Defeat replay attack with a nonce (not fully secured)


A

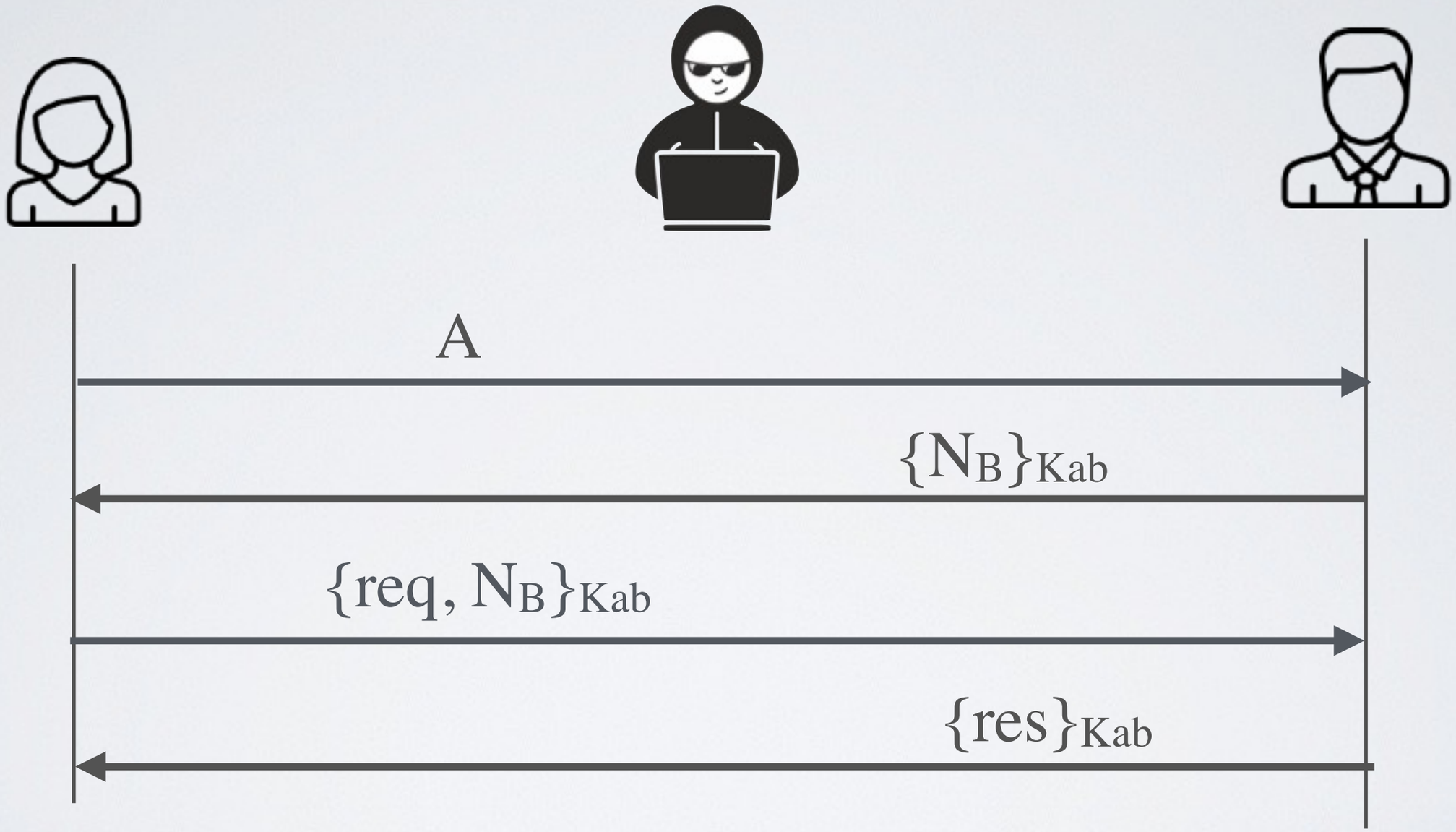
Replay attack on the response!

{req, N_B}Kab

{res}Kab

$\{N_B\}_{Kab}$

Defeat replay attack with a nonce (not fully secured)



Replay attack on the response!

Defeat replay attack with a double nonce