An Optimized Intruder Model for SAT-based Model-Checking of Security Protocols

Luca Compagna
joint work with Alessandro Armando

AI-Lab - MRG-DIST - University of Genova

ARSPA Workshop - IJCAR, Cork, 04 Jul 2004

AVISPA

Automated Validation of Internet Security Protocols and Applications (IST-2001-39252)

The EU Calculemus Training Network (HPRN-CT-2000-00102)

Motivations

- **Context:** Dramatic speed-up of SAT solvers in the last decade: problems with thousands of variables are now solved routinely in milliseconds.

  This has lead to breakthroughs in planning and hardware verification.

Motivations

- **Context:** Dramatic speed-up of SAT solvers in the last decade: problems with thousands of variables are now solved routinely in milliseconds.

  This has lead to breakthroughs in planning and hardware verification.

- **Approach:** Bounded model-checking of security protocols via reduction to SAT with iterative deepening on the number of steps.

  We proposed reductions of protocol (in)security problems to SAT that can be used to effectively find attacks on small and medium size protocols.

  To scale-up to large-scale protocols is critical to optimize the approach.

Motivations

- **Context:** Dramatic speed-up of SAT solvers in the last decade: problems with thousands of variables are now solved routinely in milliseconds.

  This has lead to breakthroughs in planning and hardware verification.

- **Approach:** Bounded model-checking of security protocols via reduction to SAT with iterative deepening on the number of steps.

  We proposed reductions of protocol (in)security problems to SAT that can be used to effectively find attacks on small and medium size protocols.

  To scale-up to large-scale protocols is critical to optimize the approach.

- **Optimization:** In this work we propose an optimized intruder model that leads in many cases to shorter attacks which can be detected in our framework by generating smaller propositional formulae.

Roadmap

- Protocol Analysis
- Modeling via a simple example:
  - Standard Model
  - Axioms and the Optimized Intruder
- Protocol Insecurity Problems with Axioms
- Encoding Protocol Insecurity Problems with Axioms into SAT
- Implementations and Results
- Conclusions and Perspectives

Protocol Analysis: Modeling

- Protocol as a state transition system in which states correspond to information possessed by participating agents.

- Perfect cryptography: an encrypted message can be neither altered nor read without the appropriate key.

- The Dolev-Yao intruder:
  - controls all the traffic in the network;
  - can compose and send fraudulent messages from the knowledge he can glean from the observed traffic and his own initial knowledge.

Protocol Analysis: Security Problems

- Specified by means of the IF rule-based language suitable for security protocols:
  - state: set of facts;
  - transition relation: labeled rewrite rules.
- Security requirements such as authentication and secrecy are reduced to reachability problems on this model.
- We focus on reachability problem with finite number of sessions.
- This is adequate in practice as attacks on well-known protocols often exploit a small number of sessions.

Modeling: Needham-Schroeder authentication prot. (1)

Let us consider the well known NSPK protocol:

$$\begin{array}{ll} 1. & A \rightarrow B: \ \{A, N_A\}_{K_B} \\ 2. & B \rightarrow A: \ \{N_A, N_B\}_{K_A} \\ 3. & A \rightarrow B: \ \{N_B\}_{K_B} \end{array}$$

Scenario: two concurrent sessions of the protocol

session 1: a talks to the intruder i;

session 2: a talks to b.

Security Requirement: B authenticates A on N_A.

Modeling: Needham-Schroeder authentication prot. (2)

States are represented as sets of the following facts:

- $fresh(N)$ means that the nonce N has not been used yet.
- $ik(T)$ means that the intruder knows T.
- $m(J, S, R, T)$ means that sender S has (supposedly) sent message T to principal R at protocol step J.
- $w(J, S, R, [T_1, \ldots, T_k], C)$ represents the state of principal R at step J of session C; it means that R
  - knows the terms stored in the lists $[T_1, \ldots, T_k]$, and
  - is waiting for a message from S (if $J \neq 0$).

Modeling: Needham-Schroeder authentication prot. (3)

- Initial State:

$$w(0, a, a, [a, i, ka, ka^{-1}, ki], 1).$$
$$w(0, a, a, [a, b, ka, ka^{-1}, kb], 2).w(1, b, a, [b, a, kb, kb^{-1}, ka], 2).$$
$$fresh(nc(n1, 1)).fresh(nc(n1, 2)).fresh(nc(n2, 2)).$$
$$ik(i).ik(a).ik(b).ik(ki).ik(ki^{-1}).ik(ka).ik(kb)$$

- Bad States:

$$w(0, a, a, [], [a, b, ka, kb, ka^{-1}], s(1)).$$
$$w(1, a, b, [], [b, a, kb, ka, kb^{-1}], 1)$$

Modeling: Needham-Schroeder authentication prot. (4)

- Labeled Rewrite Rules:
  - Behaviour of Honest Participants:

$$fresh(nc(n1,S)).w(0,A,A,[A,B,Ka,Ka^{-1},Kb],S) \xrightarrow{step_0(A,B,Ka,Kb,S)} w(2,B,A,[nc(n1,S),A,B,Ka,Ka^{-1},Kb],S).m(1,A,B,\{A,nc(n1,S)\}_{Kb})$$

  - Behaviour of the Intruder:

$$m(J,S,R,M) \xrightarrow{divert(J,M,R,S)} ik(S)$$

$$ik(\{M\}_K).ik(K^{-1}) \xrightarrow{decrypt(K,M)} ik(M).ik(\{M\}_K).ik(K^{-1})$$

Modeling: Needham-Schroeder authentication prot. (5)

The attack on the simple NSPK protocol

$$
\begin{array}{llllll}
(1.1) & a & \rightarrow & i & : & \{a, na\}_{ki} & snd \\
(2.1) & i(a) & \rightarrow & b & : & \{a, na\}_{kb} & rc + dec + dec + snd \\
(2.2) & b & \rightarrow & i(a) & : & \{na, nb\}_{ka} & rc\_snd \\
(1.2) & i & \rightarrow & a & : & \{na, nb\}_{ka} & \\
(1.3) & a & \rightarrow & i & : & \{nb\}_{ki} & rc\_snd \\
(2.3) & i(a) & \rightarrow & b & : & \{nb\}_{kb} & rc + dec + snd
\end{array}
$$

requires 3 intruder knowledge manipulations (dec) to be executed.

For industrial-scale security protocols in which messages can have a complex structure, such a number can be much more significant.

Question: can we save such decomposing transitions?

Modeling: Axioms and the Optimized Intruder

Axiom: formula that states a relation between facts of the transition system and that holds at each state of the transition system.

Axioms are particularly suited to represent relations between intruder knowledge facts. E.g.

$$ik(\{M\}_K) \wedge ik(K^{-1}) \supset ik(M)$$

"Every time the intruder knows $\{M\}_K$ and K^{-1}, then it knows instantaneously also M."

Idea: optimize the intruder by replacing decomposing rules with appropriate decomposing axioms.

Protocol Insecurity Problems with Axioms (1)

A Protocol Insecurity Problem (PIP) with axioms is a tuple $\Xi = \langle \mathcal{F}, \mathcal{L}, \mathcal{R}, \mathcal{A}, \mathcal{I}, \mathcal{G} \rangle$ where:

- $\mathcal{F}$ and $\mathcal{L}$ are sets of atomic formula of sorted 1^{st}-order languages called *facts* and *rule labels*, respectively;
- $\mathcal{R}$ is a set of labeled rewrite rules of the form $L \xrightarrow{\lambda} R$, where $L, R \subseteq \mathcal{F}$, and $\lambda \in \mathcal{L}$;
- $\mathcal{A}$ is a set of axioms of the form $\bigwedge_{i=1}^{j} p_i \supset c$, where $p_1, \ldots, p_j, c \in \mathcal{F}$
- $\mathcal{I}$ and $\mathcal{G}$ are respectively the initial state and a boolean formula representing the bad states.

Protocol Insecurity Problems with Axioms (2)

A PIP with axioms represents a state transition system in which:

- States: set of facts S (i.e. $S \subseteq \mathcal{F}$) such that $S \models \mathcal{A}$;
- Transition Relation: let S be a state and $L \xrightarrow{\lambda} R$ be a rewrite rule, then $S \overset{\lambda}{\leadsto} S'$ iff $L \subseteq S$ and $S' = (S \setminus L) \cup R$ is such that $S' \models \mathcal{A}$.

Protocol Insecurity Problems with Axioms (2)

A PIP with axioms represents a state transition system in which:

- States: set of facts S (i.e. $S \subseteq \mathcal{F}$) such that $S \models \mathcal{A}$;
- Transition Relation: let S be a state and $L \xrightarrow{\lambda} R$ be a rewrite rule, then $S \overset{\lambda}{\rightsquigarrow} S'$ iff $L \subseteq S$ and $S' = (S \setminus L) \cup R$ is such that $S' \models \mathcal{A}$.

An attack to a PIP with axioms is a sequence of rules $\lambda_1, \ldots, \lambda_n$ such that $S_i \overset{\lambda_i}{\rightsquigarrow} S_{i+1}$ for $i = 1, \ldots, n$ with $S_1 = \mathcal{I}$ and $S_n \models \mathcal{G}$.

Protocol Insecurity Problems with Axioms (2)

A PIP with axioms represents a state transition system in which:

- States: set of facts S (i.e. $S \subseteq \mathcal{F}$) such that $S \models \mathcal{A}$;
- Transition Relation: let S be a state and $L \xrightarrow{\lambda} R$ be a rewrite rule, then $S \overset{\lambda}{\rightsquigarrow} S'$ iff $L \subseteq S$ and $S' = (S \setminus L) \cup R$ is such that $S' \models \mathcal{A}$.

An attack to a PIP with axioms is a sequence of rules $\lambda_1, \ldots, \lambda_n$ such that $S_i \overset{\lambda_i}{\rightsquigarrow} S_{i+1}$ for $i = 1, \ldots, n$ with $S_1 = \mathcal{I}$ and $S_n \models \mathcal{G}$.

Attacks to a PIP with axioms can be compactly represented by means of partial-order attack.

Encoding PIP with axioms into SAT (1)

Given a PIP with axioms (without equivalence cycles) Ξ and a positive integer n, we build a propositional formula Φ^n_Ξ such that any model of Φ^n_Ξ corresponds to a partial-order attack of Ξ.

Encoding PIP with axioms into SAT (1)

Given a PIP with axioms (without equivalence cycles) Ξ and a positive integer n, we build a propositional formula Φ^n_Ξ such that any model of Φ^n_Ξ corresponds to a partial-order attack of Ξ.

To do so, we:

1. add an additional time-index parameter to each rule λ or fact p, to indicate the state at which time the rule begins or the fact holds.

2. build Φ^n_Ξ by unfolding n times the transition relation:

$$\Phi^n_\Xi = I(p^0) \wedge \bigwedge_{i=0}^{n-1} T_i(p^i, \lambda^i, p^{i+1}) \wedge G(p^n)$$

   where I, T and G are formulae defining the initial state, the transition relation and the goal states, respectively.

Encoding PIP with axioms into SAT (2)

The encoding of PIP with axioms into a SAT formulae can be done in a variety of ways (see [1,2]).

The main differences between them are reflected in the formula representing the transition relation: $\bigwedge_{k=0}^{n-1} T_i(p^i, \lambda^i, p^{i+1})$.

By introducing axioms, significant changes must be done on the encodings.

We have adapted and extended the following two for supporting axioms:

- Linear encoding, and
- Graphplan-based encoding.

[1] Armando, Compagna. *Abstraction-driven SAT-based Analysis of Security Prot.* (*SAT'03*)
[2] Armando, Compagna, Ganty.
SAT-based Model-Checking of Security Prot. using Planning Graph Analysis (*FME'03*)

Linear Encoding with Axioms (1)

The formula $T_i(p^i, \lambda^i, p^{i+1})$ for $i = 0, \ldots, n-1$ is given by the conjunction of the following:

Universal Formulae: for each rewrite rule $\lambda \in \mathcal{L}$ s.t. $(L \xrightarrow{\lambda} R) \in \mathcal{R}$

$$\begin{array}{rcl} \lambda^i & \supset & \bigwedge\{p^i \mid p \in L\} \\ \lambda^i & \supset & \bigwedge\{p^{i+1} \mid p \in R \backslash L\} \\ \lambda^i & \supset & \bigwedge\{\neg p^{i+1} \mid p \in L \backslash R\} \end{array}$$

Cardinality: $O(n|\mathcal{L}|r)$, where r max #facts in a rule (usually small).

Axioms Formulae: for each $(p_1 \wedge \cdots \wedge p_j \supset c) \in \mathcal{A}$

$$(p_1^i \wedge \cdots \wedge p_j^i) \supset c^i$$

Cardinality: $O(n|\mathcal{A}|)$.

Linear Encoding with Axioms (2)

Explanatory Frame Formulae with Axioms: for all facts $f \in \mathcal{F}$

$$(\neg f^i \wedge f^{i+1}) \supset \left(\bigvee \left\{ \lambda^i \mid (L \xrightarrow{\lambda} R) \in \mathcal{R}, f \in (R \setminus L) \right\} \vee \bigvee \{ p_1^{i+1} \wedge \cdots \wedge p_j^{i+1} \mid (p_1 \wedge \cdots \wedge p_j \supset f) \in \mathcal{A} \} \right)$$

$$(f^i \wedge \neg f^{i+1}) \supset \left(\bigvee \left\{ \lambda^i \mid (L \xrightarrow{\lambda} R) \in \mathcal{R}, f \in (L \setminus R) \right\} \vee \bigvee \{ \neg p_1^{i+1} \wedge p_2^{i+1} \wedge \cdots \wedge p_j^{i+1} \mid (\neg p_1 \wedge p_2 \wedge \cdots \wedge p_j \supset \neg f) \in \hat{\mathcal{A}} \} \right)$$

where $\hat{\mathcal{A}}$ is the set of contraposed axioms. E.g. $\neg b \supset \neg a$ is the contraposed of $a \supset b$. **Cardinality:** $O(n|\mathcal{F}| + nt|\mathcal{A}|)$, where t is the max number of preconditions in an axiom (usually small).

Linear Encoding with Axioms (3)

Conflict Exclusion Formulae with Axioms: for all distinct rule λ_1, λ_2 such that $(L_1 \xrightarrow{\lambda_1} R_1) \in \mathcal{R}, (L_2 \xrightarrow{\lambda_2} R_2) \in \mathcal{R}$ with $L_1 \cap dep_{\mathcal{A}}(L_2 \setminus R_2) \neq \emptyset$ or $L_2 \cap dep_{\mathcal{A}}(L_1 \setminus R_1) \neq \emptyset$

$$\neg(\lambda_1^i \wedge \lambda_2^i)$$

where $dep_{\mathcal{A}}(L_j \setminus R_j)$ $(j = 1, 2)$ is the set of facts from which all the facts deleted by λ_i possibly depend wrt $\mathcal{A}$. E.g. let $\mathcal{A} = \{a \supset b, b \wedge c \supset d\}$, then

$$dep_{\mathcal{A}}(\{b\}) = \{a, b\}$$
$$dep_{\mathcal{A}}(\{c\}) = \{c\}$$
$$dep_{\mathcal{A}}(\{d\}) = \{a, b, c, d\}$$

Cardinality: $O(n|\mathcal{L}|^2)$.

Implementation: SATMC

SATMC v1.0:

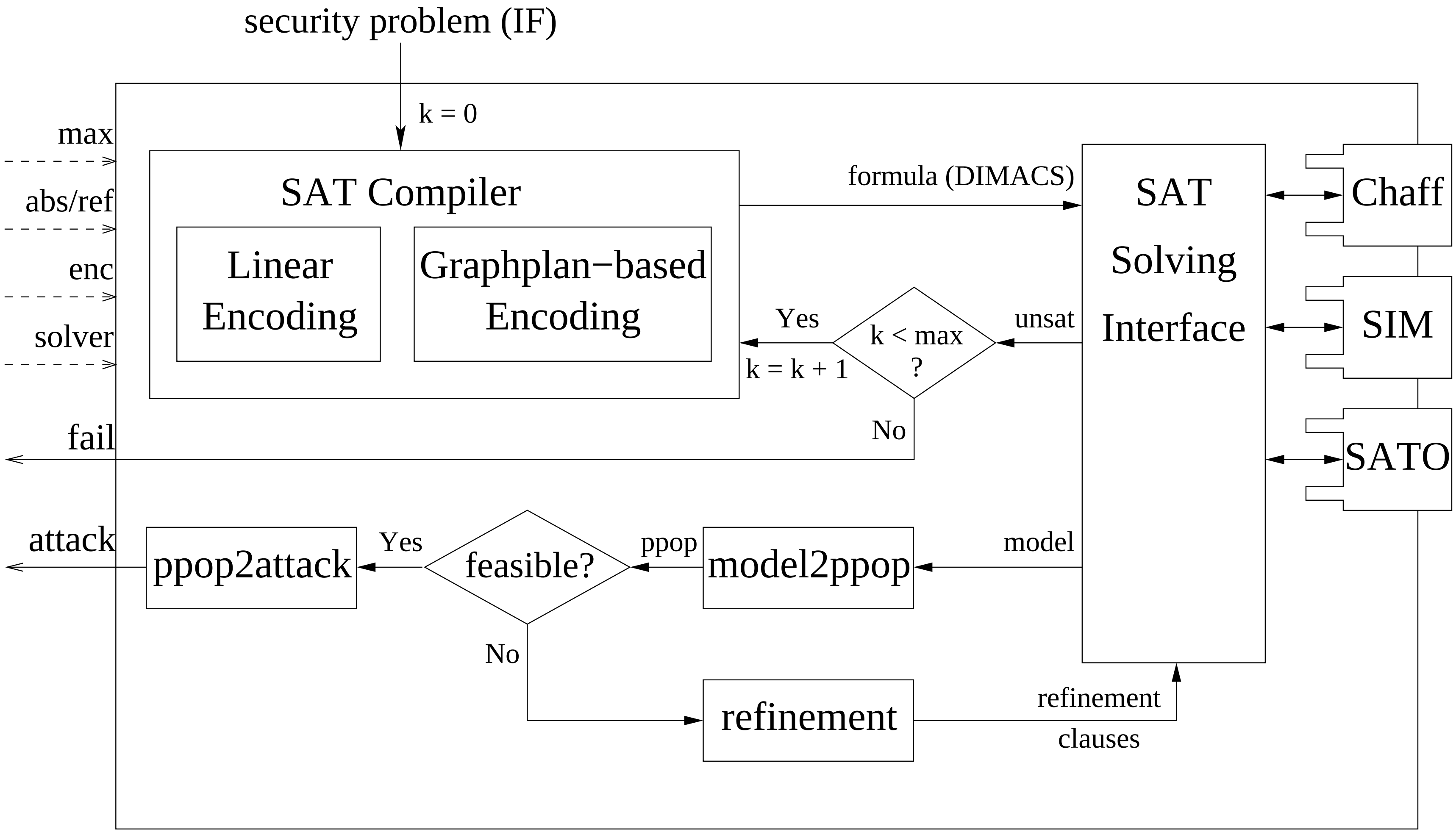
- input specification in IF v.1 language;
- set of optimizing transformations to get encodings of manageable size;
- linear encoding with iterative deepening on the number of steps.

SATMC v2.0:

- input specification in IF v.2 language;
- abstraction/refinement strategy based on neglecting mutex relations;
- an optimized graphplan-based encoding;
- support axioms.

Download it at: `http://www.mrg.dist.unige.it/satmc`

Implementation: Architecture



Experimental Results on C/J

Protocol	DY N	DY Atoms	DY Clauses	Optimized DY N	Optimized DY Atoms	Optimized DY Clauses
KaoChow 2	9	530,726	1,804,005	7	414,536	1,489,121
KaoChow 3	9	995,323	5,736,662	7	776,805	4,590,268
NSCK	9	114,530	334,086	8	88,343	298,491
NSPK	7	6,612	33,326	4	3,714	19,242
NSPK-server	8	9,157	53,741	5	5,600	33,835
Woo-Lam M	6	481,394	2,498,382	5	409,114	2,133,265

Linear Encoding

Protocol	DY N	DY Atoms	DY Clauses	Optimized DY N	Optimized DY Atoms	Optimized DY Clauses
KaoChow 2	9	726	3,065	7	458	1,784
KaoChow 3	9	990	5,019	7	587	2,606
NSCK	9	435	1,392	8	348	1,105
NSPK	7	411	1,249	4	199	549
NSPK-server	8	847	2,688	5	380	1,177
Woo-Lam M	6	481	1,518	5	358	1,137

Graphplan-based Encoding

Conclusions and Perspectives

- Proposed an optimized intruder model for SAT-based model-checking of security protocols.
- Encodings schemes extended for supporting the specification of set of axioms (without equivalence cycles).
- Up to 40% shorter attacks and up to 50% smaller SAT formulae.

Conclusions and Perspectives

- Proposed an optimized intruder model for SAT-based model-checking of security protocols.
- Encodings schemes extended for supporting the specification of set of axioms (without equivalence cycles).
- Up to 40% shorter attacks and up to 50% smaller SAT formulae.
- Investigate and extend our approach for encoding generic set of axioms also specifying equivalence cycles: algebraic equations (e.g. exponentiation in the Diffie-Hellman protocol).
- Experiment such an optimization against industrial-scale security protocols: a considerable number of intruder knowledge manipulations can be required.

Thanks for you attention