

# IT-Security Tutorübung 12

---

Dorian Zedler

21. Januar 2024

Technische Universität München

Aufgabe 1

Aufgabe 2

Aufgabe 3

- Grundbegriffe der Zugriffskontrolle
- Bell-LaPadula Modell
- Role Based Access Control (RBAC)

# Aufgabe 1

---

## Aufgabe 1a - Authentifizierung vs Autorisierung

- a) Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- **Authentifizierung:** Identität des Subjekts überprüfen
  - **Autorisierung:** Sicherstellen, dass das Subjekt die benötigten Rechte hat um die Aktion auszuführen

b) Erklären Sie die Begrifflichkeiten *Subjekt*, *Objekt*, *Zugriffsrecht* sowie *Attribut* im Kontext von Zugriffskontrolle.

- **Subjekt:** WER will den Zugriff durchführen? (z.B. Nutzer, Prozess, Service)
- **Objekt:** WORAUF will das Subjekt zugreifen? (z.B. Datei, Ordner, Datenbank)
- **Zugriffsrecht:** WIE wird auf das Objekt zugegriffen? (z.B. lesen, schreiben, ausführen)
- **Attribut:** WELCHE Bedingungen müssen erfüllt sein? (z.B. Zweck, Rolle, Uhrzeit)

- c) Was ist das Prinzip der *need-to-know* Rechtevergabe?
- Jedes Subjekt sollte nur genau die Rechte haben, die es für seine Aufgabe benötigt
  - Darüber hinaus sollte es keine weiteren Rechte haben

- d) Was ist das Prinzip der *complete mediation* Zugriffskontrolle?
- Jeder Zugriff auf jedes geschützte Objekt muss überprüft werden

- e) Was ist der Unterschied zwischen *Mandatory Access Control* und *Discretionary Access Control*?
- **Mandatory Access Control:** Zugriffsrechte werden von einer zentralen Stelle vergeben
  - **Discretionary Access Control:** Zugriffsrechte werden von den Eigentümern der Objekte vergeben

## Aufgabe 1f - Capabilities vs Access Control Lists

- f) *Capabilities* und *Access Control Lists* werden beide verwendet um Zugriffe auf Objekte zu gewähren oder abzulehnen. Worin unterscheiden diese sich?
- ACLs verwalten Zugriffsrechte pro **Objekt**
  - Capabilities verwalten Zugriffsrechte pro **Subjekt**

g) In der Vorlesung haben Sie die Konzepte Policy Decision Point (PDP) sowie Policy Enforcement Point (PEP) kennen gelernt. Erklären Sie jeweils beide Konzepte.

- **PDP:** Führt die Berechtigungskontrolle durch und stellt bei erfolgreicher Prüfung ein Ticket aus
- **PEP:** Führt die Zulässigkeitskontrolle auf Basis des Tickets durch und prüft die Gültigkeit des Tickets

- h) Inwiefern treten PDP und PEP in Aktion bei dem Öffnen und Lesen einer Datei unter Unix-basierten Dateisystemen?
- 1) `open` Syscall wird aufgerufen
  - 2) Betriebssystem prüft die Berechtigungen der Datei für den Nutzer (PDP)
  - 3) Falls der Zugriff erlaubt ist, stellt das BS einen Filedescriptor aus (Ticket)
  - 4) `read` Syscall wird aufgerufen
  - 5) Betriebssystem prüft die Gültigkeit des Filedescriptors (PEP)

## Aufgabe 2

---

- a) Nennen und beschreiben Sie die drei zentralen Regeln des Bell-LaPadula-Modells!
- **No-Read-Up:** Kein Lesen von Objekten mit höherer Sicherheitsklasse als Subjekt.
  - **No-Write-Down:** Kein Schreiben von Objekten mit niedriger Sicherheitsklasse als Subjekt.
  - **Strong-Tranquility-Regel:** Keine Änderung der Sicherheitsklassen von Subjekt oder Objekt zur Laufzeit.

- b) Welches Problem bezüglich der Zugriffsrechte tritt im Laufe der Zeit auf und wie lässt es sich lösen?
- Alle Objekte werden mit der Zeit immer vertraulicher eingestuft, wenn sie von Subjekten mit höherer Sicherheitsklasse verändert werden.
  - Lösung: vertrauliche Subjekte (z.B. Systemprozesse) umgehen die Sicherheitsregeln und stufen Objekte wieder herunter
  - Beispiel: Ein Pressebericht ist während der Entstehung als geheim klassifiziert, kann nach der Freigabe aber veröffentlicht werden

## Aufgabe 2c - Bell-LaPadula - Beispiel

- Im Krankenhaus gibt es: Pflegepersonal, Ärzte, Laboranten und Verwaltungspersonal
- Für Patienten gibt es: Stammdaten, Patientenakte, Krankengeschichte
- Die Verwaltung legt die Stammdaten an und aktualisiert sie
- Das Pflegepersonal kann die Patientenakte lesen und protokolliert Behandlungen darin
- Laboranten können die Stammdaten lesen und Ergebnisse an die Patientenakte anhängen, diese aber nicht lesen
- Ärzte können die Patientenakte lesen, die Diagnose wird vom Pflegepersonal eingetragen
- Ärzte können die Krankengeschichte lesen und nach der Behandlung die Patientenakte daran anhängen.

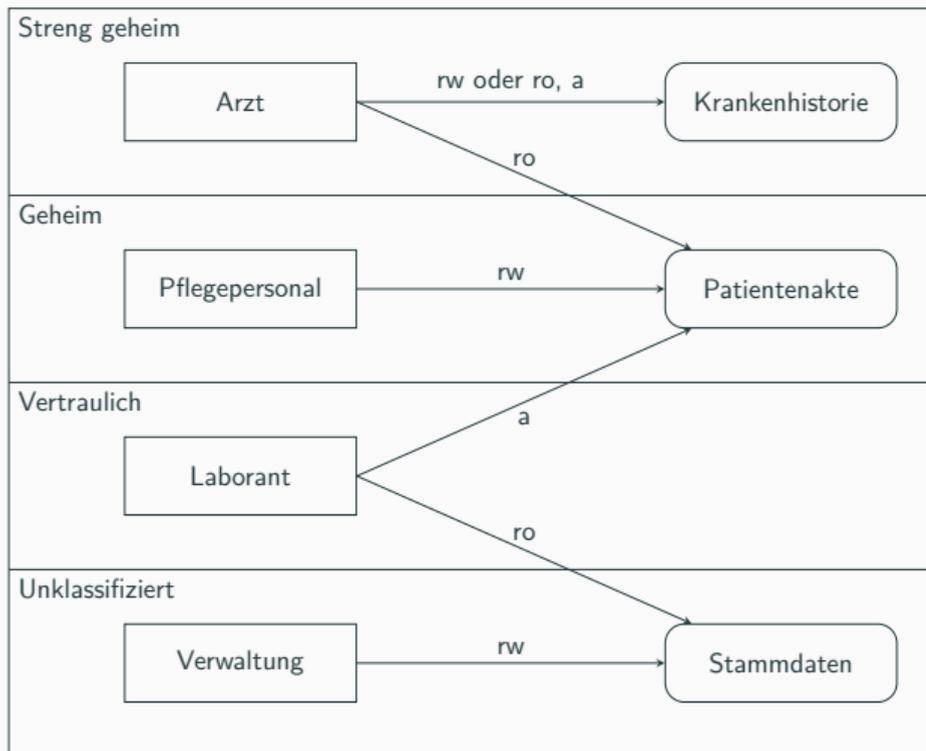
## Aufgabe 2c - Bell-LaPadula - Beispiel

- c) Modellieren Sie das Szenario als Zugriffsmatrix! Verwenden Sie dabei das Konzept der minimalen Rechte und weisen Sie jedem Subjekt nur die Berechtigungen (ro [read-only], rw [read-write], a [append]) zu, die es unbedingt benötigt.

	Stammdaten	Patientenakte	Krankenhistorie
Arzt		ro	rw oder ro, a
Pflegepersonal		rw	
Laborant	ro	a	
Verwaltung	rw		

## Aufgabe 2d - Bell-LaPadula - Beispiel

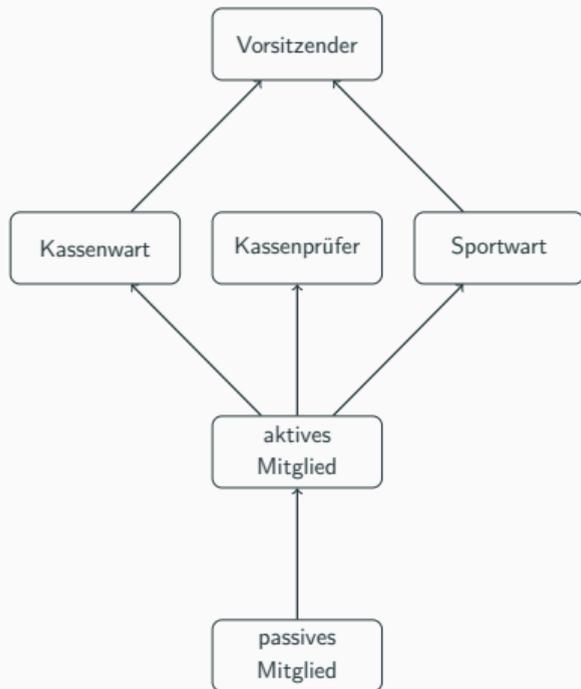
d) Modellieren Sie das Szenario im Bell-LaPadula-Modell!



## Aufgabe 3

---

# Aufgabe 3 - role based access control - Beispiel



$$pr : Role \rightarrow 2^{Permissions}$$

$\{\text{Recht Vereinsräume zu betreten}\} \subseteq pr(\text{Passives Mitglied})$

$\{\text{Wahlrecht bei Vorstandswahlen}\} \subseteq pr(\text{Aktives Mitglied})$

$\{\text{Recht Ausrüstung zu bestellen}\} \subseteq pr(\text{Sportwart})$

$\{\text{Recht Rechnungen zu bezahlen}\} \subseteq pr(\text{Kassenwart})$

$\{\text{Recht zur Kassenprüfung}\} \subseteq pr(\text{Kassenprüfer})$

$\{\text{Zugriff auf Mitgliederliste}\} \subseteq pr(\text{Vorsitzender})$

$$sr : Subject \rightarrow 2^{Role}$$

$sr(\text{Boris}) = \{\text{Vorsitzender}\}$

$sr(\text{Steffi}) = \{\text{Kassenwart, Sportwart}\}$

$sr(\text{Ivan}) = \{\text{Kassenprüfer}\}$

$sr(\text{John}) = \{\text{Passives Mitglied}\}$

- Man kann nicht gleichzeitig Kassenprüfer und Kassenwart sein
- Man kann nicht gleichzeitig die Rollen Sportwart und Kassenwart ausüben

- a) Darf Boris in der aktiven Rolle *Vorsitzender* 100 Euro für die Bezahlung einer Rechnung für Tennisbälle vom Vereinskonto entnehmen?
- Ja, da er die Rechte der Rolle *Kassenwart* erbt, darf er Geld vom Vereinskonto entnehmen.

- b) Darf Boris in seiner Rolle *Vorsitzender* eine Kassenprüfung durchführen?
- Nein, da er die Rechte nicht erbt und die Rolle *Kassenprüfer* nicht annehmen darf.
  - Statische Aufgabentrennung

- c) Darf Boris bei Vorstandswahlen sich selbst wählen?
- Ja, da er die Rechte des Aktiven Mitglieds erbt.

- d) Steffi hat in der Rolle als Sportwart Tennisbälle bestellt. Diese möchte sie gleich vom Vereinskonto aus bezahlen. Darf sie das? Wenn nein, was muss sie tun, um die Rechnung bezahlen zu können?
- Nein. Aufgrund des dynamischen Ausschlusses muss Steffi zuerst die aktive Rolle *Sportwart* aufgeben und in die Rolle *Kassenwart* wechseln.

## Aufgabe 3e - RBAC

e) Steffi gibt ihre Position als Kassenswart auf und John wird zum neuen Kassenswart gewählt. Geben Sie  $sr(\text{Steffi})$  und  $sr(\text{John})$  an.

- $sr(\text{Steffi}) = \{\text{Sportwart}\}$ ,  $sr(\text{John}) = \{\text{Kassenswart}\}$

- f) Was muss Steffi nun tun, um eine Bestellung Tennisbälle zu bezahlen?
- Steffi darf nun die Tennisbälle nicht mehr selbst bezahlen, da sie nicht mehr in die Rolle Kassenswart wechseln darf. Somit muss sie nun John (oder Boris) beauftragen dies zu erledigen.

- g) Welcher wesentliche Nachteil von RBAC-Hierarchien wird deutlich, wenn man z. B. die Rolle des Vorsitzenden betrachtet?
- Durch die Vererbung besitzt der Vorsitzende Rechte, die er eigentlich nicht benötigt. Somit ist das *Prinzip der minimalen Rechte* verletzt.

h) Nennen Sie grundsätzliche Vorteile von RBAC beim Einsatz mit oder ohne Hierarchien.

- Ohne Hierarchien:
  - Aufgabenorientiert, anwendungsspezifisch
  - Gute Skalierbarkeit
  - Mehrere gleichzeitig aktive Rollen möglich
- Mit Hierarchien:
  - Nachbilden von (Unternehmens-)Strukturen
  - Managementkomplexität verringern / einfacheres Rechtemanagement
  - Rechtevererbung über Rollenhierarchie