Review question 13

zondag 19 februari 2023 02:22

From ProVerif's output, we can conclude that this protocol is not robustly safe for secrecy; the attacker can simply masquerade as Alice the entire time, which implies Bob would share the channel over which he shares the nonce with the attacker.

Still, the protocol is safe for secrecy, since the nonce is never shared over a public channel.

The secrecy can be expressed in SPI calculus as follows:

$$P == new\ C;\ out\ net\ \{|C|\}_{Enc(B)};\ inp\ C\ x;$$

$$Q == inp\ net\ y;\ decrypt\ y\ is\ \{|x|\}_{Sec(B)};\ new\ n;\ (out\ x\ n \mid secret(n))$$

$$R == P \mid Q$$