

Modellbasierte Softwaretechniken für sichere Systeme - Übung 4

1 Fair exchange (6 Punkte)

Modellieren Sie folgendes Szenario als Aktivitätsdiagramm. Sorgen Sie dafür, dass ein "fair exchange" stattfindet und das Diagramm entsprechend annotiert ist.

Ein Kinokunde möchte sich einen Film anschauen und dafür reservieren. Dafür verbindet er sich zu dem Reservierungsserver des Kinos und fordert eine Liste der Vorstellungen an. Der Reservierungsserver liefert diese. Nachdem der Kunde eine Vorstellung gewählt hat, zeigt der Server zudem die Sitzplatzbelegung dieser Vorstellung an. Der Kunde wählt nun seine Wunschplätze und startet damit die Reservierung. Auf Seiten des Reservierungsservers wird nun geprüft, ob die Wunschplätze noch frei sind. Wenn nicht wird eine Fehlermeldung generiert und der Kinokunde bricht seine Reservierung ab. Sind die Plätze frei, generiert der Reservierungsserver ein Bestellformular welches vom Kunden ausgefüllt wird. Nach dem Übersenden der Daten fragt der Reservierungsserver nach einer Bestätigung. Hat sich der Kinokunde es nun anders überlegt, storniert er die Reservierung und der Reservierungsserver löscht die Reservierung. Bestätigt der Kunde die Reservierung wird die Reservierung fixiert und das Geld abgebucht. Auf Seiten des Servers wird nun bis 30 Minuten vor Beginn der Vorstellung gewartet. Dann wird geprüft ob die Karten abgeholt wurden. Wurden sie nicht abgeholt, wird das Geld zurück gebucht und die Reservierung gelöscht.

Der Kunde merkt sich die Reservierungsnummer und holt irgendwann die Karten ab. Die Kasse ruft nun anhand der Reservierungsnummer die Reservierung vom Reservierungsserver ab und fordert eine Authentifizierung vom Kunden. Dieser zeigt seinen Ausweis und die Kasse prüft ihn. Wenn der Ausweis nicht zur Reservierung passt, wird der Vorgang abgebrochen, ansonsten werden die Karten übergeben und dem Reservierungsserver mitgeteilt, dass die Reservierung eingelöst wurde. Dieser speichert das.

Der Kunde nimmt die Karten an und schaut dann den Film.

2 Sichere Verbindungen (4 Punkte)

Legen Sie das Verteilungsdiagramm aus Aufgabe 4 von Übungsblatt 3 zugrunde. Es soll sich dabei um das Online-Bestellsystem eines Kinos handeln, über das die Kunden online mit Hilfe einer Handyapplikation Kinokarten erwerben können. Die Mitarbeiter des Kinos an der Abendkasse haben Zugriff auf das System über interne Kassensysteme.

2.1 Modellieren Sie die Verteilung und erweitern sie das Diagramm, sodass die Verbindungen sicher sind. (1 Punkt)

2.2 Handelt es sich bei dem von Ihnen modellierten Modell um ein abhörsicheres System? (1 Punkt)

Begründen Sie Ihre Antwort. Falls nicht, vervollständigen Sie das Modell entsprechend. Gehen Sie dabei vom Standardangreifer aus.

2.3 Was sind die Auswirkungen, falls der Angreifertyp ein Innenangreifer ist? (1 Punkt)

Wie müsste das Diagramm angepasst werden, wenn ein Abhören der Daten durch einen Besucher des Kinos verhindert werden soll?

2.4 Was sind die Auswirkungen, falls der Server nicht mehr im Kino steht? (1 Punkt)

Das Kino wird von einer großen Kette aufgekauft und die Abwicklung des Kartenverkaufs geschieht nun über einen zentralen Server. Das Kino kommuniziert über eine DSL-Leitung mit dem Server. Gehen Sie wieder vom Standardangreifer aus.