

openHPI-Kurs „Digitale Identitäten“
Exkurs: Einfluss der Passwortlänge

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Passwortlänge

Passwortlänge hat einen entscheidenden Einfluss auf die Stärke/Sicherheit eines Passworts und die Effizienz möglicher Passwortattacken

Erinnerung: Hinweise zur Generierung sicherer Passwörter:

- Groß- und Kleinbuchstaben
- unterschiedliche Zeichenklassen (Buchstaben, Zahlen, Sonderzeichen (\$% &:; -_? §! ...))
- mindestens 12 Zeichen lang
- nicht aus dem Wörterbuch
- nicht aus dem Nutzerkontext ableitbar
- keine Wiederverwendung

Womit begründen sich diese Hinweise?

Brute Force Angriffe (1/2)

Brute Force Attacken sind die einfachsten und gradlinigsten Angriffe, um ein Passwort zu knacken

- **Idee:** Systematisches Durchprobieren aller möglichen Zeichenkombinationen für ausgewählte Zeichenklassen bei vorgegebener Länge
- Mit genügenden Zeitressourcen führt Brute Force stets zum Ziel, also zum Auffinden eines Passworts
- Berechnungsformel für die Anzahl aller Passwortkandidaten:

$$\text{Anzahl_Passwortkandidaten} = (\text{Umfang_des_Zeichenvorrats})^{\text{PasswortLänge}}$$

Brute Force Angriffe (2/2)

Idee: Systematisches Durchprobieren aller möglichen Zeichenkombinationen für ausgewählte Zeichenklassen bei vorgegebener Länge

$$\text{Anzahl_Passwortkandidaten} = (\text{Umfang_des_Zeichenvorrats})^{\text{PasswortLänge}}$$

Erwartungswert für die durchschnittliche Anzahl von Versuchen, ein Passwort zu finden:

$$\text{Durchschnittliche Anzahl von Versuchen} = \text{Anzahl_Passwortkandidaten} / 2$$

Um sich vor Brute Force Attacken zu schützen, muss die Anzahl der Passwortkandidaten so groß wie möglich sein

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern:

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen in jeder Position: $26 + 10 = 36$

Passwortlänge = 1

o									
---	--	--	--	--	--	--	--	--	--

36

= 36

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,001 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 2



$36 * 36$

$= 1.296$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,001 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 3

o **4** **w**

$36 * 36 * 36$

$= 46.656$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,001 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 4

o **4** **w** **f**

$36 * 36 * 36 * 36$

= 1.679.616

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,001 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 5

o 4 w f 7

$36 * 36 * 36 * 36 * 36$

$= 60.466.176$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,001 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 6

o 4 w f 7 q

$36 * 36 * 36 * 36 * 36 * 36$

$= 2.176.782.336$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,022 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 7

o 4 w f 7 q 2

$36 * 36 * 36 * 36 * 36 * 36 * 36$

$= 78.364.164.096$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 0,784 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 8

o 4 w f 7 q 2 1

$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36$

$= 2.821.109.907.456$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 28,211 \text{ sec}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 9

o 4 w f 7 q 2 1 n

$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36$

$= 101.559.956.668.416$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können

$\triangleq < 16,927 \text{ min}^*$

Berechnung der Anzahl möglicher Passwortkandidaten

Beispiel: Passwort besteht aus Kleinbuchstaben und Ziffern

Kleinbuchstaben:

■ abcdefghijklmnopqrstuvwxyz: 26 mögliche Zeichen

Ziffern

■ 0123456789: 10 mögliche Zeichen

Anzahl der möglichen Zeichen: $26 + 10 = 36$

Passwortlänge = 10

o 4 w f 7 q 2 1 n t

$$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 = 3.656.158.440.062.976$$

* Benötigte Zeit, um alle möglichen Passwortkandidaten zu testen, wenn 100.000.000.000 Passwörter pro Sekunde generiert werden können $\triangleq < 10,156 \text{ h}^*$

- Brute Force Angriffe werden häufig gegen Passworthashes durchgeführt
 - mögliche Passwortkandidaten werden ghasht
 - generierter Passworthash wird mit dem Ziel-Hash verglichen
 - bei Übereinstimmung ist Passwortkandidat das gesuchte Passwort
- Die Geschwindigkeit von Brute Force Attacken ist abhängig von der Berechnungsgeschwindigkeit der verwendeten Hashfunktion
 - MD5-Hashes lassen sich wesentlich schneller berechnen als SHA-512-Hashes

Cracking Komplexität

Passwort- länge bis	Zahlen [0-9]	Zahlen + Kleinbuchstaben [0-9a-z]	Alphanumerisch [0-9a-zA-Z]	Alphanumerisch + Sonderzeichen [0-9a-zA-Z\$% &; - _? §!...]
5	< 1 Sek	< 1 Sek	< 1 Sek	< 1 Sek
6	< 1 Sek	< 1 Sek	< 1 Sek	~ 7,43 Sek
7	< 1 Sek	< 1 Sek	~ 35,79 Sek	~ 11,76 Min
8	< 1 Sek	~ 29,02 Sek	~ 36,99 Min	~ 18,62 Std
9	< 1 Sek	~ 17,41 Min	~ 1,59 Tage	~ 2,43 Monate
10	< 1 Sek	~ 10,45 Std	~ 3,25 Monate	~ 19,24 Jahre
11	~ 1 Sek	~ 2,24 Wochen	~ 16,82 Jahre	~ 18,28 Jh
12	~ 11 Sek	~ 1,55 Jahre	~ 10,43 Jh	nahezu ewig
13	~ 1.85 Min	~ 55,79 Jahre	nahezu ewig	nahezu ewig
14	~ 18.5 Min	~ 20,08 Jh	nahezu ewig	nahezu ewig
15	~ 3.09 Std	nahezu ewig	nahezu ewig	nahezu ewig
...				
20	~ 35.33 Jahre	nahezu ewig	nahezu ewig	nahezu ewig

Benötigte Zeit zum Erstellen aller möglichen Passwortkandidaten, wenn 100 Milliarden Passwörter pro Sekunde generiert werden können