LU09c - Gegenmassnahmen BruteForce

Zeitverzögerung / Latenzzeit

Eine sehr einfache, aber effektive wie effiziente Massnahme ist das Einbauen einer kleinen Zeitverzögerung zwischen den einzelnen Versuchen. Diese Zeitverzögerung wird von den regulären Benutzenden kaum wahrgenommen. Sie summiert sich aber bei grossen Anzahl von Abfragen Mengen und sorgt dafür, dass ein Ergebnis in nützlicher Frist nicht vorliegen kann. D.h. im Falle einer Brute Force Attacke wird die maximale Suchzeit markant vergrössert.

Eine Variante ist die Zeit für den Neuversuch immer überproportional zu verlängern:

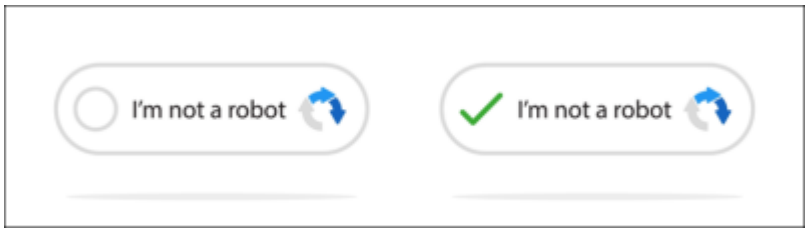
```
- Fehlversuch: 10 Sekunden warten
- Fehlversuch: 1 Minute
- Fehlversuch: 5 Minuten
- ...
```

Beschränkung der Versuche

Ebenfalls sehr einfach in der Realisierung ist die Beschränkung der Anzahl Versuche. Bei mehrmaligem, oft drei Versuche, wird das Konto gesperrt. Dieses Verfahren wird gelegentlich auch in Kombination mit einer Zeitverzögerung eingesetzt.

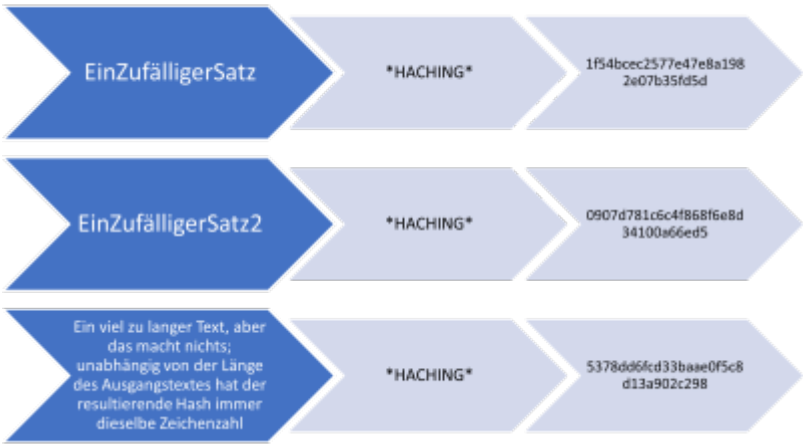
Interaktive Komponente

Eine weitere einfache Massnahme gegen Brute Force Attacken liegt darin dem User eine einfache Berechnung durchführen zu lassen. Dies kann via JavaScript durchgeführt werden. Um das Formular Absenden zu können, muss der User das korrekte Ergebnis der Rechnung eingeben. Serverseitig wird für die Weiterverarbeitung eine Bestätigung des Clients erwartet.

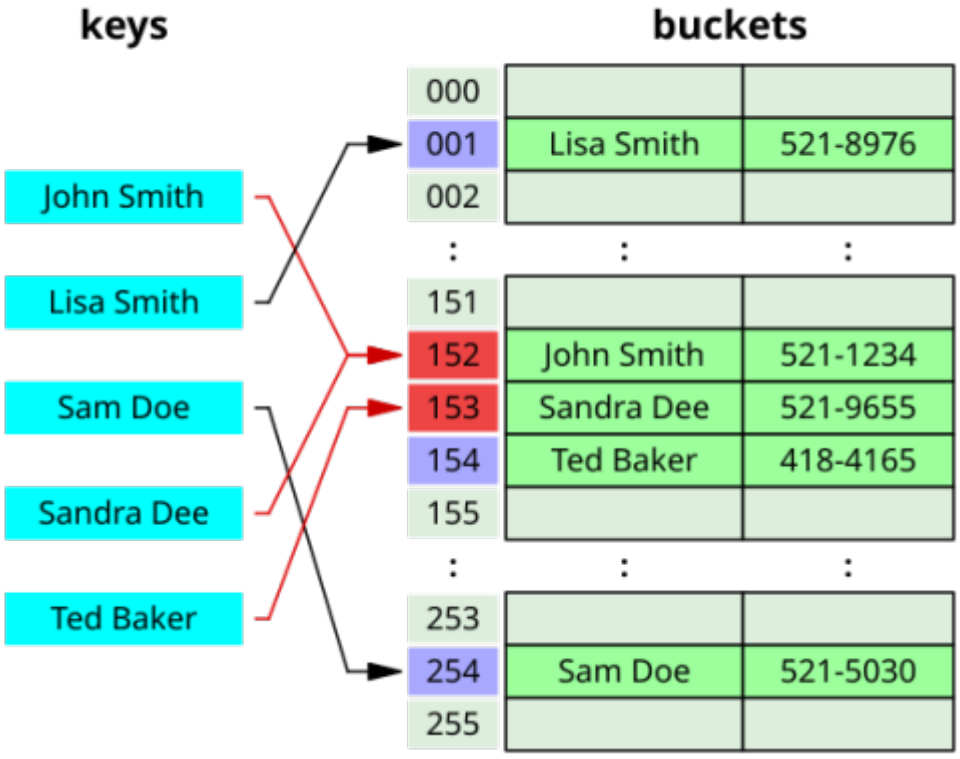


Alternativ wird häufig ein Captcha-Plugin verwendet, dass auf eine korrekte Eingabe seitens User wartet.

Hash-Funktionen



Oft sind Passwörter mit Hilfe von kryptographischen Hashfunktionen verschlüsselt. Eine Hashfunktion ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet. Eine direkte Berechnung des Passworts aus dem Hashwert ist praktisch nicht möglich.



2 Faktor-Authentifikation

Aus Gründen von Zeit und Infrastruktur, wird dieses Thema innerhaln dieses Modul nicht thematisiert.
