openHPI Course: Digital Identities – Who am I on the Internet?

Password protected Accounts – Weak Passwords

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Weak Passwords

Many users use weak passwords for services on the Internet

- **Reason: "Human Factor"**
  - convenience
  - lack of security awareness
  - complex passwords are difficult to remember
  - …

Passwords can be weak for several reasons

- Passwords of **low complexity**
- Passwords that can be **derived from user context**
- Passwords that can be **find in dictionaries**
- **Reuse** of passwords

Weak Passwords
Passwords with Low Complexity

When are passwords weak?

- Less than **12 characters**
- Use of **only one group of characters** (numbers, letters, special characters)
- Can be found in a **dictionary**
- Key pattern sequence on the keyboard, e.g. "qwerty," "qwe123,“

- Table shows **top 10 passwords** from the HPI Identity Leak Checkers database

#	Password	Frequency
1	123456	8,06 ‰
2	123456789	3,87 ‰
3	password	1,89 ‰
4	qwerty	1,83 ‰
5	12345	1,37 ‰
6	12345678	1,16 ‰
7	111111	1,15 ‰
8	qwerty123	1,01 ‰
9	1q2w3e	0,96 ‰
10	123123	0,84 ‰

Weak Passwords
Passwords From the User Context

- Many users use **personal data as passwords**, e.g.
  - first name / last name
  - name of partner / child / parent …
  - date of (own, partner's, children's) birth, birthday, …
  - favorite band, actor, author, …
- To some extent passwords are also **derived from the respective service name**
  - Adobe database: adobe123, photoshop, adobe1, …

➡ An attacker who knows his victim can easily guess such passwords.

Weak Passwords
Reuse of Passwords (1/2)

Many users use relatively secure passwords, **but**:

- The same password is often used for all accounts, **D7$4?g!inRo** is used as a password for login for every online service
  - or password is only slightly modified for different accounts
    - **D7$4?g!inRo**A for service **A**
    - **D7$4?g!inRo**B for service **B**
    - **D7$4?g!inRo**C for service **C**

➡ **If password data of only one service is leaked to the Internet, then all other services are affected!**

Weak Passwords
Reuse of Passwords (2/2)

- With our ID-Leak Checker service we analyzed **1 Billion** leaked credentials (email and password)
  - 68 Millions users with at least two accounts
- **Result**:
  - **20%** of users use identical passwords multiple times
  - **27%** of users use similar passwords multiple times
  - **But**: For similar services, reuse rate can go up to 70%

Properties of Secure Passwords

Passwords are “strong" when they are complex and difficult to guess

Some advice for choosing good passwords:

- Passwords should be **case-sensitive** and should contain both uppercase and lowercase letters
- **Combinations** of multiple words are also useful (*Passphrase*)
- In addition to letters, passwords should contain **digits** and **special characters** ($% &:; -_? §! ...)
- **Minimum length 12**
  - The longer the password length, the higher the security (because with each additional character the complexity increases exponentially)
- **No** passwords from user context or dictionary
- **No** old passwords that have already been used

Weak Passwords
Summary

Problem

- Many users choose weak passwords because of a lack of security awareness and for convenience (**human factor**)
- Weak passwords are easier to remember, but can also be quickly guessed or cracked

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 plaintext, all accounts with the same password are compromised