Klausurvorbereitung Schlegel

Single-Session vs. Multi-Session (Mehrbenutzersysteme)

Single-Session-Systeme
→ Nur **ein Benutzer gleichzeitig**

Typisch für:

- MS-DOS
- alte Handys
- z.b alte versionen bis Windows 3.1

Merkmale:

- kein paralleles Arbeiten
- keine Benutzertrennung
- kaum Rechteverwaltung

Multi-Session / Multiuser-Systeme
→ **Mehrere Benutzer gleichzeitig**

Typisch für:

- Server-Systeme
- Linux (immer Multiuser, abhängig von Ressourcen)

Historie:

- 1960 → erste Mehrbenutzersysteme
- 1982 → Commodore 64 (Single-User)
- ab 1990er → moderne Mehrbenutzersysteme

Vorteile:

- unterschiedliche Benutzerrechte
- eigener Home-Ordner pro Benutzer
- höhere Sicherheit (Admin vs. User)
- Kosteneinsparung (ein System für mehrere Nutzer)
- Gruppen mit unterschiedlichen Rechten möglich

Anmeldung (Login-Prozess)

1. Identifikation
→ Wer bist du?

- Benutzername (entscheidend)
- Anzeigename
- Token (möglich)

---

2. Authentisierung (Authentifizierung) (Systemseite)
→ Bist du wirklich diese Person?

- Eingabe von Nachweisen (Passwort, PIN, Biometrie, Token, Passkey, 2FA / MFA)
- Das System überprüft diese Angaben
- Passwort wird als Hash gespeichert
- Eingabe wird gehasht und mit dem gespeicherten Hash verglichen

---

3. Autorisierung
→ Was darfst du?

- Rechte und Berechtigungen werden geprüft
- Zugriff auf erlaubte Ressourcen wird gewährt

Hashwerte

- Nicht auf den Ausgangswert zurückführbar (Einwegfunktion)
- Kleine Änderung der Eingabe → völlig anderer Hashwert

Kollision:

- zwei verschiedene Eingaben → gleicher Hash
- Beispiel: MD5 war dafür bekannt und gilt als unsicher

Benutzer & Gruppen

Benutzer
→ Berechtigungsträger, der sich am System anmelden kann

- lokale Benutzerkonten
- zentrale Benutzerkonten, z. B. über Active Directory
- Benutzer können unterschiedliche Rechte besitzen

Gruppen
→ dienen nur zur Rechtevergabe

- mit Gruppen kann man sich nicht anmelden
- lokale Gruppen oder Domänengruppen
- vereinfachen die Rechteverwaltung

Benutzerrollen

- Administrator → volle Kontrolle zur Systemverwaltung
- Standardbenutzer → eingeschränkte Rechte
- Gast → kaum Rechte, heute selten sinnvoll
- System → mindestens Admin-Rechte, oft darüber hinaus

SID (Security Identifier)

- eindeutige interne Kennung eines Benutzers
- wird nur einmal vergeben
- bleibt auch nach Löschung eindeutig
- verhindert ungewollte Rechteübernahme nach Neuerstellung

Eigenschaften eines Benutzerkontos

- Benutzername / Anmeldename
- vollständiger Name / Anzeigename
- UPN: user @ domain.tld
- SID

PowerShell

Get-LocalUser -Name

Home-Verzeichnis

AppData → benutzerspezifische Daten
Programmdateien
ntuser.dat → versteckt, enthält benutzerspezifische Einstellungen

---

Merksätze

Benutzername = Anmeldename (wichtig für Verwaltung)
Gruppen = nur Rechtevergabe
Multiuser = mehr Sicherheit + Struktur

Revision #14
Created 15 April 2026 00:18:00 by Admin
Updated 19 May 2026 07:32:18 by Admin