Exercise for Engineering Secure Software Systems

January 14, 2021: Exercises 7, 8

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Leftovers

Exercise

Task (Rusinowitch-Turuani with specified maximal number of sessions)

We saw in the lecture that the “unbounded session” version of INSECURE is undecidable. A weaker version of that problem can be obtained by allowing instances to INSECURE to be accompanied by a maximal number of copies in which the adversary may start the corresponding protocol instance (we assume a mechanism that automatically renames variables to ensure that they are “local” to the copy in which they are used). Does the “positive” part of the Rusinowitch-Turuani theorem still hold for this generalization?

Hint: You are not expected to give a formal proof of your conjectures, an informal justification suffices. Also, be explicit about how the “maximal number of copies” is specified in the input to your generalized problem.

Discussion: Tasks for this week

Exercise

Task (Needham-Schroeder as Horn clauses)

Model the Needham-Schroeder protocol as Horn clauses and use this formalism to show that the protocol is insecure. To do this, first list the facts, Dolev-Yao deductions, protocol deductions and the target clause. Then, use logical inference to show that the protocol is in fact insecure. Do you see any limits or imprecisions in this approach?

Exercise

Task (Missing Proof)

Prove the following lemma that was stated in the lecture without proof:

If E is a convergent equational theory, then:

1. For every term t, there is a unique term $[t]$ with
   - $[t]$ is in E-normal-form,
   - $t \equiv_E [t]$.
2. For terms t and t', we have that $t \equiv_E t'$ if and only if $[t] = [t']$.

Exercise

Task (“Badly-Behaved” Equational Theories)

Define equational theories for which the resulting rewrite relation $\twoheadrightarrow_E$ is not a convergent subterm theory, i.e., one that is not confluent, not terminating, or not a subterm theory.