B.8. Sichere Passwortverwaltung

Dimcho Georgiev

Überblick

- Hash-Algorithmen
- Passwortentropie
- Hash-Table vs Rainbow-Table
- PBKDF2
- Live Demo

Hash-Algorithmen

- Was passiert wenn der Input mehr/weniger Symbolen enthält als dem fest definierten Hashwert Output?
- Verschiedene Hash-Algorithmen:
  - SHA256 – 64 Rounds, 8 Segments (32 bits each), 64 Constants
  - SHA512 – 80 Rounds
  - MD5 – 128-bit hash value, 4 Rounds, collision found
- Ist es erkennbar, wenn mehrere Benutzer(-innen) das gleiche Passwort haben?
- Kollisionen – je kürzer der Hash, desto höher die Wahrscheinlich
- Salt
- Pepper

Passwortentropie

- Maß für die Schwierigkeit
- Simple guesses (die meist 1000 verwendete Passwörter)
- Brute force (alle möglichen Kombinationen von Zeichen [mit Länge 8])
- Research (Adresse, Name von Haustier)
- R – Pool of unique characters
- L – Number of characters in your password

$$E = log_2(R^L)$$

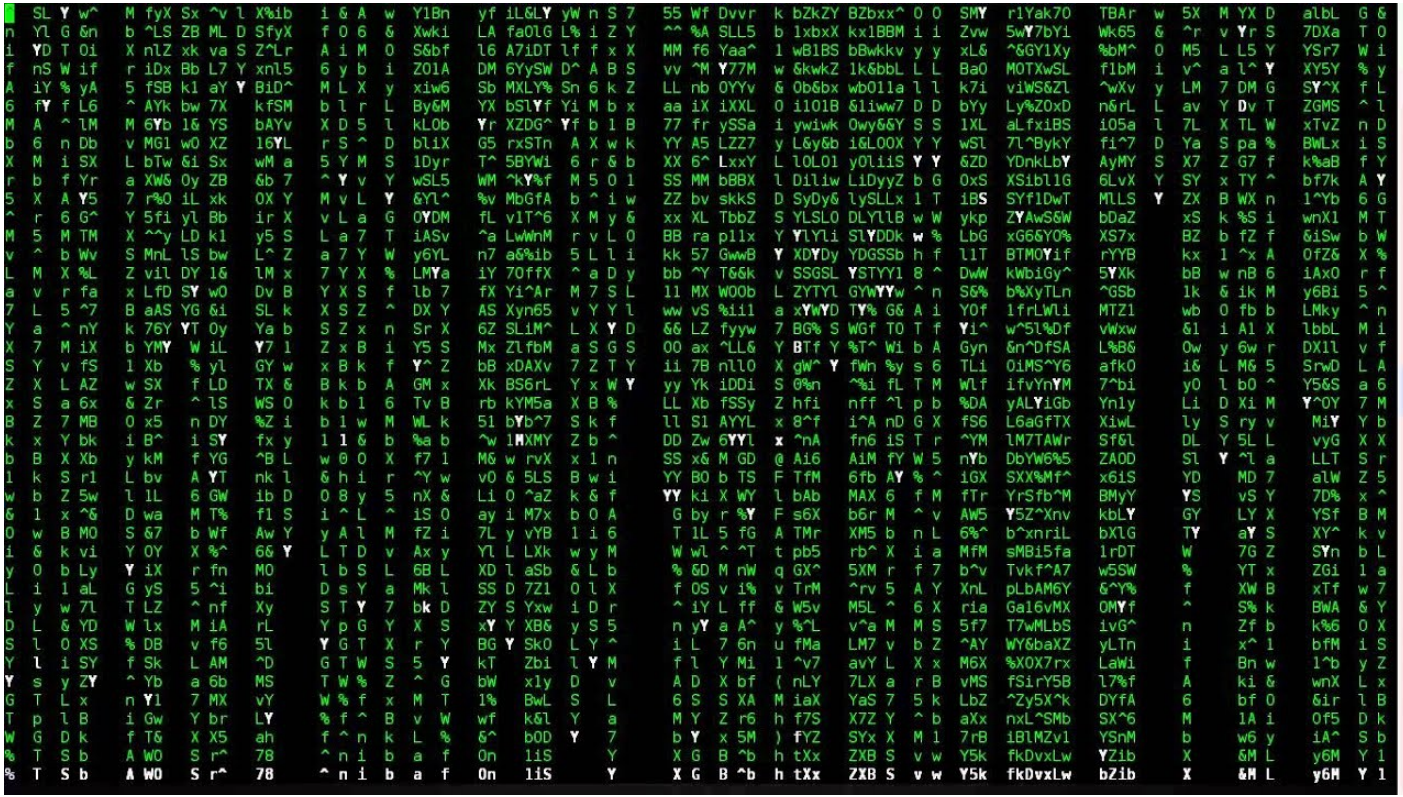
Hash-Table vs Rainbow-Table

- Rainbow-Tables fassen ähnliche Hashes zusammen, um Platz zu sparen, indem sie das Präfix nicht für jeden Hash speichern
  f2ca5152b0… and f2ca513a13... can be stored as f2ca51 -> 52b0… and 3a13...
- Beide werden zum Speichern der Ergebnisse eines Vorberechnungsangriffs verwendet
- Rainbow-Table ist langsamer zugreifbar, benötigt aber weniger Platz
- Hash-Table ist schneller zugreifbar, erfordert aber mehr Speicherplatz
- Bevor eine Rainbow-Table erstellt werden kann, wird zuerst eine Hash-Table erstellt
- Salt verhindert beide Angriffsmethoden gleichmäßig (absolute, wenn der Salz wert geheim ist)

PBKDF2

- Password-Based Key Derivation Function Version 2
- Salted password hash
- NIST - salt length of 128 bits.
- Slowness durch Wiederholung
- In 2000 the recommended number of iterations was 1 000,
- In 2021 the number of recommended iterations reached 310 000
- Computers become faster over time (Gordon Moore). Human brains do not

Live Demo



Quellen

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf - NIST
- https://security.stackexchange.com/questions/3959/recommended-of-iterations-when-using-pbkdf2-sha256/
  - PBKDF2
- https://i.ytimg.com/vi/u6_E2ggMchs/maxresdefault.jpg - Image
- https://specopssoft.com/wp-content/uploads/2021/05/Password-Entropy-of-Password-Policies-Formula.png
  - Image
- https://www.okta.com/identity-101/password-entropy/ - Entropy
- https://security.stackexchange.com/questions/92865/what-is-the-difference-between-a-hash-table-and-a-rainbow-table-and-how-are-the
  - Hash-Table vs Rainbow-Table