DSSY Assignment Week 39

Elisabeth Meijer, Luka Dekic, Marina Stanoiljovic

September 25, 2024

Exercise 6.1

requirements:

- D is able to determine, which user sent the request (1)
- A user should not know which data other users asked for (2)

threat model: adversary can read and modify network traffic
solution a:

- User A sends: $E_{pk_D}(R)$, $S_{sk_A}(E_{pk_D}(R))$, A
- if signature is approved, D sends $E_{pk_A}(data)$

solution b:

- User A sends: $E_{pk_D}(R, S_{sk_A}(R))$, A
- if signature is approved, D sends $E_{pk_A}(data)$

behavior towards requirement (1):
In solution a, the adversary knows $E_{pk_D}(R)$. He can then append his own signature on this encrypted request and his own user name. D then can not tell, that the request originally didn't come from the adversary.

In solution b, this could not happen, as the signature is encrypted, so the adversary could not change it.

behavior towards requirement (2):
in both solutions, the request is encrypted. The adversary can not break the encryption and does not find out, which data the other user requested. Under the attack described above, in solution a D would send back $E_{pk_B}(data)$ to adversary B, instead of $E_{pk_A}(data)$, because D assumes the request came from the adversary B. Then B could decrypt the data and know what the other user originally requested.

So only solution b satisfies the security policy. We learn that one should not send the exact (clear) text of what he signed and the signature separately. Otherwise, the attack for solution a described above is possible.