

Übung 7

4. Dezember 2007

Aufgabe 1 Zugriffsmatrix

Auf der Hauptbrücke eines Raumschiffes gibt es verschiedene Konsolen für die Kontrolle der unterschiedlichen Schiffssysteme. Die verschiedenen Mannschaftsmitglieder haben unterschiedliche Rechte an den Konsolen. Nehmen Sie folgendes an:

- Mannschaftsmitglieder: Captain (C), First Officer (FO), Science Officer (SO), Tactical Officer (TO), Helm Officer¹ (HO), Ensign (E)
- Konsolen: Navigation Console (NC), Sensor Console (SC), Tactical Console (TC), Self-Destruction Console (DC)
- Rechte:
 - r: (Lese-)Zugriff auf Konsole
 - w: Programmierung der Konsole
 - x: Ausführen von Aktionen auf der Konsole
 - rw: Vollzugriff auf Konsole
 - rwx: Befehligen eines anderen Mannschaftsmitglieds
- C darf alles und auch alle anderen Mannschaftsmitglieder befehligen.
- FO darf alles und auch alle anderen Mannschaftsmitglieder außer C befehligen.
- SO hat Vollzugriff auf SC.
- TO hat Vollzugriff auf TC, r-Recht an SC und darf HO befehlen.
- HO hat Vollzugriff auf NC und r-Recht an SC.
- E nimmt von allen anderen Mannschaftsmitgliedern Befehle entgegen.

¹oft auch Conn Officer genannt

Bearbeiten Sie nun folgende Aufgaben:

1. Legen Sie mit Hilfe des Zugriffsmatrix-Modells die Zugriffsrechte der beteiligten Mannschaftsmitglieder zu den unterschiedlichen Objekten und Subjekten fest.
2. Bilden Sie die transitive Hülle von TO! Welche Folgen ergeben sich dadurch?
3. Welche Probleme treten bei diesem Modell auf wenn eine statische Zugriffsmatrix verwendet wird?
4. Ist eine dynamische Zugriffsmatrix für den oben beschriebenen Fall ausreichend? Wenn nicht, welches andere Sicherheitsmodell könnte besser geeignet sein? Begründen Sie ihre Antwort.

Aufgabe 2 Role-based Access Control (RBAC)

Wir betrachten weiterhin das Raumschiffszenario aus Aufgabe 1. Nehmen Sie an, dass es folgende Mannschaftsmitglieder gibt (in Klammern die Rolle in der sie meist aktiv sind): Jean-Luc (C), William (FO), Data (SO), Natasha (TO), Geordi (HO) und Wesley (E).

Im Gegensatz zu Aufgabe 1 nehmen wir vereinfacht an, dass es nur jeweils ein Nutzungsrecht (NR) für eine Konsole gibt. Weiterhin gibt es für die Nutzung der DC zwei Rechte, NR_DC_C und NR_DC_FO. Das Recht jemandem Befehle zu erteilen sei in dieser Aufgabe außen vor gelassen.

1. Geben Sie die Zusammenhänge des RBAC-Modells für dieses Szenario an, indem sie $RBAC = (S, O, \mathcal{RL}, \mathcal{P}, sr, pr, session)$ skizzieren.
2. Skizzieren Sie eine Rollenhierarchie, die das Raumschiffszenario beschreibt.
3. In bestimmten Notsituation kann das Raumschiff selbst zerstört werden. Hierzu gibt es eine Policy, dass nur der Captain gemeinsam mit dem ersten Offizier die Selbstzerstörung initiieren darf. Es müssen dazu die beiden Rechte NR_DC_C und NR_DC_FO zusammen eingesetzt werden. Modellieren Sie diesen Fall mittels geeigneter beschränkter Rollenmitgliedschaften. Es soll aber weiterhin möglich sein, dass William in die Rolle C wechseln kann, falls der Captain von einer anderen Rasse assimiliert wird.

Aufgabe 3 Hausübung: Bell LaPadula

1. Handelt es sich beim BLP Modell um *Mandatory Access Control*, *Discretionary Access Control* oder beides? Begründen Sie ihre Antwort.
2. Welche Sicherheitsklassifikation $sc(O)$ muss ein Objekt O haben, so dass ein Subjekt S mit einer Sicherheitsklasse $sc(S) = x$ sowohl lesend als auch schreibend darauf zugreifen kann?
3. Gegeben seien die Subjekte A mit $sc(A) = 2$ und B mit $sc(B) = 7$, die Objekte o mit $sc(o) = 1$ und p mit $sc(p) = 10$, sowie die Zugriffsmatrix M_t aus Tabelle 1.

	o	p
A	{ <i>read – only</i> }	{ <i>append</i> }
B	{ <i>append, read – write, read – only</i> }	{ <i>execute</i> }

Tabelle 1: Zugriffsmatrix M_t

Welche der folgenden Zugriffe sind erlaubt? Begründen Sie ihre Antwort!

- a) A liest das Objekt o
 - b) B möchte Daten an Objekt p anhängen
 - c) B führt p aus
 - d) B liest o
4. In der Zugriffsmatrix M_t ist festgelegt, dass A ausschließlich das *append*-Recht auf das Objekt p hat. Da die Sicherheitsklassifikation von p höher ist als die Sicherheitsklasse von A , kann A somit beliebige Daten anhängen.
 - a) Geben Sie ein Beispiel an, bei dem diese Berechtigung sinnvoll sein kann.
 - b) Welches Problem kann hierbei auftreten? Betrachten Sie hierbei insbesondere die Datenintegrität.

Plagiarismus Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Mit der Abgabe einer Lösung (Hausaufgabe, Programmierprojekt, Diplomarbeit, etc.) bestätigen Sie, dass Sie/Ihre Gruppe der alleinige Autor/die alleinigen Autoren des gesamten Materials sind. Falls Ihnen die Verwendung von Fremdmaterial gestattet war, so müssen Sie dessen Quellen deutlich zitiert haben. Weiterführende Informationen zu diesem Thema finden Sie unter <http://www.informatik.tu-darmstadt.de/Plagiarism>.