Formalizing and Analyzing the Needham-Schroeder Symmetric-Key Protocol by Rewriting

Monica Nesi
Giuseppina Rucci

Dipartimento di Informatica
Università di L'Aquila (Italy)

Protocol Verification

- Aim: formally prove properties of security protocols (e.g. authentication, secrecy or confidentiality, freshness, ...)
- Rewriting techniques and strategies
- Case studies
  - the Needham-Schroeder Public-Key protocol (NSPK)
  - the Needham-Schroeder Symmetric-Key protocol (NSSK)

Related Work

- Model checking
  - FDR (Lowe 1996)
  - Murphi (Mitchell-Mitchell-Stern 1997) . . .
- Theorem proving
  - NRL (Meadows 1996)
  - Isabelle (Paulson 1997, 1998, . . .)
  - SPASS (Weidenbach 1999) . . .

Related Work

- Rewriting techniques and strategies
  - ELAN (Cirstea 2001)
  - Maude (Denker-Meseguer-Talcott 1998)
  - CASRUL (Jacquemard-Rusinowitch-Vigneron 2000) . . .
- Rewriting + abstract interpretation (Monniaux 1999)

Related Work

- Rewriting + tree automata in Timbuk (Genet-Viet Triem Tong 2001)
- Combination of different approaches
  - the combination of Genet-Klay's approximation technique and Paulson's inductive method (Oehl-Sinclair 2001, 2002)
  - AVISPA project

Outline of the Talk

- The approximation technique by Genet and Klay
- The formalization for NSSK (insecure version) through rewrite systems and tree automata
- The basic ingredients of the rewriting strategy

Outline of the Talk

- The rewriting strategy and its properties
- A verification example: authentication attacks in insecure NSSK
- Conclusions + current and future work

Approximation Technique

Aim: finding that there are no attacks on a protocol (Genet-Klay 2000).

- The protocol is operationally specified by a TRS $\mathcal{R}$.
- The initial set E of communication requests and an intruder's initial knowledge are described through a tree automaton $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) \supseteq E$.

Approximation Technique

- The property p to be proved is given through a tree automaton $\mathcal{A}_{\overline{p}}$ that models the negation of p.
- The approximation technique builds an over-approximation of the set $\mathcal{R}^*(E)$ of all $\mathcal{R}$-descendants of the set E.
- Result: an approximation automaton $\mathcal{T}_{\mathcal{R}}\uparrow(\mathcal{A})$ such that $\mathcal{L}(\mathcal{T}_{\mathcal{R}}\uparrow(\mathcal{A})) \supseteq \mathcal{R}^*(E)$.

Approximation Technique

A finite number of tree automata $\mathcal{A}_i = \langle \mathcal{F}, \mathcal{Q}, \mathcal{Q}_f, \Delta_i \rangle$ is built as follows:

1. $\mathcal{A}_0 = \mathcal{A}$;
2. $\mathcal{A}_{i+1}$ is constructed from $\mathcal{A}_i$ by computing a critical pair between a rule in $\mathcal{R}$ and the transitions in Δ_i. The rule derived from the critical pair is a new transition that is normalized using an approximation function γ and then added to Δ_i, thus yielding Δ_{i+1}. It follows that $\mathcal{L}(\mathcal{A}_i) \subset \mathcal{L}(\mathcal{A}_{i+1})$.

Approximation Technique

Step 2 is repeated until an automaton $\mathcal{A}_k$ is obtained such that $\mathcal{L}(\mathcal{A}_k) \supseteq \mathcal{R}^*(\mathcal{L}(\mathcal{A}_0))$, i.e. $\mathcal{L}(\mathcal{A}_k) \supseteq \mathcal{R}^*(E)$.

- Quality of the approximation depends on γ.
- Reachability properties on $\mathcal{R}$ and E are proved by checking whether

$$\mathcal{L}(\mathcal{T}_{\mathcal{R}}\uparrow(\mathcal{A})) \cap \mathcal{L}(\mathcal{A}_{\overline{p}}) = \emptyset.$$

Empty intersection means that property p is satisfied.

Our Approach

As in Genet-Klay's approximation technique,

- the protocol is operationally specified by a TRS $\mathcal{R}$
- the intruder's initial knowledge is described through a tree automaton $\mathcal{A}$

The approximation technique is a particular completion process using an approximation function.

Our Approach

- Aim: prove or disprove properties.
- No approximation function.
- Idea: rewriting strategy simulating the critical pairs computed in the completion process in a bottom-up manner.
- Based on a rewriting strategy for dealing with the divergence of completion (Inverardi-Nesi 1992, 1996).

The NSSK Protocol

Given agents A and B and a server S, the NSSK protocol can be described as follows:

$$
\begin{array}{lrcl}
1. & A \longrightarrow S & : & A, B, N_A \\
2. & S \longrightarrow A & : & \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \\
3. & A \longrightarrow B & : & \{K_{AB}, A\}_{K_{BS}} \\
4. & B \longrightarrow A & : & \{N_B\}_{K_{AB}} \\
5. & A \longrightarrow B & : & \{N_B - 1\}_{K_{AB}}
\end{array}
$$

Insecure version!

The NSSK Protocol

Authentication attack (Denning-Sacco 1981):
Hp: an intruder has recorded session (i) and the key K'_{AB}, created in session (i), has been compromised and is known to the intruder.

Session (ii) can develop as follows:

$$\begin{array}{lllll}
ii.1. & A \longrightarrow S & : & A, B, N_A \\
ii.2. & S \longrightarrow A & : & \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \\
ii.3. & I(A) \longrightarrow B & : & \{K'_{AB}, A\}_{K_{BS}} \\
ii.4. & B \longrightarrow I(A) & : & \{N_B\}_{K'_{AB}} \\
ii.5. & I(A) \longrightarrow B & : & \{N_B - 1\}_{K'_{AB}}
\end{array}$$

Formalizing the Protocol

A protocol is formalized through a rewrite system $\mathcal{R} = \mathcal{R}_P \cup \mathcal{R}_I$, where

- $\mathcal{R}_P$ describes the steps of the protocol and the properties to be verified,
- $\mathcal{R}_I$ defines an intruder's ability of decomposing and decrypting messages.

A TRS $\mathcal{R}_P$ for NSSK

$$goal(agt(a), agt(b), r(j)) \tag{1}$$
$$\rightarrow mesg(agt(a), serv(S), cons(N(agt(a), serv(S), r(j)), cons(agt(a), agt(b))), r(j))$$

$$mesg(a_2, a_3, cons(N(agt(a), serv(S), r(j)), cons(agt(a), agt(b))), r(j)) \tag{2}$$
$$\begin{aligned}\rightarrow mesg(&serv(S), agt(a),\\ &encr(ltk(agt(a), serv(S)), serv(S),\\ &\quad cons(N(agt(a), serv(S), r(j)),\\ &\quad\quad cons(agt(b),\\ &\quad\quad\quad cons(sk(agt(a), agt(b), r(j)),\\ &\quad\quad\quad\quad encr(ltk(agt(b), serv(S)), serv(S),\\ &\quad\quad\quad\quad\quad cons(sk(agt(a), agt(b), r(j)), agt(a))))))),\\ &r(j))\end{aligned}$$

A TRS $\mathcal{R}_P$ for NSSK

$$
\begin{aligned}
& mesg(a_4, a_5, \\
& \qquad encr(ltk(agt(a), serv(S)), a_3, \\
& \qquad\quad cons(N(agt(a), serv(S), r(j)), \\
& \qquad\qquad cons(agt(b), \\
& \qquad\qquad\quad cons(sk(agt(a), agt(b), r(i_1)), \\
& \qquad\qquad\qquad encr(ltk(agt(b), serv(S)), a_1, \\
& \qquad\qquad\qquad\quad cons(sk(agt(a), agt(b), r(i_2)), agt(a))))))), \\
& \qquad r(j)) \\
& \to mesg(agt(a), agt(b), \\
& \qquad\quad encr(ltk(agt(b), serv(S)), a_1, cons(sk(agt(a), agt(b), r(i_2)), agt(a))), \\
& \qquad\quad r(j))
\end{aligned}
\tag{3}
$$

A TRS $\mathcal{R}_P$ for NSSK

$$\begin{aligned}
&mesg(a_6, a_7, \\
&\qquad encr(ltk(agt(b), serv(S)), a_5, cons(sk(agt(a), agt(b), r(i)), agt(a))), \\
&\qquad r(j)) \\
&\to mesg(a_7, a_6, \\
&\qquad\quad encr(sk(agt(a), agt(b), r(i)), a_7, N(agt(b), agt(a), r(j))), \\
&\qquad\quad r(j))
\end{aligned} \tag{4}$$

$$\begin{aligned}
&mesg(a_8, a_6, \\
&\qquad\quad encr(sk(agt(a), agt(b), r(i)), a_7, N(agt(b), agt(a), r(j))), \\
&\qquad\quad r(j)) \\
&\to mesg(a_6, a_8, \\
&\qquad\quad encr(sk(agt(a), agt(b), r(i)), a_6, N(agt(b), agt(a), r(j))), \\
&\qquad\quad r(j))
\end{aligned} \tag{5}$$

A TRS $\mathcal{R}_P$ for NSSK

$$
\begin{aligned}
& mesg(a_8, a_6, \\
& \qquad encr(sk(agt(a), agt(b), r(i)), a_7, N(agt(b), agt(a), r(j))), \\
& \qquad r(j)) \\
& \rightarrow c_{init}(agt(a), agt(b), a_7, r(j))
\end{aligned} \tag{6}
$$

$$
\begin{aligned}
& mesg(a_{10}, a_6, \\
& \qquad encr(sk(agt(a), agt(b), r(i)), a_9, N(agt(b), agt(a), r(j))), \\
& \qquad r(j)) \\
& \rightarrow c_{resp}(agt(b), agt(a), a_9, r(j))
\end{aligned} \tag{7}
$$

A TRS $\mathcal{R}_{\mathcal{I}}$ for NSSK

$$cons(x, y) \to x \tag{8}$$

$$cons(x, y) \to y \tag{9}$$

$$encr(sk(agt(0), agt(x), w), y, z) \to z \tag{10}$$

$$encr(sk(agt(x), agt(0), w), y, z) \to z \tag{11}$$

$$encr(sk(agt(s(x_1)), agt(x), w), y, z) \to z \tag{12}$$

$$encr(sk(agt(x), agt(s(x_1)), w), y, z) \to z \tag{13}$$

$$encr(ltk(agt(0), serv(S)), y, z) \to z \tag{14}$$

$$encr(ltk(agt(s(x_1)), serv(S)), y, z) \to z \tag{15}$$

$$mesg(x, y, z, w) \to z \tag{16}$$

The Intruder's Knowledge

A tree automaton $\mathcal{A} = \langle \mathcal{F}, \mathcal{Q}, \mathcal{Q}_f, \Delta \rangle$, where $\mathcal{Q}_f = \{q_f\}$ and Δ is as follows:

$$
\begin{array}{lll}
0 \longrightarrow q_{int} & & \\
s(q_{int}) \longrightarrow q_{int} & agt(q_{int}) \longrightarrow q_{agtI} & 0 \longrightarrow q_0 \\
A \longrightarrow q_A & agt(q_A) \longrightarrow q_{agtA} & s(q_0) \longrightarrow q_1 \\
B \longrightarrow q_B & agt(q_B) \longrightarrow q_{agtB} & r(q_0) \longrightarrow q_{r_0} \\
S \longrightarrow q_S & serv(q_S) \longrightarrow q_{serv} & r(q_1) \longrightarrow q_{r_1}
\end{array}
$$

The Intruder's Knowledge

communication requests

$$goal(q_{agtA}, q_{agtB}, q_f) \longrightarrow q_f$$

$$goal(q_{agtB}, q_{agtA}, q_f) \longrightarrow q_f$$

$$goal(q_{agtA}, q_{agtI}, q_f) \longrightarrow q_f$$

$$goal(q_{agtB}, q_{agtI}, q_f) \longrightarrow q_f$$

$$goal(q_{agtI}, q_{agtI}, q_f) \longrightarrow q_f$$

$$goal(q_{agtA}, q_{agtA}, q_f) \longrightarrow q_f$$

$$goal(q_{agtB}, q_{agtB}, q_f) \longrightarrow q_f$$

$$goal(q_{agtI}, q_{agtA}, q_f) \longrightarrow q_f$$

$$goal(q_{agtI}, q_{agtB}, q_f) \longrightarrow q_f$$

The Intruder's Knowledge

intruder's initial knowledge

$$agt(q_{int}) \longrightarrow q_f$$

$$agt(q_A) \longrightarrow q_f$$

$$agt(q_B) \longrightarrow q_f$$

$$serv(q_S) \longrightarrow q_f$$

$$r(q_0) \longrightarrow q_f$$

$$r(q_1) \longrightarrow q_f$$

$$sk(q_{agtI}, q_{agtI}, q_f) \longrightarrow q_f$$

$$sk(q_{agtI}, q_{agtA}, q_f) \longrightarrow q_f$$

$$sk(q_{agtI}, q_{agtB}, q_f) \longrightarrow q_f$$

$$ltk(q_{agtI}, q_{serv}) \longrightarrow q_f$$

The Intruder's Knowledge

intruder's initial knowledge

$$mesg(q_f, q_f, q_f, q_f) \longrightarrow q_f$$

$$cons(q_f, q_f) \longrightarrow q_f$$

$$encr(q_f, q_{agtI}, q_f) \longrightarrow q_f$$

$$N(q_{agtI}, q_{agtI}, q_f) \longrightarrow q_f$$

$$N(q_{agtI}, q_{agtA}, q_f) \longrightarrow q_f$$

$$N(q_{agtI}, q_{agtB}, q_f) \longrightarrow q_f$$

$$N(q_{agtI}, q_{serv}, q_f) \longrightarrow q_f$$

Strategy: Basic Ingredients

- Simulation of critical pairs through a bottom-up strategy
- Expansion of terms
- Well-formedness of terms (to ensure termination of the expansion process)
- Recognizability by the intruder

Expansion

$$expansion(t, \mathcal{R}) =$$
$$\{s = \sigma(t[l]_p) \mid \exists\, l \rightarrow r \in \mathcal{R},\ p \in Pos'(t)\ and\ \sigma = mgu(t|_p, r)\}.$$

Expansion step = narrowing step with a reversed rule of $\mathcal{R}$.

Expansion

Possible introduction of occurrences of “new” variables in s:

- implicitly universally quantified variables
- instantiated by means of a finite set of ground terms $Inst$, thus getting the instance set $\mathcal{I}(t, Inst) = \{\sigma(t) \mid \sigma : Var(t) \rightarrow Inst\}$.

In NSSK, $Inst =$ $\{A, B, agt(A), agt(B), serv(S), agt(0), 0, s(0)\}$.

Well-Formedness

Intuition:
a term t is well-formed if it "agrees" with the syntactic structure of $\mathcal{R}$.

Examples:
(i) $t_1 = N(agt(a_1), agt(a_2), w)$ is well-formed for any variables or agent labels a_1, a_2.
(ii) $t_2 = N(agt(a_1), sk(agt(a_2), agt(a_3), w'), w)$ is not well-formed.

Well-Formedness

A term $t \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ is well-formed $wf(t)$ if

(i) $t \in \mathcal{X} \cup \mathcal{F}^0$

or (ii) $t = f(t_1, \ldots, t_n)$ with $f \in \mathcal{F}^n$ ($n > 0$)

and either $t_i \in \mathcal{X}$ or t_i satisfies the following conditions based on f ($i = 1, \ldots, n$):

- $f = agt$ and $t_1 \in L_{agt}$;
- $f = serv$ and $t_1 = S$;
- $f = r$ and $t_1 \in \mathbb{N}$;

Well-Formedness

- $f = goal$,
  $root(t_1) = root(t_2) = agt$, $root(t_3) = r$
  and $wf(t_i)$ for $i = 1, 2, 3$;
- $f = mesg$,
  $root(t_1), root(t_2) \in \{agt, serv\}$,
  $root(t_3) \in \{encr, cons\}$, $root(t_4) = r$
  and $wf(t_i)$ for $i = 1, 2, 3, 4$;
- $f = encr$,
  $root(t_1) \in \{sk, ltk\}$, $root(t_2) \in \{agt, serv\}$,
  $root(t_3) \in \{cons, N\}$
  and $wf(t_i)$ for $i = 1, 2, 3$;

Well-Formedness

- $f = ltk$,
  $root(t_1) = agt$, $root(t_2) = serv$
  and $wf(t_i)$ for $i = 1, 2$;
- $f = sk$,
  $root(t_1) = root(t_2) = agt$, $root(t_3) = r$
  and $wf(t_i)$ for $i = 1, 2, 3$;
- $f = cons$,
  $root(t_i) \in \{N, agt, sk, cons, encr\}$
  and $root(t_i)$ for $i = 1, 2$;

Well-Formedness

- $f = N$,
  $root(t_1), root(t_2) \in \{agt, serv\}$, $root(t_3) = r$
  and $wf(t_i)$ for $i = 1, 2, 3$;
- $f \in \{c_{init}, c_{resp}\}$,
  $root(t_1) = root(t_2) = root(t_3) = agt$,
  $root(t_4) = r$
  and $wf(t_i)$ for $i = 1, 2, 3, 4$.

Recognizability

A term t is recognizable by the intruder if q_f can be derived from t using Δ.

Proof system $\vdash_{\mathcal{A}}$ for recognizability:

$$\frac{t \xrightarrow{*}_{\Delta} q \quad q \in \{q_f, q_{agtI}\}}{t \vdash_{\mathcal{A}} q} \qquad \frac{t_1 \vdash_{\mathcal{A}} q_f \quad t_2 \vdash_{\mathcal{A}} q_f}{cons(t_1, t_2) \vdash_{\mathcal{A}} q_f}$$

$$\frac{t_1 \vdash_{\mathcal{A}} q_f \quad t_2 \vdash_{\mathcal{A}} q_f \quad t_3 \vdash_{\mathcal{A}} q_f \quad t_4 \vdash_{\mathcal{A}} q_f}{mesg(t_1, t_2, t_3, t_4) \vdash_{\mathcal{A}} q_f} \qquad \frac{t_1 \vdash_{\mathcal{A}} q_{agtI} \quad t_2 \vdash_{\mathcal{A}} q_f \quad t_3 \vdash_{\mathcal{A}} q_f}{N(t_1, t_2, t_3) \vdash_{\mathcal{A}} q_f}$$

$$\frac{t_1 \vdash_{\mathcal{A}} q_f \quad t_2 \vdash_{\mathcal{A}} q_{agtI} \quad t_3 \vdash_{\mathcal{A}} q_f}{encr(t_1, t_2, t_3) \vdash_{\mathcal{A}} q_f} \qquad \frac{t_1 \vdash_{\mathcal{A}} q_{agtI} \quad t_2 \vdash_{\mathcal{A}} q_f \quad t_3 \vdash_{\mathcal{A}} q_f}{sk(t_1, t_2, t_3) \vdash_{\mathcal{A}} q_f}$$

Recognizability

$$\overline{rec}(t) = \emptyset \qquad if \;\; t \vdash_{\mathcal{A}} q_f$$

otherwise

$$\overline{rec}(t) = \{t_i \;\mid\; t = \mathcal{C}[t_i] \; and \; t_i \not\vdash_{\mathcal{A}} q_f\}$$

subterms labelling the unsolved leaves of the proof tree of t.

The Strategy

Input:

- the rewrite system $\mathcal{R} = \mathcal{R}_P \cup \mathcal{R}_I$,
- the predicate wf,
- the instantiation set $Inst$,
- the intruder's initial knowledge Δ in $\mathcal{A}$,
- the well-formed term t_{in} describing the property under consideration.

The Strategy

Definition: a set of inference rules over configurations.

Configurations: (finite) sets of well-formed terms or elements of the set $\{success, failure\}$.

Initial configuration: $E_0 = \{t_{in}\}$.

Inference Rules

Well-formed Expansion: $$\frac{t \in E \quad expansion(t, \mathcal{R}) = E'}{E \setminus \{t\} \cup \{t' \in E' \mid wf(t')\}}$$

Failure: $$\frac{E = \emptyset}{failure}$$

Success$_1$: $$\frac{t \in E \quad \exists t'.subterm(t, t') \ \wedge \ root(t') = goal}{success}$$

Inference Rules

$$\text{Cut: } \frac{t \in E \quad expansion(t, \mathcal{R}_P) = \emptyset \quad subterm(t, t_{in}) \qquad \exists t'.subterm(t, t') \ \wedge \ root(t') = mesg}{E \setminus \{t\}}$$

$$\text{Success}_2\text{: } \frac{t \in E \quad expansion(t, \mathcal{R}_P) = \emptyset \quad not(subterm(t, t_{in})) \qquad \exists t'.subterm(t, t') \ \wedge \ root(t') = mesg \qquad \mathcal{I}(t, Inst) = E_1 \quad \exists t_1 \in E_1. \overline{rec}(t_1) = \emptyset}{success}$$

Inference Rules

$$\text{Split:}\ \frac{t \in E \quad expansion(t, \mathcal{R}_P) = \emptyset \quad not(subterm(t, t_{in})) \\ \exists t'.subterm(t, t') \ \wedge \ root(t') = mesg \\ \mathcal{I}(t, Inst) = \{t_1, \ldots, t_k\} \quad \forall i.\overline{rec}(t_i) \neq \emptyset}{E \setminus \{t\} \cup \overline{rec}(t_1) \cup \ldots \cup \overline{rec}(t_k)}$$

The rewriting strategy is:

$$((\text{Well-formed Expansion} + \text{Cut})^*. \\ (\text{Failure} + \text{Success}_1 + \text{Success}_2 + \text{Split}))^*$$

Properties of the Strategy

Given $\mathcal{R}$, wf, $Inst$, $\mathcal{A}$ with transitions Δ and $\mathcal{A}_{\overline{p}}$, we have the following (Nesi-Rucci-Verdesca 2003).

Proposition (correctness)
Let $t_{in} \in \mathcal{L}(\mathcal{A}_{\overline{p}})$.
(i) If $\{t_{in}\} \vdash success$, then the transition $t_{in} \rightarrow q_f$ can be generated from critical pairs.
(ii) If $\{t_{in}\} \vdash failure$, then the transition $t_{in} \rightarrow q_f$ cannot be generated from critical pairs.

Properties of the Strategy

Proposition (termination)
The rewriting strategy terminates on any input term $t_{in} \in \mathcal{L}(\mathcal{A}_{\overline{p}})$.

Corollary (completeness)
Let $t_{in} \in \mathcal{L}(\mathcal{A}_{\overline{p}})$.
(i) If the transition $t_{in} \rightarrow q_f$ can be generated from critical pairs, then $\{t_{in}\} \vdash success$.
(ii) If the transition $t_{in} \rightarrow q_f$ cannot be generated from critical pairs, then $\{t_{in}\} \vdash failure$.

Deriving the Attack

$t_{in} = c_{resp}(agt(B), agt(A), agt(0), r(s(0))) \in \mathcal{L}(\mathcal{A}_{\overline{a}})$

By expansion with rules (7), (5) and (4) in $\mathcal{R}_P$, the last three steps of session (ii) are performed backward:

$\{c_{resp}(agt(B), agt(A), agt(0), r(s(0)))\}$

$\vdash \{mesg(a_{10}, a_6,$

$\quad encr(sk(agt(A), agt(B), r(i)), agt(0), N(agt(B), agt(A), r(s(0)))), r(s(0)))\}$

$\vdash \{mesg(a_6, agt(0),$

$\quad encr(sk(agt(A), agt(B), r(i)), a_7, N(agt(B), agt(A), r(s(0)))), r(s(0)))\}$

$\vdash \{mesg(agt(0), a_6,$

$\quad encr(ltk(agt(B), serv(S)), a_5, cons(sk(agt(A), agt(B), r(i)), agt(A))),$

$\quad r(s(0)))\}$

Deriving the Attack

$$\{c_{resp}(agt(B), agt(A), agt(0), r(s(0)))\}$$
$$\vdash \{mesg(agt(0), a_6,$$
$$encr(ltk(agt(B), serv(S)), a_5, cons(sk(agt(A), agt(B), r(i)), agt(A))),$$
$$r(s(0)))\}$$

The last term cannot be further expanded. Using Split, by instantiating with $\sigma = \{agt(B)/a_6, serv(S)/a_5, 0/i\}$ and applying $\overline{rec}$, we have to derive the recognizability of subterm

$$\bar{t} = encr(ltk(agt(B), serv(S)), serv(S), cons(sk(agt(A), agt(B), r(0)), agt(A)))$$

Deriving the Attack

$\bar{t} = encr(ltk(agt(B), serv(S)), serv(S), cons(sk(agt(A), agt(B), r(0)), agt(A)))$

By expansion with rules (16), (3), (2) and finally (1), the first three steps of session (i) are executed, thus obtaining $success$:

$$
\begin{array}{l}
\bar{t} \\
\vdash mesg(x, y, \bar{t}, w) \\
\vdash mesg(a_4, a_5, \\
\quad\quad encr(ltk(agt(A), serv(S)), a_3, \\
\quad\quad\quad cons(N(agt(A), serv(S), r(j)), \\
\quad\quad\quad\quad cons(agt(B), \\
\quad\quad\quad\quad\quad cons(sk(agt(A), agt(B), r(i_1)), \\
\quad\quad\quad\quad\quad\quad encr(ltk(agt(B), serv(S)), serv(S), \\
\quad\quad\quad\quad\quad\quad\quad cons(sk(agt(A), agt(B), r(0)), agt(A))))))), \\
\quad\quad r(j))
\end{array}
$$

Deriving the Attack

$\vdash mesg(a_2, serv(S), cons(N(agt(A), serv(S), r(0)), cons(agt(A), agt(B))), r(0))$

$\vdash goal(agt(A), agt(B), r(0))$

$\vdash success$

Thus, $\bar{t} \to q_f$ and hence $t_{in} \to q_f$.

Lowe's multiplicity attack on NSSK

Using Split with substitution
$\sigma' = \{agt(B)/a_6, serv(S)/a_5, s(0)/i\}$ also derives $success$.

Conclusions

- No approximation function γ
- Property satisfied or not
- Feedback on error location
- Combination of reduction (e.g. narrowing) with deduction (e.g. recognizability)
- Compromise between the full efficiency of the approximation technique and the full power of theorem proving based methods

Conclusions

Need more general criteria for

- formalizing the steps of a protocol and the properties to be checked into rules,
- ensuring the termination of the strategy (well-formedness).

Current and Future Work

- Extension of the properties under consideration
- Application of the approach to other (classes of) protocols
- Implementation of the strategy in a theorem proving environment
- Formalization only based on rewrite systems (no tree automata)