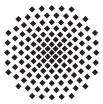

Universität Stuttgart

RSS
Reliable Software Systems

Übungsblatt 3

Sichere und zuverlässige Softwaresysteme (WiSe 2018/2019)

Abgabe: Fr. 30.11.2018, 23:55 Uhr — Besprechung: Montag, 03.12.2018

- Bitte lösen Sie die Übungsaufgabe in **Gruppen von 4 Studenten** und wählen EINEN Studenten aus, welcher die Lösung im ILIAS (Ordner `Abgaben/Übungsblatt 3/`) als **Gruppenabgabe** (unter Angabe aller Gruppenmitglieder) einstellt.
- Für schriftliche Aufgaben erstellen Sie EINE **PDF-Datei**, die Projekte für Programmieraufgaben fügen Sie als **ZIP-Datei** hinzu. Geben Sie beide Dateien ab und verzichten Sie darauf, diese in einer weiteren ZIP-Datei zusammenzuführen. Geben Sie bitte nicht nur den Sourcecode, sondern stets das komplette Projekt ab!
- Erstellen Sie ein **Titelblatt**, welches die Namen der Studenten, die Matrikelnummern, und die E-Mail-Adressen enthält. Im Quellcode fügen Sie diese Informationen bitte als Kommentar hinzu.
- Benennen Sie die Dateien nach dem folgenden Schema:
  SZS[**Blattnummer**]**-**[**Nachnamen der Teammitglieder, alphabetisch**]**.**[**pdf oder zip**].

Aufgabe 1 Grundlagen der Verschlüsselung

(a) In dieser Aufgabe sollen Sie das verschlüsselte Wort mit Kenntniss des Verschlüsselungsverfahrens entschlüsseln. Das Lösungswort ist ein sinnvolles Wort. Geben Sie auch den **Rechenweg** an! Die benötigten Verschlüsselungsverfahren für diese Aufgabe finden Sie nicht in den Vorlesungsfolien, sondern müssen selbst recherchiert werden. Für diese Aufgabe werden nur Großbuchstaben und keine Umlaute oder Satzzeichen betrachtet. Dabei gelten die folgenden Bezeichnungen für die 26 Buchstaben: A = 0, B = 1, ... , Z = 25.

Die **Caesar-Verschlüsselung** ist eine sehr einfache Methode zur Verschlüsselung, die bereits vom römischen Feldherrn Julius Caesar eingesetzt wurde (und teilweise sogar heute noch verwendet wird[1]). Sie ist ein (einfaches) Beispiel für substitutionsbasierte Verschlüsselungsverfahren. Bei dieser Art der Verschlüsselung werden die Buchstaben durch andere Buchstaben ersetzt. Die Caesar-Verschlüsselung wählt die Buchstaben dabei durch eine Verschiebung im Alphabet aus.
Der geheime Text: ELE Eqogdufk Gqngzs
Schlüssel: 12 bzw. "O" — d. h. aus dem Klartext "A" wird der verschlüsselte Text "O".

(b) Es gibt zwei grundlegende Verschlüsselungskonzepte: **Symmetrische und Asymmetrische Verschlüsselung**. Beschreiben Sie die Konzepte kurz und erklären Sie die wichtigsten Unterschiede.

(c) Wenn Sie das HTTPS-Protokoll (HTTP Secure) verwenden, kommen beide Konzepte zum Einsatz. Beschreiben Sie, wozu diese jeweils eingesetzt werden und warum es sinnvoll ist, hier beide Konzepte zu kombinieren.

Aufgabe 2 Bedrohungsanalyse

STRIDE ist ein Ansatz zur Klasssifikation von Bedrohungen. In dieser Aufgabe soll STRIDE auf folgendes Szenario angewandt werden:

Alice verwendet einen E-Mail Web-Client von Provider A, um Bob, der seinen Account bei Provider B hat und einen Desktop-Client verwendet, eine E-Mail zu senden.

[1] `http://www.dkriesel.com/blog/2016/0703_verschluesselung_von_spiegelonline-bezahlartikeln_extrem_einfach_knackbar`

Zerlegen Sie hierzu zunächst das Szenario in Teilszenarien (z. B. *Alice sendet zu sendende E-Mail an ihren Provider A*). Wählen Sie drei dieser Teilszenarien aus und analysieren diese mit STRIDE. Geben Sie dazu jeweils tabellarisch an, welche Kategorien von STRIDE für die jeweiligen Teilschritte relevant sind und welche nicht und was für die jeweiligen Kategorien mögliche Bedrohungen sein könnten.

Aufgabe 3 Gefährliche Softwarefehler

In der Vorlesung haben Sie bereits die 25 gefährlichsten Programmierfehler kennen gelernt. Im Folgenden sollen Sie einige Code-Beispiele betrachten und kurz beschreiben, warum diese Beispiele sich negativ auf die Security der Software auswirken können. Versuchen Sie außerdem, die folgenden Beispiele mindestens einer der 25 Fehlerarten zuzordnen. Begründen Sie ihr Zuordnung kurz.

(a) JAVA:

```
public String coordinateTransformLatLonToUTM(String coordinates){
  String utmCoords = null;
  try {
    String latlonCoords = coordinates;
    Runtime rt = Runtime.getRuntime();
    Process exec = rt.exec("cmd.exe /C latlon2utm.exe -"
                           + latlonCoords);
    // process results of coordinate transform
    // ...
  }
  catch(Exception e) {...}
  return utmCoords;
}
```

(b) C:

```
void manipulate_string(char* string){
  char buf[24];
  strcpy(buf, string);
...
```

(c) JAVA:

```
public boolean VerifyAdmin(String password) {
  if (password.equals("68af404b513073584c4b6f22b6c63e6b")) {
    System.out.println("Entering Diagnostic Mode...");
    return true;
  }
  System.out.println("Incorrect Password!");
  return false;
}
```

(d) JAVA:

```
public class RedirectServlet extends HttpServlet {
  protected void doGet(HttpServletRequest request, HttpServletResponse
```

```
                                response) throws ServletException, IOException {
    String query = request.getQueryString();
    if (query.contains("url")) {
      String url = request.getParameter("url");
      response.sendRedirect(url);
    }
  }
}
```

(e) PL/SQL:

```
procedure get_item ( itm_cv IN OUT ItmCurTyp,
                     usr in varchar2, itm in varchar2)
is open itm_cv for
  ' SELECT * FROM items WHERE ' || 'owner = '|| usr ||
  ' AND itemname = ' || itm || ';
end get_item;
```

(f) JAVA:

```
Cookie[] cookies = request.getCookies();
for (int i =0; i< cookies.length; i++) {
  Cookie c = cookies[i];
  if (c.getName().equals("role")) {
    userRole = c.getValue();
  }
}
```

Code-Beispiele von `http://cwe.mitre.org`.

Hinweise zu den Übungen:

- Durch die Teilnahme am Übungsbetrieb können Sie sich bis zu **3 Bonuspunkte für die Klausur** verdienen.
- Bedingungen:
  - Während des Semesters darf maximal eine Abgabe im ILIAS ausgelassen werden.
  - Während des Semesters darf pro Person max. eine Hörsaalübung ausgelassen werden.
  - Jede Gruppe muss im Laufe des Semesters eine Aufgabe in der Hörsaalübung präsentieren.
  - Jede Präsentation wird mit folgender Skala bewertet:
    * 3 Punkte: Korrekt
    * 2 Punkt: Sinnvoll aber fehlerhaft
    * 1 Punkte: Sinnlos/falsch oder fehlt (Basispunkt für Präsentation)

Viel Erfolg!