Security Proofs

Monica Nesi

Dipartimento di Informatica
Università di L'Aquila - Italy
Security Protocols

- Dolev-Yao model
- Cryptography
  - Asymmetric/public key
  - Symmetric/shared key
  - Hybrid protocols
- Properties: authentication, freshness, secrecy, type flaws, etc.
- Alice & Bob notation
The NSSK protocol

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

1. \( A \rightarrow S : A, B, N_A \)
2. \( S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \)
3. \( A \rightarrow B : \{K_{AB}, A\}_{K_{BS}} \)
4. \( B \rightarrow A : \{N_B\}_{K_{AB}} \)
5. \( A \rightarrow B : \{N_B - 1\}_{K_{AB}} \)

Insecure version!
The NSSK protocol

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

Session (ii) can develop as follows:

\begin{align*}
\text{ii.1. } & A \rightarrow S : A, B, N_A \\
\text{ii.2. } & S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_K_{BS}\}_K_{AS} \\
\text{ii.3. } & I(A) \rightarrow B : \{K^\prime_{AB}, A\}_K_{BS} \\
\text{ii.4. } & B \rightarrow I(A) : \{N_B\}_K^\prime_{AB} \\
\text{ii.5. } & I(A) \rightarrow B : \{N_B - 1\}_K^\prime_{AB}
\end{align*}
Protocol Verification

- **Aim**: formally prove properties of security protocols (e.g. authentication, secrecy, ...)
- Proof procedures based on rewriting techniques
- Rewrite rules formalizing:
  - protocol steps
  - an intruder's abilities
- Proof strategy based on expansion and reduction of terms
Case Studies

- the Needham-Schroeder Public-Key and Symmetric-Key protocols (NSPK, NSSK)
- the Otway-Rees protocol (OR)
- the Tatebayashi-Matsuzaki-Newman protocol (TMN)
- the Yahalom protocol (version by Burrows-Abadi-Needham)
Outline of the Talk

- The formalization of a protocol (e.g. NSSK) through rewrite systems
- The ingredients of the proof strategy
- The strategy
- A verification example: authentication attacks in insecure NSSK
- Proofs of adaptation of mobile context-aware applications
- Future work inside PaCo?
Formalizing the Protocol

As in the approximation technique (Genet-Klay 2000), a protocol is specified by a TRS $R = R_P \cup R_I$, where

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

\begin{align*}
goal(\text{agt}(a), \text{agt}(b), \text{serv}(x), r(j)) & \quad (1) \\
\rightarrow \text{msg}(\text{agt}(a), \text{serv}(x), \text{cons}(\text{agt}(a), \text{cons}(\text{agt}(b), N(\text{agt}(a), \text{serv}(x), r(j)))), r(j)) \\
\end{align*}

\begin{align*}
\text{msg}(a_2, a_3, \text{cons}(\text{agt}(a), \text{cons}(\text{agt}(b), N(\text{agt}(a), \text{serv}(x), r(j)))), r(j)) & \quad (2) \\
\rightarrow \text{msg}(\text{serv}(x), \text{agt}(a), \\
\text{encr}(\text{ltk}(\text{agt}(a), \text{serv}(x)), \text{serv}(x), \\
\text{cons}(N(\text{agt}(a), \text{serv}(x), r(j)), \\
\text{cons}(\text{agt}(b), \\
\text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(j)), \\
\text{encr}(\text{ltk}(\text{agt}(b), \text{serv}(x)), \text{serv}(x), \\
\text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(j)), \text{agt}(a))))))), \\
r(j))
\end{align*}
A TRS \( R_P \) for NSSK

\[
\begin{align*}
\text{msg}(a_4, a_5, \\
en\text{cr}(\text{ltk}(\text{agt}(a), \text{serv}(x)), a_3, \\
\text{cons}(N(\text{agt}(a), \text{serv}(x), r(j)), \\
\text{cons}(\text{agt}(b), \\
\text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i_1)), \\
en\text{cr}(\text{ltk}(\text{agt}(b), \text{serv}(x)), a_1, \\
\text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i_2)), \text{agt}(a)))),)) \\
r(j)) \\
\rightarrow \text{msg}(\text{agt}(a), \text{agt}(b), \\
en\text{cr}(\text{ltk}(\text{agt}(b), \text{serv}(x)), a_1, \text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i_2)), \text{agt}(a))), \\
r(j))
\end{align*}
\]
A TRS $\mathcal{R}_P$ for NSSK

\begin{align*}
\text{mesg}(a_6, a_7, \text{ & } (4) \\
\quad \text{encr}(\text{ltk}(\text{agt}(b), \text{serv}(x)), a_5, \text{cons}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i)), \text{agt}(a))), \text{ & } r(j)) \\
\rightarrow \text{mesg}(a_7, a_6, \text{ & } r(j)) \\
\text{encr}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i)), a_7, N(\text{agt}(b), \text{agt}(a), r(j))), \text{ & } r(j))
\end{align*}

\begin{align*}
\text{mesg}(a_8, a_6, \text{ & } (5) \\
\quad \text{encr}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i)), a_7, N(\text{agt}(b), \text{agt}(a), r(j))), \text{ & } r(j)) \\
\rightarrow \text{mesg}(a_6, a_8, \text{ & } r(j)) \\
\text{encr}(\text{sk}(\text{agt}(a), \text{agt}(b), r(i)), a_6, p(N(\text{agt}(b), \text{agt}(a), r(j))), \text{ & } r(j))
\end{align*}
A TRS $R_P$ for NSSK

\[\text{mesg}(a_8, a_6,\]
\[
    \text{encr}(sk(\text{agt}(a), \text{agt}(b), r(i)), a_7, N(\text{agt}(b), \text{agt}(a), r(j))),
\]
\[
r(j))
\]
\[
\rightarrow c_{\text{init}}(\text{agt}(a), \text{agt}(b), a_7, r(j))
\]

\[\text{mesg}(a_{10}, a_6,\]
\[
    \text{encr}(sk(\text{agt}(a), \text{agt}(b), r(i)), a_9, p(N(\text{agt}(b), \text{agt}(a), r(j)))),
\]
\[
r(j))
\]
\[
\rightarrow c_{\text{resp}}(\text{agt}(b), \text{agt}(a), a_9, r(j))\]
A TRS $\mathcal{R}_I$ for NSSK

\begin{align*}
\text{cons}(x, y) & \rightarrow x \quad (I_1) \\
\text{cons}(x, y) & \rightarrow y \quad (I_2) \\
\text{encr}(\text{sk}(\text{agt}(0), \text{agt}(x), w), y, z) & \rightarrow z \quad (I_3) \\
\text{encr}(\text{sk}(\text{agt}(x), \text{agt}(0), w), y, z) & \rightarrow z \quad (I_4) \\
\text{encr}(\text{sk}(\text{agt}(s(x_1)), \text{agt}(x), w), y, z) & \rightarrow z \quad (I_5) \\
\text{encr}(\text{sk}(\text{agt}(x), \text{agt}(s(x_1)), w), y, z) & \rightarrow z \quad (I_6) \\
\text{encr}(&\text{ltk}(\text{agt}(0), \text{serv}(x)), y, z) \rightarrow z \quad (I_7) \\
\text{encr}(\text{ltk}(\text{agt}(s(x_1)), \text{serv}(x)), y, z) & \rightarrow z \quad (I_8) \\
\text{mesg}(x, y, z, w) & \rightarrow z \quad (I_9)
\end{align*}
Intruder’s Initial Knowledge

Verification of properties as a process of recognizability of terms by an intruder.

No need of recognizability process ⇒ a set of terms in $R_I$-normal form.

For a symmetric-key protocol, the initial knowledge $IK$ of an intruder $agt(i) (i \in \mathbb{N})$ is

\[
\{ agt(l) \mid l \in L_{agt} \} \cup \{ serv(x) \mid x \in L_{serv} \} \cup \{ r(i) \mid i \in \mathbb{N} \} \cup \\
\{ goal(x, y, z, w) \mid x, y agent, z server, w run \} \cup \\
\{ sk(agt(i), x, w) \mid i \in \mathbb{N}, x agent, w run \} \cup \{ sk(x, agt(i), w) \mid x agent, i \in \mathbb{N}, w run \} \cup \\
\{ ltk(agt(i), serv(x)) \mid i \in \mathbb{N}, x \in L_{serv} \} \cup \{ N(agt(i), x, w) \mid i \in \mathbb{N}, x agent, w run \}
\]
Strategy: Basic Ingredients

- Recognizability of terms by an intruder as reduction into $IK$ by a completion process on $R$ in a bottom-up manner
- Simulation of critical pairs by expansion and reduction of terms
- Well-formedness of terms (to ensure termination of the expansion process)
- Outermost “constrained” reduction in $RI$
Expansion

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

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

Possible introduction of occurrences of “new” (implicitly universally quantified) variables.
Well-Formedness

Intuition:
a term $t$ is **well-formed** (written $\text{wf}(t)$) if it "agrees" with the syntactic structure of $R$.

Examples:
(i) $t_1 = N(\text{agt}(a_1), \text{agt}(a_2), w)$ is well-formed for any agent labels $a_1, a_2$ and protocol run $w$.
(ii) $t_2 = N(\text{agt}(a_1), \text{sk}(\text{agt}(a_2), \text{agt}(a_3), w'), w)$ is not well-formed.
Recognizability

- Backward execution of the protocol (expansion with $R_P$)
- Message decomposition and decryption (reduction with $R_I$ - intruder's analysis)
- Message construction and encryption (expansion with $R_I$ - intruder's synthesis)
The Strategy

Input:

- the rewrite system $\mathcal{R} = \mathcal{R}_P \cup \mathcal{R}_I$,
- the predicate $wf$,
- the well-formed term $t_{in}$ describing the property under consideration.
The Strategy

Definition: a set of inference rules over configurations.

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

Initial configuration: \((E_0, C_0) = (\{t_in\}, \emptyset)\).
Inference Rules

Well-formed Expansion($\mathcal{R}'$):

\[
\frac{t \in E \quad E' = \text{expansion}(t, \mathcal{R}')}{(E \setminus \{t\} \cup \{t' \in E' \mid \text{wf}(t')\}, C \cup \{t\})}
\]

Success:

\[
\frac{t \in E \quad \forall t' \in \mathcal{R}_I-\text{nf}(t). \quad t' \in \text{IK}}{	ext{success}}
\]

Reduction:

\[
\frac{t \in E \quad E' = \{t' \mid t' \in \mathcal{R}_I-\text{nf}(t) \land t' \notin \text{IK} \} \neq \emptyset}{(E \setminus \{t\} \cup E', C \cup \{t\})}
\]
Inference Rules

Failure:

\[
E = \emptyset \\
\frac{}{\text{failure}}
\]

Cut:

\[
t \in E \\
\exists \tilde{t} \in C. \ t \sim \tilde{t} \\
\frac{}{(E \setminus \{t\}, C)}
\]

The proof strategy is:

(Well-formed Expansion(\(\mathcal{R}_P\)). Cut*.
(Failure + Success +
(Reduction. Well-formed Expansion(\(\mathcal{R}_I\))^*)))*
Properties

Correctness (Nesi-Nocera 2006)

(i) If \((\{t_{in}\}, \emptyset) \vdash success\), then there exists a derivation path in \(\mathcal{R}\)

\[
t_{in} = t_0 \overset{\mathcal{R}_P}{\leftrightarrow} t_1 \overset{*}{\rightarrow}_{\mathcal{R}_I} t'_1 \overset{*}{\leftrightarrow}_{\mathcal{R}_P} t_1 \overset{*}{\leftrightarrow}_{\mathcal{R}_I} t_2 \overset{*}{\rightarrow}_{\mathcal{R}_I} t'_2 \overset{*}{\leftrightarrow}_{\mathcal{R}_I} t_2 \overset{*}{\leftrightarrow}_{\mathcal{R}_P} t_3 \ldots \overset{*}{\leftrightarrow}_{\mathcal{R}_P} t_{k-1} \overset{*}{\leftrightarrow}_{\mathcal{R}_P} t_k
\]

for some \(k > 0\) such that for all \(t' \in \mathcal{R}_I - \text{nf}(t_k)\) we have \(t' \in \mathcal{I}K\).

(ii) If \((\{t_{in}\}, \emptyset) \vdash failure\), then there exists no derivation path in \(\mathcal{R}\) for the recognizability of \(t_{in}\).
Properties

Termination
The rewriting strategy terminates on any well-formed input term \( t_{in} \).

Completeness
(i) If there exists a derivation path in \( \mathcal{R} \) for the recognizability of \( t_{in} \), then \( (\{t_{in}\}, \emptyset) \vdash success. \)
(ii) If there exists no derivation path in \( \mathcal{R} \) for the recognizability of \( t_{in} \), then \( (\{t_{in}\}, \emptyset) \vdash failure. \)
Applying the Strategy

\[ t_{in} = c_{resp}(agt(B), agt(A), agt(0), r(j)) \quad j \in \mathbb{N} \]

By Well-formed Expansion with rule (7) in \( R_P \):

\[
(\{c_{resp}(agt(B), agt(A), agt(0), r(j))\}, \emptyset) \\
\vdash (\{t_1 = mesg(a_{10}, a_6, encr(sk(agt(A), agt(B), r(i)), agt(0), p(N(agt(B), agt(A), r(j)))), r(j))\}, \{t_{in}\})
\]

By Reduction and Expansion with rule (I_9) in \( R_I \), and then Expansion with rule (5) in \( R_P \) (omitting the set \( C \)):

\[ t_1 \vdash t_2 = mesg(a_8, agt(0), encr(sk(agt(A), agt(B), r(i)), a_7, N(agt(B), agt(A), r(j))), r(j)) \]
Looking for Attacks

By iterating intruder's analysis and synthesis and expanding with rule (4) in $\mathcal{R}_P$:

$$t_2 \vdash t_3 = \text{msg}(a'_6, a'_7, \text{encr}(\text{ltk}(\text{agt}(B), \text{serv}(x)), a'_5, \text{cons}(\text{sk}(\text{agt}(A), \text{agt}(B), r(i)), \text{agt}(A))), r(j))$$

And then expanding with rule (3) in $\mathcal{R}_P$:

$$t_3 \vdash t_4 = \text{msg}(\overline{a}_4, \overline{a}_5,$$

$$\text{encr}(\text{ltk}(\text{agt}(A), \text{serv}(x)), \overline{a}_3,$$

$$\text{cons}(N(\text{agt}(A), \text{serv}(x), r(j_3)),$$

$$\text{cons}(\text{agt}(B),$$

$$\text{cons}(\text{sk}(\text{agt}(A), \text{agt}(B), r(i_1)),$$

$$\text{encr}(\text{ltk}(\text{agt}(B), \text{serv}(x)), a'_5,$$

$$\text{cons}(\text{sk}(\text{agt}(A), \text{agt}(B), r(i)), \text{agt}(A)))))),$$

$$r(j_3))$$
Deriving two Attacks

By iterating intruder's analysis and synthesis and expanding with rule (2) in \( R_P \):

\[ t_4 \vdash t_5 = mesg(a_2, a_3, cons(agt(A), cons(agt(B), N(agt(A), serv(x), r(j_3)))), r(j_3)) \]

And then expanding with rule (1) in \( R_P \):

\[ t_5 \vdash goal(agt(A), agt(B), serv(x), r(j_3)) \vdash success \]

By composing the substitutions along the path:
if \( \text{value}(j_3) < \text{value}(j) \), then Denning-Sacco's attack
if \( \text{value}(j_3) = \text{value}(j) \), then Lowe's multiplicity attack
Conclusions

- Verification as a backward recognizability process of terms by an intruder
- Feedback on error location (reconstruction of the attack)
- Type flaw attacks in the OR protocol derived in our “typed” approach
- Need more general criteria for ensuring the termination of the strategy (well-formedness) and scaling-up the formalization of protocols and properties
Adaptable Applications

- Heterogeneous environments w.r.t. resource availability and characterization
- Mobile context-aware applications
- Proving the correctness of an application w.r.t. the execution environment (adaptation predicate) by theorem proving
- Performing the adaptation of application: proof $\Rightarrow$ configuration
Security in PaCo

- Study of security aspects of performability-aware applications
- Investigation of security properties involved in the composition and adaptation of applications
- Development of proof techniques for deriving suitable configuration policies
- ...
Related Work

- Model checking
  - FDR (Lowe 1996)

- Theorem proving
  - NRL (Meadows 1996)
  - Isabelle (Paulson 1997, 1998, . . .)
  - SPASS (Weidenbach 1999) . . .

- Process calculi (Abadi-Gordon 1999, . . .)
Related Work

- Horn clauses (Blanchet 2002)
- Rewriting techniques and strategies
  - ELAN (Cirstea 2001)
  - Maude (Denker-Meseguer-Talcott 1998)
  - CASRUL (Jacquemard-Rusinowitch-Vigneron 2000)...
- Multiset rewriting and strand spaces (Cervesato et al. 2005)
Related Work

- Rewriting + abstract interpretation (Monniaux 1999)
- Rewriting + tree automata in Timbuk (Genet-Viet Triem Tong 2001)
- Combination of different approaches
  - AVISPA project
  - Maude-NPA (NRL Protocol Analyzer)