Aufgabe 1: Rechnersicherheit

Aufgabe 1.1: Zugangs- und Zugriffskontrolle

- a)

  Zungangskontrolle: Beschränkt, wer überhaupt Zugang zu dem System hat. Z.B.: Username/Passwort-Abfrage auf bei der Anmeldung auf einem Server.

  Zugriffskontrolle: Beschränkt, auf was genau im System der User Zugriff hat, nachdem ihm Zugang gewährt wurde.

- b) Grundsätzlich ist diese Möglichkeit nicht auszuschließen. Beispielsweise in Systemen mit wenigen oder einzig und allein vertrauenswürdigen Nutzern, oder in Systemen, in denen Benutzer einfach grundsätzlich nichts schlimmes anstellen können.

- c) Man kann die Zugriffsrechte eines Users nicht überprüfen/durchsetzen, wenn man ihn nicht vorher identifiziert hat. Um einen User zu identifizieren, benötigt man mindestens Zugangskontrolle.

- d) Es wird hier von einer Zugriffskontrolle auf *Ordner-Ebene* geredet. Das bedeutet, dass für bestimmte Ordner die Zugriffskontrolle *aufgehoben* wird. Diese Ordner sind dann öffentlich zugänglich. Ordner, die nicht freigegeben sind, sind weiterhin nur für eingeloggte Benutzer sichtbar, die Zugangskontrolle ist also weiterhin aktiv und es gilt das Statement aus aufgabe c).

Aufgabe 2: Timing-Attack

- 1.

```
boolean isTimingAttackPossible()
{
    char[] pass1 = ['h','a','s','e'];
    char[] pass2 = ['t','i','g','e','r','e','n','t','e'];

    int t1 = System.nanoTime();
    passwordCompare(pass1, pass1);
    int t2 = System.nanoTime();

    int result1 = math.abs(t1 - t2);

    t1 = System.nanoTime();
    passwordCompare(pass1, pass2);
    t2 = System.nanoTime();

    int result2 = math.abs(t1 - t2);
```

```
        return result1 == result2;
    }
```

Man könnte beide Varianten von passwordCompare zwischen den Zeitmessungen mehrfach ausführen, um die Zeitunterschiede deutlicher zu machen.

- 2. Eine Timing-Attack ist hier möglich, da in passwordCompare entweder sofort abgebrochen, oder eine naive for-Schleife ausgeführt wird. Dies kann zu sehr unterschiedlichen Ausführungszeiten führen.
- 3. Zunächst versucht der Angreifer, die Länge des Passworts herauszufinden. Hierfür probiert er der Reihe nach Passwörter verschiedener Länge (und mit beliebigem Inhalt) aus: `a`, `aa`, `aaa`, `aaaa` etc. Dabei sollten alle Passwörter bis auf eines gleich lang brauchen. Das eine Passwort, das länger braucht (da das Programm nicht sofort abbricht, sondern beginnt, die Passwörter Zeichen für Zeichen zu vergleichen), hat die richtige Länge.

  Nun beginnt der Angreifer, das erste Zeichen des Passwortes zu knacken. Hierfür probiert er Passwörter mit der richtigen Länge aus und ändert dabei immer das erste Zeichen, z.B. (bei einer Länge von 4) `aaaa`, `baaa`, `caaa`, `daaa` etc. Auch hier wird wieder ein Passwort länger brauchen als die anderen, da das Programm das erste Zeichen dieses Passwortes als richtig ansieht und noch (mindestens) das zweite Zeichen vergleicht. So kann der Angreifer sicher sein, dass das erste Zeichen dieses Passwortes das richtige ist und wendet nun die gleiche Methode auf das zweite Zeichen an. Nachdem er jedes Zeichen geknackt hat, besitzt der Angreifer das korrekte Passwort.
- 4.