



## Aufgabe 1: Rechnersicherheit

### Aufgabe 1.1: Zugangs- und Zugriffskontrolle

- a)

Zugangskontrolle: 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) Dies würde implizieren, dass man dem User vertraut, was grober Fahrlässigkeit entspricht. ;-)
- c) Man kann die Zugriffsrechte eines Users nicht überprüfen/durchsetzen, wenn man ihn nicht vorher identifiziert hat.
- d) Die Zugangskontrolle besteht darin, dass nicht jeder den Link kennt. Die Kenntnis des Links gewährt also Zugang, und Zugriff wird nicht weiter kontrolliert, da über den Link ja sowieso nur ein Ordner bereitgestellt wird.

## Aufgabe 2: Timing-Attack

- 1.

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

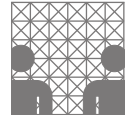
    int t1 = System.nanoTime();
    passwordCompare(pass1, pass1);
    int t2 = System.nanoTime();

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

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

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

    return result1 == result2;
}
```



- 2.
- 3.
- 4.