TD 1: LTS, security properties, process calculus

Margot Catinaud margot.catinaud@lmf.cnrs.fr
Théo Vignon theo.vignon@lmf.cnrs.fr

November 15, 2024

Exercise 1: Terms and equational theory

Consider the signature $\Sigma = \{\mathsf{senc}/2, \mathsf{sdec}/2, \mathsf{pair}/2, \mathsf{proj}_1/1, \mathsf{proj}_2/1, \mathsf{ok}/0\}$ (intuitively representing a symmetric encryption scheme and a pairing function). In this exercise, we consider the semantic induced by some equational theory E. For now, E is composed of $\mathsf{sdec}(\mathsf{senc}(x, y), y)\ E\ x$. This equation models the correctness of the encryption scheme.

1. What relations are necessary to add to E to model the projections?
2. Expend the signature to add the necessary components for
   (a) an asymmetric encryption scheme
   (b) an signature scheme
   (c) an authenticated encryption with associated data (i.e. an asymmetric encryption with some extra plaintexts that will not be encrypted but still be authenticated)
3. Expend E to model the correctness of the previous add-ons to the signature

Exercise 2: Another interpretation

We want to define another interpretation on terms, not based on a equational theories but on random variables. These random variables will be parameterized by some security parameter $\eta \in \mathbb{N}$ and a "random" tape of bits ρ to draw the randomness (the interpretation of the names). Intuitively, η is an natural number that represent some characteristic number of the protocol, the length of keys is a classical example. As for the randomness, one way of doing it is to consider, for each $\eta \in \mathbb{N}$, a finite subset $\mathbb{T}_\eta$ of $\{0,1\}^*$ with all elements of the same length. Formally, we can define the interpretation domain $\mathcal{D}$ that correspond to those random variables as:

$$\mathcal{D} := \Big\{ X : \mathbb{N} \times \{0,1\}^* \to \{0,1\}^* \cup \{\bot\} \mid \forall \eta \in \mathbb{N}, \rho \in \{0,1\}^*, \rho \notin \mathbb{T}_\eta \Rightarrow X(\eta, \rho) = \bot \Big\}$$

Therefore the interpretation function $[\![\cdot]\!]$ go from terms to $\mathcal{D}$ (we will write $[\![\cdot]\!]^{\eta,\rho}$ for $[\![\cdot]\!](\eta, \rho)$).
We also require that:

- we can split any tape ρ in two, ρ_n, ρ_o such that the interpretation of the names are sampled independently and uniformly at random of size η in ρ_n and the interpretation of any other symbols does not depend on ρ_n.
- the interpretation is compositional, meaning that you can give an interpretation of a function symbol f of arity n as a function from $\mathcal{D}^n$ to $\mathcal{D}$, and then get the interpretation of the terms recursively as intended (i.e. for all term $u_1, \ldots, u_n$ we have $[\![f(u_1, \ldots, u_n)]\!] = [\![f]\!]([\![u_1]\!], \ldots, [\![u_n]\!])$).

We can now take a look at the interpretation of function symbols. Considering the function symbols neq and eq that we want to use to represent the non-equality and equality between two terms.

1. Find a valid interpretation for neq and eq to make them match their respective description.
2. With your interpretation, what is the interpretation of those terms:

   (a) $\mathsf{neq}(n, n)$ (b) $\mathsf{neq}(n, n')$ (c) $\mathsf{eq}(n, n)$ (d) $\mathsf{eq}(n, n')$

   where in each case, n and n' designate names

Exercise 2: Another interpretation

3. Does the interpretation of those terms match your expectation? Why?
4. Can you find a way to interpret neq and eq to make it work?
   Hint: Do you think an universal or existential quantification over ρ will work?
   Advice: Do not spend too much time on this question during the exercise session (5-10 minutes), after come to ask us.

Exercise 3: Alternative LTS definitions

Remember that a Labelled Transition System (LTS for short) is defined by $(\mathcal{Q}, \mathcal{L}, \mathsf{Vars}, q_\varepsilon, \sigma_\varepsilon, \delta)$ where:

- $\mathcal{Q}$ (resp. $\mathcal{L}$) is the set of states (resp. labels);
- Vars the set of state variables;
- q_ε (resp. σ_ε) the initial state (resp. initial substitution for state variables);
- δ the transition function associating to every state q an finite set $\delta(q)$ of transition of the form (l, c, t, σ_n, q') where l is a label, c is a term representing the conditions under which the transition can happens, t is the term outputted on the network, σ_n is the new substitution for state variables and q' is the state of arrival.

1. Another alternative definition of LTS does not contains the conditionals c in the transitions δ. Under some condition, the two definitions are equivalent (meaning that it is an isomorphism between the two underlying (labelled) graph).
   What are those conditions? Then prove that under these conditions the two definitions are indeed equivalent.
   Hint: One of the condition is to have a if _ then _ else _ function on terms to be able to express conditionals in terms.
2. Another alternative definition of LTS does not introduce labels in $\mathcal{L}$.
   Prove that the two definitions are indeed equivalent.

Exercise 4: Security Properties

Try to find a way to express these security properties in protocol between two parties A and B:

1. **Secrecy of some name s:** This mean that the adversary cannot know the name s;
2. **Unlinkability:** Here there is multiple A (with the same process but different identities) and multiple sessions of each A (i.e. each identity can be executed multiple times), the goal of the adversary is to know one A talking multiple times or not;
3. **Authentication:** Here at some point B want to be sure that she has indeed talked to A;
4. **Mutual authentication:** Here at some point B (resp. A) want to be sure that she talked to A (resp. B);
5. **Strong secrecy of some name s:** The adversary cannot know *anything* about the name s.

Hint: you can assume there is some event in the process to help you.

Exercise 5: A first protocol, and a first attack

Consider the following protocol between A and B defined as followed:

$$A \to B \ \ (A, \{s\}_{\mathsf{pk}(B)})$$
$$B \to A \ \ (B, \{s\}_{\mathsf{pk}(A)})$$

1. Write it down formally in the process calculus, without forget to explicit the signature used (as well as some underlying assumptions on the interpretation you assume).
2. Translate your process calculus into an labelled transition system
3. Show that the secrecy of s is not ensured. You can do it either with the LTS or the process calculus

Exercise 6: A flawed fix

Consider the following protocol between A and B defined as followed:

$$A \to B \ \ (\{A, \{s\}_{\mathsf{pk}(B)}\}_{\mathsf{pk}(B)})$$
$$B \to A \ \ (\{B, \{s\}_{\mathsf{pk}(A)}\}_{\mathsf{pk}(A)})$$

Show (informally) that the secrecy of s is not ensured.

Exercise 7: The Needham-Schroeder protocol

Consider the following protocol between A and B defined as followed:

$$A \to B \ \ \{A, N_A\}_{\mathsf{pk}(B)}$$
$$B \to A \ \ \{N_A, N_B\}_{\mathsf{pk}(A)}$$
$$A \to B \ \ \{N_B\}_{\mathsf{pk}(B)}$$

1. Write it down formally in the process calculus.
2. Translate your process calculus into an labelled transition system.
3. Write the property representing the secrecy of N_A, and the one representing the authentification of A regarding B.
4. Show that the secrecy of N_A is still not ensured. (Explicit the assumption you made on the interpretation to do it.)
5. Can you find a fix of this protocol to have the secrecy of N_A?

Exercise 8: A first fix: the Needham-Schroeder-Lowe protocol

Consider the following protocol between A and B defined as followed:

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

1. Write it down formally in the process calculus.
2. Show that the secrecy of N_A is finally ensured. (Explicit the assumption you made on the interpretation to do it.)

Exercise 9: Process Calculus to LTS

1. With all the examples of process calculus to LTS (in previous exercises), can you came up with a way to translate the process calculus to a LTS?
2. Does the operational semantics of the process calculus match the semantics given by the translated LTS?