

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. \mathcal{J}_1 has a single receive/send action $[x_1, \dots, x_i] \rightarrow \text{enc}_k^S([t_1, t_2])$, with
$$\begin{aligned} t_1 &= [x_1, [x_2, [x_3, [x_4, [\dots, [x_{i-1}, [x_i, 0]] \dots]]]] \\ t_2 &= [[[[[\dots [[0, x_i], x_{i-1}], \dots], x_4], x_3], x_2], x_1]. \end{aligned}$$
 2. \mathcal{J}_2 has a single receive/send action $\text{enc}_k^S(y, y) \rightarrow \text{FAIL}$.
- 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?

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, σ) such that there is a variable x with $\sigma(x) \neq x$ and $\sigma(x) \notin \text{DY}(S)$, where S is the set of terms available to the adversary at the step where the first term containing $\sigma(x)$ is sent?