

Vorlesung Betriebssysteme 1

Aufgabenblatt 5 zu Unit OS7

(Besprechung im Übungstermin gemäß Ankündigung auf der Vorlesungs-Website)

Die Aufgaben auf diesem und den folgenden Übungsblättern sollen Ihnen helfen, Ihr Selbststudium zu strukturieren und Ihnen ein Gefühl dafür geben, welchen Wissensstand Sie bisher in der Veranstaltung erlangt haben sollten. Um die gemeinsame Zeit mit den Tutoren optimal nutzen zu können, sollten Sie versuchen, bis zum jeweiligen Tutorengespräch möglichst viele der Aufgaben zu bearbeiten.

Die Bearbeitung sollte in einer Art und Weise erfolgen, dass a) Sie und Ihre Gruppe gut mit den Ergebnissen arbeiten können und b) sich im Gespräch mit den Tutoren über den Stoff der Aufgaben austauschen können. Es bestehen keine weiteren formalen Anforderungen an die Aufgabebearbeitung unsererseits.

1. Ein Dateiserver habe die Benutzer *alice*, *bob*, *eve* und *nobody*. Es gibt die Ordner `/home/alice`, `/home/bob`, `/tmp`, `/bin`, `/etc` und `/secret`. Die Gruppe `users` beinhaltet alle genannten Personen. Die Gruppe `programmers` enthält *alice*, *bob* und *eve*.
 - (a) Beschreiben Sie kurz den Aufbau einer *Access Control List* (ACL). Wie entscheidet Windows zur Laufzeit für den Zugriff eines Nutzers auf ein Objekt anhand der ACL des Objekts, ob der Zugriff gewährt wird oder nicht? Inwiefern ist die Reihenfolge der *Access Control Entries* (ACE) für die Evaluation der Zugriffsrechte in einer ACL relevant?
 - (b) Geben Sie für die Verzeichnisse `/home/alice` und `/home/bob` ACLs an, die *alice* und *bob* Lesezugriff auf sowohl `/home/alice` als auch `/home/bob` erlauben, aber das Schreiben auf `/home/alice` nur *alice* und auf `/home/bob` nur *bob* erlauben. Achten Sie darauf, dass keine anderen als die beschriebenen Rechte gewährt werden.
 - (c) Geben Sie eine ACL an, die jedem Nutzer das Lesen von `/etc` erlaubt, aber nur den Personen in der Gruppe `programmers` das Recht gibt, schreibend zuzugreifen.

- (d) Geben Sie eine ACL für das Verzeichnis `/bin` an, die jedem Nutzer erlaubt, die Programme in `/bin` auszuführen, aber nur Mitgliedern der Gruppe `programmers` erlaubt, die Programm-Dateien zu lesen, und nur `eve` erlaubt, die Programm-Dateien in `/bin` zu schreiben.
- (e) Betrachten Sie die folgende ACL für das Verzeichnis `/secret`:

$$\Rightarrow \left| \begin{array}{c} \text{DENY} \\ \text{eve} \\ \text{READ} \end{array} \right| \Rightarrow \left| \begin{array}{c} \text{ALLOW} \\ \text{programers} \\ \text{READ} \end{array} \right| \Rightarrow \left| \begin{array}{c} \text{ALLOW} \\ \text{users} \\ \text{WRITE} \end{array} \right|$$

Welche der folgenden Zugriffe werden erlaubt? Beschreiben Sie den Ablauf bei der Evaluation der ACL.

- Der User `nobody` greift schreibend auf `/secret` zu.
 - Die User `alice` und `Eve` greifen lesend auf `/secret` zu.
2. Unix unterstützt – als Alternative zu den in Windows üblichen ACLs – *RWX-Bits* (**R**ead/**W**rite/**E**xecute) zur Formulierung von Zugriffsrechten für Nutzer und Gruppen auf Dateisystemobjekte.
- (a) Beschreiben Sie den Aufbau einer typischen RWX-Bit Konfiguration für eine Datei bzw. ein Verzeichnis.
- (b) Formulieren Sie die Berechtigungen für die Teilaufgaben 1.b, 1.c und 1.d in RWX-Bits anstatt in ACLs. Erstellen Sie, falls nötig, weitere Gruppen. Achten Sie darauf, dass keine weiteren als die beschriebenen Zugriffsrechte durch Ihre RWX-Bits gewährt werden. Geben Sie die jeweiligen RWX-Bits sowohl in logischer (`rxr-xr-x`), als auch in oktaler (`0755`) Schreibweise an.

3. Lesen Sie Ken Thompson's Turing-Award-Dankesrede:

"Reflections on Trusting Trust"

(https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf).

Beschreiben Sie, aus welchem Grund Quelltextanalysen nicht ausreichend sich erstellen, dass in einem Programm kein Schadcode enthalten ist.

4. Windows hat als ein Designziel die Sicherheits-Anforderung formuliert, dass Prozesse voneinander isoliert werden, sodass der Zustand des Speichers vor fremden Lesezugriffen geschützt ist, und die Ressourcen der Prozesse privat sind. Diskutieren Sie, welche der in der Vorlesung besprochenen Konzepte der *Prozessorverwaltung* und *Speicherverwaltung* eingesetzt werden, um dieses Ziel zu erreichen.