# TD 1: Security properties and process calculus

Margot Catinaud margot.catinaud@lmf.cnrs.fr

### Exercise 1 (A first protocol, and a first attack)

Consider the following protocol between $A$ and $B$ defined as follows:

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

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. Show that the secrecy of $s$ is not ensured.

### Exercise 2 (A flawed fix)

Consider the following protocol between $A$ and $B$ defined as follows:

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

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

### Exercise 3 (Secrecy property)

Consider a protocol between two parties $A$ and $B$. Try to find a way to express the secrecy property of some name $s$, *i.e.* an adversary cannot know the name $s$.

### Exercise 4 (Terms and interpretation)

We recall that $\mathcal{T}(\mathcal{X}, \mathcal{N}, \Sigma)$ is the set of *terms* where elements of $\mathcal{X}$ are called *variables*, elements of $\mathcal{N}$ are called *names* and $\Sigma$ is the *signature* set. An *interpretation of* $\mathcal{T}(\mathcal{X}, \mathcal{N}, \Sigma)$ *on a domain* $\mathcal{D}$ is a function

$$[\![ \cdot ]\!] : \underbrace{\mathcal{T}(\mathcal{X}, \mathcal{N}, \Sigma)}_{\textbf{term}} \times \underbrace{(\mathcal{X} \longrightarrow \mathcal{D})}_{\textbf{substitution}} \longrightarrow \mathcal{D}.$$

We write $[\![ t ]\!]^\sigma$ for $[\![ \cdot ]\!](t, \sigma)$. For a *model* $\mathbb{M} : \mathcal{N} \cup \Sigma \longrightarrow \mathcal{D}$ and a substitution $\sigma : \mathcal{X} \longrightarrow \mathcal{D}$, $[\![ \cdot ]\!]$ is defined recursively as follows:

- $[\![ n ]\!]^\sigma \overset{\text{def}}{=} \mathbb{M}(n)$ for $n \in \mathcal{N}$ a name ;
- $[\![ x ]\!]^\sigma \overset{\text{def}}{=} \sigma(x)$ for $x \in \mathcal{X}$ a variable ;
- $[\![ f(t_1, \dots, t_n) ]\!]^\sigma \overset{\text{def}}{=} \mathbb{M}(f)\Big([\![ t_1 ]\!]^\sigma, \dots, [\![ t_n ]\!]^\sigma\Big)$ for $(f/n) \in \Sigma$ a function symbol.

Consider the signature $\Sigma = \big\{\mathsf{senc}/2, \mathsf{sdec}/2, \mathsf{pair}/2, \mathsf{proj}_1/1, \mathsf{proj}_2/1, \mathsf{ok}/0\big\}$ (intuitively representing a symmetric encryption scheme and a pairing function). Besides, we suppose that the interpretation of $\mathsf{senc}$ and $\mathsf{sdec}$ match with we expect of symmetric encryption :

$$\forall\, m, k \in \mathcal{T}(\mathcal{X}, \mathcal{N}, \Sigma),\ \forall\, \sigma : \mathcal{X} \longrightarrow \mathcal{D},\ [\![ \mathsf{sdec}(\mathsf{senc}(m, k), k) ]\!]^\sigma = [\![ m ]\!]^\sigma.$$

1. What constraints do the interpretation $[\![ \cdot ]\!]$ need to satisfies to model projections?
2. Expend the signature to add the necessary components for
   (a) an asymmetric encryption scheme ;
   (b) a 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. Add necessary constraints on $[\![ \cdot ]\!]$ to model the correctness of the previous add-ons to the signature.

**Exercise 5 (The Needham-Schroeder protocol)**

Consider the following protocol between $A$ and $B$ defined as follows:

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

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

**Exercise 6 (A first fix: the Needham-Schroeder-Lowe protocol)**

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

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

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 7 (An interpretation of terms)**

We want to define an interpretation on terms, based on random variables. These random variables will be parameterized by some security parameter $\eta \in \mathbb{N}$ and a "random" tape of bits $\rho \in \{0,1\}^*$ to draw the randomness (the interpretation of the names). Intuitively, $\eta$ 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:

$$\mathcal{D} \overset{\text{def}}{=} \left\{ X : \mathbb{N} \times \{0,1\}^* \rightarrow \{0,1\}^* \cup \{\bot\} \;\middle|\; \forall \eta \in \mathbb{N},\ \forall \rho \in \{0,1\}^*,\ \rho \notin \mathbb{T}_\eta \Rightarrow X(\eta, \rho) = \bot \right\}$$

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

- we can split any tape $\rho$ in two, $\rho_h, \rho_a$ such that the interpretation of the names in $\mathcal{N}$ are sampled independently and uniformly at random of size $\eta$ in $\rho_h$ and the interpretation of any other symbols does not depend on $\rho_h$.
- the interpretation is compositional, meaning that you can give an interpretation of a function symbol $(f/n) \in \Sigma$ of arity $n$ as a function from $\mathcal{D}^n$ to $\mathcal{D}$, and then get the interpretation of the terms recursively as intended: for all terms $t_1, \ldots, t_n$ we have $[\![ f(t_1, \ldots, t_n) ]\!]^\sigma = \mathbb{M}(f)\Big([\![ t_1 ]\!]^\sigma, \ldots, [\![ t_n ]\!]^\sigma\Big)$.

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

1. Find a valid interpretation for $\mathsf{neq}$ and $\mathsf{eq}$ 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 in $\mathcal{N}$.
3. Does the interpretation of those terms match your expectation? Why?
4. Can you find a way to interpret $\mathsf{neq}$ and $\mathsf{eq}$ to make it work?
   **Hint:** Do you think an universal or existential quantification over $\rho$ will work?
   **Advice:** Do not spend too much time on this question during the exercise session (5-10 minutes)