Intruder Theories

Hubert Comon-Lundh

LSV, CNRS

INRIA project SECSI

École Normale Supérieure de Cachan

SUMMARY

1. Setting
2. Motivation(s)
3. Constrained sequent calculus
4. The main theorem (conjecture) and its consequences
5. Homework problems in rewriting and unification theory

CRYPTOGRAPHIC PROTOCOLS

A model checking problem:

CRYPTOGRAPHIC PROTOCOLS

A model checking problem:

$$M_I \models \phi$$

CRYPTOGRAPHIC PROTOCOLS

A model checking problem:

$$M_I \models \phi$$

Infinite state, infinitely branching, with some specificities

CRYPTOGRAPHIC PROTOCOLS

A model checking problem:

$$M_I \quad \models \quad \phi$$

Infinite state, infinitely branching, with some specificities

A security property ($\neq$ temporal formula)

Cryptographic Protocols

A model checking problem:

$$M_I \models \phi$$

Infinite state, infinitely branching, with some specificities

This talk

A security property ($\neq$ temporal formula)

The model description

A finite number of roles:

$$\begin{array}{ll} A(x_1, \ldots, x_k) & \texttt{role name and parameters} \\ \quad \nu N_1, \ldots, N_k & \texttt{name generation (nonces)} \\ \left.\begin{array}{ccc} u_1 & \rightarrow & v_1 \\ & \cdots & \\ u_n & \rightarrow & v_n \end{array}\right\} & \texttt{protocol rules} \end{array}$$

$u_1, \ldots, u_n, v_1, \ldots, v_n$ are terms with variables; variables stand for nonces generated by other roles, or encrypted data, which cannot be decrypted.

u_i, v_i can be empty (0). Terms are untyped.

$Var(v_i) \subseteq \{x_1, \ldots, x_k\} \cup Var(u_1, \ldots, u_i)$.

Example of transition

$A(B) : \nu N_A.$

$$\begin{array}{lrcl} 1. & 0 & \rightarrow & \mathsf{enc}(< A, N_A >, pub(B)) \\ 2. & \mathsf{enc}(< N_A, x >, pub(A)) & \rightarrow & \mathsf{enc}(x, pub(B)) \end{array}$$

$$\left(\begin{array}{l} I : \\ \qquad \cdots \\ \qquad \mathsf{enc}(< N_A(1), N_B(2) >, pub(a)) \\ \\ a : \\ \qquad 1 : \; 1, A, i, N_A(1) \\ \qquad 3 : \; \cdots \\ b : \cdots \end{array} \right) \rightarrow \left(\begin{array}{l} I : \\ \qquad \cdots \\ \qquad \mathsf{enc}(< N_A(1), N_B(2) >, pub(a)) \\ \qquad \mathsf{enc}(N_B(2), pub(i)) \\ \\ a : \\ \qquad 1 : \; 2, A, i, N_A(1) \\ \qquad 3 : \cdots \\ b : \cdots \end{array} \right)$$

Example of transition

$B() : \nu N_B.$

$$\begin{array}{lrcl} 1. & \mathsf{enc}(< A, x >, pub(B)) & \rightarrow & \mathsf{enc}(< x, N_B >, pub(A)) \\ 2. & \mathsf{enc}(N_B, pub(B)) & \rightarrow & 0 \end{array}$$

$$\left(\begin{array}{l} I : \\ \quad \cdots \\ \quad \mathsf{enc}(< a, N_A(1) >, pub(i)) \\ \\ b : \emptyset \\ a : \cdots \end{array} \right) \rightarrow \left(\begin{array}{l} I : \\ \quad \cdots \\ \quad \mathsf{enc}(< a, N_A(1) >, pub(i)) \\ \quad \mathsf{enc}(< N_A(1), N_B(2) >, pub(a)) \\ \\ b : \\ \quad 2 : \; 1, B, N_B(2) \\ a : \cdots \end{array} \right)$$

INTRUDER CAPABILITIES

An example of offline theory.

$$\frac{T \vdash < u, v >}{T \vdash u} \qquad \frac{T \vdash < u, v >}{T \vdash v} \qquad \frac{T \vdash u \quad T \vdash v}{T \vdash < u, v >}$$

$$\frac{T \vdash \mathsf{enc}(u, v) \quad T \vdash v}{T \vdash u} \qquad \frac{T \vdash u \quad T \vdash v}{T \vdash \mathsf{enc}(u, v)} \qquad \frac{}{T, t \vdash t}$$

CRITICISMS ON THE STATE OF THE ART

- Many provers/model-checkers for the so-called Dolev-Yao intruder model.
- They assume perfect cryptography: the set of messages is a free term algebra
- Security properties mostly limited to confidentiality and some versions of agreement.

But...

- Various intruder models
- Many protocols rely on algebraic properties of cryptographic primitives. Typical examples: exclusive or, modular exponentiation.
- Many different security properties

RNTL PROUVÉ (LSV, LORIA, CRIL, France Telecom, VERIMAG).

INTRUDER CAPABILITIES (2)

An example of offline theory.

$$\frac{T \vdash < u, v >}{T \vdash u} \qquad \frac{T \vdash < u, v >}{T \vdash v} \qquad \frac{T \vdash u \quad T \vdash v}{T \vdash < u, v >}$$

$$\frac{T \vdash \mathsf{enc}(u, v) \quad T \vdash v}{T \vdash u} \qquad \frac{T \vdash u \quad T \vdash v}{T \vdash \mathsf{enc}(u, v)} \qquad \frac{}{T, t \vdash t}$$

$$\frac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash (u_1 \oplus \cdots \oplus u_n) \downarrow}$$

Equational theory:

$$\begin{array}{rcl} x \oplus x \oplus y & \rightarrow & y \\ x \oplus x & \rightarrow & 0 \\ x \oplus 0 & \rightarrow & x \end{array} \qquad \begin{array}{rcl} x \oplus (y \oplus z) & = & (x \oplus y) \oplus z \\ x \oplus y & = & y \oplus x \end{array}$$

OUR GOALS

Find general decision techniques, parametrized by the intruder theory and the equational theory.

However:

We assume a bounded number of sessions.

Advantages: nonces can be eliminated and many security properties can be reduced to reachability questions.

ANOTHER MOTIVATION

Chevalier, Küsters, Rusinowitch, Turuani (LICS 2003) :
Protocol insecurity with `xor` is NP-complete

Comon-Lundh, Shmatikov (LICS 2003) : Constraint solving and protocol insecurity with `xor`

What are the exact relationships ?

SOME KNOWN RESULTS

Bounded number of instances of each role: decision results, depending on the offline theory:

- Dolev-Yao theory: the problem is co-NP- complete ([Rusinowitch, Turuani, CSFW 2001])
- theory of exclusive or (with slight restrictions on protocol roles): the problem is co-NP-complete ([Chevalier, Küster, Rusinowitch, Turuani, LICS 2003])
- theory of exclusive or : the problem is decidable ([Comon-Lundh, Shmatikov, LICS 2003])
- theory of Diffie-Helmann exponentiation (with slight restrictions on protocol roles): the problem is co-NP-complete ([Chevalier, Kusters, Rusinowitch, Turuani, FST/TCS 2003])
- theory of Abelian groups: the problem is decidable (Millen, Shmatikov 2004)
- a(nother) theory of Diffie-Helmann exponentiation ([Shmatikov, ESOP 2004])
- theory of guessing attacks: the problem is co-NP-complete (Delaune, Jacquemard, 2004)

Online intruder deductions

Intruder's point of view: there is an additional deduction rule:

$$\frac{T \vdash u_i\sigma}{T \vdash v_i\sigma}$$

if some agent reached step $i-1$ in the role to which belongs the rule $u_i \to v_i$ and σ is compatible with the partial bindings at this stage.
Confidentiality is then a deducibility problem in some formal proof system.

Our thesis

Increasing complexity of proofs.

The same ingredients are used:

- Normal (offline) proofs
- Bounds on the sizes of the substitutions

The online theory is the right framework.
All previous results are particular cases of a proof normalization theorem

A Formal proof system

We consider constrained sequents $T \vdash u \; [\![E]\!]$. For arbitrary rules in the offline theory:

$$\frac{T \vdash u_1 \qquad \cdots \quad T \vdash u_n}{T \vdash u}$$

A FORMAL PROOF SYSTEM

We consider constrained sequents $T \vdash u \; \llbracket E \rrbracket$. For arbitrary rules in the offline theory:

$$\frac{T \vdash u_1 \;\; \llbracket E_1 \rrbracket \quad \cdots \quad T \vdash u_n \;\; \llbracket E_n \rrbracket}{T \vdash u \;\; \llbracket E_1 \wedge \ldots \wedge E_n \rrbracket}$$

A FORMAL PROOF SYSTEM

We consider constrained sequents $T \vdash u \; [\![E]\!]$. For arbitrary rules in the offline theory:

$$\frac{T \vdash u_1 \;\; [\![E_1]\!] \quad \cdots \quad T \vdash u_n \;\; [\![E_n]\!]}{T \vdash u \;\; [\![E_1 \wedge \ldots \wedge E_n]\!]}$$

$$\frac{T \vdash u \; [\![E \wedge x_{s,A,k-1} = 1]\!]}{T \vdash w_k \; [\![E \wedge x_{s,A,k} = 1 \wedge u = v_k]\!]}$$

$v_k \to w_k$ is the kth rule of the s instance of role A.

A Formal proof system

We consider constrained sequents $T \vdash u\ [\![E]\!]$. For arbitrary rules in the offline theory:

$$\frac{T \vdash u_1 \quad [\![E_1]\!] \quad \cdots \quad T \vdash u_n \quad [\![E_n]\!]}{T \vdash u \quad [\![E_1 \wedge \ldots \wedge E_n]\!]}$$

$$\frac{T \vdash u\ [\![E \wedge x_{s,A,k-1} = 1]\!]}{T \vdash w_k\ [\![E \wedge x_{s,A,k} = 1 \wedge u = v_k]\!]}$$

$v_k \to w_k$ is the kth rule of the s instance of role A.

$$\frac{T \vdash x\ [\![E \wedge x = u]\!]}{T \vdash u\ [\![E \wedge x = u]\!]}$$

A FORMAL PROOF SYSTEM

We consider constrained sequents $T \vdash u \; [\![E]\!]$. For arbitrary rules in the offline theory:

$$\frac{T \vdash u_1 \;\; [\![E_1]\!] \quad \cdots \quad T \vdash u_n \;\; [\![E_n]\!]}{T \vdash u \;\; [\![E_1 \wedge \ldots \wedge E_n]\!]}$$

$$\frac{T \vdash u \; [\![E \wedge x_{s,A,k-1} = 1]\!]}{T \vdash w_k \; [\![E \wedge x_{s,A,k} = 1 \wedge u = v_k]\!]}$$

$v_k \to w_k$ is the kth rule of the s instance of role A.

$$\frac{T \vdash x \; [\![E \wedge x = u]\!]}{T \vdash u \; [\![E \wedge x = u]\!]}$$

Constraint solving rule: $E \mapsto E'$ if E' is a solved form of E.

THE MAIN RESULT

Theorem
For equational theories and offline systems (which satisfy hypotheses specified later),
if there is a proof of a secret s in the online theory, then there is a proof in which all sequents are of the form

$$T \vdash u \; [\![E]\!]$$

where

- $u \in \mathsf{St}(T, s, P)$
- E is a conjunction of equations between terms in $\mathsf{St}(T, s, P)$ and control equations $x_{s,A,k} = 1$.

St(T) is, roughly, the set of subterms of T

Hypotheses on the offline theory

Locality:

- if there is a proof of $T \vdash u$, then there is a proof which only involves subterms of T, u.
- if there is a proof of $T \vdash u$ such that v never occurs as a right member, then replacing v with w in the proof, we get again a proof.

Such hypotheses are satisfied by Dolev-Yao, `xor`, inverse key theory. In some other cases, they have to be weakened: use a more general notion of subterm and a finite set of possible replacements.

Hypotheses on the equational theory

$\mathcal{E} = \mathcal{E}_1 \uplus \mathcal{E}_2$ and

- a matching equation $u = t$ modulo $\mathcal{E}_2$ is equivalent to a finite disjunction of solved forms $x_1 = t_1 \wedge \ldots \wedge x_n = t_n$ where $t_1, \ldots, t_n \in \mathsf{St}(t, u)$.
- $\mathcal{E}$ can be oriented into a convergent rewrite system (modulo AC)
- For every term t, we can compute a finite set of instances $t\sigma$ such that, for every θ, there is some σ and some τ s.t.

$$t\theta \downarrow =_{\mathcal{E}_2} (t\sigma \downarrow)\tau$$

	$\mathcal{E}_1$	$\mathcal{E}_2$
D.Y.	$\emptyset$	$\emptyset$
`xor`	$x \oplus x \oplus y \rightarrow y$ $x \oplus x \rightarrow 0$ $x \oplus 0 \rightarrow x$	$x \oplus (y \oplus z) = (x \oplus y) \oplus z$ $x \oplus y = y \oplus x$

CONSEQUENCES OF THE MAIN RESULT

For a bounded number of sessions, we get a decision algorithm

1. Guess E
2. Use a marking (fixed point) algorithm

Complexity is Non-deterministic Size($\mathsf{St}(T, s, P)$)

Examples

- For the D.Y. intruder, $\mathsf{St}(T, s, P)$ is the (linear) set of subterms of T, s, P: we get an NP decision procedure as in [RusinowitchTuruani 2001]
- For the theory of `xor`
  - Either assuming additional properties of the protocol rules, we can choose again for St the set of subterms; we get [Chevalier et al. 2003] result
  - Or, in general, St is the set of sums of subterms and we get [Comon-Lundh,Shmatikov 2003] result

More examples ?

	$\mathcal{E}_1$	$\mathcal{E}_2$
Homomorphism	$\emptyset$	$f(g(x,y)) \to g(f(x), f(y))$
Inv. Key	$\mathsf{dec}(\mathsf{enc}(x,y), y^{-1}) \to x$ $\mathsf{enc}(\mathsf{dec}(x,y), y^{-1}) \to x$ $(x^{-1})^{-1} \to x$	$\emptyset$
Abelian Groups	$x \bullet x^{-1} \bullet y \to y$ $x \bullet x^{-1} \to 1$ $x \bullet 1 \to x$	$x \bullet (y \bullet z) = (x \bullet y) \bullet z$ $x \bullet y = y \bullet x$ $(x^{-1})^{-1} \to x$ $(x \bullet y)^{-1} \to y^{-1} \bullet x^{-1}$ $1^{-1} \to 1$

CONCLUSION

- A proof normalisation, which yields a decision procedure for a bounded number of sessions
- Parametrisation by the intruder theory and the equational theory (cf. “oracle rules in [Chevalier et al 2003]).
- New problems in rewriting and unification
- A complete strategy, which should be well-suited for implementation