Analyzing NR Protocols

Automatic Methods for Analyzing Non-Repudiation Protocols with an Active Intruder

Francis Klay & Laurent Vigneron

France Telecom R&D — *LORIA, Nancy University*

AVOTE, Cachan, Sept. 12, 2008

Outline

Introduction

Context:

- Security of communications over an open network (wireless or not)
- Handled at software level by cryptographic protocols

Model The Dolev-Yao model which is a logical model (not a computational one).

Standard properties intensively studied:

- Secrecy
- Authentication

Efficient analysis methods and automatic tools already exist for several years

Some security properties are rarely considered:

- Non-repudiation
- Fair exchange

What is non-repudiation?

- Impossibility to deny participation to the communication

What is the role of non-repudiation protocols?

- To generates evidences of participation to the protocol
  Easy!... by digital signatures for example
- But, need of **fairness**: reciprocity and synchronization of non-repudiation
  Much more difficult: a trusted third party (TTP) is needed for fair exchanges

Properties of a Non-Repudiation Protocol and Evidences
Roughly speaking given a session where A sends M to B.

- *non-repudiation of receipt*: if A gets the set of receiving evidences of M by B then B has effectively received M.
- *non-repudiation of origin*: if B gets the set of sending evidences of M by A then A has effectively send M for B.
- *fairness* (also called *strong fairness*): at the protocol end either A and B get their evidences sets, or none of them has any valuable information.
- *timeliness*: whatever happens during the protocol run, all participants can reach a state that preserves fairness, in a finite time.

Non-Repudiation Protocols

Kinds of fair non-repudiation protocols with TTP

- *With full involvement of a TTP:* used as delivery agent of evidences
  Problem: strong activity of the TTP; may be a bottleneck
  Example: Fair Zhou-Gollmann protocol (light TTP)
- *Optimistic protocols:* use of a TTP only if needed
  Based on the use of several protocols
  Permits each party to complete its protocol, even in case of problem
  Example: Cederquist-Corin-Dashti protocol
- *Transparent TTP* have been introduced (impossible to deduce if the TTP was involved from the evidences)
  Example: S.Kremer & 0.Markowitch 2001

Example: the Fair Zhou-Gollmann Protocol

A simple protocol for guaranteeing the fair exchange of a message between two agents; involves a TTP.

History of this protocol:

- Presented by Zhou and Gollmann in 1996
- Several analyzes by ZG, Schneider, Bella-Paulson,. . .
- First attack found by Gürgens & Rudolph in 2003
- *but still a good example for practicing*

The FairZG Protocol

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

At the end: A and B know M, and can prove the participation of each other to the communication

FairZG Protocol: Properties

Non-repudiation of origin with the evidences set for B:

$$\{NRO, ConK\} = \{\{fNRO.B.L.\{M\}_K\}_{inv(Ka)}, \{fCON.A.B.L.K\}_{inv(Kttp)}\}$$

Non-repudiation of receipt with the evidences set for A:

$$\{NRR, ConK\} = \{\{fNRR.A.L.\{M\}_K\}_{inv(Kb)}, \{fCON.A.B.L.K\}_{inv(Kttp)}\}$$

Fairness:
at the end of the protocol run, either A and B have both their evidences, or none of them has them.

Hypothesis:
Evidences are supposed to be correctly defined.

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Prop 1: If $auth(B, A, NRO)$, $auth(TTP, A, SubK)$ and $auth(B, TTP, ConK)$, then $NRO_B(A)$ is valid.

Non-Repudiation as authentication

As non-repudiation is a form of authentication, we try to translate the non-repudiation of origin as authentication

Evidences set: $\mathcal{NRO}_{\mathcal{B}}(A) = \{NRO, ConK\}$

1. $A \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$ — for $\{M\}_K$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Ka)}$
2. $B \rightarrow A$: $fNRR.A.L.NRR$
   where $NRR = \{fNRR.A.L.\{M\}_K\}_{inv(Kb)}$
3. $A \rightarrow TTP$: $fSUB.B.L.K.SubK$ — for K
   where $SubK = \{fSUB.B.L.K\}_{inv(Ka)}$

4a. $B \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$ — for K
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

4b. $A \leftrightarrow TTP$: $fCON.A.B.L.K.ConK$

Prop 1: If $auth(B, A, NRO)$, $auth(TTP, A, SubK)$ and $auth(B, TTP, ConK)$, then $NRO_B(A)$ is valid.

Limitations of this Approach

Similarly for the non-repudiation of receipt we get:

Prop 2: If $auth(A, B, NRR)$, $auth(A, TTP, ConK)$ and $auth(B, TTP, ConK)$, then $NRR_A(B)$ is valid.

Limitations of this Approach

- Handling dishonnest agents is difficult in tools since they can generate request/witness as they want.
- Optimistic non-repudiation protocols include sub-protocols like *abort* or *resolve*. This non-deterministic context implies at least a disjunction of distinct authentications.

Consequence: non-repudiation as authentication does not seem to be the simplest way to handle non repudiation.

Non-Repudiation as Agents Knowledge

- **Idea:** to be able to check if an agent knows its evidences
- **Mean:** to annotate the protocol with a predicate $aknows(t)$, for asserting when an agent knows or can deduce t (here t is an evidence part).
- **Properties:** to describe properties like NR, we use LTL formulas combining *aknows* and *deduce* predicates.

Results

Th 1: Given a non-repudiation service of receipt for A against B about a message M with the set of evidences $\mathcal{NRR}_{\mathcal{A}}(\mathcal{B})$. If at the session end the following formula is true then the non-repudiation of receipt is valid.

$$\begin{array}{lcl} aknows(A, \mathcal{NRR}_{\mathcal{A}}(\mathcal{B})) & \Longrightarrow & aknows(B, M) \\ deduce(A, \mathcal{NRR}_{\mathcal{A}}(\mathcal{B})) & \Longrightarrow & aknows(A, \mathcal{NRR}_{\mathcal{A}}(\mathcal{B})) \end{array}$$

Remark:

- $\mathcal{NRR}_{\mathcal{A}}(\mathcal{B})$ needs "to depend" on M (well-formed evidences set).

Results

Th 2:
Given A and B playing in the same session of a protocol P with valid NRR and NRO services. P is fair iff:

$$aknows(A, \mathcal{NRO}_{\mathcal{B}}(\mathcal{A})) \iff aknows(A, \mathcal{NRR}_{\mathcal{A}}(\mathcal{B}))$$

Remark:

- We give a more general result, for any non-repudiation service.

FairZG Protocol: Analysis

Two sessions between an intruder Ai and B, using the same TTP.

3. $Ai \rightarrow TTP$: $fSUB.B.L.K.SubK$
   where $SubK = \{fSUB.B.L.K\}_{inv(Kai)}$
5. $Ai \leftrightarrow TTP$: $fCON.Ai.B.L.K.ConK$
   where $ConK = \{fCON.A.B.L.K\}_{inv(Kttp)}$

Ai waits for the TTP retention timeout.

1. $Ai \rightarrow B$: $fNRO.B.L.\{M\}_K.NRO$
   where $NRO = \{fNRO.B.L.\{M\}_K\}_{inv(Kai)}$
2. $B \rightarrow Ai$: $fNRR.Ai.L.NRR$
   where $NRR = \{fNRR.Ai.L.\{M\}_K\}_{inv(Kb)}$

- Now Ai has its evidences set $\{NRR, ConK\}$
- But B can no more get $ConK$ from the TTP to build its evidences set $\{NRO, ConK\}$

Remark: The previous attack (Gürgens & Rudolph in 2003) needs no retention on the TTP at the session end.

Conclusion

- We have also studied a more complex protocol, CCD, discovering two attacks.
- We give a very simple procedure to handle non-repudiation protocols for a bounded number of sessions.
- In future works we will take care of the juge.