MPRI 2.30, Exercises

Unbounded Verification with Proverif

David Baelde

November 15, 2019

1 Resolution with selection (exam 2017/18)

We consider a Proverif model containing only the following primitives:

```
fun ok:bitstring.
fun senc(bitstring,bitstring):bitstring.
reduc forall x:bitstring, k:bitstring;
  sdec(senc(x,k),k) = x.
```

We assume a public channel c and private bitstrings n and k, and take the following process as the system under study:

```
in(c,x:bitstring);
let y:bitstring = sdec(x,k) in
out(c,senc(n,k))
```

Question 1 Give the clauses generated by Proverif for the primitives and for the system. Since we only use a public channel c, you can (and must) ignore the $\mathsf{mess}(\cdot,\cdot)$ predicate and the associated attacker clauses: your generated clauses should only mention the $\mathsf{att}(\cdot)$ predicate. Please give names (or numbers) to your clauses.

Question 2 Saturate the previous set of clauses by resolution with selection, assuming that the selection function selects, when possible, exactly one hypothesis of the form $\mathsf{att}(t)$ where t is not a variable, and selects no hypothesis otherwise. You should not use any optimization involving subsumption, but you can drop clauses that have one of their hypotheses as conclusion. Please give names to the generated clauses, indicate from which clauses they have been obtained, and underline selected hypotheses.

Question 3 Considering the set of solved clauses of the saturated set previously computed, what would Proverif conclude regarding the secrecy of n, k, and $\mathsf{senc}(n,k)$?

Question 4 Describe what happens if the selection function never select any hypothesis: describe the shape of solved clauses, the result of saturation, and discuss its usefulness with respect to Proverif's procedure for semi-deciding secrecy. In particular, illustrate what would happen on the above example: what would the saturation do, what would be the result of the three secrecy queries?

Question 5 Describe what happens if the selection function selects all hypotheses in all clauses: describe the shape of solved clauses, the set of solved clauses of a saturated set of clauses, and discuss its usefulness with respect to Proverif's procedure for secrecy. In particular, illustrate what would happen on the above example: what would the saturation do, what would be the result of the three secrecy queries?

2 Protocol analysis (exam 2018/2019)

In this exercise we consider asymmetric encryption and pairs, both encoded with reduction rules. In particular we have $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pub}(y)), y) \to x$ as in the lectures on symbolic semantics. We use the notation $\{u_1, u_2\}_v$ for $\mathsf{aenc}(\mathsf{pair}(u_1, u_2), v)$. Consider the following processes, where a and b are names:

$$\begin{array}{lcl} A & := & \mathsf{out}(c_A, \{\mathsf{pub}(a), \{k\}_{\mathsf{pub}(b)}\}_{\mathsf{pub}(b)}) \\ B & := & \mathsf{in}(c_B, x). \\ & & \mathsf{let}\ y = \mathsf{proj}_1(\mathsf{adec}(x, b))\ \mathsf{in} \\ & & \mathsf{let}\ z = \mathsf{adec}(\mathsf{proj}_2(\mathsf{adec}(x, b)), b)\ \mathsf{in} \\ & & \mathsf{out}(c_B, \{\mathsf{pub}(b), \{z\}_y\}_y) \\ P & := & \mathsf{new}\ a, b.\ (\mathsf{out}(c, \mathsf{pub}(a)) \mid \mathsf{out}(c, \mathsf{pub}(b)) \mid A \mid B \mid B) \end{array}$$

This protocol does not ensure the secrecy of k: the attacker can learn it by interacting with P. In this exercise, we go through the discovery of this attack using constraint solving and Horn clauses.

Question 1 Give the symbolic configuration resulting from the following trace:

$$\mathsf{out}(c, w_0).\mathsf{out}(c, w_1).\mathsf{out}(c_A, w_2).\mathsf{in}(c_B, x_1).\mathsf{out}(c_B, w_3).\mathsf{in}(c_B, x_2).\mathsf{out}(c_B, w_4)$$

You should make the most general choices (e.g. in the symbolic evaluation steps) so that the resulting symbolic configuration accounts for all concrete configurations, in the sense of the completeness result of the symbolic semantics.

Question 2 Let Φ and $\mathcal{C}$ be the frame and constraint system from the previous symbolic configuration. Show that $\mathcal{C} \wedge \Phi \vdash^? k$ has a solution, using the deducibility constraint solving rules seen in the lectures.

Question 3 Give some useful Horn clauses that Proverif would generate for P, and show how it can be used to derive $\mathsf{att}(k)$ using resolution with the selection strategy where any hypothesis that is not of the form $\mathsf{att}(x)$ is selected.