Undecidability of Secrecy for Security Protocols

– addendum to CDC –

Prof.Dr. Ferucio Laurenţiu Ţiplea

Department of Computer Science

“Al.I.Cuza” University of Iasi

Iasi, Romania

E-mail: fltiplea@mail.dntis.ro

Contents

- Modeling security protocols
- Undecidability of secrecy

Excerpt from:

- F.L. Ţiplea, C. Enea, C.V. Bîrjoveanu. *Decidability and Complexity Results for Security Protocols*, Proceedings of VISSAS 2005, IOS Press

Modeling security protocols

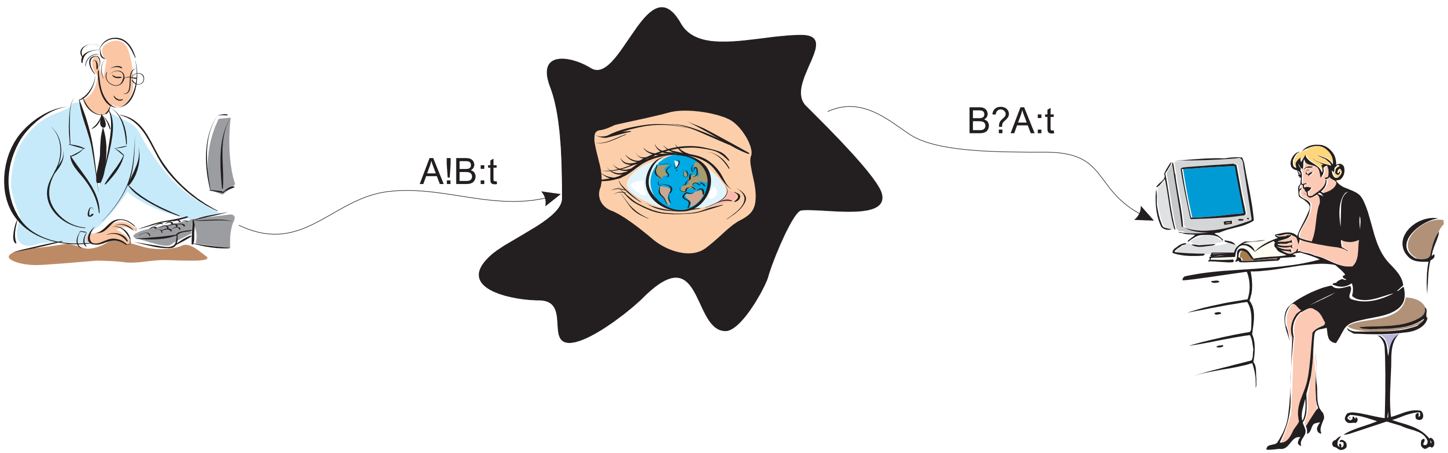
- Specification = set of rules which defines the protocol's goal
  - $A \to B \; : \; t$

- Example: the Woo-Lam authentication protocol:

$$
\begin{array}{llcl}
1. & A \to B & : & A \\
2. & B \to A & : & N_b \\
3. & A \to B & : & \{A, B, N_b\}_{K_{AS}} \\
4. & B \to S & : & \{A, B, \{A, B, N_b\}_{K_{AS}}\}_{K_{BS}} \\
5. & S \to B & : & \{A, B, N_b\}_{K_{BS}}
\end{array}
$$

Modeling security protocols

- Analysis and verification – the intruder should be taken into consideration



Modeling security protocols

- Dolev-Yao intruder's capabilities:
  - can copy every communication in the system
  - can block any message
  - can impersonate any honest agent
  - has unlimited computational power
  - can keep record of any public system event and utilize it at any later time
- Dolev-Yao intruder cannot
  - generate honest agents' secrets
  - break encryptions
- any group of Dolev-Yao intruders colluding with one another cannot cause more attacks than a single intruder acting alone (Syvervon et. al., 1999)

Modeling security protocols

- rules $A \rightarrow B : t$ are decomposed into actions:
  - $A!B \ : \ (M)t$ (send action)
  - $B?A \ : \ t$ (receive action)

  (M is the set of all fresh nonces and keys in t).
- protocol – $\mathcal{P} = (\mathcal{S}, \mathcal{C}, w)$, where:
  - $\mathcal{S}$ is a protocol signature (agents, keys, nonces);
  - $\mathcal{C}$ is the set of protocol constants;
  - w is a sequence of actions.
- role = $w|_A$, where $A \in \mathcal{A}$.

Modeling security protocols

- substitution – used to instantiate protocols:
  - agents $\stackrel{\sigma}{\to}$ agents;
  - keys $\stackrel{\sigma}{\to}$ keys;
  - nonces $\stackrel{\sigma}{\to}$ arbitrary terms;
- event = instantiated action;
- analz and synth – standard rules of analysis and synthesis
  - $\overline{X} = synth(analz(X))$
- state
  - $s = (s_A | A$ agent);
  - s_A a set of terms (A's knowledge).

Modeling security protocols

We write $s[e\rangle s'$ if and only if:

- if the action of e is $A!B : (M)t$, then:
  - $t \in \overline{s_A \cup M}$ and $M \cap Sub(s) = \emptyset$ (enabling condition)
  - $s'_A = s_A \cup M \cup \{t\}$, $s'_I = s_I \cup \{t\}$, and $s'_C = s_C$, for all $C \in \mathcal{A} - \{A, I\}$;
- if the action of e is $A?B : t$, then:
  - $t \in \overline{s_I}$ (enabling condition)
  - $s'_A = s_A \cup \{t\}$ and $s'_C = s_C$, for all $C \in \mathcal{A} - \{A\}$.

Runs are obtained by interleaving instantiated roles under the enabling condition and preserving the order of events in each role.

Modeling security protocols

Let $\mathcal{T}_0$ be the set of basic terms (agents, keys, nonces).

- $t \in \mathcal{T}_0$ is called secret at a state s if $t \in analz(s_A) - analz(s_I)$, for some honest agent A;
- $t \in \mathcal{T}_0$ is called secret along a run $\xi = e_1 \cdots e_k$ if it is secret at s, where $s_0[e_1 \cdots e_k\rangle s$;
- a run $\xi = e_1 \cdots e_k$ is leaky w.r.t. $T \subseteq \mathcal{T}_0$ if there exists $t \in T$ such that t is secret along some proper prefix of ξ but it is not secret along ξ. When $T = \mathcal{T}_0$, ξ is called a leaky run;
- secrecy problem (w.r.t. T) = decide whether or not a given protocol has leaky runs (w.r.t. T).

Undecidability of secrecy

Reduce the halting problem for counter machines to the secrecy problem. Two cases are to be taken into consideration

- infinitely many nonces and bounded-length messages
- finitely many nonces and arbitrary-length messages

Infinitely many nonces and bounded-length messages

Notation on counter machines:

- 2-counter machine: $M = (Q, \delta, q_0, F)$, where

$$\delta \subseteq Q \times \{0,1\}^2 \times Q \times \{-1,0,1\}^2$$

  such that

$$(\forall k)(q, i_1, i_2, q', j_1, j_2) \in \delta \ \wedge \ j_k = -1 \ \Rightarrow \ i_k = 1)$$

- Computation: $(q, n_1, n_2) \vdash (q', n_1 + j_1, n_2 + j_2)$ iff
  - $(q, i_1, i_2, q', j_1, j_2) \in \delta$, and
  - $(\forall k)(i_k = 0 \ \Leftrightarrow \ n_k = 0)$

Infinitely many nonces and bounded-length messages

- Encoding natural numbers by nonces:
  - 0 is encoded by a fixed nonce z;
  - $n > 0$ is encoded by a nonce u_n for which there exist distinct nonces $u_0 = z, \ldots, u_{n-1}$ such that $\{u_i, u_{i+1}\}_K \in \overline{s_I}$, for all $0 \leq i < n$;
- Incrementation:
  - $n \mapsto n+1$: generate a new nonce u_{n+1} and send $\{u_n, u_{n+1}\}_K$
- Decrementation:
  - $n \mapsto n-1$: the intruder has already $\{u_{n-1}, u_n\}_K$

Infinitely many nonces and bounded-length messages

The protocol associated to a 2CM:

- $A!B \quad : \quad \{z,z\}_K, \{q_0,z,z\}_K, \{z,z\}_K$

- a transition $t = (q, 0, 1, q', 1, -1) \in \delta$ is simulated by:

$$\begin{array}{lcl} C_t?D_t & : & \{z,z\}_K, \{q,z,v\}_K, \{v',v\}_K \\ C_t!D_t & : & (\{u'\})\,\{z,u'\}_K, \{q',u',v'\}_K, \{z,z\}_K \end{array}$$

- $$\begin{array}{lcl} F_q?E_q & : & \{q,u,v\}_K \\ F_q!E_q & : & (\{x\})\,\{x\}_K \\ F_q!E_q & : & x \end{array}$$

  where $q \in F$.

Infinitely many nonces and bounded-length messages

Theorem 1 M halts iff $\mathcal{P}_M$ reveals the secret.

The main characteristics of this simulation:

- infinitely many nonces;
- bounded-depth encryptions;
- bounded-length messages.

Corollary 1 Secrecy for protocols under infinitely many nonces and bounded-length messages is undecidable.

Finitely many nonces and unbounded-length messages

- Encoding natural numbers by nonces:
  - $\underline{0} = z$;
  - $\underline{n} = (\underline{n-1}, z)$, if $n > 0$.
- Incrementation:
  - $n \mapsto n+1$: send $(\underline{n}, z)$
- Decrementation:
  - $n \mapsto n-1$: decompose $\underline{n} = (\underline{n-1}, z)$

Finitely many nonces and unbounded-length messages

The protocol associated to a 2CM:

- $A!B \quad : \quad \{\underline{q_0}, z, z\}_K$

- a transition $t = (q, 0, 1, q', 1, -1) \in \delta$ is simulated by:

  $$\begin{array}{lcl} C_t?D_t & : & \{\underline{q}, z, (v, z)\}_K \\ C_t!D_t & : & \{\underline{q}', (z, z), v\}_K \end{array}$$

- $$\begin{array}{lcl} F_q?E_q & : & \{\underline{q}, u, v\}_K \\ F_q!E_q & : & (\{x\})\,\{x\}_K \\ F_q!E_q & : & x \end{array}$$

  where $q \in F$.

Finitely many nonces and unbounded-length messages

Theorem 2 M halts iff $\mathcal{P}_M$ reveals the secret.

The main characteristics of this simulation:

- finitely many nonces;
- bounded-depth encryptions;
- arbitrary-length messages.

Corollary 2 Secrecy for protocols under finitely many nonces and unbounded-length messages is undecidable.