TU München, Fakultät für Informatik
Lehrstuhl III: Datenbanksysteme
Prof. Alfons Kemper, Ph.D.

Übung zur Vorlesung
Einsatz und Realisierung von Datenbanksystemen im SoSe14

Moritz Kaufmann (moritz.kaufmann@tum.de)
http://www-db.in.tum.de/teaching/ss14/impldb/

Blatt Nr. 3

Aufgabe 1

Skizzieren Sie die Funktionsweise von SSL. Erläutern Sie hierzu, wie der einfache TLS Handshake funktioniert. Eine Lösungsmöglichkeit wäre das Zeichnen eines passenden Message Sequence Charts.

Aufgabe 2

Erläutern Sie Probleme, die bei der naiven Implementierung von SSL auftreten können. Lesen Sie hierzu beispielsweise `http://www.ietf.org/mail-archive/web/tls/current/msg07553.html` und skizzieren Sie sowohl den traditionellen Angriff mittels eines Botnets sowie den dort neu vorgestellten Angriff mittels Renegotiation. Wie können derartige Angriffe verhindert werden?

Aufgabe 3

Implementieren Sie den RSA - beispielsweise in Java unter Nutzung der BigInteger Klassen. Verdeutlichen Sie sich die Funktionsweise des RSA an einem geeigneten Beispiel, d.h. verschlüsseln Sie eine kleine Nachricht mit einem (nicht zu großen) Schlüssel und bringen Sie das Beispiel inklusive Verschlüsselung und Entschlüsselung mit in die Übung.

Aufgabe 4

Eine statistische Datenbank ist eine Datenbank, die sensitive Einträge enthält, die aber nicht einzeln betrachtet werden dürfen, sondern nur über statistische Operationen. Legale Operationen sind beispielsweise Summe, Durchschnitt von Spalten und Anzahl der Tupel in einem Ergebnis (**count**, **sum**, **avg**, ...). Ein Beispiel wäre eine Volkszählungsdatenbank. Für diese Art von Systemen existiert das in der Einleitung erwähnte *Inferenzproblem*.

Nehmen wir an, Sie haben die Erlaubnis, im **select**-Teil einer Anfrage ausschließlich die Operationen **sum** und **count** zu verwenden. Weiterhin werden alle Anfragen, die nur ein Tupel oder alle Tupel einer Relation betreffen, abgewiesen. Sie möchten nun das Gehalt eines bestimmten Professors herausfinden, von dem Sie wissen, dass sein Rang „C4“ ist und er den höchsten Verdienst aller C4-Professoren hat. Beschreiben Sie Ihre Vorgehensweise.

Aufgabe 5

Wolfgang S.[1] hat sich eine Internetseite programmiert und dabei folgenden Pseudocode verwendet:

[1] Die Wahl des Namens und der weitere Text stellen keinen politischen Kommentar der Übungsleitung dar. Vielmehr wird Bezug darauf genommen, dass die Webseite der betroffenen Person mindestens ein Mal auf diese Weise gehackt wurde.

```
string id = GET_PARAMS['id'];

string query = "select␣title,content␣from␣news␣where␣";
query+=        "␣id='" + id + "'␣and␣visible='1';";
Process proc("sqlite3␣wolfgang.sqlite3");
proc.write(query);
string result = proc.read();

display(result);
```

Die Seite wird etwa wie folgt aufgerufen: `http://wolfgangs.de/news?id=15`. Der `GET`-Parameter `id` wird hierbei in eine Variable gespeichert und dann in das gezeigte SQL Statement eingefügt. Anschließend wird die so entstandene Anfrage an einen SQLite Client übergeben, der diese ausführt und das Resultat dem Benutzer angezeigt.

- Geben Sie den genauen Code an, wie Sie sich hier Zugriff auf die Tabelle "users" verschaffen können.
- Wie kann eine solche SQL Injection verhindert werden?

Aufgabe 6

Sie haben Wolfgangs Users-Tabelle ausgelesen, jedoch scheint sein Passwort uncharakteristisch kompliziert zu sein. Das von Ihnen erhaltene Resultat ist das Folgende:

```
id          name        password
----------  ----------  --------------------------------
1           wolfgang    4d75e8db6a4b6205d0a95854d634c27a
```

- Was könnte der Grund für dieses hexadezimale, 32 Stellen lange Passwort sein?
- Können Sie trotzdem den Klartext finden?
- Wie können Sie das Passwort sicherer Speichern?
- Wie können Sie für diese Art von Passwortspeicherung Bruteforce-Attacken erschweren?

Aufgabe 7

Nehmen Sie an, dass es in der Universitätswelt einige Fakultäten gibt, denen die Professoren zugeordnet sind. Lese- und Schreibrechte auf Vorlesungen sollen nun nach Fakultät vergeben werden, z.B. gibt es eine Benutzergruppe, die nur Vorlesungen der Fakultät für Physik ändern darf. Definieren Sie ein Schema mit Sichten so, dass die Benutzergruppen Änderungen durchführen können, aber die dritte Normalform der Relationen nicht verletzt wird.

Hinweise:

- Überlegen Sie, welches Subset der bekannten Universitätsdatenbank modelliert werden muss.
- Skizzieren Sie Ihre Modellierung, bestimmen Sie die vorliegenden FDs und weisen Sie nach, dass sich Ihre Modellierung in 3. Normalform befindet.
- Erstellen Sie eine passend beschränkte Sicht. Wann ist eine Sicht updatebar?
- Weisen Sie den Mitgliedern der Gruppe 'PProfessoren" Rechte auf die zuvor definierte Sicht zu.