

Modellbasierte Softwaretechniken für sichere Systeme - Übung 10

1 Zeichnen Sie einen Bedrohungsbaum für das CEPS-System. (2 Punkte)

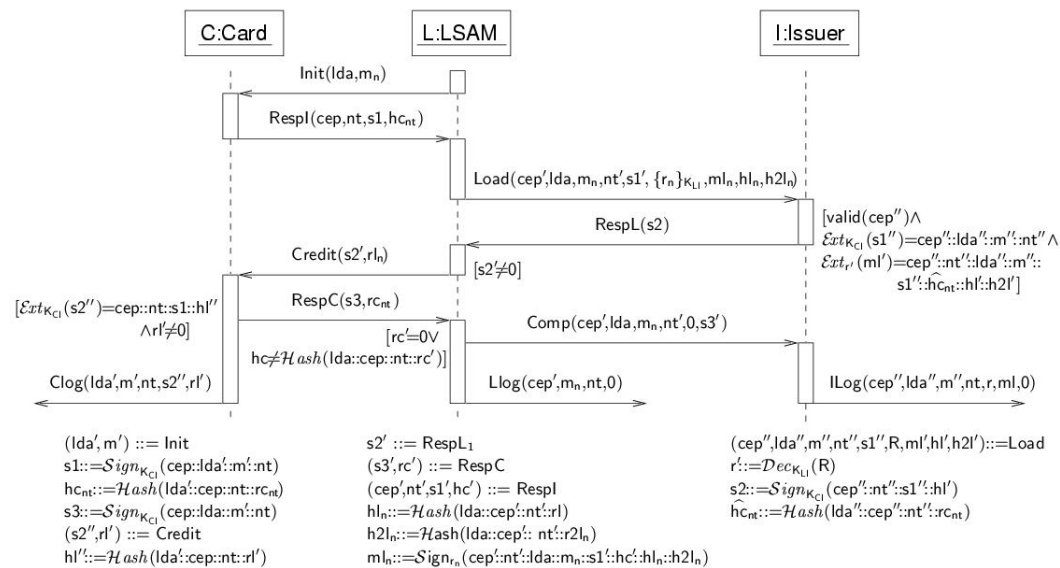
2 Welche Sicherheitseigenschaft, die für Bargeldnutzer im allgemeinen erfüllt ist, wird durch das Post-Transaktions-Abrechnungssystem eingeschränkt? (1 Punkt)

Bedenken Sie dabei, dass die Karte über ein Bankkonto aufgeladen wird.

3 Welcher Angriff wäre möglich, wenn es den in der Vorlesung genannten Transaktionszähler NT beim Bezahlen mit der Karte nicht geben würde? (1 Punkt)

3.1 Zeichnen Sie den Angriff als Sequenzdiagramm. (2 Punkte)

4 CEPS Ladeprotokoll



Aus der Analyse des Sequenzdiagramms ergibt sich, dass das Protokoll keine Sicherheit für die Ladestation gegen interne Angreifer bietet.

- 4.1 ~~Modifizieren Sie das Sequenzdiagramm gemäß der in den Vorlesungsfolien genannten Änderung. (2 Punkte)~~**
- 4.2 Was bewirkt diese Änderung? Ist diese Lösung nun sicherer ist als vorher und warum? (2 Punkte)**