10. Mai 2012

Protokollsicherheit

Exercise Sheet 4

Exercise 4-1. (Labelled Operational Semantics – Easy) What are the possible transitions that the following process can perform:

$$P = \nu x.(\nu y.(\overline{x}\langle y\rangle.\overline{y}\langle x\rangle) \mid \nu y.(x(x).\overline{y}\langle x\rangle \mid y(y).y(y).\overline{k}\langle y\rangle))$$
$$Q = \nu o.(\nu g.(\overline{g}\langle o\rangle \mid g(o).\overline{o}\langle 3\rangle)).$$

Exercise 4-2. (Labelled Operational Semantics – Medium) Consider a process of the form $P \mid Q$. What are the possible processes that could be reached from this process by performing a single labelled transition?

Exercise 4-3. (Labelled Bisimulation – Easy) Consider the following pair of processes: $!\nu c.\overline{d}\langle c\rangle.P(0)$ and $\nu c.!\overline{d}\langle c\rangle.P(0)$. Prove that they are not labelled bisimular by showing that there is no bisimulation relation. Also show a context that can distinguish them, that is, show that they are not observational equivalent.

Exercise 4-4. (Proverif – Medium) In our first lecture, we showed several flawed protocols and their corresponding attacks. Try to use Proverif to find these attacks. Use correspondence properties whenever needed.