Cryptographic protocols: formal and computational proofs
Mid Term exam

December 2, 2015
Duration 3h. All documents are allowed

Problem

We consider the following (informally described) handshake protocol

$$\begin{array}{rl} A \to B: & \nu n, \nu r, \nu s. \{\langle n, \langle s, A\rangle\rangle\}_k^r \\ B \to A: & \nu n'. \langle n, n'\rangle \\ A \to B: & \nu r'. \{\langle s, n'\rangle\}_k^{r'} \end{array}$$

in which k is a shared key between A, B.

1. Give a reasonable definition of the processes $P_A(a)$ and $P_B(a)$, in which a plays the role A (this is checked by the process P_B)
2. We wish to check the agreement property on the nonce n. Include in the above processes the appropriate events and state formally the agreement property.
3. We consider the scenario $\nu k.(P_A(a) \| P_B(a))$ in a context, in which the initial attacker's knowledge is only $\{a\}$.
   (a) Explain why complete traces of the above process (i.e., traces with 3 input actions and 3 output actions) must correspond to the following sequence of actions: 1. output of P_A 2. input of P_B 3. output of P_B 4. input of P_A 5. output of P_A 6. input of P_B.
   (b) Compute the deducibility constraint representing all possible complete traces.
   (c) Solve the above deducibility constraints.
   (d) List all possible attacks on the agreement property that was stated in the previous question. (Justify that there is no other attack)
   (e) Show that there is no attack on the secrecy of s in this scenario.
   (f) Show an attack on the secrecy of s in the scenario $\nu k.(P_A(a) \| P_B(a) \| P_B(a))$.
4. Give a Horn clause translation $\mathcal{H}$ of $\nu k.(P_A(a) \| P_B(a))$.
5. Show how the attacker clauses, together with $\mathcal{H}$, allow to deduce $\texttt{Att}(s)$.
6. In the senario $\nu k.(P_A(a) \| P_B(a))$ is there any attack on the agreement on n' ?

7. (**Bonus**) What are the possible attacks on the agreement on n (resp. n') in a scenario $\nu k.(!P_A(a) \parallel !P_B(a))$?

8. (**Bonus**) Assume the encryption scheme is IND-CPA, do we get more attacks in the computational semantics ?

Exercise 2

We assume here that the encryption scheme is IND-CPA. k_1, k_2, k_3, r, r' are arbitrary distinct names. u, v are arbitrary terms.
Which of the following are true ? false (at least for some IND-CPA encryption schemes) ? Justify your answer.

1. $[\![\{k_1\}_{k_2}^r, \{\langle k_1, k_2\rangle\}_{k_3}^{r'}, k_1]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_1, k_2\rangle\}_{k_3}^{r'}, k_1]\!]$
2. $[\![\{k_2\}_{k_1}^r, \{\langle k_1, k_3\rangle\}_{k_2}^{r'}, k_1]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_2, k_3\rangle\}_{k_2}^{r'}, k_1]\!]$
3. $[\![\{k_2\}_{k_1}^r, \{\langle k_1, k_2\rangle\}_{k_1}^{r'}, k_2]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_2, k_3\rangle\}_{k_2}^{r'}, k_3]\!]$
4. $[\![\{\{u\}_{k_1}^r\}_{k_2}^{r'}]\!] \approx [\![\{\{u\}_{k_1}^r\}_{k_1}^{r'}]\!]$

Exercise 3

If a symmetric encryption scheme uses the specific BC mode, we assume that it is possible to compute $\{u\}_k^r$ from $\{\langle v, u\rangle\}_k^r$ (for all u, v, k, r).

Give an example of a protocol, a scenario and a (weak) secrecy property, which is secure in the Dolev-Yao model, but insecure for a symmetric encryption scheme using such a BC mode.