Betriebssysteme und Sicherheit, WS 2023/24

9. Aufgabenblatt – Sicherheit I

Geplante Bearbeitungszeit: 11.12.2023 – 15.12.2023

Aufgabe 9.1 Schutzziele

(a) Nennen und begründen Sie mögliche Schutzziele, die beim Versenden einer E-Mail relevant sein könnten.

(b) Nennen Sie (mindestens) ein mögliches Schutzziel, das die entsprechende Maßnahme adressieren soll.

1. Passwort
2. Hashwert
3. Checkbox: „AGB gelesen“
4. Redundanz

Aufgabe 9.2 Schwachstellen

(a) Gegeben sei folgender C-Code:

```c
#include <stdio.h>
#include <string.h>

void read_something() {
  char foo[4] = "foo";
  char bar[4];
  char baz[4] = "baz";
  printf("Gib eine Zeichenkette ein: ");
  gets(bar);

  printf("Variable foo: %.3s\n", foo);
  printf("Variable bar: %.3s\n", bar);
  printf("Variable baz: %.3s\n", baz);
}

int main() {
  read_something();
  printf("Programm ist fertig.\n");
  return 0;
}
```

Beantworten Sie die folgenden Fragen und begründen Sie Ihre Antwort.

1. Ist das Programm sicher?
2. Was passiert bei der Eingabe „`bar`“ (ohne Anführungszeichen)?
3. Was passiert bei der Eingabe „`bar_bar`“ (ohne Anführungszeichen)?
4. Was passiert bei der Eingabe „`bar_bar_bar`“ (ohne Anführungszeichen)?
5. Was passiert bei einer noch längeren Eingabe?
6. Wie kann man das Programm absichern?

(b) Die folgenden Codeausschnitte enthalten Schwachstellen in Form von Programmierfehlern. Finden Sie diese Schwachstellen und beschreiben Sie was Angreifer:innen damit machen könnten.
Hinweis: Es handelt sich um eine Bonusaufgabe, die zeigt wie subtile Programmierfehler zu Schwachstellen werden können.

1. `SELECT * FROM users WHERE name = '$user' AND age = 2;`

   Die Variable `$user` wird von Nutzer:innen übergeben und in die SQL-Abfrage hinzugefügt.

2. ```
   <?php $var = $_GET['user'];
   eval($var); ?>
   ```

   Der `user` wird als Parameter in der URL von Nutzer:innen übergeben. Ein möglicher Aufruf könnte dementsprechend wie folgt aussehen: `http://www.example.com/index.php?user=admin`.

Aufgabe 9.3 Malware

(a) Wie wird Malware bezeichnet, die den Zugriff auf ein Computersystem einschränkt, indem sie Dateien verschlüsselt oder das gesamte System sperrt, bis Benutzer:innen die gewünschte Aktion ausführt?

- ☐ Virus
- ☐ Ransomware
- ☐ Trojaner
- ☐ Adware

(b) Wie wird ein Computerprogramm bezeichnet, das sich über ein Netzwerk verbreitet, um beispielsweise die Systemressourcen und die Netzwerkbandbreite zu beeinträchtigen?

- ☐ Spyware
- ☐ Wurm
- ☐ Trojaner
- ☐ Spam

(c) Eine Art von Software, die sich als ein nützliches Programm tarnt, aber dabei unerwünschte und schädliche Aktionen durchführt, wird als Trojanisches Pferd bezeichnet. Diese Art von Malware kann sich wie ein legitimes Programm verhalten und alle erwarteten Funktionen haben, enthält allerdings auch bösartigen Code, der Nutzer:innen nicht bekannt ist.

- ☐ richtig
- ☐ falsch

Aufgabe 9.4 Passwörter und Hash-Funktionen Nehmen Sie an, dass Sie sich Zugriff zu einer Datenbank mit den Nutzerpasswörtern einer populären Webseite verschafft haben. Sie haben herausgefunden, dass die Passwörter vor dem Abspeichern nach dem folgenden Prinzip gehasht wurden: Zunächst wird jeder Buchstabe in der Eingabe durch seine numerische Position im Alphabet ersetzt. Der Hash-Wert einer Eingabe ist dann die Summe dieser Zahlen modulo 1000.

(a) Hashen Sie die folgenden Wörter wie zuvor beschrieben.

1. cause
2. race
3. dog
4. salt

Nehmen Sie dafür folgendes an:

- Bei dem Eingabealphabet handelt sich um das lateinische Alphabet mit 26 Zeichen.
- Die Eingabe darf nur aus Kleinbuchstaben bestehen.

(b) Suchen Sie zwei Wortpaare mit dem gleichen Hash-Wert.

(c) Nennen Sie mindestens zwei Gründe, warum dieser Algorithmus nicht für sensible Daten wie Passwörter verwendet werden sollte.
   ```

Aufgabe 9.5 Passwortsicherheit Nehmen Sie an, dass bei einer Sicherheitsüberprüfung eines Systems die simulierte Angreifer:in eine Liste mit Passwort-Hashes bekommen hat.

(a) Wie könnte diese Liste verwendet werden, um sich Zugang zum System zu verschaffen?

(b) Wie lange dauert maximal ein Brute-Force Angriff, wenn man 64 Gigahashes pro Sekunde berechnen kann und wenn Passwörter 12 Zeichen (nur Buchstaben) umfassen?

(c) Wie kann man es einer Angreifer:in erschweren das Passwort zu erraten?