CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL
Institut für Informatik · AG Software Engineering
Priv.-Doz. Henning Schnoor

# Engineering Secure Software Systems Winter 2020/21
# Exercise Sheet 5

**issued:** December 1, 2020 **due:** December 10, 2020

## Exercise 5.1, Formal Protocol Model: Features and Omissions (10 Points)

There are a couple of usually assumed properties of cryptographic systems that are not explicitly expressed in our protocol model. Which of the following properties are implicitly expressed in our model, and which are not? Are any of the "omissions" problematic?

- Nonces are indeed used only once, and are freshly generated for each session.
- Private keys are never sent over the network.
- There is a complete public-key infrastructure PKI available.
- Nonces are long enough so that the adversary cannot guess them correctly.
- The adversary knows the involved algorithms, including the protocol (Kerckhoffs's principle).
- In the absence of an adversary, the network simply forwards the protocol participant's messages as intended.

## Exercise 5.2, exponential attack size (10 Points)

For $i \in \mathbb{N}$, the protocol $P_i$ is defined as follows:

- There are two instances:
  1. $\mathscr{I}_1$ has a single receive/send action $[x_1, \ldots, x_i] \to \mathsf{enc}^{\mathsf{s}}_k([t_1, t_2])$, with

     $t_1 = [x_1, [x_2, [x_3, [x_4, [\ldots, [x_{i-1}, [x_i, 0]]\ldots]]]]]$
     $t_2 = [[[[[\ldots[[0, x_i], x_{i-1}], \ldots], x_4], x_3], x_2], x_1]$.
  2. $\mathscr{I}_2$ has a single receive/send action $\mathsf{enc}^{\mathsf{s}}_k(y, y) \to \mathsf{FAIL}$.
- The initial adversary knowledge is the set $\{0, 1\}$.

Show that each protocol $P_i$ is insecure, but a successful attack requires terms of exponential length. How can you use DAGs to obtain a shorter representation of the involved terms?

**Solution** In order to derive FAIL, the adversary must be able to derive a term of the form $\mathsf{enc}^{\mathsf{s}}_k(t, t)$ for some term $t$. The only way to generate any term encrypted with the secret key $k$ for the adversary is to supply, via a substitution $\sigma$, values for the variables $x_1, \ldots, x_i$ to $\mathscr{I}_1$. As a reply, the adversary receives the term $\mathsf{enc}^{\mathsf{s}}_k([t_1\sigma, t_2\sigma])$. Therefore, a successful attack consists of a substitution $\sigma$ that satisfies $t_1\sigma = t_2\sigma$ (the execution order consists of the two obvious steps). We denote the subterms of $t_1$ and $t_2$ as follows:

- with $t_1^{j\rightarrow}$, denote the term $[x_j, [x_{j+1}, \ldots, [x_{i-1}, [x_i, 0]]\ldots]]$,
- with $t_2^{j\rightarrow}$, denote the term $[[\ldots[[0, x_i], x_{i-1}], \ldots, x_{j+1}], x_j]$.

By construction, $t_1 = t_1^{1\rightarrow}$ and $t_2 = t_2^{1\rightarrow}$, further:

- $t_1^{j\rightarrow} = [x_j, t_1^{j+1\rightarrow}]$ and

- $t_2^{j\rightarrow} = [t_2^{j+1\rightarrow}, x_j]$.

Assume that $\sigma$ is a substitution with $t_1\sigma = t_2\sigma$. We show inductively that for all $j$, we have that $t_1^{j\rightarrow}\sigma = t_2^{j\rightarrow}\sigma$. For $j = 1$, the claim follows since $t_a = t_a^{1\rightarrow}$. Now assume the claim is true for $j$, i.e., $t_1^{j\rightarrow}\sigma = t_2^{j\rightarrow}\sigma$. By the above, we have

$$t_1^{j\rightarrow} = [x_j, t_1^{j+1\rightarrow}] \text{ and } t_2^{j\rightarrow} = [t_2^{j+1\rightarrow}, x_j].$$

By applying $\sigma$ to both components of the terms, we obtain

- $\sigma(x_j) = \sigma(t_2^{j+1\rightarrow})$ (left-hand side of the pair), and
- $\sigma(x_j) = \sigma(t_1^{j+1\rightarrow})$ as claimed.

This additionally establishes that for all $j$, $\sigma(x_j) = \sigma(t_1^{j+1\rightarrow}) = \sigma(t_2^{j+1\rightarrow})$.

We now show inductively that $\left|\sigma(x_j)\right|$ is at least $2^{i-j}$. For $j = 1$, this completes the proof. The induction start $j = i$ is clear, as $\sigma(x_i) = 0$. For the induction step, assume that $\left|\sigma(x_j)\right| \geq 2^{i-j}$, we show the claim for $j-1$. By the above, we have that

$$\sigma(x_{j-1}) = \sigma(t_1^{j\rightarrow}) = \sigma(t_2^{j\rightarrow}).$$

By the definition of $t_\cdot^{j\rightarrow}$, we get

$$\sigma(x_{j-1}) = \sigma([x_j, t_1^{j+1\rightarrow}]) = [t_2^{j+1\rightarrow}, x_j].$$

Therefore, $\sigma(x_{j-1}) = [\sigma(x_j), \sigma(x_j)]$, and in particular, $\left|\sigma(x_{j-1})\right| \geq 2\left|\sigma(x_j)\right| \geq 2 \cdot 2^{i-j} = 2^{i-(j-1)}$, as claimed.

## Exercise 5.3, no unique successful minimal attack (10 Points)

Show that in general, there is no unique minimal successful attack on a protocol. That is, construct a protocol and two different successful attacks on it that both have minimal size.

## Exercise 5.4, parsing lemma proof (10 Points)

In the proof of the Parsing Lemma, we showed that in that particular setting, the term $\sigma(x)$ is constructed by the adversary. Is this generally true? More precisely: Is there a protocol $P$ with initial knowledge $I$ and a successful minimal attack $(o, \sigma)$ such that there is a variable $x$ with $\sigma(x) \neq x$ and $\sigma(x) \notin \mathsf{DY}(S)$, where $S$ is the set of terms available to the adversary at the step where the first term containing $\sigma(x)$ is sent?

**Solution** Consider the following rules:

Alice:

- $\epsilon \rightarrow \mathsf{enc}^{\mathsf{a}}_{k_B}\left(\mathsf{enc}^{\mathsf{s}}_{k_{AB}}(N_A)\right)$

Bob:

- $\mathsf{enc}^{\mathsf{a}}_{k_B}\left(\mathsf{enc}^{\mathsf{s}}_{k_{AB}}(x)\right) \rightarrow \mathsf{FAIL}$

Then in any successful attack, $\sigma(x) = N_A$, since there is no other way for the adversary to generate a ciphertext encrypted with $k_{AB}$, but clearly the adversary cannot derive $N_A$. Here, $N_A$ can be replaced with an arbitrarily complex term to also match the $|\sigma(x)| > 1$ condition.