2/27/07

$A \rightarrow B: \quad ID_A$

$B \rightarrow A: \quad N$ (challenge)

$A \rightarrow B: \quad E_{K_{AB}}[N]$

B authenticates A

$A \rightarrow B: \quad ID_A$

$B \rightarrow A: \quad E_{K_{AB}}[N]$

$A \rightarrow B: \quad N$

Otway - Rees

1. $A \rightarrow B$: $N_c \| ID_A \| ID_B \| E_{K_A}[N_A \| N_c \| ID_A \| ID_B]$

2. $B \rightarrow KDC$: $E_{K_A}[N_A \| N_c \| ID_A \| ID_B] \| E_{K_B}[N_B \| N_c \| ID_A \| ID_B]$

3. $KDC \rightarrow B$: $N_c \| \underline{E_{K_A}[N_A \| K_{AB}] \| E_{K_B}[N_B \| K_{AB}]}$

4. $B \rightarrow A$: $E_{K_A}[N_A \| K_{AB}]$

5. $A \rightarrow B$: $E_{K_{AB}}[N_c - 1]$

Needham-Schroeder

1. $A \rightarrow KDC: N_1 \| ID_B$
2. $KDC \rightarrow A: E_{K_A}[N_1 \| ID_B \| K_{AB} \| E_{K_B}[K_{AB} \| ID_A]]$
3. $A \rightarrow B: E_{K_B}[K_{AB} \| ID_A] \| E_{K_{AB}}[N_2]$
4. $B \rightarrow A: E_{K_{AB}}[N_2 - 1 \| N_3]$
5. $A \rightarrow B: E_{K_{AB}}[N_3 - 1]$

Expanded NS.

$A \rightarrow B$: Req to B

$B \rightarrow A$: $E_{K_B}[N_B]$

$A \rightarrow KDC$: $N_1 \| ID_A \| ID_B \| E_{K_B}[N_B]$

~~$KDC \rightarrow A$: $E_{K_A}[N_1 \| ID_B \| E_{K_B}[N_B]$~~

$KDC \rightarrow A$: $E_{K_A}[N_1 \| ID_B \| K_{AB} \| E_{K_B}[K_{AB} \| ID_A \| N_B]]$

$A \rightarrow B$: $E_{K_B}[K_{AB} \| ID_A \| N_B] \| K_{AB}[N_2]$

$B \rightarrow A$: $E_{K_{AB}}[N_2 - 1, N_3]$

$A \rightarrow B$: $E_{K_{AB}}[N_3 - 1]$

Session 1

$T \rightarrow B: \; E_{K_{AB}}[N_1]$

Rinciple: Use different Keys to authenticate

$A \longleftrightarrow B$

K'_{AB}

K^2_{AB}

$A \rightarrow B: \quad ID_A \,||\, E_{K_{AB}}(TS)$

$A \rightarrow B: \quad ID_A \,||\, N_2$

$B \rightarrow A: \quad N_1 \,||\, E_{K_{AB}}[N_2]$

$A \rightarrow B: \quad E_{K_{AB}}[N_1]$ ✗

T A to B

Session 1

$T \rightarrow B: \quad ID_A \,||\, N_2$

$B \rightarrow T: \quad N_1 \,||\, E_{K_{AB}}[N_2]$

Session 2

$T \rightarrow B: \quad ID_A \,||\, N_1$

$B \rightarrow T: \quad N_3 \,||\, E_{K_{AB}}[N_1]$