Intruder deductions with AC symbols.

Sergiu Bursuc
work with Hubert Comon and Stephanie Delaune

ARTIST 2 Workshop, May 2006

Outline

1. An approach to the analysis of cryptographic protocols.
   - From protocol specification to formal models of security.
   - Handling algebraic properties: Finite variant property.
2. Current problem.
   - Definition.
   - Examples.
   - Partial results.

Protocol specification and intruder theory.

Protocol specification: agents send and receive messages.

$$A(\overline{z}) = \lambda \overline{x} \nu \overline{N} : \begin{cases} u_1 \longrightarrow v_1 \\ u_2 \longrightarrow v_2 \\ \ldots \\ u_m \longrightarrow v_m \end{cases}$$

Protocol execution: bounded number of sessions.

$$A(p, q) \mid A(q, r) \mid A(p, r) \mid B(p, q) \mid B(q, r)$$

Intruder capabilities:

- Knows any message from the network.
- Knows the information of compromised agents.
- Can construct and send messages to any agent.
- $T_0, I, \ E.$

Intruder modelisation.

Execute the protocol: guess an interleaving of actions

$$\begin{cases} u_1 & \longrightarrow & v_1 \\ u_2 & \longrightarrow & v_2 \\ & \dots & \\ u_n & \longrightarrow & v_n \end{cases}$$

Security issue: accessibility of this guess

$$\begin{cases} T_0 & \Vdash & u_1 \\ T_0, v_1 & \Vdash & u_2 \\ & \dots & \\ T_0, v_1, \dots, v_{n-1} & \Vdash & u_n \\ T_0, v_1, \dots, v_{n-1}, v_n & \Vdash & secret \end{cases}$$

Formal model - constraint systems

Ground deducibility: $v_1, \ldots, v_n \vdash_{I,E} u$

Constraint systems: Syntax

$$C = \begin{cases} T_1 & \Vdash & u_1 \\ T_1, T_2 & \Vdash & u_2 \\ & \ldots & \\ T_1, T_2, \ldots, T_n & \Vdash & u_n \end{cases}$$

Syntactic properties:

- Monotonicity: no information is lost.
- Origination: a variable first appears on the right.

Semantics: σ satisfies C in (I, E) if

$$\begin{cases} T_1\sigma & \vdash_{I,E} & u_1\sigma \\ T_1\sigma, T_2\sigma & \vdash_{I,E} & u_2\sigma \\ & \ldots & \\ T_1\sigma, T_2\sigma, \ldots, T_n\sigma & \vdash_{I,E} & u_n\sigma \end{cases}$$

Equational theories and finite variant property.

H.Comon-Lundh and S.Delaune - 2005

Protocol insecurity $\equiv$ Satisfiability of C in (I, E).

Finite variant property: reduce E to AC.

- $C \longrightarrow Var(C)$
- $I \longrightarrow Var(I)$
- C is satisfiable in (I, E) iff
  $\exists C' \in Var(C)$: C' is satisfiable in $(Var(I), AC)$.

Relevant equational theories: AG, ACUN, Diffie-Helman, etc.

Example: AG.

$$x * (y * z) = (x * y) * z \qquad x * x^{-1} = 1$$
$$x * y = y * x \qquad x * 1 = x$$

Practical protocol: France Telecom.

Definition of the problem.

Terms.
- *Constants*: $a_1, a_2, ..., a_n$
- *Ground terms*: $t = \Sigma_i \lambda_i a_i$, where $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$
- *Terms with variables*: $v = t + \Sigma_x \lambda_x x$.

Deducibility relation for ground terms.

$v_1, v_2, ..., v_n \vdash u$ if $\exists \lambda_1, \ldots, \lambda_n \in \mathbb{N}$: $u = \Sigma_i \lambda_i v_i$.

Constraint systems:

$$\begin{cases} T_1 & \Vdash & u_1 \\ T_1, T_2 & \Vdash & u_2 \\ & \ldots & \\ T_1, T_2, \ldots, T_n & \Vdash & u_n \end{cases}$$

Monotonicity: no information is lost.

Origination: a variable first appears on the right.

Question: Is there a substitution σ s.t. for any i:

$T_1\sigma, T_2\sigma, ..., T_i\sigma \vdash u_i\sigma$?

Examples

- Example 1.

$$\begin{cases} 2a & \Vdash & X + a \\ 2a, X + c & \Vdash & Y + c \\ 2a, X + c, Y & \Vdash & 2a + c \end{cases}$$

Solution: $X = a, \ Y = a$

- Example 2.

$$\begin{cases} a + 2b & \Vdash & 2X \\ a + 2b, X + b & \Vdash & 2X + a \end{cases}$$

Solution: does not exist.

- Example 3.

$$\begin{cases} a & \Vdash & X \\ a, X + b & \Vdash & Y + b \\ a, X + b, Y + c & \Vdash & 2X + c \end{cases}$$

Dependencies: $Y = X + \lambda a, 2X = Y + \lambda' a$

Difficulties

Undecidability: without monotonicity.

- i.e code multiplication.

Straightforward approach: introduces non-linearities.

- $\left\{\begin{array}{rcl} a & \Vdash & X \\ a, X & \Vdash & Y \end{array}\right.$
- $\left\{\begin{array}{l} X = \lambda a \\ Y = \lambda' a + \lambda'' \lambda a \end{array}\right.$

Particular case - a single variable on the right.

Definition: $\left\{ \begin{array}{lll} T_1 & \Vdash & u_1 \\ T_2 & \Vdash & u_2 \\ & \dots & \\ T_n & \Vdash & u_n \end{array} \right.$, where $u_i = \beta_i X_i + \gamma_i$

Approach:

- Search for minimal solutions.
- Partition the set of variables into equivalence classes.
- Characterize the relation between minimal solutions of some subsystems.
- Reduce the system to a smaller one by eliminating the minimal class.

Details of the proof

Useful terms: Guess $U_i \subseteq T_i$

Occurence relation: $X \prec_{occ} Y$ iff $\exists i, v$ s.t $\begin{cases} Y \in Var(u_i) \\ X \in Var(v) \\ v \in U_i \end{cases}$

Equivalence classes: $X =_{occ} Y$ iff $X \prec_{occ} Y$ and $Y \prec_{occ} X$

Goal of the following lemmas: Eliminate a minimal class of $=_{occ}$.

Details of the proof

Lemma 1: If $=_{occ}$ has a single equivalence class.
Then $\exists C$ which bounds the λ-coefficient of every non-ground term.

$$X_1 \prec_{occ} X_2 \prec_{occ} \dots \prec_{occ} X_n \prec_{occ} X_1$$

$$\begin{cases} \lambda_1 X_1 + t_1 & = & \beta_1 X_2 + \gamma_1 \\ \lambda_2 X_2 + t_2 & = & \beta_2 X_3 + \gamma_2 \\ & \dots & \\ \lambda_n X_n + t_n & = & \beta_n X_1 + \gamma_n \end{cases}$$

Corollary: Linear system $(X, \Lambda) = (X_0, \Lambda_0) + \Sigma c_i w_i$

Minimal class: M, S' - the subsystem determined by M, $X \in M$

$X\sigma = X\theta + \Sigma c_i w_i^X$

σ - a general solution of S'

θ - a minimal solution of S'

w_i - minimal solutions of S'_h

Details of the proof

Notation: x - the index of the constraint introducing X.

Lemma 2: $\exists\beta$ s.t. $\beta w_i^X = \Sigma\lambda_t t$, with $t \in T_x$ and t-ground.

Proof: $X \prec'_{occ} Y$ iff $(X \prec_{occ} Y, x < y)_{lex}$
Use induction.

Lemma 3: If σ - minimal solution of S and $X \in M$ then
$\exists\theta$ - a minimal solution of S',
$\exists w(S')$ - a vector depending only on S' s.t.
$X\sigma \leq X\theta + w$.

Proof: Use Lemma 2, origination and monotonicity.

Corollary: Eliminate M by solving S'

Future work

- Decidability of the (general) pure AC case.
- Combination results.
- Long term goal: be able to make a program for analysing real-world protocols from a generic class (i.e. France Telecom protocol)