Exercise 15

Sunday, 19 February 2023 18:11

a) $Send(A, B, pkB) == out\ net\ A;\ inp\ net\ y;\ new\ s;\ (out\ net\ \{|(s,y)|\}_{pkB};\ |\ secret(s))$

$Recv(A, B, skB) == inp\ net\ x;\ new\ n;\ out\ net\ n;\ inp\ net\ z;\ decrypt\ z\ is\ \{|z_1|\}_{skB};\ split\ z_1\ is\ (z_2, z_3);\ if\ z_3 = n\ then\ stop$

$P == new\ A, B, k;\ !Send(A, B, Enc(k))\ |\ !Recv(A, B, Dec(k))$

assuming the parameters are given

here, we have secrecy; since the message is encrypted with Bob's key, it can only be decrypted by Bob (and hence not by the attacker)

---

b) $Send == out\ net\ A;\ inp\ net\ y;\ new\ s;\ out\ net\ \{|(s,y)|\}_{pkB};$

$Recv == inp\ net\ x;\ new\ n;\ out\ net\ n;\ inp\ net\ z;\ decrypt\ z\ is\ \{|z_1|\}_{skB};\ split\ z_1\ is\ (z_2, z_3);\ if\ z_3 = n\ then\ secret(z_2)$

$P = !Send\ |\ !Recv$

This time, we have an opponent process do the sender's work. This process will be working as follows:

$O == out\ net\ A;\ inp\ net\ y;\ new\ s;\ out\ net\ \{|(s,y)|\}_{pkB};\ out\ net\ s;$

Taking $P\ |\ O$, we can ~~easily~~ see that

$P|O \equiv P|(Recv|O) \rightarrow^* secret(s)\ |\ out\ net\ s;\ |\ P$ which ~~clearly~~ violates robust safety for secrecy.

since this is an error state.