

Exercise Sheet 1

Out: Thu, Oct 22, 2009

Due: Tue, Nov 3, 2009, 10am

Problem 1: Designing a symbolic model (10 Points)

In the lecture we have seen various symbolic models for analyzing protocols involving group arithmetic. For each of these models we have seen three examples of protocols that are secure with respect to the Dolev-Yao model but insecure when implemented cryptographically (see Definition 7, Definition 8, and Definition 10 in the lecture notes).

- Design a symbolic model (i.e., a set of messages M and relations \approx, \vdash) in which all three protocols are insecure. (Of course, you should not do this by adding a rule that gives the adversary too much power such as the rule $\frac{S \vdash g(M)}{S \vdash M}$.)
- For each of the three protocols from the lecture notes, prove that it is insecure (in the sense of Lemma 1, Lemma 2, and Lemma 3 in the lecture notes).
- You can get extra points if you can find additional problems with the symbolic models presented in the lecture and solve these problems in your symbolic model.

Problem 2: A security proof in the Dolev-Yao model (10 Points)

Consider the following set of messages:

$$M ::= N | N_A | enc(M, M) | hash(M).$$

Here N and N_A represent countably infinite sets.

The interpretation of $enc(M_1, M_2)$ is a symmetric encryption of M_2 with key M_1 , the interpretation of $hash(M)$ is a hash value of M .

The deduction relation \vdash is the smallest relation satisfying the following rules:

$$\frac{M_1 \in S}{S \vdash M_1} \text{ELEM} \quad \frac{N \in N_A}{S \vdash N} \text{ADVNONCE} \quad \frac{S \vdash M_1 \quad S \vdash enc(M_1, M_2)}{S \vdash M_2} \text{DEC}$$

$$\frac{S \vdash M_1, M_2}{S \vdash enc(M_1, M_2), hash(M_1)} \text{CONS}$$

Here M_1, M_2 are messages.

→

Consider the following protocol:

- Bob chooses nonces $N_{secret}, K_1, K_2 \in N$.
- Bob sends $hash(K_1), enc(K_1, K_2)$ to the adversary.
- Bob expects a message M_1 from the adversary.
- If M_1 is of the form $enc(K_1, K')$ for some message K' , Bob sends $enc(K', N_{secret})$ to the adversary.

Show that this protocol does not leak the nonce N_{secret} . More precisely, show the following claim:

Claim 1 *Let $S_1 := \{hash(K_1), enc(K_1, K_2)\}$. Assume that $S_1 \vdash enc(K_1, K')$. Let $S_2 := S_1 \cup \{enc(K', N_{secret})\}$. Then $S_2 \not\vdash N_{secret}$.*

(Although you do not need to do so for solving this problem, I strongly recommend that you make it clear for yourself why Claim 1 indeed expresses that the nonce N_{secret} is not leaked in the protocol.)

Hint: To show Claim 1, first try to find some invariant (1) that holds for all M with $S_1 \vdash M$. For every rule from the definition of \vdash , show that if M_1, M_2 satisfy the invariant (1), then the message in the conclusion of the rule also satisfies invariant (1). Then you can use your invariant to show what K' must be. Then try to find some invariant (2) that holds for all M with $S_2 \vdash M$. For every rule from the definition of \vdash , show that if M_1, M_2 satisfy the invariant (2), then the message in the conclusion of the rule also satisfies invariant (2). Finally, use that N_{secret} does not satisfy invariant (2) and you are done.