DSSY Assignment Week 41

Elisabeth Meijer, Luka Dekic, Marina Stanoiljovic

October 9, 2024

Exercise 9.1

Protocol

1. A chooses random R and sends $E_{pk_B}(E_{pk_B}(R))$
2. B decrypts R and sends back $E_{pk_B}(R)$
3. A checks if B sent back the correct $E_{pk_B}(R)$, if so, A sends OK

Questions

(1) If B is honest, can B ensure a message came from A (after getting OK in step 3 with correct MAC)?

For B to receive a message correctly encrypted under R and a correct MAC, the sending party needs to know R. But if e.g. an adversary E had interfered with the protocol from step 1 on, and had sent his own R' to B, B thinks he is talking to A but is in fact talking to E. A message arriving now with correct encryption and MAC might then be also from E.

(2) If B is honest (got OK), B sends $E_R(m)$, can B trust only A will be able to decrypt m?

To decrypt B's message, the other party needs to know R. If B is actually talking to A, only A can decrypt. In the scenario from (1), adversary E can decrypt the message.

(3) If A is honest (sent OK), can A ensure a message with correct MAC came from B only?

Imagine adversary E opens a new session with B using the same messages as A when opening its session (E has to send $E_{pk_B}(E_{pk_B}(R))$ which it saw previously, and OK). Then B might sends something (unrelated to A) to E using the same R for the MAC. E can forward that to A, and A can not know that the message did not come directly from B.

If R is sth, that could also be $E_{pk_B}(R')$ of some R', to get R, adversary E can do the following: E knows $E_{pk_B}(R)$ from listening to the protocol beginning of A and B. Now E starts an own session with B, sending $E_{pk_B}(R)$ as first message. Then B thinks the new R' for this session is $Dec_{sk_B}(R)$ and sends back $E_{pk_B}(R') = R$ to E in step 2. So now E knows R. (*)

With this, E can send any message to A without A noticing it did not come from B.

(4) If A is honest (sent OK), B sends $E_R(m)$, can B trust only A will be able to decrypt m?

To decrypt, the adversary needs R. Take attack (*) described in (3). With this, E knows R and can decrypt anything, so A has no guarantee that only B can read its messages.