Symbolic Verification of Cryptographic Protocols

Protocol Analysis in the Applied Pi-Calculus

David Baelde

LSV, ENS Paris-Saclay

2018
Problem
Given $\Phi$ and $u$, does $S \vdash u$?

Theorem
*For the standard primitives, the intruder detection problem is in PTIME.*
A deducibility constraint system is either $\bot$ or a (possibly empty) conjunction of deducibility constraints of the form

$$T_1 \vdash ? u_1 \land \ldots \land T_n \vdash ? u_n$$

such that

- $T_1 \subseteq T_2 \subseteq \ldots \subseteq T_n$ (monotonicity)
- for every $i$, $\text{fv}(T_i) \subseteq \text{fv}(u_1, \ldots, u_{i-1})$ (origination)

The substitution $\sigma$ is a solution of $C = T_1 \vdash ? u_1 \land \ldots \land T_n \vdash ? u_n$ when $T_i \sigma \vdash u_i \sigma$ for all $i$ and $\text{img}(\sigma) \subseteq T_c(\mathcal{N})$. 
Example: Needham-Schroeder

\[ S_1 := \langle sk_i, pub(sk_a), pub(sk_b) \rangle, \text{aenc}(\langle pub(sk_a), n_a \rangle, pub(sk_i)) \]

\[ S_1 \vdash ? x \]
Example: Needham-Schroeder

\[ S_1 := \langle sk_i, pub(sk_a), pub(sk_b)\rangle, aenc(\langle pub(sk_a), n_a\rangle, pub(sk_i)) \]
\[ S_1 \vdash? aenc(\langle x_a, x_{na}\rangle, pub(sk_b)) \]
Example: Needham-Schroeder

- $S_1 := \langle sk_i, pub(sk_a), pub(sk_b) \rangle, aenc(\langle pub(sk_a), n_a \rangle, pub(sk_i))$
  $S_1 \vdash? aenc(\langle x_a, x_{na} \rangle, pub(sk_b))$

- $S_2 := S_1, aenc(\langle x_{na}, n_b \rangle, x_a)$
  $S_2 \vdash? aenc(\langle n_a, x_{nb} \rangle, pub(sk_a))$
Example: Needham-Schroeder

\[ S_1 := \langle sk_i, pub(sk_a), pub(sk_b) \rangle, aenc(\langle pub(sk_a), n_a \rangle, pub(sk_i)) \]
\[ S_1 \vdash? aenc(\langle x_a, x_{na} \rangle, pub(sk_b)) \]

\[ S_2 := S_1, aenc(\langle x_{na}, n_b \rangle, x_a) \]
\[ S_2 \vdash? aenc(\langle n_a, x_{nb} \rangle, pub(sk_a)) \]

\[ S_3 := S_2, aenc(x_{nb}, pub(sk_i)) \]
\[ S_3 \vdash? aenc(n_b, pub(sk_b)) \]
Example: Needham-Schroeder

- $S_1 := \langle sk_i, pub(sk_a), pub(sk_b) \rangle, aenc(\langle pub(sk_a), n_a \rangle, pub(sk_i))$
  
  $S_1 \vdash ? \ aenc(\langle x_a, x_{na} \rangle, pub(sk_b))$

- $S_2 := S_1, aenc(\langle x_{na}, n_b \rangle, x_a)$
  
  $S_2 \vdash ? \ aenc(\langle n_a, x_{nb} \rangle, pub(sk_a))$

- $S_3 := S_2, aenc(x_{nb}, pub(sk_i))$
  
  $S_3 \vdash ? \ aenc(n_b, pub(sk_b))$

- $S_4 := S_3, senc(secret, n_b)$ and $x_a = pub(sk_a)$
  
  $S_4 \vdash ? \ secret$
Constraint resolution

Solved form

A system is solved if it is of the form

\[ T_1 \vdash ? x_1 \land \ldots \land T_n \vdash ? x_n \]

Proposition

*If C is solved, then it admits a solution.*
A system is solved if it is of the form

\[ T_1 \vdash ? \  x_1 \land \ldots \land T_n \vdash ? \ x_n \]

**Proposition**

*If \( C \) is solved, then it admits a solution.*

**Theorem**

*There exists a terminating relation \( \leadsto \) such that for any \( C \) and \( \theta \), \( \theta \in \text{Sol}(C) \) if and only if there is \( C \leadsto^* C' \) solved and \( \theta = \sigma \theta' \) for some \( \theta' \in \text{Sol}(C') \).*
Simplification of constraint systems

Here systems are considered modulo AC of $\land$.

\[(R_1) \quad C \land T \vdash^? u \rightarrow C \quad \text{if } T \cup \{x \mid (T' \vdash^? x) \in C, T' \subsetneq T\} \vdash u\]

\[(R_2) \quad C \land T \vdash^? u \rightarrow^\sigma C\sigma \land T\sigma \vdash^? u\sigma \quad \text{if } \sigma = \text{mgu}(t, u), t \in \text{st}(T), t \neq u, \text{ and } t, u \notin \mathcal{X}\]

\[(R_3) \quad C \land T \vdash^? u \rightarrow^\sigma C\sigma \land T\sigma \vdash^? u\sigma \quad \text{if } \sigma = \text{mgu}(t_1, t_2), t_1, t_2 \in \text{st}(T), t_1 \neq t_2\]

\[(R_4) \quad C \land T \vdash^? u \rightarrow \bot \quad \text{if } \text{fv}(T \cup \{u\}) = \emptyset, T \not\vdash u\]

\[(R_f) \quad C \land T \vdash^? f(u_1, \ldots, u_n) \rightarrow C \land \bigwedge_i T \vdash^? u_i \quad \text{for } f \in \Sigma_c\]

\[(R_{pub}) \quad C \rightarrow C[x := \text{pub}(x)] \quad \text{if } \text{aenc}(t, x) \in T \text{ for some } (T \vdash^? u) \in C\]
Examples of simplifications

1. \( \text{senc}(n, k) \vdash? \text{senc}(x, k) \)

2. \( \text{senc}(\text{senc}(t_1, k), k) \vdash? \text{senc}(x, k) \) (two opportunities for \( R_2 \))

3. \( S \vdash? x \land S, n \vdash? y \land S, n, \text{senc}(m, \text{senc}(x, k)), \text{senc}(y, k) \vdash? m \)

4. \( S \vdash? x \land S \vdash? \langle x, x \rangle \)

5. \( n \vdash? x \land n \vdash? \text{senc}(x, k) \)
Proposition (Validity)

If $C$ is a deducibility constraint system, and $C \rightsquigarrow_{\sigma} C'$, then $C'$ is a deducibility constraint system.
Proposition (Validity)

If $C$ is a deducibility constraint system, and $C \overset{\sigma}{\rightsquigarrow} C'$, then $C'$ is a deducibility constraint system.

Proposition (Soundness)

If $C \overset{\sigma}{\rightsquigarrow} C'$ and $\theta \in \text{Sol}(C')$ then $\sigma \theta \in \text{Sol}(C)$.

Proposition (Termination)

Simplifications are terminating, as shown by the termination measure $(v(C), p(C), s(C))$ where:

- $v(C)$ is the number of variables occurring in $C$;
- $p(C)$ is the number of terms of the form $\text{aenc}(u, x)$ occurring on the left of constraints in $C$;
- $s(C)$ is the total size of the right-hand sides of constraints in $C$. 
Left-minimality & Simplicity

A derivation \( \Pi \) of \( T_i \vdash u \) is left-minimal if, whenever \( T_j \vdash u \), \( \Pi \) is also a derivation of \( T_j \vdash u \).

A derivation is simple if it is non-repeating and all its subderivations are left-minimal.

Proposition

*If* \( T_i \vdash u \), *then it has a simple derivation.*

Lemma

*Let* \( C = \bigwedge_j T_j \vdash ? u_j \) *be a constraint system,* \( \theta \in \text{Sol}(C) \), *and* \( i \) *be such that* \( u_j \in X \) *for all* \( j < i \).

*If* \( T_i \theta \vdash u \) *with a simple derivation starting with an axiom or a decomposition, then there is* \( t \in \text{subterm}(T_i) \setminus X \) *such that* \( t\theta = u \).
Lemma

Let \( C = \bigwedge_j T_j \vdash? u_j, \sigma \in \text{Sol}(C) \).
Let \( i \) be a minimal index such that \( u_i \notin X \).
Assume that:

- \( T_i \) does not contain two subterms \( t_1 \neq t_2 \) such that \( t_1\sigma = t_2\sigma \);
- \( T_i \) does not contain any subterm of the form \( \text{aenc}(t,x) \);
- \( u_i \) is a non-variable subterm of \( T_i \).

Then \( T'_i \vdash u_i \), where \( T'_i = T_i \cup \{ x \mid (T \vdash? x) \in C, T \subsetneq T_i \} \).
Lemma

Let $C = \bigwedge_j T_j \vdash ? u_j$, $\sigma \in \text{Sol}(C)$.
Let $i$ be a minimal index such that $u_i \notin X$.
Assume that:
- $T_i$ does not contain two subterms $t_1 \neq t_2$ such that $t_1\sigma = t_2\sigma$;
- $T_i$ does not contain any subterm of the form $\text{aenc}(t, x)$;
- $u_i$ is a non-variable subterm of $T_i$.

Then $T_i' \vdash u_i$, where $T_i' = T_i \cup \{x \mid (T \vdash ? x) \in C, T \subsetneq T_i\}$.

Proposition (Completeness)

If $C$ is unsolved and $\theta \in \text{Sol}(C)$, there is $C \leadsto_{\sigma} C'$ and $\theta' \in \text{Sol}(C')$ such that $\theta = \sigma\theta'$. 
Concluding remarks

**Improvements**

- A complete strategy can yield a polynomial bound, hence a small attack property
- Equalities and disequalities may be added
- Several variants and extensions may be considered: sk instead of pub, signatures, xor, etc.

**We have not answered the original question yet!**

- Symbolic semantics, (dis)equality constraints
- The enumeration of all interleavings is too naive

**Complexity**

- Deciding whether a system has a solution is NP-hard
- Reminder: for a general theory, security is undecidable