Passwort-Würfeltabelle

Einleitung

Dieses Dokument enthält eine Anleitung wie Passwörter zufällig mittels eines Würfels und einer unten aufgeführten Tabelle ohne Computer generiert werden können.

Es wird auch diskutiert aus wie vielen Zeichen ein Passwort bestehen sollte.

Generierung von Passwörtern

Passwörter werden im Folgenden aus diesen 72 Zeichen gebildet:

```
abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
!”$%&/#*:=
```

Für jedes Zeichen, das dem Passwort hinzugefügt werden soll, machen Sie drei Würfe mit einem Würfel, der die Zahlen eins bis sechs in gleicher Wahrscheinlichkeit hervorbringt. Mit dem ersten Wurf entscheidet sich, ob ein Zeichen aus Tabelle 1 oder 2 verwendet wird. Bei einem ersten Wurf kleiner vier wird das nächste Zeichen aus Tabelle 1 genommen, sonst aus Tabelle 2. Mit dem zweiten Wurf bestimmt man die Spalte und mit dem dritten Wurf die Zeile des Zeichens.

Wurf 1 = 1, 2 oder 3							
		Wurf 2					
		1	2	3	4	5	6
Wurf 3	1	A	j	/	4	q	3
	2	w	O	V	R	6	t
	3	#	8	F	d	J	T
	4	G	9	L	g	Q	1
	5	Y	0	h	*	o	2
	6	7	p	S	H	D	e

Tabelle 1: Wurf 1 zwischen 1 und 3

Wurf 1 = 4, 5 oder 6							
		Wurf 2					
		1	2	3	4	5	6
Wurf 3	1	z	&	W	B	N	s
	2	a	%	X	:	m	I
	3	Z	f	K	U	c	E
	4	"	5	n	!	y	r
	5	u	b	M	C	k	x
	6	P	$	i	l	v	=

Tabelle 2: Wurf 1 zwischen 4 und 6

Beispiel: Erster Wurf: 4. Zweiter Wurf: 1. Dritter Wurf: 6. Der erste Wurf (4) entscheidet, dass die Tabelle 2 verwendet wird. Der zweite Wurf (1) legt fest, dass die erste Spalte verwendet wird. Der dritte Wurf (6) legt fest, dass die sechste Zeile verwendet wird. In Tabelle 2 befindet sich in der ersten Spalte, in der sechsten Zeile, das Zeichen `P`. Also fügen Sie Ihrem Passwort das Zeichen `P` hinzu.

Im Beispiel werden weitere Zufallszeichen erzeugt:

gewürfelt:	4 1 6	4 2 2	2 2 2	1 5 5	1 2 3	5 1 5	2 6 6	5 2 2	2 2 5	6 3 1
Passwort:	P	%	O	o	8	u	e	%	0	W

Variationstabelle

Für die in diesem Dokument beschriebene Vorgehensweise, mit einem Alphabet von 72 Zeichen, ergeben sich Variationszahlen wie in Tabelle 3 dargestellt. In der ersten Spalte steht die Anzahl der Zeichen des Passworts. In der zweiten Spalte steht die Anzahl der Variationen, die sich für die jeweilige Passwortlänge bilden lassen. Zum Beispiel gibt es 26 873 856 unterschiedliche Passwörter, die aus genau 4 Zeichen unseres 72-Zeichen-Alphabets bestehen.

In der dritten Spalte ist aufgeführt, wie lange eine leistungsfähige Grafikkarte benötigt, um alle Passwort-Variationen der gegebenen Zeichenanzahl zu enttarnen. Gemeint ist der Fall, dass der Angreifer an die abgespeicherten, sogenannten hash-codierten, Passwortdaten gelangt ist. Passwörter werden hoffentlich nicht im Klartext gespeichert. Bei dieser Angriffsart wird eine riesige Anzahl von vermeintlichen Klartextpassworten in jeweils ein hash-codiertes Passwort verwandelt. Gleicht eines davon dem ausgespähten, hash-codierten Passwort, ist das Passwort enttarnt. Das ist ähnlich wie wenn man bei einem Tresor nacheinander Zahlenkombinationen ausprobiert.

Heutzutage, Stand 2024, kann eine leistungsfähige Grafikkarte bis zu 20 Milliarden (20×10^9) Passwörter pro Sekunde auf diese Art prüfen. Die Zahl kann je nach Hash-Verfahren variieren. Aus der Spalte drei kann man entnehmen, dass diese Grafikkarte nur etwa 0.001 s brauchen würde, um alle möglichen 4 Zeichen langen Passwörter unseres 72-Zeichen-Alphabets zu testen.

Versucht der Angreifer über eine Benutzerschnittstelle, z.B. beim Online-Banking, Passwörter zu testen, wird dies viel langsamer geschehen. Und hoffentlich nach ein paar Fehlversuchen durch den Dienstleister unterbunden.

Für eine gegebene Passwortlänge, kann jede Variation, jedes Passwort, mit der gleichen Wahrscheinlichkeit auftreten, da wir die Zeichen zufällig durch Würfeln bestimmen. Ein Passwort wird statistisch schon nach dem Durchprobieren der Hälfte aller möglichen Variation enttarnt sein. In der vierten Spalte wird die durchschnittliche Zeit für einen Enttarnungsversuch mit der Rechenkraft von 100 Grafikkarten angegeben. Zum Beispiel: Ein 9 Zeichen langes zufallsgeneriertes Passwort wird bei einem Enttarnversuch mit 100 Grafikkarten im Durchschnitt nach 3.61 h aufgedeckte werden.

Die Länge von Passwörtern

Wie schnell ein Passwort durch Erraten enttarnt wird, hängt von verschieden Faktoren ab. Je größer die Menge von Passworten ist, die ein Angreifer durchprobieren muss, um auf das gesuchte Passwort zu kommen, je länger hält das Passwort dem Angriff, statistisch gesehen, stand.

Angreifer machen sich zu Nutzen, dass Benutzer sich Passwörter auswählen, die sich leicht merken lassen. Sie testen also zuerst kurze Passwörter (wie „Ki99_“) und solche, die einen Sinn ergeben (wie „Dampfschiffahrt“) oder auf einer Tastatur ein einfaches Muster bilden (wie „qwertzui“).

Wie sieht es aus, wenn man Kombinationen aus ganzen bekannten Worten bildet? Zum

Beispiel 'PyramideLaufen'. Auch solche Passwörter haben Angreifer im Visier. Sie testen Kombinationen aus bekannten Worten. Nimmt man den Wortschatz eines Deutschsprachigen mit 50 000 Wörtern an, ergibt sich eine Anzahl von $50\,000 \cdot 50\,000 = 2\,500\,000\,000$ Kombinationen für zwei-Wort Passwörter. Das benötigt mit der angenommenen Grafikkarte ebenso weniger als eine Sekunde zum Enttarnen.

Die in diesem Dokument beschriebene Methode zur Passwortgenerierung erzeugt nur unwahrscheinlich bekannte Wörter oder solche die ein einfaches Muster auf der Tastatur bilden. Bleibt die Überlegung wie lange das Passwort sein sollte.

Für die Wahl der Passwortlänge betrachten wir

- die angenommenen Rechenleistung, die Anzahl eingesetzter Grafikkarten eines potentiellen Angreifers: N_G
- die Zeit, die der Angreifer vermutlich aufwendet: T
- die akzeptierte Wahrscheinlichkeit der Enttarnung des Passworts: P_{Ent}

Die Variationstabelle 3 kann nicht die Rechenzeiten für beliebige Anzahlen von Grafikkarten und beliebige Enttarnwahrscheinlichkeiten darstellen. Daher berechnen wir aus den obigen Faktoren die Rechenzeit T_1, die eine einzelnen Grafikkarte benötigte, um das Passwort mit 100 % Wahrscheinlichkeit zu enttarnen.

$$T_1 = N_G \cdot T \cdot \frac{1}{P_{Ent}}$$

Diese Rechenzeit T_1 ist eben in Spalte 3 der Tabelle 3 aufgeführt. Man kann dann in der ersten Spalte nachsehen aus wie viele Zeichen das entsprechende Passwort besteht.

Beispiel 1: Ein Angreifer arbeitet mit einer einzelnen Grafikkarte. Die Wahrscheinlichkeit, dass er das Passwort innerhalb von 1 Woche aufdeckt soll kleiner als $1\,\% = {}^1\!/_{100}$ sein. Daraus folgt, dass eine einzelne Grafikkarte bei 100 % Enttarnwahrscheinlichkeit

$$T_1 = (1 \cdot 1/52 \cdot 100)\,\text{Jahre} \approx 1.92\,\text{Jahre}$$

benötigt. Die Spalte 3 der Tabelle 3 zeigt, ab einer Passwortlänge von 10 Zeichen ist dies gegeben.

Beispiel 2: Ein mächtiger Angreifer arbeitet mit 1000 Grafikkarten. Die Wahrscheinlichkeit, dass er das Passwort innerhalb von 2 Jahren aufdeckt soll kleiner als $0.01\,\% = {}^1\!/_{10\,000}$ sein. Daraus folgt, dass eine einzelne Grafikkarte bei 100 % Enttarnwahrscheinlichkeit

$$T_1 = (1000 \cdot 2 \cdot 10\,000)\,\text{Jahre} = 20\,000\,000\,\text{Jahre}$$

benötigt. Die Spalte 3 der Tabelle 3 zeigt, ab einer Passwortlänge von 14 Zeichen ist dies gegeben.

Nach momentanem Stand würde ich Passwörter bis einschließlich 7 Zeichen Länge als 'schwach' und nach der hier beschriebenen Methode generierte Passwörter mit 14 oder mehr Zeichen als 'stark' bezeichnen.

Anforderung von Sonderzeichen in Passwörtern

Manchmal wird beim Anlegen eines Passworts verlangt und überprüft, dass mindestens ein Sonderzeichen und/oder eine Zahl und/oder ein Großbuchstabe und/oder ein Kleinbuchstabe enthalten ist. Falls das nach obiger Methode ausgewürfelte Passwort diese Anforderung nicht erfüllt, hängen Sie nach belieben, ohne Würfeln, fehlende Zeichen an. Durch dieses Verlängern des Passworts kann es nicht leichter enttarnt werden.

Beispiel: Sie kommen zum Schluss, dass ein 12-Zeichen-Passwort ihren Anforderungen genügt und erfwürfeln: `G7fdsUM5q1Tx`. Falls gefordert, hängen sie dann ein beliebiges Sonderzeichen an: `G7fdsUM5q1Tx*`

Die Leistungssteigerung von Computer-Hardware

Die Leistungssteigerung von Computer-Hardware wird oft als exponentiell angenommen. Das hieße, jedes Jahr könnten neu entwickelte Grafikkarten im Vergleich zum Vorjahr um einen bestimmten Faktor mehr Passwörter pro Zeit testen. Es wäre also nur eine Frage der Jahre bis ein Passwort, das heute als lang genug angesehen wird, mit schnellerer Computer-Hardware enttarnt werden kann.

Wie sollte also die Passwortlänge im Laufe der Jahre angepasst werden? – Auch die Stärke (Variationszahl) von Passwörtern wächst exponentiell mit ihrer Länge, sofern sie zufallsgeneriert sind. Nach unserem Verfahren wächst die Variationszahl für jedes zusätzliche Zeichen um den Faktor 72. Das heißt, um das exponentielle Geschwindigkeitswachstum der Hardware zu kompensieren, müssen wir jeweils nach einer konstanten Anzahl von Jahren unsere Passwortlänge um eins erhöhen.

Rechenbeispiel: Nehmen wir an, die Computer-Hardware wird alle 4 Jahre um den Faktor 2 schneller. Dies entspricht einem jährlichen Faktor von $2^{1/4} \approx 1.19$. Dann bräuchte es $\log_{2^{1/4}} 72 \approx 24.7$ Jahre bis die Leistungssteigerung den Faktor 72 erreicht hat. Entsprechend müssten wir in die Zukunft schauend für alle 24.7 Jahre unsere Passwortlänge um eins erhöhen.

Nehmen wir an, die Computer-Hardware wird alle 2.5 Jahre um den Faktor 2 schneller. Dann sollten wir alle $\log_{2^{1/2.5}} 72 \approx 15.4$ Jahre das Passwort um ein Zeichen länger wählen.

Passwort-länge	Variationen	Zeit (1 Grafikkarte)	halbe Zeit (100 Grafikkarten)
1	72	<0.001 s	<0.001 s
2	5184	<0.001 s	<0.001 s
3	373 248	<0.001 s	<0.001 s
4	26 873 856	0.001 s	<0.001 s
5	1 934 917 632	0.097 s	<0.001 s
6	139 314 069 504	6.97 s	0.035 s
7	10 030 613 004 288	502 s	2.51 s
8	7.22×10^{14}	10.0 h	181 s
9	5.20×10^{16}	30.1 d	3.61 h
10	3.74×10^{18}	5.94 a	10.8 d
11	2.70×10^{20}	427 a	2.14 a
12	1.94×10^{22}	30 772 a	154 a
13	1.40×10^{24}	2 215 572 a	11 078 a
14	1.01×10^{26}	159 521 178 a	797 606 a
15	7.24×10^{27}	1.15×10^{10} a	57 427 624 a
16	5.22×10^{29}	8.27×10^{11} a	4.13×10^{9} a
17	3.76×10^{31}	5.95×10^{13} a	2.98×10^{11} a
18	2.70×10^{33}	4.29×10^{15} a	2.14×10^{13} a
19	1.95×10^{35}	3.09×10^{17} a	1.54×10^{15} a
20	1.40×10^{37}	2.22×10^{19} a	1.11×10^{17} a
21	1.01×10^{39}	1.60×10^{21} a	8.00×10^{18} a
22	7.27×10^{40}	1.15×10^{23} a	5.76×10^{20} a
23	5.23×10^{42}	8.29×10^{24} a	4.15×10^{22} a
24	3.77×10^{44}	5.97×10^{26} a	2.99×10^{24} a
25	2.71×10^{46}	4.30×10^{28} a	2.15×10^{26} a
26	1.95×10^{48}	3.10×10^{30} a	1.55×10^{28} a
27	1.41×10^{50}	2.23×10^{32} a	1.11×10^{30} a
28	1.01×10^{52}	1.60×10^{34} a	8.02×10^{31} a
29	7.29×10^{53}	1.16×10^{36} a	5.78×10^{33} a
30	5.25×10^{55}	8.32×10^{37} a	4.16×10^{35} a
31	3.78×10^{57}	5.99×10^{39} a	3.00×10^{37} a
32	2.72×10^{59}	4.31×10^{41} a	2.16×10^{39} a
33	1.96×10^{61}	3.11×10^{43} a	1.55×10^{41} a
34	1.41×10^{63}	2.24×10^{45} a	1.12×10^{43} a
35	1.02×10^{65}	1.61×10^{47} a	8.05×10^{44} a
36	7.31×10^{66}	1.16×10^{49} a	5.80×10^{46} a
37	5.26×10^{68}	8.35×10^{50} a	4.17×10^{48} a
38	3.79×10^{70}	6.01×10^{52} a	3.00×10^{50} a
39	2.73×10^{72}	4.33×10^{54} a	2.16×10^{52} a
40	1.96×10^{74}	3.12×10^{56} a	1.56×10^{54} a
41	1.41×10^{76}	2.24×10^{58} a	1.12×10^{56} a
42	1.02×10^{78}	1.61×10^{60} a	8.07×10^{57} a

Tabelle 3: Anzahl Variationen in Abhängigkeit der Passwortlänge bei einem Alphabet von 72 Zeichen. s: Sekunden, h: Stunden, d: Tage, a: Jahre.