

openHPI course "Digital Identities
Attacks on accounts -
Weak point "Weak passwords"

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

Weak passwords

Many users use weak passwords for services on the Internet

Reason: "Human Factor".

- convenience
- lack of safety awareness
- complex passwords are hard to remember
- ...

Passwords can be weak for several reasons

1. Passwords of **low complexity**
2. Passwords with **derivation from user context**
3. **Reuse of** passwords

Weak passwords: Passwords with low complexity

■ When are passwords too simple?

- < 12 characters
- Use only one Character group (numbers, letters, special characters)
- Findable in a dictionary
- Key sequence on the keyboard, e.g. "qwertz", "qwe123", ...

password	frequency
123456	1,19%
123456789	0,52%
12345678	0,35%
12345	0,19%
password	0,15%
111111	0,11%
11111111	0,10%
123123	0,09%
1234567	0,08%
000000	0,07%

Source: HPI Identity Leak Checker

- ## ■ Table shows **top 10 passwords** the database of the HPI Identity Leak Checker

Weak passwords:

Passwords from the user context

- Many users use **personal details as passwords**
 - Username, name of partner / child / parent
 - date of birth
 - ...

 - Some passwords are also **derived from the authenticating service.**
 - Adobe database: adobe123, photoshop, adobe1, ...
- Attacker who knows his victim can easily guess such passwords

Weak passwords: Reuse of passwords (1/2)

Most users use relatively secure passwords

But:

- Same password is often used for all accounts
 - e.g. password ***D7\$4?g!inRo*** is used for each service
 - A slightly different password is used for different accounts.
 - ***D7\$4?g!inRoA*** for service A, ***D7\$4?g!inRoB*** for service B,
D7\$4?g!inRoC for service C
- If password file of only one service is leaked and lands on the Internet, then all other services are also affected ...

Weak passwords:

Reuse of passwords (2/2)

- Problem: **63%** of data thefts are due to improper use of passwords (Verizon Breach Report, 2016)
 - Password reuse is particularly critical
- HPI researchers have researched 1 billion user passwords
 - 68 billion users with at least two accounts
- observation
 - **20%** of users use **identical passwords** more than once
 - **27%** of users use **similar passwords** more than once
 - But: with **similar services**, reuse is sometimes **50%**.

Properties of secure passwords

- No information from the **user context**, i.e. no information that attackers could research about their victim.
 - e.g. username, name, date of birth, ...
- No words from a **dictionary** or proverbs
- At least **12 characters**
- Made up of different **character groups** (special characters, upper and lower case letters and digits)
- Use of **different passwords** for accounts and no reuse of old passwords
- Compliance with these rules considerably complicates the misuse of all accounts

- See also "Protective measure: Secure passwords" this week

Summary: Weak passwords

■ **issue**

- Many users often choose weak passwords (**human factor**) due to lack of security awareness and convenience.
- Weak passwords are easier to remember, but can also be guessed or cracked faster

■ **Weak passwords**

- Have a low complexity
- Can be derived from the user context

■ **password reuse**

- Reused passwords are considered weak
- If a (strong) password is leaked in plain text, all accounts with the same password are at risk.

Summary: Weak passwords

■ **issue**

- Many users often choose weak passwords (**human factor**) due to lack of security awareness and convenience.
- Weak passwords are easier to remember, but can also be guessed or cracked faster

■ **Weak passwords**

- Have a low complexity
- Can be derived from the user context

■ **password reuse**

- Reused passwords are considered weak
- If a (strong) password is leaked in plain text, all accounts with the same password are at risk.