lK^T8(
`"%ld!QG2DGA
GTDeUZ#-7
IF=Qd6U*n{q
enalAjOj% (en-al-Aj-Oj-PERCENT_SIGN)

NeubOcaj< (Neub-Oc-aj-LESS_THAN)

Beispiele 2 (aus Gründen, wie bei "mittel")

]aj~-kn4vYc/wg
jfVN/QAfak
rVG1s<K*^5j
l=.y)Q*utZKd
udGifwis# (ud-Gif-wis-CROSSHATCH)
yewt^Shrak' (yewt-CIRCUMFLEX-Shrak-APOSTROPHE

Wahrscheinlichkeit:
Insgesamt etwas niedriger als bei **mittel**

6 Sehr hoch

Als **Sehr hoch** gelten solche Passwörter, die jenen Regeln folgen:

* Das Passwort muß mindestens 14 Zeichen lang sein.
* Es muß mindestens ein alphabetisches Zeichen enthalten.
* Es muß mindestens ein numerisches Zeichen enthalten.
* Es muß mindestens ein Sonderzeichen enthalten.
* Es muß mindestens ein Leerzeichen enthalten
* Es dürfen keine drei Zeichen in Folge gleich sein.
* Es dürfen keine drei Zeichen in Folge aus dem Benutzernamen enthalten sein.
* Die Zeichenfolge darf nicht aussprechbar sein.
* Es hat eine Lebensdauer von maximal einem Monat.

Beispiel 1:

3'cIy`a$ d\mWK(0e¤'lp
Y6E6hE®5U.Z$aQ;>|/Ps$&]R
\-IOæbq}zE&EA2
N3$a jw%{TI¢E{/%
YZ# #þ0M uyAs!'Pb
shSz*GP)1 X¾$=A(H~RXc

Beispiel 2 (Wieder die Gründe, wie bei **mittel** und **hoch**):

TIQ-Ndx¡¬O 0~]i
@6Fi=,K¹-:µ^_SG@jg~n
x)/@£z-&- _.E%_MTK2gm}5;
KmZªfc(7ÐnZziUÞR(;FQAd[r
M0 & hr}!_p14>~©KKzqaU
(R,EP md]U(Pd,A1»ZBnzi

Wahrscheinlichkeit:
0,0000000000000000000013% bei einer Länge von 14 und einer Auswahl aus 256 Zeichen.
0,000000000000000000000000000000000000000000001% bei einer Länge von 24 und der gleichen Auswahl.

(Sie ist eigentlich etwas höher, da einige Passwörter rausfallen. Allerdings nicht signifikant)

7 Laufzeit

Was nützt das beste Passwort, wenn es ewig haltbar ist. Je mehr Zeit vergeht, desto eher besteht die Möglichkeit, daß es doch noch geknackt, verraten oder gestohlen wird. Deshalb ist es zu empfehlen, die Laufzeit von Passwörtern zu begrenzen. Je nach Sicherheitsanspruch kann das von einigen Stunden bis hin zu einem Jahr gehen. Die Beziehung zwischen der Lebensdauer eines Passwortes und dessen Sicherheit ist direkt proportional. Auch ein **niedriges** Passwort kann ausreichend Sicherheit geben, wenn es stündlich gewechselt wird, wie ein **hohes** durchaus Schwachstellen aufweist, wenn es jahrelang beibehalten wird.

Beispiel

Ein Password aus der Kategorie **Niedrig** mit einer Laufzeit von einem Monat und eine Länge von 8 Zeichen hat statt 2,5% bei einer Laufzeit von einem Jahr nun nur noch 0,2% Wahrscheinlichkeit, innerhalb dieser Zeit geknackt werden zu können.

Ein Password der Kategorie **Hoch** mit 14 Zeichen Länge hat bei einer Laufzeit von einem Jahr statt einem Monat nur noch eine Wahrscheinlichkeit von 1,5e-23 statt wie vorher 1,2e-24. Das ist fast das Zehnfache und könnte vielleicht reichen.

8 Extrem

Es gibt auch noch die Gruppe der **extremen Passwörter**, die sehr lang sind. Zu lang, um sie noch von Hand eingeben zu können, geschweige denn, sie sich überhaupt zu merken. Diese Passwörter werden als Schlüssel benutzt, z.B. auf elektronisch lesbaren Karten. Diese Schlüssel sind meist 1024 Bytes lang.

Hier mal ein Beispiel (in ASCII, der Lesbarkeit wegen):

+iG8<3u9+%CY9_w5UZI6(Yt*f*DS3]&7 nHK8Z.kG^3R%jeSQB+rE ?U[,8{)boYiv!CNI"yo=5DgR/
oT%7K9u7k%o,gF>D-9cKp0[>_U='_G~l8=?E8ITdIK) iwKqB^.2u@wVKQ}7iF-0H?P"d FaqG=v4U
lx3cu.zHoo`m'}dGFx VIY%]~3mcSKkA]8)j(o&cUezo@sf\VP _W9|0{&>b?N4Ix@s;99'{PRMd~?
{r8$4Q&H9-@eKybMkZ.GW^| ^cKP{%RC`,)O^7.9>vlFa0r;:MG$V89eIssCo6*YA^U8.<<&`,YwmF@
r6z\(u%I"D^8`tY9E6YbyIX\Va<wto!0gR?N@W#3Bvz;3#s[6Umk<bf-p?M/_:g5Q3^txeW1SVmg^
KSq>Z1qNt8[SP5)zV,.nR5"F]$c`uBq!Y[wk@!5t^|&g>9p4)-yF(kosG[C%n-zI _kPAiK2&T_V{{m
\M?biIpc[1CTQOay,b ;^txeW1SVmg^KSq>Z1qNt8[SP5)zV,.nR5"F]$c`uBq!Y[wk@!5t^|&g>9p 4)-
(kosG[C%n-zI"_kPAiK2&T_V{{m\M?biIpc[1CTQOay, $d;@-mlpj&Kzj&XK\5@v@-mlpj&Kz
j&XK\5@vW,{x1,c;/$;]7w><?yN!r#$.9Xf.*d<}K -KP83~FE[TbG+2l/U~e9pGf{2Zd{}2Yp3XA^!
H0K.%/Tfr=TyQx7K0sXID}tzc;Q~E*}1a{AmQ/ITj>94Qs,RbZ/E2(zKH+(Teu<^>xXW'UEk@y,\0IA
"S4pvgC|*&7plMP5Yf?C}@C0{bkX0N<q!_ uQ6$U3s,Bmk6\V)[RhGC?7w2c*lV$i'/CWY]iVuXWYIl
E]Mz%Cq))tvU8F%<1/(<Ra!>UqKYNV)jBHW,?Tv!8&YyTPo0F}V/zV=\P>":b,i5ry~P%YW(%./;w2/
&qn;w->3,9e94qkI!Zgs9yeQbrn/SkX&WCK\K;Q,w|(G3 q{?a4cjbS$)\9eNZZ;F^7>#,mUWtQZ~Q3
:C[wiS`cDVVnWP9C(\Yhf?3IrjrX#GKfB!^;7:0/&;bq&PZHrFA8Ig!9tl;(bl#_KoufHpWM6kC"^(a
~VQ<Qh?bf@K<Md #/0Uep@`|T/KI(f^/c9 WA"G1NV(I}_

Der entscheidende Nachteil solcher Schlüssel ist, daß sie irgendwo aufgeschrieben sein müssen. Man kann sie zwar noch mit einem normalen Passwort kombinieren, das nützt allerdings nichts und verführt zudem zu noch lässigerem Umgang als so schon üblich.

Alle Beispiele wurden mit `apg` (**Automated Password Generator** Adel I. Mirzazhanov http://www.adel.nursat.kz/apg/) generiert. Dieser Generator in der Version, wie hier benutzt (2.0.0final (PRNG: X9.17/CAST)) generiert allerdings keine Leerzeichen und keine Zeichen oberhalb dezimal 128, die habe ich selber eingefügt.

9 Beruhigung

Wie man anhand der aufgelisteten Wahrscheinlichkeiten sieht, reicht schon der regelmäßige Wechsel eines gutgewählten Passwortes mit 8 Zeichen.