TD 4: Intruder deduction problem and locality

Margot Catinaud margot.catinaud@lmf.cnrs.fr

Exercise 1 (Intruder deduction problem and locality)

Recall the definition of locality for a deduction system and the intruder deduction problem:

Definition 1: Locality

A deduction system $\mathcal{D}$ is local if for all T finite set of terms and term s such that $\mathsf{T} \vdash \mathsf{s}$, there is a proof tree Π of that fact such that

$$\mathsf{Terms}(\Pi) \subseteq \mathsf{st}(\mathsf{T} \cup \{\mathsf{s}\}).$$

Where $\mathsf{Terms}(\Pi)$ is the set of terms that appear in a given proof tree Π and $\mathsf{st}(\mathsf{E})$ is the set of sub-terms of terms in E.

Definition 2: Intruder deduction problem

Let $\mathcal{I}$ be an inference system. The intruder deduction problem is:

Input: a finite set of terms T and a term s.

Output: whether $\mathsf{T} \vdash_{\mathcal{I}} \mathsf{s}$.

1. Show that the intruder deduction problem is decidable for a local deduction system.
   Hint: You can find a PTIME algorithm that decides this problem.
2. Can you find an inference system for which the intruder deduction problem is undecidable?

Exercise 2 (Dolev-Yao inference system)

Consider the following deduction system:

$$\frac{x \quad y}{\langle x\,,\, y\rangle} \qquad \frac{\langle x\,,\, y\rangle}{x} \qquad \frac{\langle x\,,\, y\rangle}{y}$$

$$\frac{x \quad y}{\mathsf{senc}(x,y)} \qquad \frac{\mathsf{senc}(x,y) \quad y}{x}$$

$$\frac{x \quad y}{\mathsf{aenc}(x,y)} \qquad \frac{\mathsf{aenc}(x,\mathsf{pk}(y)) \quad y}{x}$$

1. Show that it is local.
   Hint: A valid proof tree to consider is any minimal (in the number of terms (with multiplicity)) proof tree.
2. Conclude that the intruder deduction system is decidable on this inference system.

We are now interested in a new procedure for deciding if a term s is deducible from a set of term T in the inference system described above, we propose the following algorithm:

Algorithm 1: Procedure for deducibility of terms

- Apply the decryption and projection rules as much as possible. This leads to a (finite) set of terms called $\mathtt{analz}(\mathsf{T})$
- Check whether s can be obtained by applying the encryption and the pairing rules. The (infinite) set of terms obtained by applying the composition rules is denoted $\mathtt{synth}(\mathtt{analz}(\mathsf{T}))$.
- Return $\mathsf{s} \in \mathtt{synth}(\mathtt{analz}(\mathsf{T}))$.

3. Show that this algorithm terminates.
4. Show that this algorithm is sound, *i.e.* if the algorithm returns yes then $\mathsf{T} \vdash \mathsf{s}$.

5. The algorithm is not complete, *i.e.* there exists T and s such that $\mathsf{T} \vdash \mathsf{s}$, and for which the algorithm returns no. Find an example illustrating this fact.
6. Give a hypothesis on T that allows one to restore completeness.
7. Show that the algorithm is complete with this added hypothesis.

Exercise 3 (Blind signature and intruder deduction problem)

In this exercise, we consider *blind signatures* represented by the following inference system:

Definition 3: Blind signatures inference system $\mathcal{I}_{\mathsf{blind}}$

$$\frac{x \quad y}{\langle x\,,\, y\rangle} \qquad \frac{\langle x\,,\, y\rangle}{x} \qquad \frac{\langle x\,,\, y\rangle}{y}$$

$$\frac{x \quad y}{\mathsf{blind}(x,y)} \qquad \frac{x \quad y}{\mathsf{sign}(x,y)} \qquad \frac{\mathsf{sign}(\mathsf{blind}(x,y),z) \quad y}{\mathsf{sign}(x,z)} \qquad \frac{\mathsf{blind}(x,y) \quad y}{x}$$

1. Find a set of messages T and a name n such that $\mathsf{T} \vdash n$ with this inference system but $\mathsf{T} \nvdash n$ with the inference system of the previous exercise.
2. Show that this inference system is not local.
3. Provide an algorithm to decide the intruder deduction problem for this inference system.
   Hint: you can "adapt" the definition of locality with an extended notion of subterms: the set $\mathsf{st}_{\mathsf{ext}}(t)$ is the smallest set such that
   - $\mathsf{st}(t) \subseteq \mathsf{st}_{\mathsf{ext}}(t)$
   - if $\mathsf{sign}(\mathsf{blind}(x,y),z) \in \mathsf{st}_{\mathsf{ext}}$ then $\mathsf{sign}(x,z) \in \mathsf{st}_{\mathsf{ext}}(t)$

Exercise 4 (Back to the Needham-Schroeder-Lowe protocol)

We recall the Needham-Schroeder protocol between A and B:

$$\begin{aligned} A &\to B : \{A, N_A\}_{\mathsf{pk}(B)} \\ B &\to A : \{N_A, N_B\}_{\mathsf{pk}(A)} \\ A &\to B : \{N_B\}_{\mathsf{pk}(B)} \end{aligned}$$

1. Explicit the signature set Σ and the rewriting rules set that captures all primitives needed for this protocol.
2. Write this protocol in the process calculus.
3. Express the secrecy property of N_A and N_B, and the one representing the authentication of A regarding B.
4. Give a trace of the protocol for one session of both A and B. Moreover, for each step, give the set of messages that are deducible by an attacker.

Then, we recall the Needham-Schroeder-Lowe protocol between A and B which fix the attack against the secrecy of N_A and N_B:

$$\begin{aligned} A &\to B : \{A, N_A\}_{\mathsf{pk}(B)} \\ B &\to A : \{B, N_A, N_B\}_{\mathsf{pk}(A)} \\ A &\to B : \{N_B\}_{\mathsf{pk}(B)} \end{aligned}$$

5. Write this protocol in the process calculus.
6. We consider in this question an unbounded number of sessions of A and B. Show that in this case, secrecy of N_A and N_B are ensured.
   Hint: Give an invariant of the protocol on N_A and N_B.