TRIPLEX: Tool for the analysis of privacy aspects of mobile identity protocols

TU/e-SEC
Goal / How to

- Tool for the analysis of privacy aspects of mobile identity protocol
  - analyse the communication between parties
  - validate privacy properties of identification systems and protocols

- We developed a framework (TRIPLEX) which allows
  - modelling identification protocols
  - stating/analysing privacy properties
  - capturing the knowledge of a single agent or a coalition of agents after the execution of one or more given protocols
Case study: ParelSnoer initiative

- Roles
  - Hospital
  - Central Infrastructure
  - Researcher
  - Patient
- Protocol Collect
  - Hospital sends to central infrastructure: h(bsn), d1, d2, d3
- Protocol Distribute
  - Central infrastructure sends to researcher: h(h(bsn), researcherID), d1, d2
- Test:
  - 2 protocol sessions for each protocol
  - 2 hospitals: umc1, umc2
  - 1 central infrastructure: ci
  - 1 researcher: r
  - 1 patient: u
TRIPLEX

**Abstract**

protocol(s)

**Scenario**

Initial knowledge

**Protocol instance**

Coalition graph

Analysis

Collect

\[ \text{ip[umc]} \rightarrow \text{ip[ci]}: [\text{hash(bsn[u,ID]}), d1\{u,D\}, d2\{u,D\}, d3\{u,D\}] \]

Distribute

\[ \text{ip[ci]} \rightarrow \text{ip[r]}: [\text{hash([hash(bsn[u,ID]}, \text{dom[r,ID]})), d1\{u,D\}, d2\{u,D\}] \]
TRIPLEX

Abstract protocol(s)

Scenario

Initial knowledge

Protocol instance

Coalition graph

Analysis
TRIPLEX

Abstract protocol(s)

Scenario

Initial knowledge

Protocol instance

Coalition graph

Analysis
TRIPLEX

Abstract protocol(s)

Scenario

Initial knowledge

Protocol instance

Coalition graph

Analysis
TRIPLEX

Abstract protocol(s)

Scenario

Initial knowledge

Protocol instance

Coalition graph

Analysis
Abstract protocol(s)

Scenario

Initial knowledge

Protocol instance

Coalition graph

Analysis