Datenbanken-Praktikum Sommersemester 2006
Fallstudie 3:
Sicherheit

Um den Service zur Handhabung von Prüfungen und Notenvergaben zu implementieren, wurde zunächst einmal ein Datenbankserver auf dem Rechner SNAREDRUM aufgesetzt. Das Datenbankschema wurde angelegt. Datenbankseitig wurden ein Benutzer angelegt, mit dem der Server auf CONGA sich auf der Datenbank auf SNAREDRUM einloggt. Diesem Benutzer wurden uneingeschränkte Rechte auf allen Tabellen eingeräumt. Passwörter werden in der Tabelle *Person* MD5-verschlüsselt in der Spalte *passwort* gehalten.

Besser: Mehrere Datenbank-Accounts für mehrere Rollen

Die Authentifizierung läuft folgendermassen ab:

(a) Der Benutzer gibt auf dem Client TABLA seine Benutzer-ID und das Passwort ein

(b) Der Client erzeugt einen MD5-Hash des Passworts

(c) Benutzer-ID und Passwort-Hash werden an den Server geschickt

(d) Der Service CONGA prüft die Benutzer-ID auf unzulässige Zeichen (wie '-' oder ';'); findet er diese, lehnt er sofort die Authentifizierung ab.

Ausschließen von SQL-Exploits

(e) Der Service auf CONGA loggt sich auf der Datenbank auf SNAREDRUM ein und setzt folgendes Statement ab:

Kein Problem hier

```
SELECT * FROM Person WHERE id='benutzer-id'
                       AND passwort='passwort'
```

'benutzer-id' und 'passwort' werden dabei durch die übermittelte ID und das Passwort ersetzt. Der so zusammengesetzte String wird an die Datenbank geschickt und von dieser ausgeführt. Liefert die Datenbank kein Ergebnis zurück, gilt die Authentifizierung als gescheitert und es wird eine Fehlermeldung an TABLA geliefert; andernfalls wird nun geprüft, ob es sich um einen Studenten oder Dozenten handelt:

```
SELECT id FROM Student WHERE id='benutzer-id'
```

Liefert diese Abfrage ein Ergebnis zurück, wird dem Client mitgeteilt, dass es ein Student ist; ansonsten wird dem Client gesagt, dass es sich um einen Dozenten handelt.

Nachdem der Benutzer erfolgreich authentifiziert wurde, holt sich der Client auf TABLA nun alle Prüfungen und Kurse vom Server. Diese Daten werden entsprechend der Rolle des Benutzers vom Client aufbereitet.

Alle Daten gehen unverschlüsselt über's Netz, Abhören und Man-in-the-Middle Attack möglich! Lösung: SSL mit Zertifizierung

- Ist der Benutzer Student, kann er alle Kurse und Prüfungen mit seiner Matr.Nr. einsehen. Der Client sortiert also alle Prüfungen raus, die nicht zum Benutzer gehören (deren Einträge eine andere Matr.-Nr. haben); das Resultat wird dem Benutzer vom Client präsentiert. Ferner werden alle Kurse angezeigt, so dass der Student sich für neuen Prüfungen anmelden kann.
- Ist der Benutzer Dozent, kann er alle seine Kurse sehen und die entsprechenden Prüfungen. Der Client auf TABLA zeigt somit alle Kurse zu der übergebenen Benutzer-ID (Dozent_Id) an. Zu jedem angezeigten Kurs

werden auch die entsprechenden Prüfungen angezeigt, so dass der Dozent nun Noten vergeben kann.

Sobald eine Änderung vorgenommen wurde, wird im Client ein entsprechender Funktionsaufruf generiert und an den Server geschickt; die Benutzer-ID und die durchzuführenden Änderungen werden dabei übermittelt. Der Service auf CONGA verbindet sich zur Datenbank und führt die entsprechende Operation aus.

Funktionsaufrufe gehen unverschlüsselt über's Netz; diese können abgehört und modifiziert oder später von einem „bösen Client" simuliert werden: Lösung: SSL mit Zertifizierung

Die Betreiber des Systems argumentieren, dass ihr System sicher sei, da die Authentifizierung auf dem Server erfolgt und somit korrekte Passwörter aus der Datenbank gar nicht erst über das Netzwerk gehen. Ferner sind Passwörter verschlüsselt und SQL-Statements werden auf mögliche Exploits untersucht.

- Was haltet ihr von dieser Aussage? Welche Maßnahmen wurden unternommen, um das System sicher zu machen? Wo liegen mögliche Gefahren? Hinweis: Wenn Passwörter vom Client an den Server geschickt werden, sind sie verschlüsselt, und vom Server kommen keine Passwörter an den Client. Was aber ist mit den restlichen Daten?
- Welche Änderungen würdet ihr vornehmen, um das System sicherer zu machen?