# Article information:

密码强度：实证分析 | IEEE 会议出版物 | IEEE探索
<https://ieeexplore.ieee.org/abstract/document/5461951>

# Article summary:

1. User-chosen passwords are somewhat predictable and attackers can reduce the number of attempts needed to guess a password by using tools such as dictionaries or probabilistic models.

2. The effectiveness of different password cracking techniques depends on the size of the search space that an attacker can afford to explore, and there is a wide variance in password strength.

3. The study provides figures that can help system designers assess the security of their systems and estimate the cost of cracking any password. It also suggests using information about single-guess iteration costs to create better active password checkers for users and security audit tools for system administrators.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article titled "Password Strength: An Empirical Analysis" provides an analysis of the effectiveness of various password cracking techniques. The authors compare the search space versus the number of cracked passwords for guessing techniques including dictionary attacks, brute force, dictionary mangling, probabilistic context-free grammars, and Markov chains. They cross-validate their experiments on three large datasets of passwords, different in terms of application domain and user localization.

The article provides valuable insights into the resilience of passwords against advanced password-cracking techniques. However, there are some potential biases and limitations to consider. Firstly, the study only evaluates password cracking techniques using homogeneous metrics and on different datasets. This approach may not account for system-specific characteristics such as hashing algorithms and computational power of attackers.

Secondly, the study does not provide evidence for some claims made. For instance, the authors claim that even very powerful attackers would not be able to break some passwords. However, they do not provide evidence to support this claim.

Thirdly, the study does not explore counterarguments or alternative perspectives on password strength evaluation. For example, it does not consider alternative authentication methods such as biometrics or two-factor authentication.

Fourthly, the article may have promotional content towards creating more effective password checkers and security audit tools. While these tools may be useful in improving password security, it is important to note that they are not foolproof solutions.

Finally, while the article notes potential risks associated with weak passwords in internet applications' authentication systems, it does not present both sides equally by focusing solely on password strength evaluation rather than exploring alternative authentication methods or addressing potential privacy concerns associated with storing plain text passwords.

In conclusion, while "Password Strength: An Empirical Analysis" provides valuable insights into password strength evaluation and its limitations against advanced password-cracking techniques, it is important to consider its potential biases and limitations when interpreting its findings.

# Topics for further research:

* Alternative authentication methods for internet applications
* Risks associated with storing plain text passwords
* Privacy concerns with password security measures
* Two-factor authentication for improved security
* Biometric authentication for internet applications
* Limitations of password cracking techniques in specific systems

# Report location:

<https://www.fullpicture.app/item/5544ab2ce3fc81cecf0bf0a58e2971e7>