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:

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

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:

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

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 $\mathcal{R} = \mathcal{R}_P \cup \mathcal{R}_I$, 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

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

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

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

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

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

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

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

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

$$mesg(a_8, a_6, \\ encr(sk(agt(a), agt(b), r(i)), a_7, N(agt(b), agt(a), r(j))), \\ r(j)) \\ \to c_{init}(agt(a), agt(b), a_7, r(j)) \tag{6}$$

$$mesg(a_{10}, a_6, \\ encr(sk(agt(a), agt(b), r(i)), a_9, p(N(agt(b), agt(a), r(j)))), \\ r(j)) \\ \to c_{resp}(agt(b), agt(a), a_9, r(j)) \tag{7}$$

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

$$cons(x,y) \rightarrow x \tag{I_1}$$

$$cons(x,y) \rightarrow y \tag{I_2}$$

$$encr(sk(agt(0), agt(x), w), y, z) \rightarrow z \tag{I_3}$$

$$encr(sk(agt(x), agt(0), w), y, z) \rightarrow z \tag{I_4}$$

$$encr(sk(agt(s(x_1)), agt(x), w), y, z) \rightarrow z \tag{I_5}$$

$$encr(sk(agt(x), agt(s(x_1)), w), y, z) \rightarrow z \tag{I_6}$$

$$encr(ltk(agt(0), serv(x)), y, z) \rightarrow z \tag{I_7}$$

$$encr(ltk(agt(s(x_1)), serv(x)), y, z) \rightarrow z \tag{I_8}$$

$$mesg(x,y,z,w) \rightarrow z \tag{I_9}$$

Intruder's Initial Knowledge

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

No need of recognizability process
$\Rightarrow$ a set of terms in $\mathcal{R}_I$-normal form.

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

$$\{agt(l) \mid l \in L_{agt}\} \cup \{serv(x) \mid x \in L_{serv}\} \cup \{r(i) \mid i \in \mathbb{N}\} \cup$$
$$\{goal(x,y,z,w) \mid x,y \text{ agent}, z \text{ server}, w \text{ run}\} \cup$$
$$\{sk(agt(i),x,w) \mid i \in \mathbb{N}, x \text{ agent}, w \text{ run}\} \cup \{sk(x,agt(i),w) \mid x \text{ agent}, i \in \mathbb{N}, w \text{ run}\} \cup$$
$$\{ltk(agt(i),serv(x)) \mid i \in \mathbb{N},\ x \in L_{serv}\} \cup \{N(agt(i),x,w) \mid i \in \mathbb{N}, x \text{ agent}, w \text{ run}\}$$

Strategy: Basic Ingredients

- Recognizability of terms by an intruder as reduction into IK by a completion process on $\mathcal{R}$ 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 $\mathcal{R}_I$

Expansion

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

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 $wf(t)$) 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 agent labels a_1, a_2 and protocol run w.
(ii) $t_2 = N(agt(a_1), sk(agt(a_2), agt(a_3), w'), w)$ is not well-formed.

Recognizability

- Backward execution of the protocol (expansion with $\mathcal{R}_P$)
- Message decomposition and decryption (reduction with $\mathcal{R}_I$ - intruder's analysis)
- Message construction and encryption (expansion with $\mathcal{R}_I$ - 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($\mathcal{R}'$):

$$\frac{t \in E \qquad E' = expansion(t, \mathcal{R}')}{(E \setminus \{t\} \cup \{t' \in E' \mid wf(t')\}, C \cup \{t\})}$$

Success:

$$\frac{t \in E \qquad \forall t' \in \mathcal{R}_I\text{--}nf(t).\ t' \in IK}{success}$$

Reduction:

$$\frac{t \in E \qquad E' = \{t' \mid t' \in \mathcal{R}_I\text{--}nf(t) \wedge t' \notin IK\} \neq \emptyset}{(E \setminus \{t\} \cup E', C \cup \{t\})}$$

Inference Rules

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

Cut: $$\frac{t \in E \qquad \exists \bar{t} \in C.\ t \sim \bar{t}}{(E \setminus \{t\}, C)}$$

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

$$t_{in} = \bar{t}_0 \leftsquigarrow_{\mathcal{R}_P} t_1 \xrightarrow{*}_{\mathcal{R}_I} t'_1 \overset{*}{\leftsquigarrow}_{\mathcal{R}_I} \bar{t}_1 \leftsquigarrow_{\mathcal{R}_P} t_2 \xrightarrow{*}_{\mathcal{R}_I} t'_2 \overset{*}{\leftsquigarrow}_{\mathcal{R}_I} \bar{t}_2$$
$$\leftsquigarrow_{\mathcal{R}_P} t_3 \ \ldots \ \bar{t}_{k-1} \leftsquigarrow_{\mathcal{R}_P} t_k$$

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

(ii) If $(\{t_{in}\}, \emptyset) \vdash \mathit{failure}$, 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

$t_{in} = c_{resp}(agt(B), agt(A), agt(0), r(j)) \qquad j \in \mathbb{N}$

By Well-formed Expansion with rule (7) in $\mathcal{R}_P$:

$$
\begin{aligned}
&(\{c_{resp}(agt(B), agt(A), agt(0), r(j))\}, \emptyset)\\
&\vdash (\{t_1 = mesg(a_{10}, a_6, encr(sk(agt(A), agt(B), r(i)), agt(0), p(N(agt(B), agt(A), r(j)))), r(j))\},\\
&\quad \{t_{in}\})
\end{aligned}
$$

By Reduction and Expansion with rule (I_9) in $\mathcal{R}_I$, and then Expansion with rule (5) in $\mathcal{R}_P$ (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 $\mathcal{R}_P$:

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

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

$$\begin{aligned}
t_3 \vdash t_4 = mesg(&\overline{a}_4, \overline{a}_5,\\
&encr(ltk(agt(A), serv(x)), \overline{a}_3,\\
&\quad cons(N(agt(A), serv(x), r(j_3)),\\
&\qquad cons(agt(B),\\
&\qquad\quad cons(sk(agt(A), agt(B), r(i_1)),\\
&\qquad\qquad encr(ltk(agt(B), serv(x)), a'_5,\\
&\qquad\qquad\quad cons(sk(agt(A), agt(B), r(i)), agt(A))))))),\\
&r(j_3))
\end{aligned}$$

Deriving two Attacks

By iterating intruder's analysis and synthesis and expanding with rule (2) in $\mathcal{R}_P$:

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

And then expanding with rule (1) in $\mathcal{R}_P$:

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

By composing the substitutions along the path:

if value(j_3) $<$ value(j), then Denning-Sacco's attack

if value(j_3) $=$ 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)
  - Murphi (Mitchell-Mitchell-Stern 1997) ...
- 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
  - Genet-Klay's approximation technique and Paulson's inductive method (Oehl-Sinclair 2001, 2002)
  - AVISPA project
  - Maude-NPA (NRL Protocol Analyzer)