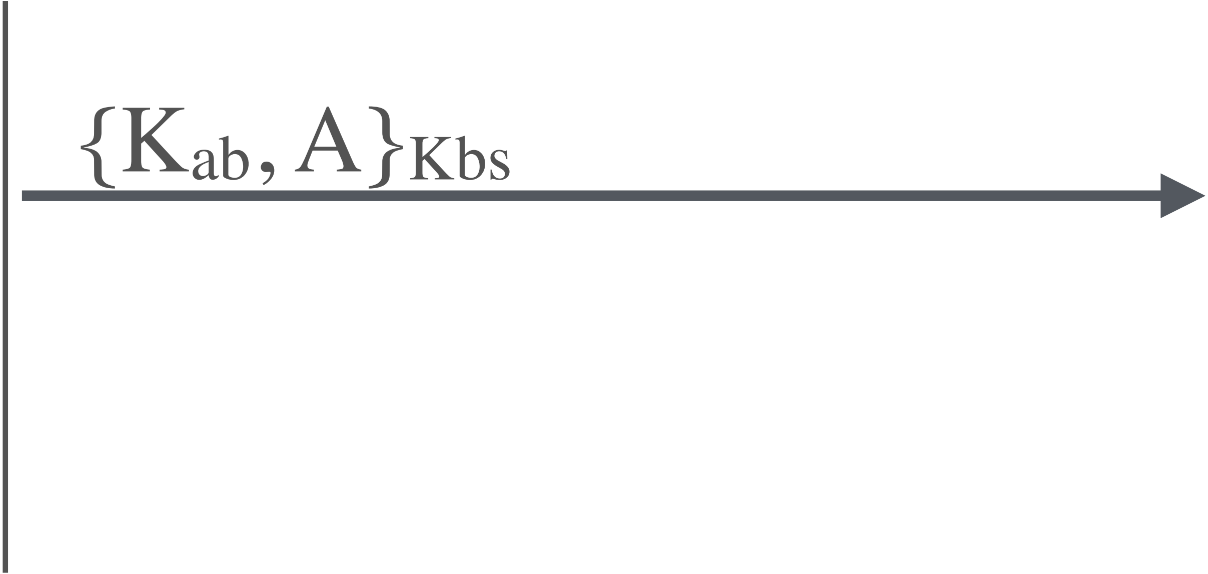
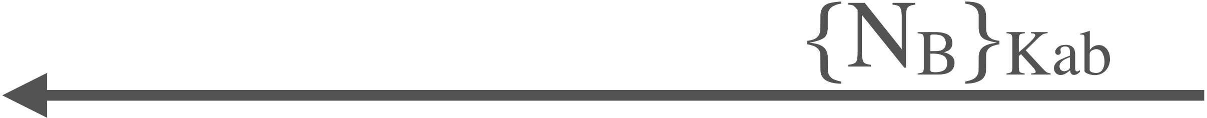
Replay attack (1981)



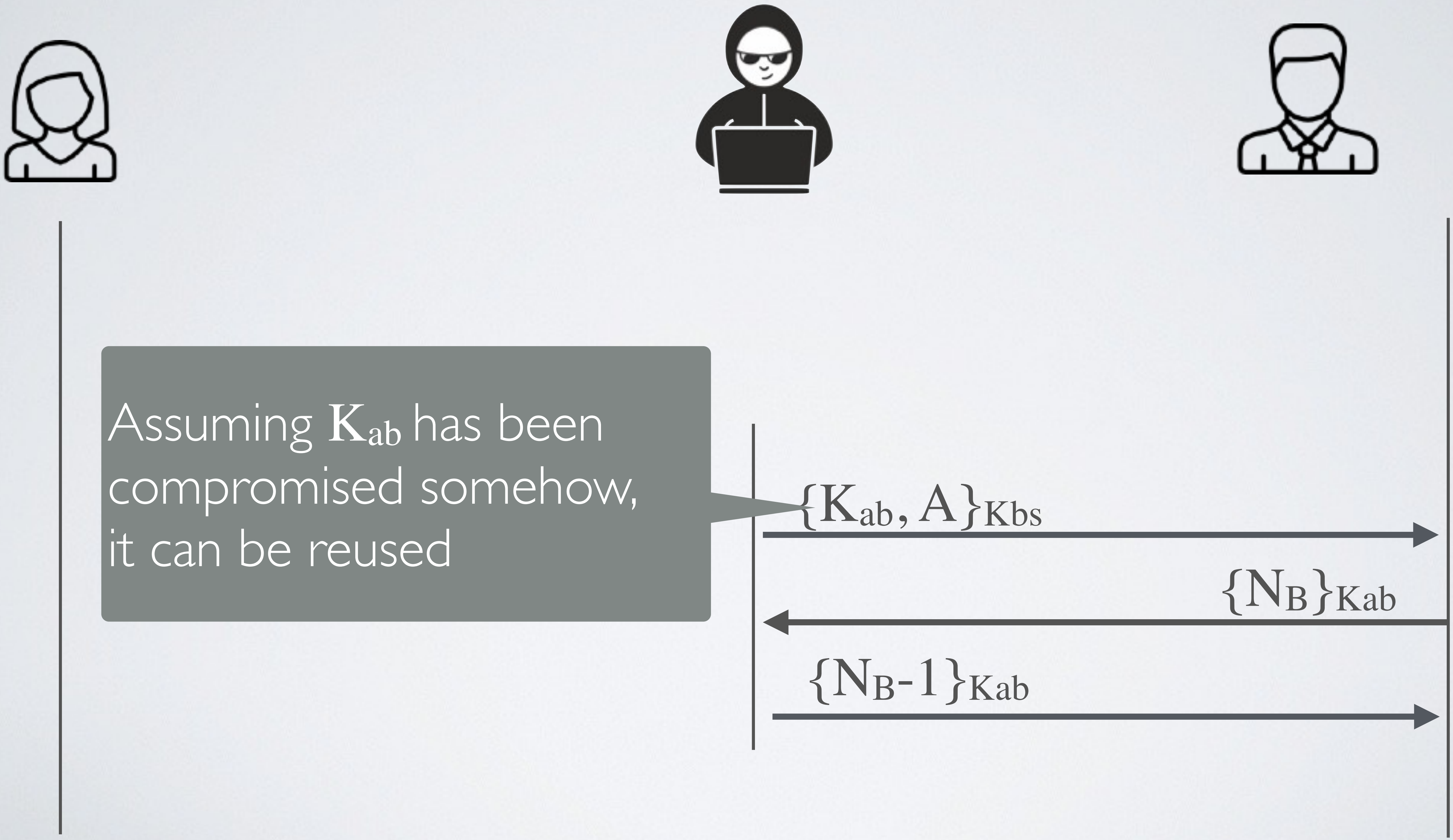
$\{K_{ab}, A\}_{K_{bs}}$


{NB}Kab

$\{N_B\text{-}1\}_{Kab}$

Assuming K_{ab} has been compromised somehow, it can be reused

Replay attack (1981)



$\{K_{ab}, A\}_{K_{bs}}$

$\{N_B\}_{K_{ab}}$

$\{N_B\text{-}1\}_{K_{ab}}$

Assuming $\mathbf{K}_{ab}$ has been compromised somehow, it can be reused

The fix (1987)