Betriebsystem

- Klausurvorbereitung Schlegel
- Test Fragen zur Klausur
- Mein Abgleich der Klausurvorbereitung und PDF von herrn Schlegel

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

Test Fragen zur Klausur

Single-Session vs. Multi-Session – Test (40 Fragen)

1. Was ist ein Single-Session-System?

Ein System, bei dem nur ein Benutzer gleichzeitig arbeiten kann.

2. Nenne ein Beispiel für ein Single-Session-System.

MS-DOS oder Windows 3.1.

3. Was ist ein Multiuser-System?

Ein System, bei dem mehrere Benutzer gleichzeitig arbeiten können.

4. Wo werden Multiuser-Systeme typischerweise eingesetzt?

Auf Server-Systemen.

5. Ist Linux ein Multiuser-System?

Ja, Linux ist immer ein Multiuser-System.

6. Wann entstanden die ersten Mehrbenutzersysteme?

Um 1960.

7. Welches System war wieder ein Single-User-System (1982)?

Der Commodore 64.

8. Nenne einen Vorteil von Multiuser-Systemen.

Unterschiedliche Benutzerrechte möglich.

9. Warum sind Multiuser-Systeme sicherer?

Weil Rechte getrennt sind (Admin vs. Benutzer).

10. Was ist ein Home-Verzeichnis?

Der persönliche Speicherbereich eines Benutzers.

11. Was bedeutet Identifikation?

Der Benutzer gibt an, wer er ist (z. B. Benutzername).

12. Was ist Authentisierung?

Überprüfung, ob der Benutzer wirklich diese Person ist.

13. Nenne ein Beispiel für Authentisierung.

Passwort oder Fingerabdruck.

14. Was ist Autorisierung?

Festlegen, welche Rechte ein Benutzer im System hat.

15. In welcher Reihenfolge laufen die Schritte ab?

Identifikation → Authentisierung → Autorisierung.

16. Was ist ein Hashwert?

Ein verschlüsselter Wert, der aus Eingabedaten berechnet wird.

17. Kann man einen Hash zurückrechnen?

Nein, er ist nicht zurückrechenbar.

18. Was passiert bei kleiner Änderung der Eingabe?

Der Hashwert ändert sich komplett.

19. Was ist eine Kollision?

Zwei verschiedene Eingaben haben denselben Hash.

20. Welcher Hash-Algorithmus ist unsicher?

MD5.

21. Was ist ein Benutzer?

Ein Berechtigungsträger im System.

22. Was ist eine Gruppe?

Eine Sammlung von Benutzern zur Rechtevergabe.

23. Kann man sich mit einer Gruppe anmelden?

Nein.

24. Was ist ein Administrator?

Ein Benutzer mit vollen Systemrechten.

25. Was darf ein Standardbenutzer nicht?

Keine Systemverwaltung durchführen.

26. Was ist der Gast-Account?

Ein Benutzer mit sehr eingeschränkten Rechten.

27. Was ist das System-Konto?

Ein Konto mit sehr hohen Rechten (mehr als Admin).

28. Was ist eine SID?

Eine eindeutige interne Kennung eines Benutzers.

29. Warum ist die SID wichtig?

Sie identifiziert Benutzer eindeutig im System.

30. Wird eine SID wiederverwendet?

Nein, sie ist einmalig.

31. Was ist ein UPN?

User Principal Name (z. B. user @ domain.tld).

32. Was ist der Unterschied zwischen Benutzername und Anzeigename?

Benutzername = Login, Anzeigename = sichtbarer Name.

33. Was macht der Befehl Get-LocalUser?

Zeigt lokale Benutzerkonten an.

34. Was befindet sich im Home-Verzeichnis?

Benutzerspezifische Daten und Einstellungen.

35. Was ist AppData?

Ein Ordner für benutzerspezifische Programmdaten.

36. Was ist ntuser.dat?

Eine versteckte Datei mit Benutzereinstellungen.

37. Warum spart Multiuser Kosten?

Mehrere Nutzer teilen sich ein System.

38. Warum sind Gruppen wichtig?

Sie vereinfachen die Rechteverwaltung.

39. Was bedeutet: Benutzername = Anmeldename?

Beide sind identisch und wichtig für die Verwaltung.

40. Was ist der Unterschied zwischen Authentisierung und Autorisierung?

Authentisierung prüft Identität, Autorisierung legt Rechte fest.

Mein Abgleich der Klausurvorbereitung und PDF von herrn Schlegel

Ergänzung zur Klausurvorbereitung – Benutzermanagement (wichtige Zusatzinfos aus Unterricht/PDF)

Single- vs. Multi-Session (Windows genauer verstehen)

- Windows kann Single-Session und Multi-Session
- Desktop = meist Single-Session
- Server / Enterprise = Multi-Session möglich
- Wichtig: Windows = Multiuser-fähig, aber Sessions sind getrennt

---

Warum Multiuser? (nicht nur „mehr Benutzer“)

- bessere Ressourcennutzung
- getrennte Benutzerbereiche
- Schutz vertraulicher Daten
- abgestufte Rechte
- Rechtevergabe über Gruppen

Login-Prozess (Begriffe sauber können!)

1. Identifikation = Benutzername
2. Authentisierung = Passwort / Nachweis
3. Autorisierung = Rechte werden zugewiesen

- Authentifikation = Überbegriff (Prüfung der Angaben)

Administrator (wichtige Details!)

- integrierter Administrator existiert, ist oft deaktiviert
- erster Benutzer bekommt automatisch Adminrechte
- Admin darf:
  - alles installieren
  - Benutzer verwalten
  - Rechte vergeben
  - System komplett kontrollieren

Standardbenutzer (konkret können!)

- darf Programme ausführen
- darf im eigenen Home schreiben
- darf andere Dateien nur lesen
- darf NICHT:
  - Programme installieren
  - Benutzer verwalten
  - System ändern

Gastkonto (Klausur-Falle!)

- standardmäßig deaktiviert
- oft ohne Passwort
- großes Sicherheitsrisiko → sollte deaktiviert bleiben

SYSTEM-Konto (SEHR WICHTIG!)

- internes Konto vom Betriebssystem
- nicht sichtbar im Benutzer-Manager
- hat Vollzugriff auf alles → wichtiger als Administrator!

Spezielle Systemkonten

- Netzwerkdienst → Netzwerkzugriffe
- Lokaler Dienst → eingeschränkte lokale Rechte
- DefaultAccount → systeminterne Prozesse
- WDAGUtilityAccount → Sicherheitsfunktionen

→ keine normalen Benutzer!

SID (Security Identifier)

- eindeutige interne ID eines Benutzers
- wird nur einmal vergeben
- bleibt einzigartig, auch nach Löschen → verhindert Rechteübernahme bei neuem Benutzer

---

Passwort-Speicherung (sehr wichtig!)

- Speicherort: C:\Windows\System32\config\SAM
- Passwörter werden nicht im Klartext gespeichert

Benutzerprofil

- wird beim ersten Login erstellt
- Pfad: %userprofile%
- enthält:
  - persönliche Ordner
  - AppData → Programmeinstellungen
  - NTUSER.DAT → Registry vom Benutzer

UAC (Benutzerkontensteuerung)

- seit Windows Vista
- auch Admin arbeitet eingeschränkt
- Änderungen müssen bestätigt werden → Schutz vor Schadsoftware

---

Wichtige Merksätze

- Windows = Multiuserfähig, aber Session-basiert
- SYSTEM > Administrator (wichtig!)
- Gruppen = nur Rechtevergabe
- Benutzername ≠ entscheidend → SID ist entscheidend
- UAC schützt vor ungewollten Änderungen