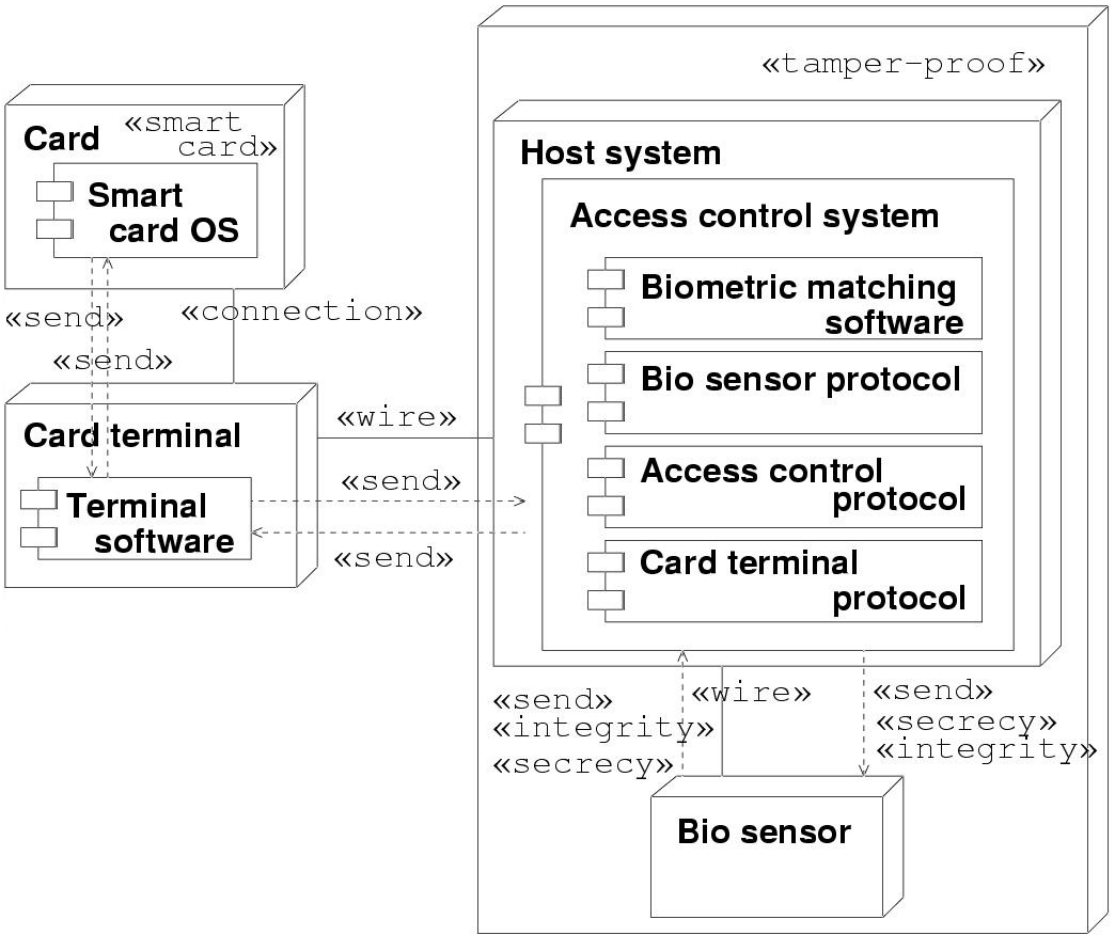
technische universität dortmund

Prof. Dr. Jan Jürjens, Christian Wessel
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
Modellbasierte Softwaretechniken
für sichere Systeme – 12.06.2012

Modellbasierte Softwaretechniken für sichere Systeme - Übung 9

1 Sicherheit beim Smartcard-Protokoll

Das folgende Szenario beschreibt ein System zur biometrischen Authentifizierung.



~~1.1 Erklären Sie die in dem Modell modellierten Sicherheitsmaßnahmen (1 Punkt)~~

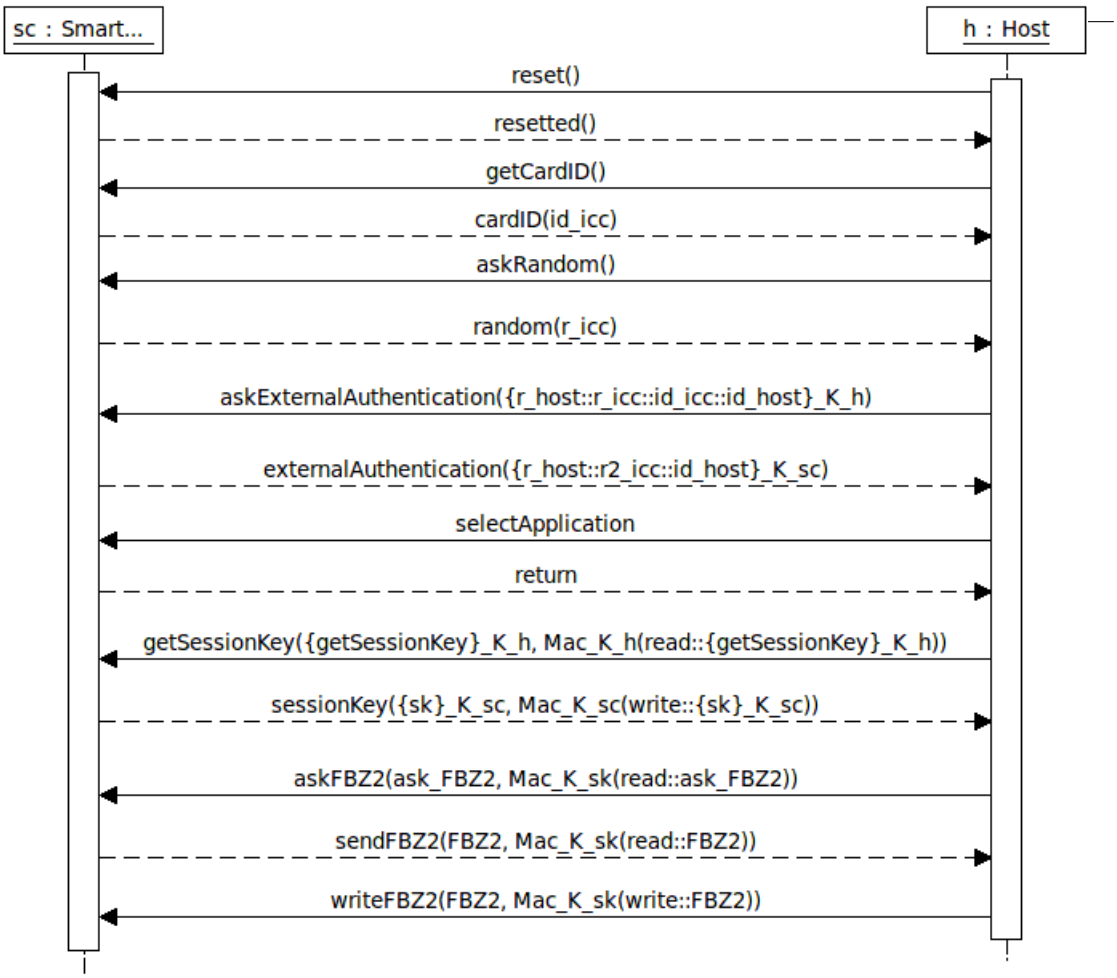
1.2 An welchen Stellen existieren in dem Modell Schwachstellen, die das System angreifbar machen und welche sind das? (1 Punkt)

1.3 Wie könnte man diese Schwachstellen verbessern, sodass das System sicherer wird? (1 Punkt)

2 Smartcard-Protokollanalyse

Betrachten Sie den folgenden Ausschnitt der Kommunikation eines Lesegerätes mit einer Smartcard in Form eines Sequenzdiagramms. Nachdem das Lesegerät die Karte initialisiert hat und diese dementsprechend geantwortet hat, beginnt der Nachrichtenaustausch. Dafür werden als erstes die ID der Karte und eine von ihr generierte Zufallszahl übertragen. Daran schließt sich die Authentifizierung an und der Austausch eines Sitzungsschlüssels an Fehlversuche werden im FBZ1 gespeichert und die Weiterführung nach einer gewissen Anzahl fehlgeschlagener Versuche abgebrochen. Ansonsten werden Daten zwischen der Karte und dem Lesegerät verschlüsselt ausgetauscht. Bei der Verschlüsselung handelt es sich um eine symmetrische Verschlüsselung mit K_h = K_sc. Der Zähler FBZ2 begrenzt die Versuche der biometrischen Verifikation. Bei der Abfrage des Zählers durch das Lesegerät wird dieser von der Karte ausgelesen, dekrementiert und wieder auf der Karte gespeichert. Dabei seien die Bezeichner wie folgt belegt:

- id_icc = Vom Host empfangene ID der Karte
- r_icc = Vom Host empfangene Zufallszahl der Karte
- r_host = Vom Host übertragene Zufallszahl des Hosts
- id_host = Vom Host übertragene ID des Hosts
- K_h = Schlüssel des Hosts
- K_sc = Schlüssel der Karte
- sk = Sitzungschlüssel
- FBZ1 = Fehlbenutzungszähler der Authentifizierung
- FBZ2 = Fehlbenutzungszähler der biometrischen Verifikation



2.1 Was ist die Funktion der Zufallszahl r_host im Protokoll? (1 Punkt)

2.2 Welcher Angriff ist möglich, falls das Protokoll nicht die Übertragung einer Zufallszahl vom Lesegerät vorsehen würde? (1 Punkt)

2.3 Skizzieren Sie den Angriff als Sequenzdiagramm (2 Punkte)

2.4 Ist diese Art von Angriff auch möglich wenn das Protokoll auf die Benutzung von r_icc verzichten würde? Begründen Sie Ihre Antwort. (1 Punkt)

2.5 Welche Art von Angriff ist möglich, wenn der Angreifer den symmetrischen Schluessel K_C = K_H kennt? (1 Punkt)

2.6 Welcher Angriff ist möglich, falls der Angreifer den Sitzungschlüssel sk kennt? (1 Punkt)