UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

# Übungsblatt 5

## Security Models

Abgabe bis 23. Mai 2023 um 12:00 Uhr im Moodle

*Cybersecurity* im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

### Einführung

Ihre Erläuterungen zur Zugriffstrennung in Betriebssystemen haben der Entwicklungsabteilung von ITS sehr geholfen: Mit Ihrer Unterstützung konnten sie eine effiziente technische Lösung implementieren, die sehr feingranulare Zugriffsrechte ermöglicht. Nun fehlt es nur noch an einem Konzept, wie diese Zugriffsrechte genau verteilt werden müssen. Das Konzept „jeder bekommt Administratorzugriff“ hat sich zwar bewährt, aber auch das Management sieht ein, dass das langfristig vermutlich suboptimal ist.

Nach langwierigen und ergebnislosen Beratungen findet ein Manager schließlich abends vorm Fernseher die Lösung: Man könne doch einfach „so ein hierarchisches Sicherheitsstufendings wie in diesen Agentenfilmen“ implementieren, um gewisse Ebenen in der Unternehmenshierarchie voneinander abzuschirmen.

### Aufgabe 1 Lattice-basierte Modelle (10 Punkte)

Das Management hat bereits einen Praktikanten damit beauftragt für jede Abteilung einen Beschäftigten in Leitungsfunktion zu befragen, und so die Datenflüsse zwischen diesen zu bestimmen. Dies ist das Ergebnis:

a) Anke fragt den Systemstatus der einzelnen Abteilungen ab und meldet den gesammelten Zustand der Firmensysteme dann an Monika.

b) Bob holt sich von Thorsten die aktuellen Abrechnungsdaten, um daraus Rechnungen für die jeweiligen Kunden zu erzeugen.

c) Bob versorgt Walter mit einer Liste von Kunden, die dieser dann besucht, um ihnen das innovative neue Abrechnungsverfahren schmackhaft zu machen.

d) Monika bittet Bob um eine Statistik aller Buchungen aus dem vergangenen Quartal, um daraus ihre Geschäftszahlen abzuleiten.

e) Niemand hat Lesezugriff auf Monikas Daten.

f) Thorsten beauftragt Erika mit der Entwicklung einer auf seine Abteilung zugeschnittenen Benutzeroberfläche zur Migration von Kunden auf das neue Abrechnungssystem, und testet diese anschließend mit ihr auf echten Kundendaten.

g) Walter meldet den Erfolg seiner Werbeaktion an Bob, der dann die Kundendatenbank aktualisiert. Dieselben Ergebnisse meldet er auch in Monika, in der Hoffnung, eine großzügige Provision dafür zu bekommen.

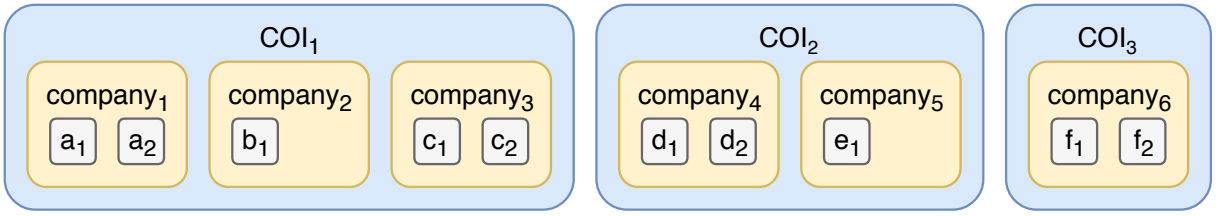
Während der Praktikant an dieser Liste arbeitete, hat das Management derweil ein bisschen im Internet nach “hierarchisches Sicherheitsstufendings” recherchiert und ist dabei auf den Namen Bell-LaPadula gestoßen. Das Modell scheint bestens auf die gestellten Anforderungen zu passen, sofern geeignete Sicherheitsstufen identifiziert werden können.

1. Leiten Sie aus den obigen Datenflüssen passende Sicherheitsstufen ab.
2. Ist Ihre Lösung eindeutig? Falls ja, begründen Sie Ihre Antwort, falls nein, geben Sie eine alternative Lösung an.
3. Um versehentlichem Datenverlust vorzubeugen, soll zusätzlich das Integrität-sichernde BiBa-Modell umgesetzt werden. Ist dies möglich? Wenn ja, wie? Begründen Sie Ihre Antwort.

## Aufgabe 2 Chinese-Wall-Modell (10 Punkte)

Da die von ITS betreuten Kunden oft in ähnlichen Branchen arbeiten und damit Konkurrenten sind, soll zusätzlich zu den Sicherheitsstufen eine geeignete horizontale Zugriffsbeschränkung eingeführt werden, sodass Techniker nicht "versehentlich" sensible Daten von konkurrierenden Kunden lesen und weitergeben können. Ein hierfür geeigneter Ansatz könnte das Chinese-Wall-Modell sein: Conflict-of-Interest-Klassen wären dann die Branchen der Kunden, Companies die jeweiligen Kunden, und Objekte deren Dateien.

1. Um dem Management das Modell zu erklären, zeichnen Sie folgendes Beispiel auf:




   Technikerin Tanja hat bereits auf die Objekte $c_1$ und $d_2$ zugegriffen. Auf welche Objekte darf sie nun noch zugreifen, auf welche nicht?

2. Erkennen Sie praktische Einschränkungen bei der Nutzung des Chinese-Wall-Modells in diesem Anwendungsszenario? Wenn ja, welche?

3. Da ITS (noch) eine große Anzahl von Kunden hat, soll die Bestimmung, ob ein Techniker Lesezugriff auf einen bestimmten Kundenserver bekommt, möglichst automatisch ablaufen. Hierfür ließ das Management einen Praktikanten bereits ein textbasiertes Dateiformat entwerfen, das als Eingabe für solch ein Programm genutzt werden kann. Die Eingabedateien sind folgendermaßen aufgebaut (es handelt sich bei allen Einträgen um `Integer`-Zahlen in Dezimaldarstellung):

   - COI-Anzahl $1 \leq$ `coiCount` $\leq 10^3$
   - Firmenanzahl $1 \leq$ `companyCount` $\leq 10^5$
   - `companyCount` viele Einträge $\texttt{coiId}_i$, die jeder Firma deren (nullbasierte) COI-ID zuordnen
   - Objektanzahl $1 \leq$ `objectCount` $\leq 10^6$
   - `objectCount` viele Einträge $\texttt{companyId}_i$, die jedem Objekt dessen (nullbasierte) Firmen-ID zuordnen
   - Subjektanzahl $1 \leq$ `subjectCount` $\leq 10^4$
   - Zugriffsanforderungs-Anzahl $1 \leq$ `objectAccessCount` $\leq 10^5$
   - `objectAccessCount` viele Paare $(\texttt{subjectId}_i, \texttt{objectId}_i)$, die jeweils eine Zugriffsanforderung eines Subjekts mit der gegebenen (nullbasierten) ID auf ein Objekt mit der gegebenen (nullbasierten) ID darstellen.

   Zum Testen des Dateiformats hat der Praktikant eine Klasse `InputFileParser` erstellt, die entsprechende Eingabedateien einlesen kann (Sie müssen dies also nicht selbst implementieren). Es ist nun eine Funktion zu ergänzen (siehe markierte Stellen in `ChineseWall.java`), die für jede Zugriffsanforderung überprüft, ob dem Techniker Lesezugriff gewährt oder verweigert wird.

   Testen Sie Ihre Implementierung mit den dem Moodle-Template beigelegten Eingabedateien, und laden Sie dann den Code in der vorgesehenen Aktivität im Moodle hoch. Evaluieren Sie anschließend das hochgeladene Programm erneut mit den dort konfigurierten Testfällen. Bitte verändern Sie nicht das vorgegebene Ausgabeformat des Programms.

   *Hinweise:*

   - Sie können zum lokalen Laden der Eingabe und Speichern der Ausgabe folgenden Linux-Befehl benutzen:

```
cat testcaseX.txt | java ChineseWall > testcaseX_out.txt
```

   - Die Lösungen für die ersten beiden Eingabedateien liegen dem Template bei, sodass Sie diese mit Ihrer Ausgabe abgleichen können.