UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Übungsblatt 3

Access Control and Operating System Security

Abgabe bis 09. Mai 2023 um 12:00 Uhr im Moodle

Cybersecurity im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

Einführung

Die erste Hürde ist geschafft! Die Entwicklungsabteilung von *Immature Technical Solutions* hat beschlossen, dass die von Ihnen geäußerten Sicherheitsbedenken *out of scope* sind, da sie nicht im offiziellen Angriffsmodell „Angreifer von außerhalb des Netzwerks“ enthalten sind, und man den firmeneigenen Angestellten bedingungslos vertrauen kann. Die Einwände eines Praktikanten, dass das wohl eher nach einer Komfortentscheidung klänge, um keinen komplexen Code schreiben zu müssen, und dass es durchaus schon Fälle von internen Angriffen gegeben hätte, wurden wohlwollend zur Kenntnis genommen und eben jener Praktikant wegen offensichtlicher Nicht-Vertrauenswürdigkeit fristlos entlassen. Anschließend wurde das Authentifizierungsprotokoll samt Hashfunktion gemäß ursprünglichem Vorschlag in Rekordzeit implementiert und in der gesamten Firma installiert. Der Unternehmensvorstand war begeistert und ließ die PR-Abteilung sogleich eine entsprechende Erfolgsnachricht an die Aktionäre versenden.

Kurze Zeit später fällt einer Managerin während des Mittagessens auf, dass die Techniker am Nachbartisch erstaunlich gut über die aktuellen Geschäftszahlen informiert sind, die sie eigentlich gar nichts angehen. Daraufhin stellt sie die Chefin der Entwicklungsabteilung zur Rede, die darüber gar nicht verwundert ist, da das neue System gemäß Spezifikation des Vorstands lediglich Mitarbeiter authentifizieren, aber keine Zugriffsrechte überprüfen soll.

Im weiteren Dialog kommt heraus, dass es um die Zugriffstrennung sogar noch schlimmer bestellt ist als gedacht: Da es in der Vergangenheit immer mal wieder merkwürdige Fehlermeldungen der Sorte „Zugriff verweigert“ gab, wurde von irgendjemand wichtigem einst beschlossen, einfach jeden Angestellten mit einem Administratoraccount arbeiten zu lassen, was alle derartigen Probleme auf einen Schlag löste.

Da es also offenbar auch an Erfahrung mit Technologien zur Zugriffstrennung fehlt, bittet das Management Sie, zuerst die Entwicklungsabteilung im Bereich Betriebssystemsicherheit zu schulen, bevor im nächsten Schritt ein wirksames System auf Basis eines guten Sicherheitsmodells implementiert werden kann.

Aufgabe 1 Begriffe (4 Punkte)

Zuallererst benötigt die Entwicklungsabteilung Hilfe bei der Zuordnung von Firmenressourcen auf entsprechende Begriffe aus dem Bereich der Zugriffskontrolle.

1. Welche der folgenden Entitäten sind Subjekte und/oder Objekte im Sinne eines Betriebssystems?
   a) Mitglied des Firmenvorstands
   b) Drucker im Sekretariat
   c) Datenbank für Kundendaten
   d) Kundendatei auf dem Server
   e) Kundenprozess auf dem Server
   f) Nutzergruppe `praktikanten`

g) Mailkonto des Hausmeisters

2. Ein Betriebssystem arbeitet mit sogenannter *Domain Separation*, d.h. einer Aufteilung der Zugriffsebenen in Ring 0 (*kernel mode*) bis Ring 3 (*user mode*). Ordnen Sie die folgenden Programme der entsprechenden Zugriffsebene zu.

   a) Email-Client

   b) Linux-Kernelmodul

   c) Bootloader

   d) Gerätetreiber

   e) Kundenprogramme

   f) Linux-Kernel

Aufgabe 2 Access Control Data (7 Punkte)

Im Anschluss bittet die Entwicklungsabteilung Sie um eine Erklärung zur Vergabe von Zugriffsrechten.

Hierzu erstellen Sie für eine kleine Anzahl von Beschäftigten eine Access Control Matrix:

Gruppe	print	db1	db2	calendar	config
Thorsten	x	rw			
Tina	x	rw	a		r
Anke	rwx	rw	rw	rw	rw
Rolf	x			rw	
Monika	x	r	rw	rw	r
Markus	x	rw	rw	rw	

Alle Angestellten von ITS sind in der Gruppe `mitarbeiter`. Die Techniker Thorsten und Tina sind zusätzlich in der Gruppe `techniker`, die Manager Monika und Markus in der Gruppe `manager`. Administratorin Anke und Rezeptionist Rolf sind ausschließlich in der Gruppe `mitarbeiter`.

Es gibt die folgenden Objekte:

- `print`: Ein Programm zum Senden von Druckaufträgen. Alle Mitarbeiter dürfen dieses Programm benutzen.
- `db1`: Eine Datenbank mit Kunden- und Zugangsdaten, die von den Technikern verwaltet wird.
- `db2`: Eine Datenbank mit Geschäftszahlen und Statistiken, die vom Management verwaltet wird. Technikerin Tina lädt dort regelmäßig aktuelle Abrechnungsdaten hoch, kann die Datenbank aber sonst nicht einsehen.
- `calendar`: Ein Terminkalender für die einzelnen Manager. Rezeptionist Rolf pflegt dort regelmäßig Termine ein.
- `config`: Systemkonfiguration.

1. Überführen Sie die Matrix in eine *minimale* Access Control List.

   „Minimal“ heißt hier, dass möglichst viele Rechte bei den jeweiligen Gruppen liegen und vererbt werden; explizite Rechte für Benutzer werden nur für die Ausnahmefälle angegeben.

2. Was sind die Vorteile einer Access Control Matrix gegenüber einer Access Control List, was sind die Nachteile?

3. Erklären Sie kurz, worum es sich bei Role-based Access Control handelt. Lässt sich dieses Modell auch auf das obige Beispiel anwenden? Begründen Sie Ihre Antwort.

Aufgabe 3 Zugriffsrechte (9 Punkte) *[optional bei bestandenem Praktikum]*

Diese Aufgabe muss nicht bearbeitet werden, wenn Sie stattdessen das "Dateirechte"-Praktikum bestehen. Bitte geben Sie Ihren Gruppennamen aus dem Praktikum an, um die Korrektur zu erleichtern.

Zum Schluss sollen Sie einmal exemplarisch Zugriffsrechte für drei einfache Accounts konfigurieren.

Die Accounts heißen `monika`, `rolf` und `tina`, mit den folgenden Gruppenzugehörigkeiten:

- `monika`: `monika`, `verwaltung`
- `rolf`: `rolf`, `verwaltung`
- `tina`: `tina`

Monika möchte in ihrem Homeverzeichnis nun einige Dateien und Ordner erstellen, auf die verschiedene Benutzer und Gruppen Zugriff haben sollen. Die Rechte für Monikas Homeverzeichnis sind wie folgt:

```
drwxr-xr-x monika monika 70 Jul 16 11:34 monika/
```

Geben Sie jeweils die Zugriffsrechte (im Linux-Format) und den Besitzer an.

1. Auf den Ordner `termine` soll ausschließlich Monika Zugriff haben (lesen und schreiben), die anderen Benutzer sollen diesen weder öffnen noch lesen können.
2. Auf den Ordner `veranstaltungen` soll Monika Lese- und Schreibzugriff haben, Rolf nur Lesezugriff. Tina soll den Ordner weder öffnen noch lesen können.
3. Das Programm `share_calendar` soll es (ausschließlich) Mitgliedern der Gruppe `verwaltung` erlauben, den Inhalt des Ordners `termine` aufzulisten.

Aufgabe 4 Wechsel zwischen Kernel- und Userspace (6 Punkte)

Zuletzt tritt Managerin Monika an Sie heran: Bei einem Austausch mit den Technikern bekam sie die Idee, ein neues Abrechnungssystem zu etablieren, bei dem den Kunden jeder Wechsel zwischen Kernel- und Userspace in Rechnung gestellt wird, sofern dieser durch das Kundenprogramm ausgelöst wurde. Während die Konkurrenz noch solch altmodische Metriken wie Speicherverbrauch und Rechenzeit als Grundlage für ihre Abrechnung einsetzt, verspricht dieser Ansatz erhebliche finanzielle Ressourcen zu erschließen, vor allem da die Hauptkunden von ITS sehr gern Dateien lesen und schreiben. Monika bittet Sie nun um eine Einschätzung, ob und wie sich das ganze umsetzen ließe.

1. Betrachten Sie den angegebenen Quelltext. In welchen Zeilen/zwischen welchen Zeilen wird ein Übergang zwischen Kernel- und Userspace (oder umgekehrt) stattfinden, und warum?

```
1  import java.util.concurrent.TimeUnit;
2  import java.util.Scanner;
3  import java.io.File;
4
5  class context_switch
6  {
7      public static void main(String args[]) throws InterruptedException
8      {
9          TimeUnit.SECONDS.sleep(1);
10
11         int sum = 0;
12         int counter;
13         for(counter = 0; counter < 10; ++counter)
14             sum += counter;
15
16         System.out.println("Enter array size: ");
17         Scanner sc = new Scanner(System.in);
18         int size = sc.nextInt();
19
20         int array[] = new int[size];
21
22         ++counter;
```

```
23          array[0] = counter;
24
25          File f = new File("file.txt");
26          if(f.exists())
27              sum = sum / 10;
28      }
29  }
```

2. Ist diese Art der Abrechnung technisch praktikabel? Begründen Sie Ihre Antwort.