technische universität dortmund

Prof. Dr. Jan Jürjens, Christian Wessel
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
Modellbasierte Softwaretechniken
für sichere Systeme – 29.05.2012

Modellbasierte Softwaretechniken für sichere Systeme - Übung 7

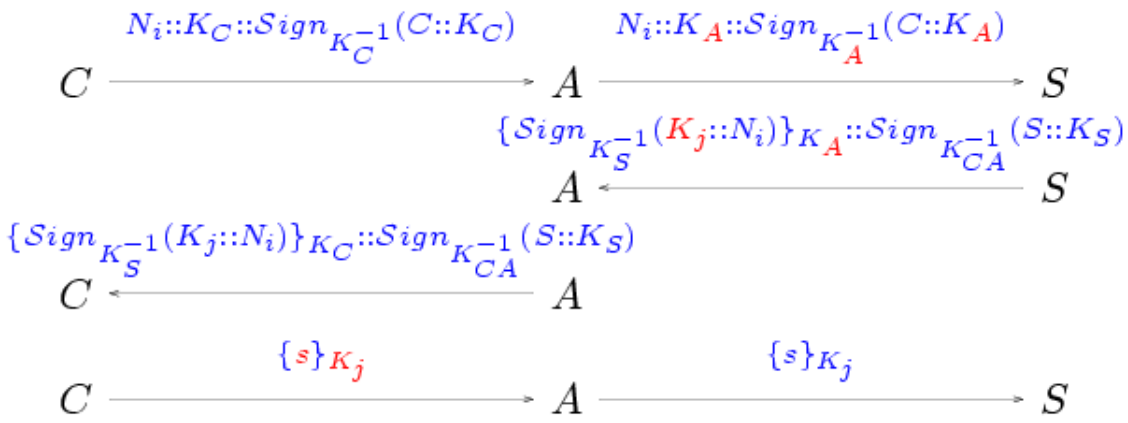
1 Secure Dependencies (4 Punkte)

Das Softwaresystem einer Versicherung besteht aus den folgenden Klassen:

- `Insurance`
  - `saveNewPolicy(Policy:p):void`
  - `writeLog(String:msg):void`
  - `payPolicy():void`
  - `getPoliciesForCustomer(String:customerID):Policy[]`
- `Logging`
  - `log(String:msg):void`
- `PaymentSystem`
  - `pay():void`
- `EmployeeGUI`
  - `concludePolicy(Policy:p):void`
- `CustomerGUI`
  - `showPolicies():void`

Der Versicherungsmakler schließt über seine Benutzeroberfläche Versicherungen für den Kunden ab. Diese werden im System gespeichert. Da dabei personenbezogene Daten übermittelt werden, ist es wichtig, dass die Datenübertragung geschützt wird. Kunden können über eine Benutzeroberfläche Informationen über ihre laufenden Versicherungen einholen. Auch diese Daten sind sensibel und müssen geschützt werden. Das System prüft, ob Versicherungen ausbezahlt werden sollen und beauftragt falls erforderlich das `PaymentSystem` damit. Bei dieser Aktion dürfen die Daten auf keinen Fall verändert oder mitgelesen werden. Um die Transaktionen später nachvollziehen zu können, schreibt das System eine Logdatei. Hier muss lediglich darauf geachtet werden, dass die geschriebenen Daten nicht verändert werden können.

2 Protokollanalyse (6 Punkte)



Zeigen Sie, wie der Angriff in der gegebenen Abbildung in Form einer logischen Ableitung demonstriert werden kann. Benutzen Sie dazu die Regeln aus der Datei *tlsvariant_tptp.txt* von der Vorlesungswebseite. Beginnen Sie mit der Regel `Conjecture`.