technische universität dortmund

Prof. Dr. Jan Jürjens, Christian Wessel
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
Modellbasierte Softwaretechniken für sichere Systeme – 22.05.2012

Modellbasierte Softwaretechniken für sichere Systeme - Übung 6

1 Kryptografische Ausdrücke

1.1 Sind die folgenden Ausdrücke korrekt? Begründen Sie Ihre Anwort. (3 Punkte)

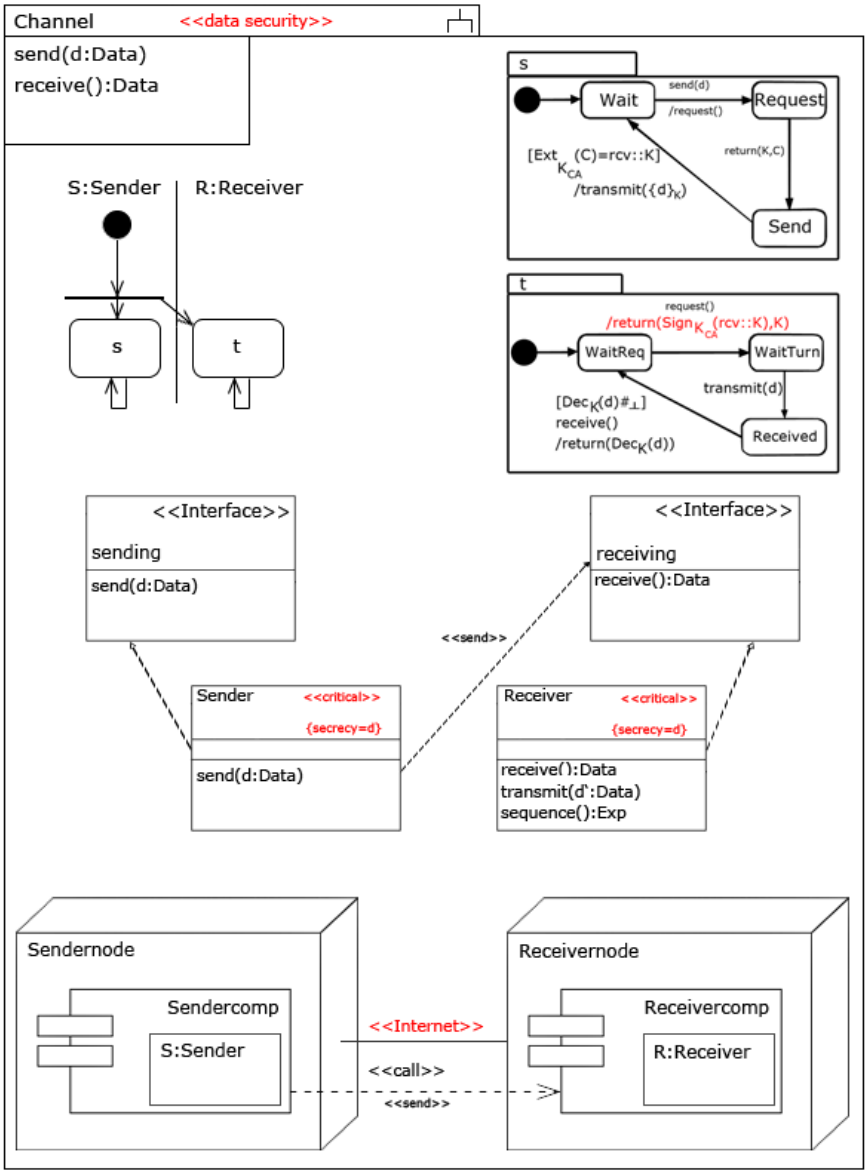
Dabei sei E eine Nachricht und K ein Schlüssel.

- $\forall E, K : Dec_K(\{E\}_{K^{-1}}) = \{Dec_{K^{-1}}(E)\}_K$
- $\forall E_1, E_2, E_3 : tail(E_1 :: head(E_2 :: E_3)) = E_2.$
- $\forall E, K : Ext_K(Dec_{K^{-1}}(E)) = E.$

1.2 Geben Sie für den folgenden Satz den entsprechenden kryptografischen Ausdruck an. (1 Punkt)

Eine Nachricht E_2 wird an die Nachricht E_1 gehängt. Danach wird für das Ergebnis eine Signatur mit dem Schlüssel K_1 erzeugt und ebenfalls an die Nachricht angehängt. Das Resultat wird dann mit dem Schlüssel K_2 verschlüsselt. Bevor die Nachricht verschickt wird, wird dieser noch der Header E_3 vorangestellt. Die gesamte Nachricht wird dann mit der Methode `send()` verschickt.

2 Kryptobasierte Protokolle



2.1 ~~Zeichne den regulären Protokollablauf (d.h. ohne Angriff) des Protokolls~~ aus der Abbildung als Sequenzdiagramm. (2 Punkte)

2.2 Angenommen, der Angreifer kommt in Besitz des zum Schlüssel $\{K\}_{CA}$ gehörenden vertraulichen Signaturschlüssels der Certification Authority. Wie kann er damit in Besitz des zu übertragenden Geheimnisses d kommen? (2 Punkte)

2.3 Zeichne den Angriffsablauf als Sequenzdiagramm. (2 Punkte)