TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2024/25

9. Aufgabenblatt – Systemsicherheit

Besprechungszeitraum: 07.01.2025 – 10.01.2025

Aufgabe 9.1 In einem als statisch betrachteten System gebe es zwei Subjekte A und B, sowie ein Objekt D. Folgendes ist gegeben:

- Mit Ausnahme von A und B darf jeder D lesen und schreiben.
- B darf D nur lesen.
- A hat keinerlei Zugriff auf D.

(a) Konstruieren Sie für das oben genannte Beispiel eine Rechtezuteilung einerseits mittels einer Access Control List (ACL), andererseits mittels Capabilities. Sollten bei der Interpretation Ihrer Lösung bestimmte Voraussetzungen erforderlich sein, so beschreiben Sie diese.

(b) Diskutieren Sie die jeweiligen Vor- und Nachteile von ACLs und Capabilities.

Aufgabe 9.2 Die folgenden Fragen und Aufgaben beziehen sich auf die „klassische“ Sicherheitsarchitektur von UNIX.

(a) Welche Informationen werden beim Öffnen einer Datei durch das Betriebssystem überprüft? Was sind gemäß der Vorlesung die beteiligten „Subjekte“ und „Objekte“? Wie ist der Ablauf im Betriebssystem, der entscheidet, ob eine Datei geöffnet werden darf oder nicht?

(b) Formulieren Sie eine Rechtezuteilung mittels des Unix-Rechtesystems für folgende Situation:

- Nutzer A darf die Datei D nur lesen.
- Die Mitglieder der Gruppe G dürfen die Datei D lesen, schreiben und ausführen.
- Alle anderen Nutzer im System dürfen die Datei nur lesen und ausführen.

(c) Welche Probleme treten auf, wenn man das Beispiel der letzten Teilaufgabe um folgende Bedingung erweitert?

- Nutzer B darf die Datei D weder lesen, schreiben noch ausführen.

(d) 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!