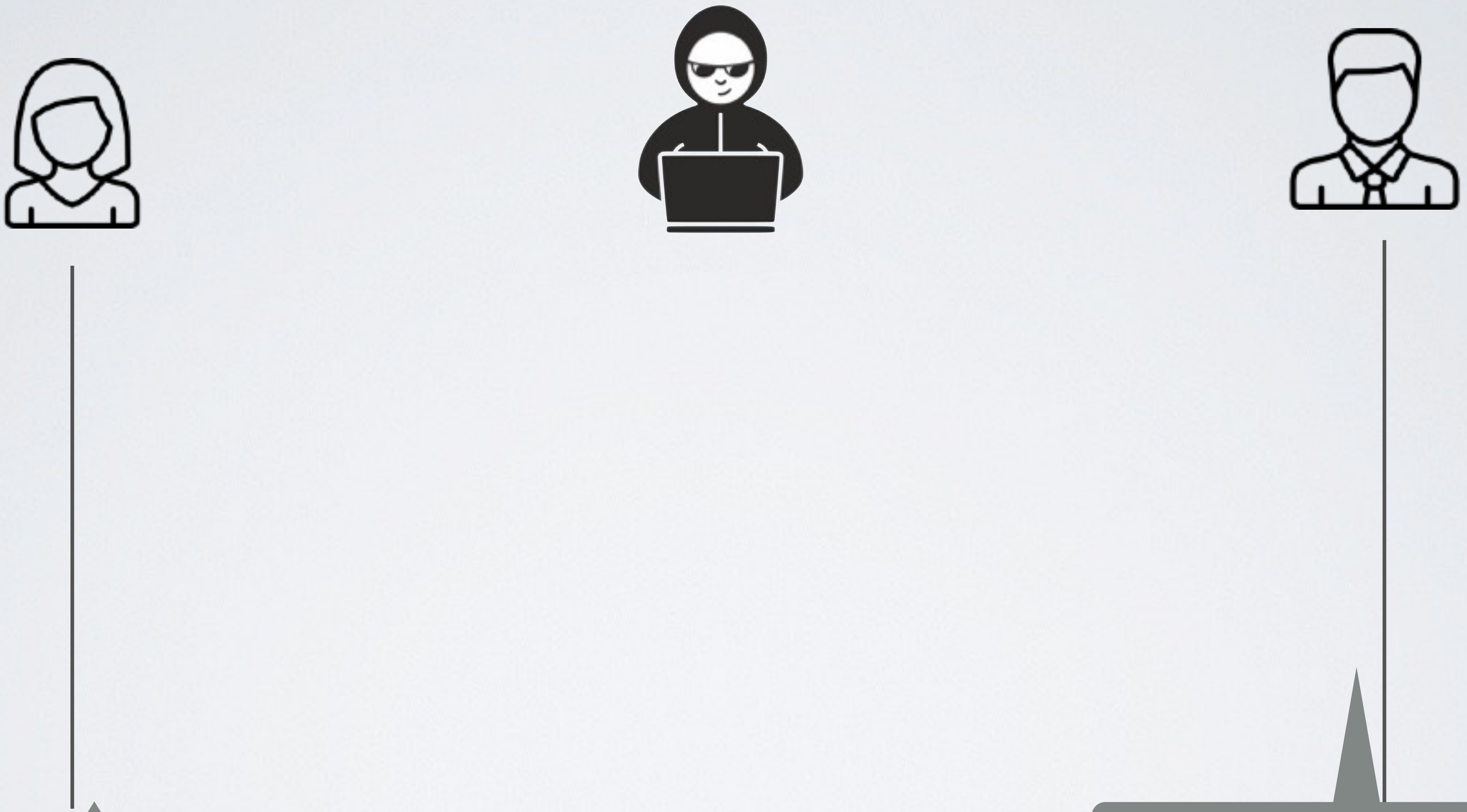
Counter replay attacks

- ✓ **Storage-based solution**
  Store the message entirely (log), or ID or encryption nonce or timestamp and check whether the same message has been replayed

- ✓ **Protocol-based solution**
  Add a nonce in the interaction and verify that the nonce is sent back

Double Nonce Protocol



Alice must check that the nonce $\mathbf{N_A}$ received match the original one

Bob must check that the nonce $\mathbf{N_B}$ received match the original one