Exercise for Engineering Secure Software Systems

December 17, 2019, “Lockdown Edition”: Exercises 5, 6

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

ESSS Student Meetings?

suggestion from you

meet and discuss tasks among yourselves

possibilities, if interest

- use `https://wetalk.informatik.uni-kiel.de/home/channels/inf-esss`
- I can set up Zoom Meeting
- comments?

Leftovers

Exercise

Task (Formal Representation of the Woo Lam Protocol)

Study the authentication protocol by Woo and Lam (see slide 17 of the lecture from November 10).

1. Specify the protocol as sequence of receive/send actions, once in the intended execution between Alice and Bob, and once in a form that allows to model the attack introduced in the lecture.
2. Specify the attack on the protocol formally.
3. How can we modify the protocol in order to prevent this attack?

Exercise

Task (exponential attack size)

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

- There are two instances:
  1. $\mathcal{I}_1$ has a single receive/send action $[x_1, \ldots, x_i] \rightarrow \mathrm{enc}_k^s([t_1, t_2])$, 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. $\mathcal{I}_2$ has a single receive/send action $\mathrm{enc}_k^s(y, y) \rightarrow \mathsf{FAIL}$.
- 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?

Exercise

Task (no unique successful minimal attack)

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.

Task (parsing lemma proof)

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 $\sigma(x) \notin \mathrm{DY}(S)$, where S is the set of terms available to the adversary at the step where the first term containing $\sigma(x)$ is sent?

Discussion: Tasks for this week

Exercise

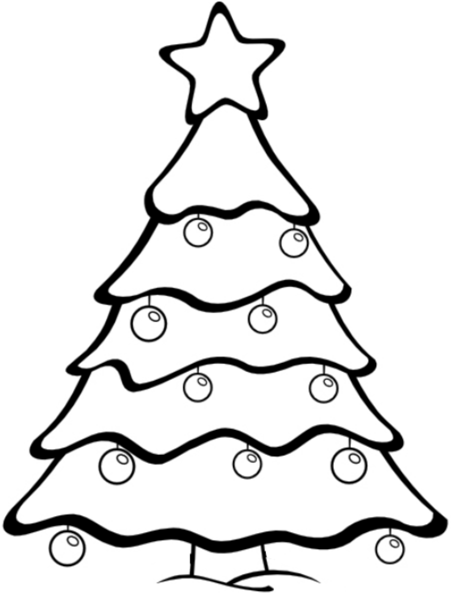
Task (applying the Rusinowitch Turuani Theorem)

In the lecture, modelled the Needham-Schroeder protocol as an input to INSECURE such that the attack is detected. However, this required us to already specify the "correct" sessions ("Alice with Charlie, Charlie with Bob") manually. For automatic analysis, such a manual step should not be required. Can you come up with a pre-processing step that makes this manual step unnecessary?

More precisely: Can you come up with a mechanism translating a natural representation of a protocol (e.g., as the list of "intended instances" for a single session) into a protocol P such that

- P can be used as input for the Rusinowitch-Turuani algorithm for INSECURE,
- P contains all relevant protocol instances (i.e., an initiator with Alice's identity expecting to communicate with a responder with Charlie's identity, and a responder with Bob's identity expecting to communicate with an initiator with Alice's identity),
- P is formally insecure if and only if there is a successful attack on any number of sessions with any set of identities in which the original protocol is run?

Note: You do not need to make your constructions formal.



Merry Christmas

and

a Happy New Year!