GSS-Übungsblatt 3 zum 14.05.2014

A. Struck, S. Haase, E. Böhmecke

13. Mai 2014

1 Rechnersicherheit

1.1 Zugangs- und Zugriffskontrolle

a)

Zugangskontrolle:
Beschränkung (durch spezielle Eigenschaften, Biometrie, Wissen, Besitz) wer Zugang zu einem System bekommt.
Zugriffskontrolle:
Beschränkung auf welchen Inhalt/Funktionalitäten im System ein User Zugriff hat.

b)

Dies kommt auf das System an. Keine Zugriffskontrolle impliziert dass jeder Nutzer auf der selben Vertrauensebene operiert, dies kann bei Systemen mit einer größeren Zahl von Anwendern zu großen Vertrauensproblemen führen. Allerdings ist nicht auszuschließen, dass Systeme gewünscht werden in denen jeder Nutzer die selben Rechte besitzt.

c)

Die Rechte eines unidentifizierten Nutzers (Zugangskontrolle) können nicht durchgesetzt werden, in so fern ist eine Zugangskontrolle vor Zugriffskontrolle von Nöten.

d)

Die Zugangskontrolle besteht hier durch die Kenntnis des Links, dies ist zwar schwächer, als eine Kombination aus Nutzerkonto und Passwort, erfüllt aber den selben Zweck.

1.2 Biometrische Techniken: EasyPASS

a)

Optional

b)

Optional

1.3 Biometrische Techniken: Tippverhalten

a)

Optional

b)

Optional

1.4 Realisierung eines Online-Tickets

a)

Optional

b)

Optional

2 Timing-Attack

1.

```
public void isTimingAttackPossible(){
  char[] password1 = "123456789".toCharArray;
  char[] password2 = "qwert".toCharArray;

  long pwTimeTemp = System.nanoTime();
  passwordCompare(password1, password1);

  long result = System.nanoTime() - pwTimeTemp;
  System.out.println("Gleiche Passwörter in ns: " + result);

  pwTimeTemp = System.nanoTime();
  passwordCompare(password1, password2);

  result = System.nanoTime() - pwTimeTemp
  System.out.println("Unterschiedliche Passwörter in ns: " + result);
}

boolean passwordCompare(char[] a, char[] b){
  int i;
  if(a.length != b.length) return false;
  for(i=0; i<a.length && a[i]==b[i]; i++);
  return i == a.length;
}
```

2.

Optional

3.

TODO

4.

Optional

3 Real-World Bruteforce

Optional