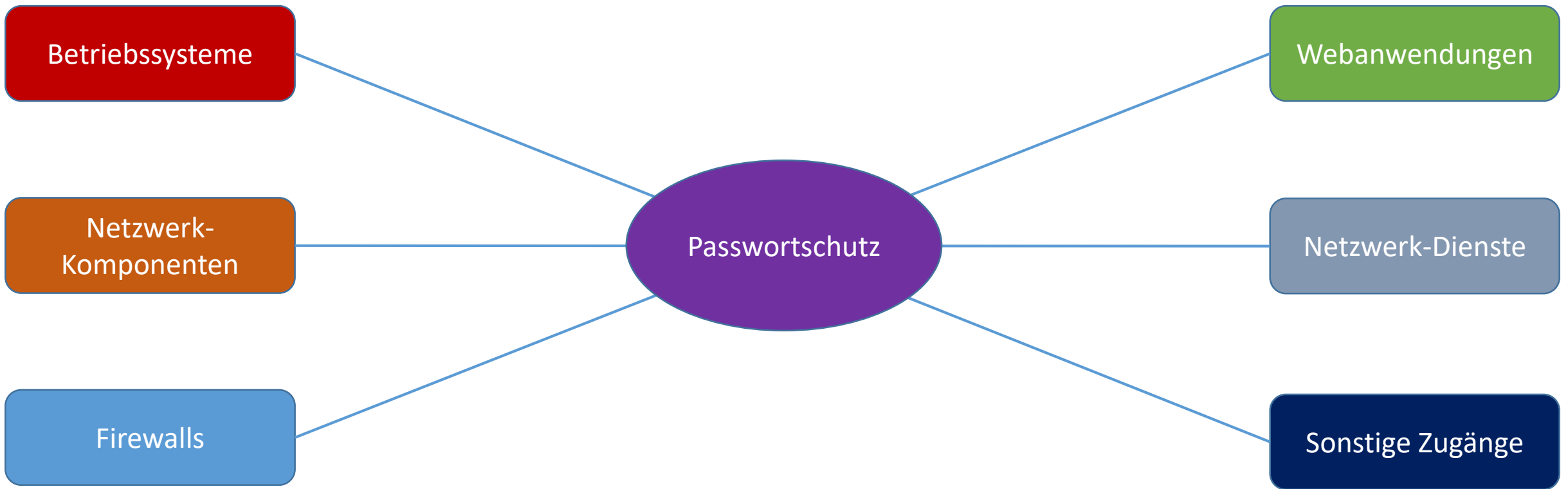


So werden Passwörter gespeichert

Passwörter sind der häufigste Zugangsschutz in Computernetzwerken und werden mit oder ohne Benutzernamen verwendet



Angriffsvektoren auf Passwörter

Wie kommen wir
an das Passwort heran?

Passwort am Login
eingeben (raten?)

Passwort-Datei
besorgen

Übermitteltes
Passwort abfangen

Abfangen und
Replay Attacke

Passwort

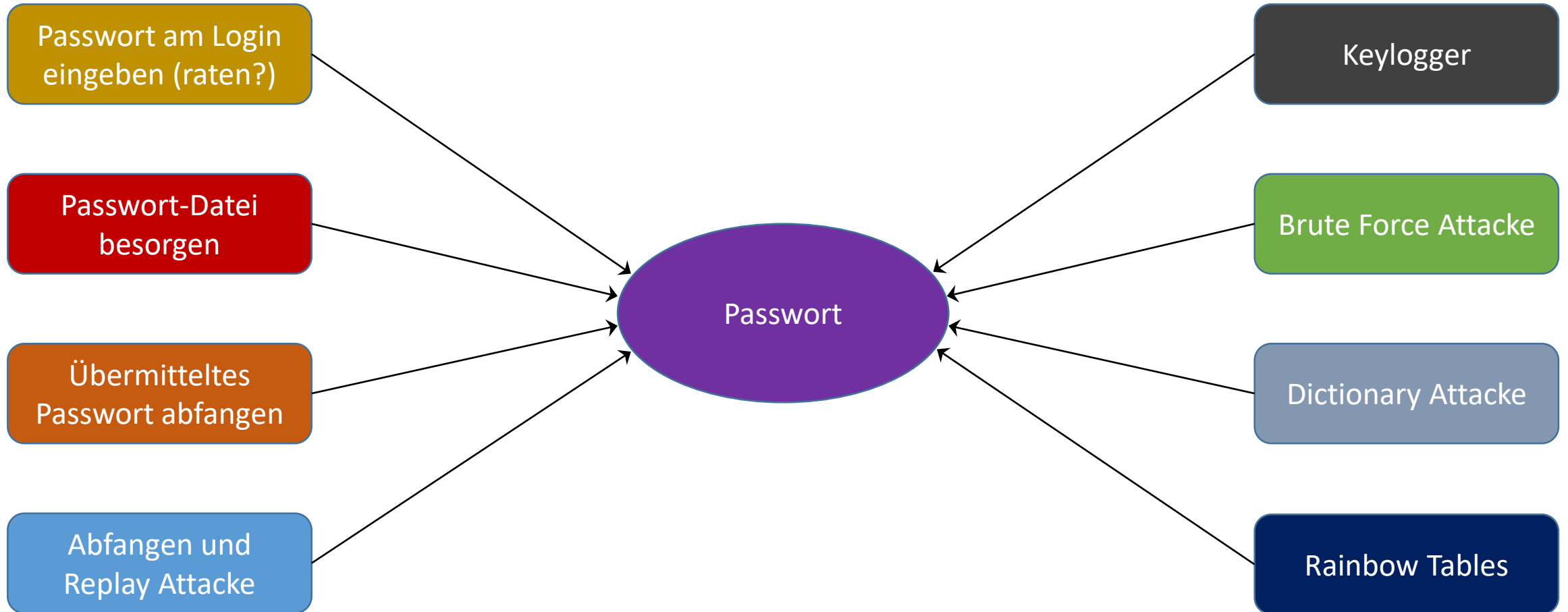
Wie finden wir das
Passwort heraus?

Keylogger

Brute Force Attacke

Dictionary Attacke

Rainbow Tables



Hashwerte

Passwörter werden aus Sicherheitsgründen meistens als **Hashwert** gespeichert

Hashfunktionen erstellen aus einem (beliebig) langen Ausgangswert eine immer gleichlange, eindeutige Zeichenkette

Dies ist ein beliebig langer Text, der durch die Hashfunktion verarbeitet wird, und bla bla bla [...]

Hash-Funktion

w8kU9w02rKWvc3pRaYeZZwe37

Krypto-Hashfunktionen:

- **MD5 (128 Bit)**
- SHA-1 (160 Bit)
- SHA-2:
 - SHA-224
 - SHA-256
 - SHA-384
 - **SHA-512**
- **SHA-3**

Passwort-Hashfunktionen:

- **LM-Hash**
- **PBKDF2**
- **Bcrypt**
- **Scrypt**

Der Salt – Salz in der Suppe

Salt ist eine zufällige Zeichenfolge, die der Eingabe für eine Hashfunktion hinzugefügt wird, um Brute-Force-Angriffe zu erschweren

