GSS Abgabe 03

Carolin Konietzny, Paul Bienkowski, Julian Tobergte, Oliver Sengpiel

13. Mai 2015

1.1 Rechnersicherheit: Zugangs- und Zugriffskontrollen

a) Eine Zugangskontrolle

- regelt, ob überhaupt eine Kommunikation zwischen System und User stattfindet.
- findet statt, bevor überhaupt Dienste in anspruch genommen werden können

Eine Zugriffskontrolle

- regelt, welche Dienste des Systems von dem User benutzt werden können
- setzt voraus, dass der User eine Zugangsberechtigung für das System hat
- kann Rechte für einzelne Operationen auf Objekten verwalten

b) Ja, es kann sinnvoll sein, wenn mit dem Zugangsrecht alle Zugriffe verbunden sind. Beispiel: [TODO]

c)

d) Nein, dies widerspricht nicht der Vorherigen Teilaufgabe, da der Besitz des Links an sich bereits eine Zugangskontrolle ist. Wer den Link kennt, ist zugangsberechtigt. Der „geheime" Teil des Links, der zugleich Identifikation für den Ordner ist, ist schwer zu erraten und gilt als „Zugangsdaten".

2 Timing-Attack

1.
```
public class Timer {
    public static boolean passwordCompare(String a, String b) {
        int i;

        if (a.length() != b.length()) return false;

        for (i = 0; i < a.length() && a.charAt(i) == b.charAt(i); i++);

        return i == a.length();
    }

    public static void main(String[] args) {
        long start, end;

        start = System.nanoTime();
        passwordCompare("abcdefghijklmnopqrstuv", "abcdefghijklmnopqrstuv");
        end = System.nanoTime();
        System.out.println("Gleiche Wörter: " + (end - start) + " ns");
```

```
        start = System.nanoTime();
        passwordCompare("abcdefghijklmnopqrstuv", "vabcdefghijklmnopqrstu");
        end = System.nanoTime();
        System.out.println("Unterschiedliche Wörter: " + (end - start) + " ns");
    }
}
```

Die Ausgabe des Programmes ist wie folgt:

```
$ java -Djava.compiler=None Timer
Gleiche Wörter: 11426 ns
Unterschiedliche Wörter: 2308 ns
```

Der signifikante Unterschied (bei gleicher Länge) ergibt sich daraus, dass bereits der erste Buchstabe vom korrekten Passwort abweicht.

3. Zuerst wird die Länge des Passwortes ermittelt. Da die Funktion frühzeitig abbricht, sind Eingaben mit falscher Länge immer früher fertig. Daher werden zuerst Passwörter „a", „aa", „aaa", ... ausprobiert, bis eines deutlich länger braucht.

   Dann werden „von vorne" Buchstaben erraten. Die for-loop läuft länger, je mehr Buchstaben vom Anfang aus korrekt sind. Also kann man alle Passwörter „axxxxx", „bxxxxx", ... mit korrekter Länge ausprobieren, eines davon wird ein wenig länger brauchen. Damit hat man den ersten Buchstaben erraten und kann mit dem nächsten fortfahren.