LU09a - Grundlagen BruteForce

Lernziele

- Den Unterschied zwischen einer Brute-Force-Methode (BFM) und Brute-Force-Attacke (BFA) erläutern.
- In eigenen Worten den Begriff und die Funktionsweise einer BFA erklären.
- Basierend auf der Varianz des Passworts die Kombinationsmöglichkeiten zu dessen Offenlegung berechnen.

Einleitung

Die Brute-Force-Methode (englisch für „rohe Gewalt“) bzw. Methode der rohen Gewalt ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller (oder vieler) möglichen Varianten beruht.

Ein wichtiger Anwendungsbereich findet sich in der Computersicherheit. Ein oft angeführtes Anwendungsbeispiel für die Brute-Force-Methode ist hier das Brechen oder umgangssprachlich *Knacken* von Passwörtern.

Die Brute-Force-Suche ist einfach zu implementieren und dazu bestimmt, die korrekte Lösung zu finden. Allerdings steigt der Aufwand an Rechenoperationen proportional zur Anzahl der zu probierenden, möglichen Lösungen, wobei die Anzahl dieser möglichen Lösungen mit steigendem Umfang der Probleme häufig exponentiell ansteigt.

Mögliche Kombinationen

Die mathematische Berechnungsformel der Kombinationsmöglichkeiten lautet:

$$\text{Kombinationen} = \text{Zeichenanzahl}^{\text{Passwortlänge}}$$

Rechenbeispiel: Unser Alphabet umfasst 26 Grossbuchstaben. Bei einer Passwortlänge von 7 Zeichen ergibt sich dann die folgende Rechnung:

- Kombinationen = 26 * 26 * 26 * 26 * 26 * 26 * 26<
- = 8‘031‘810‘176 → 8 Mrd. Kombinationen

Je nach Rechenkapazität und Länge des Passwortes kann das Finden des Passwortes Wochen bis Monate dauern.

 Volkan Demir

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m183/learningunits/lu09/01

Last update: **2025/12/08 09:08**