TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2020/21

6. Aufgabenblatt – Sicherheit

Geplante Bearbeitungszeit: eine Woche

Aufgabe 6.1 Erläutern Sie die für ein Schutzsystem wesentlichen Begriffe Schutzmatrix, Access Control List und Capability Liste. Betrachten Sie das System zunächst als statisch und geben Sie an wie Zugriffsrechte bei den drei genannten Ansätzen gespeichert werden. Diskutieren Sie Vor- und Nachteile.

Aufgabe 6.2 In einem weiterhin statisch betrachteten System gebe es zwei Nutzer A und B, eine Gruppe G, sowie eine Datei D. Nutzer können dabei Mitglied maximal einer Gruppe sein. Konstruieren Sie eine Rechtezuteilung einerseits mittels ACL, andererseits mittels Capabilities, die folgendes bewirkt:

- Mit Ausnahme der Nutzer A und B darf jeder die Datei D lesen und ausführen.
- Die Mitglieder der Gruppe G dürfen zusätzlich auch schreibend auf D zugreifen.
- Nutzer B darf die Datei nur lesen.
- Nutzer A hat keinerlei Zugriff auf D.

Sollten bei der Interpretation Ihrer Lösung bestimmte Voraussetzungen erforderlich sein, so beschreiben Sie diese.

Aufgabe 6.3 Nach der statischen Betrachtungsweise soll nun die dynamische Perspektive auf das System diskutiert werden, d. h. die Sicht zur Laufzeit und insbesondere die Möglichkeit Rechte weiterzugeben. Betrachten Sie dazu die Erstellung einer Datei durch Prozess A und erteilen Sie Prozess B Zugriff auf diese. Benutzen Sie zunächst ACLs und anschließend Capability-Listen. Diskutieren Sie auch die Vor- und Nachteile.

Aufgabe 6.4 Die folgenden Fragen und Aufgaben beziehen sich auf die „klassische“ Sicherheitsarchitektur von Unix.

(a) Welche Objekte, Subjekte und Operationen/Rechte spielen hier eine Rolle?

(b) Werden Zugriffssteuerlisten (ACL) oder Capability-Listen eingesetzt?

(c) Welche Attribute sind den beim Öffnen einer Datei beteiligten „Objekten“ (im allgemeinen Sinn) zugeordnet und wie wird die Entscheidung gefällt, ob eine Datei geöffnet werden darf?

(d) Formulieren Sie die in Aufgabe 2 geforderte Rechtezuteilung mittels des Unix-Rechtesystems. Welche Probleme treten dabei auf?

(e) Verdeutlichen Sie ein weiteres Problem, das mit dem Rechtesystem von Unix verbunden ist, anhand des Änderns eines Passworts in einem Unix-Betriebssystem. Die verschlüsselten Passwörter sind in einer Datei `passwd` gespeichert, die von jedem gelesen, aber nur mit Hilfe eines speziellen (gleichnamigen) Programms geschrieben werden kann. Die relevanten Spezifikationen für diese beiden Objekte lauten:

```
rw- r-- r-- root root /etc/passwd
rwx r-x r-x root root /usr/bin/passwd
```

Beschreiben Sie zunächst das Problem, das beim Ausführen des Programms auftritt, und anschließend die Lösung dieses Problems.

Klausuraufgabe I

In einem System existieren die fünf Benutzer *Alice*, *Bob*, *Carol*, *Dave* und *Oskar*. Alice und Bob möchten auf einfache Weise miteinander kommunizieren und nutzen für diesen Zweck eine Datei `postfach`. Möchte bspw. Alice eine Nachricht für Bob hinterlassen, legt sie diese in der Datei ab. Zu einem späteren Zeitpunkt liest Bob die Nachricht und löscht sie bzw. ersetzt sie durch seine Antwort. Um ihre Kommunikation vertraulich zu halten soll die Datei `postfach` dabei *ausschließlich* für Alice und Bob zugreifbar sein.

a) Geben Sie für die Datei `postfach` eine geeignete Rechtezuweisung mittels Zugriffssteuerlisten (ACL) an.

b) Geben Sie eine mögliche Rechtezuweisung für `postfach` im Rahmen des klassischen Unix-Rechtemodells an. Welche zusätzlichen Voraussetzungen sind dabei erforderlich?

c) Die Datei `postfach` wurde in einem Verzeichnis `public_dir` angelegt, das folgende Rechtezuweisung besitzt

```
rwx rwx rwx   root   root   public_dir
```

Wie könnte *Oskar* diese Situation ausnutzen, um die Kommunikation zwischen *Alice* und *Bob* in Zukunft mitzulesen?

Hinweis: Wir gehen davon aus, dass *Alice* und *Bob* arglos sind und nicht mit einem Angriff rechnen.

Ein zentraler Systemdienst hat aufgrund eines Programmierfehlers eine Datei *system.d* mit den folgenden Unix-Rechten angelegt

```
rws rws rwx   root   root   system.d
```

d) Erläutern Sie, warum dies ein Sicherheitsproblem darstellt.

Klausuraufgabe II

Gegeben sei ein fiktives System des Herstellers *Herkules*. Neben dem Besitzer des Systems, *Bernd*, gibt es einen weiteren Anwender *Hans*. Sowohl *Bernd* als auch *Hans* gehören zur Gruppe *Users*.

a) *Bernd* lädt von der Internetseite des Herstellers die Programmerweiterung *Zeus* herunter. Er möchte sicherstellen, dass die Erweiterung tatsächlich von der Firma *Herkules* stammt und nicht von Dritten manipuliert worden ist. Nennen Sie ein dafür geeignetes Verfahren oder erläutern Sie kurz warum dieses Problem prinzipiell nicht lösbar ist!

b) Geben Sie eine Rechtezuweisung im Rahmen des klassischen Unix-Rechtesystems an, die allen Benutzern *ausschließlich die Ausführung* des Programms `zeus` erlaubt!
Nutzen Sie dafür die Notation `<Rechte-Bits> <Besitzer> <Gruppe>`.

c) Um das Prinzip der geringst-möglichen Privilegisierung umzusetzen, gibt es einen Benutzer *dialout* welcher keiner Gruppe zugehört. Nur der Benutzer *dialout* darf auf das Modem zugreifen, beispielsweise um es durch die Eingabe der PIN freizuschalten. Für das Übergeben der PIN ans Modem gibt es ein Programm `enterpin`. Nur Mitglieder der Gruppe *Users* sollen damit die PIN eingeben dürfen.
Setzen Sie die nötigen Unix-Zugriffsrechte für `enterpin`, so dass *Bernd* die PIN auf seinem System eingeben kann!

d) Geben Sie eine Umsetzung der in b) beschriebenen Rechtezuweisung mittels Capability-Listen an und nennen Sie einen Nachteil von Capability-Listen gegenüber dem klassischen Unix-Rechtesystem!