



openHPI course "Digital Identities Excursus: Password length

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

password length

- The length of a password has a big influence on the strength of the password and the efficiency of possible password attacks.

Remember: Our tips for generating good passwords:

- Upper and lower case letters
- Different character classes (letters, numbers, special characters (\$ % & : ; - _ ? § ! ...))
- At least 12 characters long
- Not from the dictionary
- Not derivable from the user context
- No reuse

But why are these hints necessary at all?

Brute Force Attack

- Brute force attacks are the simplest and most straightforward attacks to find a password.
 - Testing all possible character combinations for a given length and selected character classes
 - Can find any password if enough time is available

$$\text{Number_of_password_candidates} = (\text{number_of_possible_characters})^{\text{Password length}}$$

- Average number of attempts to find a password:
 $\text{Number_of_password_candidates} / 2$
- To protect against brute force attacks, the number of password candidates should be as large as possible.

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = \mathbf{36}$
- **Password length = 1**



$$36 = 36$$
$$\triangleq < 0.001 \text{ sec}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = \mathbf{36}$
- **Password length = 2**



$36 * 36$

$= 1.296$

$\triangleq < 0.001 \text{ sec}^*$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = \mathbf{36}$
- **Password length = 3**

o **4** **w**

36 * 36 * 36

= 46.656

≙ < 0.001 sec*

* Required time to generate all possible password candidates when
100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = \mathbf{36}$
- **Password length = 4**

o 4 w f

$36 * 36 * 36 * 36$

$= 1.679.616$

$\triangleq < 0.001 \text{ sec}^*$

* Required time to generate all possible password candidates when
100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 5**

o	4	w	f	7					
---	---	---	---	---	--	--	--	--	--

$$36 * 36 * 36 * 36 * 36 = 60.466.176$$
$$\triangleq < 0.001 \text{ sec}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 6**

o	4	w	f	7	q				
---	---	---	---	---	---	--	--	--	--

$$36 * 36 * 36 * 36 * 36 * 36 = 2.176.782.336$$
$$\triangleq \sim 0.022 \text{ sec}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 7**

o 4 w f 7 q 2

36 * 36 * 36 * 36 * 36 * 36 * 36

= 78.364.164.096

≙ ~ 0.784 sec*

* Required time to generate all possible password candidates when
100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 8**

o	4	w	f	7	q	2	1		
---	---	---	---	---	---	---	---	--	--

$$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 = 2.821.109.907.456$$
$$\triangleq \sim 28,211 \text{ sec}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 9**

o 4 w f 7 q 2 1 n

$$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 = 101.559.956.668.416$$
$$\triangleq \sim 16,927 \text{ min}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Calculation of Number of possible password candidates

Example: Password consisting of lower case letters and numbers

- Lower case:
 - abcdefghijklmnopqrstuvwxyz - 26 possible characters
- figures
 - 0123456789 - 10 possible characters
- Number of possible characters: $26 + 10 = 36$
- **Password length = 10**

o 4 w f 7 q 2 1 n t

$$36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 * 36 = 3.656.158.440.062.976$$
$$\triangleq \sim 10,156 \text{ h}^*$$

* Required time to generate all possible password candidates when 100 billion passwords can be generated per second

Brute force attacks against password hashes

- Brute force attacks are often performed against password hashes
 - Possible password candidates are hashed
 - Generated password hash is compared with target hash
 - If there is a match, the password candidate is the correct password.

- The speed of brute force attacks depends on the calculation speed of the hash function used.
 - MD5 hashes can be calculated much faster than SHA-512 hashes

Cracking Complexity

Password length up to	figures [0-9]	Numbers + lower case letters [0-9a-z]	Alphanumeric [0-9a-zA-Z]	Alphanumeric + special characters [0-9a-zA-Z\$% &; - _? §!...]
5	< 1 sec	< 1 sec	< 1 sec	< 1 sec
6	< 1 sec	< 1 sec	< 1 sec	~ 7,43 sec
7	< 1 sec	< 1 sec	~ 35,79 sec	~ 11,76 Min
8	< 1 sec	~ 29,02 sec	~ 36,99 Min	~ 18.62 hours.
9	< 1 sec	~ 17,41 Min	~ 1,59 days	~ 2.43 months
10	< 1 sec	~ 10.45 hours	~ 3.25 months	~ 19,24 years
11	~ 1 sec	~ 2,24 weeks	~ 16.82 years	~ 18,28 Jdh
12	~ 11 sec	~ 1.55 years	~ 10,43 Jdh	almost eternal
13	~ 1.85 min	~ 55.79 years	almost eternal	almost eternal
14	~ 18.5 min	~ 20,08 Jdh	almost eternal	almost eternal
15	~ 3.09 hours	almost eternal	almost eternal	almost eternal
...				
20	~ 35.33 years	Almost forever	almost eternal	almost eternal

- Time required to create all possible password candidates when 100 billion passwords can be generated per second

Cracking Complexity

Password length up to	figures [0-9]	Numbers + lower case letters [0-9a-z]	Alphanumeric [0-9a-zA-Z]	Alphanumeric + special characters [0-9a-zA-Z\$% &; - _? §!...]
5	< 1 sec	< 1 sec	< 1 sec	< 1 sec
6	< 1 sec	< 1 sec	< 1 sec	~ 7,43 sec
7	< 1 sec	< 1 sec	~ 35,79 sec	~ 11,76 Min
8	< 1 sec	~ 29,02 sec	~ 36,99 Min	~ 18.62 hours.
9	< 1 sec	~ 17,41 Min	~ 1,59 days	~ 2.43 months
10	< 1 sec	~ 10.45 hours	~ 3.25 months	~ 19,24 years
11	~ 1 sec	~ 2,24 weeks	~ 16.82 years	~ 18,28 Jdh
12	~ 11 sec	~ 1.55 years	~ 10,43 Jdh	almost eternal
13	~ 1.85 min	~ 55.79 years	almost eternal	almost eternal
14	~ 18.5 min	~ 20,08 Jdh	almost eternal	almost eternal
15	~ 3.09 hours	almost eternal	almost eternal	almost eternal
...				
20	~ 35.33 years	Almost forever	almost eternal	almost eternal

- Time required to create all possible password candidates when 100 billion passwords can be generated per second