MPS[1] Protocol – BAN logic

Sign Up Real Protocol

M_1: A → S: $K_a, E_{k_s}(A, N_a)$

M_2: S → A: $E_{k_a}(A, N_a, N_s, K_{as}) || E_{k_s^-}(S(E_{k_a}(A, N_a, N_s, K_{as})))$

M_3: A → S: $E_{k_{as}}(A, N_s, g_a, p_a)$

M_4: S → A: $E_{k_{as}}(A, N_s + 1, g_a, p_a)$

Sign Up Idealized Protocol

M_1: A → S: $\{A, N_a\}_{k_s}$

M_2: S → A: $\left\{A, N_a, \#(N_a), N_s, (A \overset{k_{as}}{\leftrightarrow} S)\right\}_{k_a} || \left\{S(\left\{A, N_a, \#(N_a), N_s, (A \overset{k_{as}}{\leftrightarrow} S)\right\}_{k_a})\right\}_{k_s^-}$

M_3: A → S: $\{A, N_s, \#(N_s), g_a, p_a\}_{k_{as}}$

M_4: S → A: $\{A, N_s + 1, \#(N_s), g_a, p_a\}_{k_{as}}$

Sign Up Protocol Analysis

Objectives

$S \models (g_a, p_a)$

$A \models S \models (g_a, p_a)$ # Diffie Hellman Parameters

$A \models A \overset{k_{as}}{\leftrightarrow} S$ # Symmetric Key

$S \models A \models A \overset{k_{as}}{\leftrightarrow} S$

Assumptions

$A \models \overset{k_s}{\rightarrow} S$ # Hardcoded Server's Public Key

$S \models \overset{k_a}{\rightarrow} A$ # Alice's Public Key sent in plaintext in the first message

$S \Rightarrow A \overset{k_{as}}{\leftrightarrow} S$ # Symmetric Key

$S \models A \Rightarrow g_a, p_a$

After M_1:

$S \lhd \{A, N_a\}_{k_s}$

[1] Magherini – Pochiero – Sieni (MPS)

After M_2:

$$\frac{A \models \overset{k_s}{\rightarrow} S \ , \ A \lhd \left\{A, N_a, \ \#(N_a), N_s, (A \overset{k_{as}}{\leftrightarrow} S)\right\}_{k_s^-}}{A \models S \mid\sim (A, N_a, \ \#(N_a), N_s, (A \overset{k_{as}}{\leftrightarrow} S))}$$

$$\frac{A \models S \mid\sim \left(A, N_a, \ \#(N_a), N_s, (A \overset{k_{as}}{\leftrightarrow} S)\right), \ A \models \#(N_a)}{A \models S \models (A, N_a, \ \#(N_a), N_s, \left(A \overset{k_{as}}{\leftrightarrow} S\right))}$$

$$\frac{A \models S \models \left(A, N_a, \ \#(N_a), N_s, \left(A \overset{k_{as}}{\leftrightarrow} S\right)\right), S \Rightarrow A \overset{k_{as}}{\leftrightarrow} S}{A \models A \overset{k_{as}}{\leftrightarrow} S}$$

After M_3:

$$\frac{S \models A \overset{k_{as}}{\leftrightarrow} S \ , \ S \lhd \left\{A, N_s, \#(N_s), g_a, p_a, (A \overset{k_{as}}{\leftrightarrow} S)\right\}_{k_{as}}}{S \models A \mid\sim (A, N_s, \#(N_s), g_a, p_a, (A \overset{k_{as}}{\leftrightarrow} S))}$$

$$\frac{S \models A \mid\sim (A, N_s, \#(N_s), g_a, p_a, (A \overset{k_{as}}{\leftrightarrow} S)), \ S \models \#(N_s)}{S \models A \models (A \overset{k_{as}}{\leftrightarrow} S)}$$

$$\frac{S \models A \Rightarrow g_a, p_a, S \models A \models (A, N_s, \#(N_s), g_a, p_a, (A \overset{k_{as}}{\leftrightarrow} S))}{S \models (g_a, p_a)}$$

After M_4:

$$\frac{A \models A \overset{k_{as}}{\leftrightarrow} S \ , \ A \lhd \{A, N_s, \ \#(N_s), g_a, p_a\}_{k_{as}}}{A \models S \mid\sim (A, N_s, \ \#(N_s), g_a, p_a)}$$

$$\frac{A \models S \mid\sim (A, N_s, \ \#(N_s), g_a, p_a), \ A \models \#(N_s)}{A \models S \models g_a, p_a}$$

Authentication Real Protocol

M_1: A → S: $E_{k_{as}}(A, N_a)$

M_2: S → A: $E_{k_{as}}(A, N_a, N_s)$

M_3: A → S: $E_{k_{as}}(A, N_s)$

Authentication Idealized Protocol

M_1: A → S: $\{A, N_a\}_{k_{as}}$

M_2: S → A: $\{A, N_a, \#(N_a), N_s\}_{k_{as}}$

M_3: A → S: $\{A,\ N_s, \#(N_s)\}_{k_{as}}$

Authentication Analysis

Objectives

$A \models \#(N_s)$, $S \models A \models \#(N_s)$ # Session ID Establishing

Assumptions

$A \models A \overset{k_{as}}{\leftrightarrow} S$ $S \models A \overset{k_{as}}{\leftrightarrow} S$ # Key Registration

$A \models S \Rightarrow N_s$, $S \models \#(N_s)$ # Nonce Authority

After M_1:

$$\frac{S \models A \overset{k_{as}}{\leftrightarrow} S,\ S \lhd \{A, N_a, \#(N_a), N_s\}_{k_{as}}}{S \models A \mid\sim (A, N_a, \#(N_a), N_s)}$$

After M_2:

$$\frac{A \models A \overset{k_{as}}{\leftrightarrow} S,\ A \lhd \{A, N_a, \#(N_a), N_s\}_{k_{as}}}{A \models S \mid\sim (A, N_a, \#(N_a), N_s)}$$

$$\frac{A \models S \mid\sim (A, N_a, \#(N_a), N_s),\ A \models \#(N_a)}{A \models S \models (A, N_a, \#(N_a), N_s)}$$

$$\frac{A \models S \models N_s,\ A \models S \Rightarrow N_s}{A \models N_s}$$

$$\frac{A \models N_s,\ A \models \#(N_a)}{A \models \#(N_s)}$$

After M_3:

$$\frac{S \models A \overset{k_{as}}{\leftrightarrow} S \ , \ S \lhd \{A, \ N_s, \#(N_s)\}_{k_{as}}}{S \models A \mid\sim (A, \ N_s, \#(N_s))}$$

$$\frac{S \models A \mid\sim (A, \ N_s, \#(N_s)), \ S \models \#(N_s)}{S \models A \models \#(N_s)}$$

Online Key Exchange Real Protocol

M_1: A → S: $E_{k_{as}}(A, B, N_{sa})$

M_2: S → A: $E_{k_{as}}\left(A, B, N_{sa}, g_b, p_{b,} k_{b,} E_{k_{bs}}(k_a, N_{sb}, N_{sa})\right)$

M_3: A → B: $E_{k_b}\left(A, B, Y_A, E_{k_{bs}}(k_a, N_{sb}, N_{sa})\right) || E_{k_a^-}(S(E_{k_b}\left(A, B, Y_{A,} E_{k_{bs}}(k_a, N_{sb})\right)))$

M_4: B → A: $E_{k_a}\left(A, B, Y_B, N_{sa}, E_{k_{ab}}(N_b)\right) || E_{k_b^-}(S(E_{k_a}\left(A, B, Y_B, E_{k_{ab}}(N_b)\right)))$

M_5: A → B: $E_{k_{ab}}(N_b)$

M_x: A → B: $E_{k_{ab}}(data, \ SeqNum)$

Online Key Exchange Idealized Protocol

M_1: A → S: $\{A, B, N_{sa}\}_{k_{as}}$

M_2: S → A: $\left\{A, B, N_{sa}, g_b, p_{b,} \overset{k_b}{\rightarrow} B, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sa})\right\}_{k_{as}}$

M_3: A → B: $\left\{A, B, Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sb})\right\}_{k_b} || \left\{S(\left\{A, B, Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}\right\}_{k_{bs}}, \#(\overset{k_a}{\rightarrow} A)\right\}_{k_b})\right\}_{k_a^-}$

M_4: B → A: $\left\{A, B, Y_b, N_{sa}, \{N_b\}_{k_{ab}}\right\}_{k_a} || \left\{S(\left\{A, B, Y_b, \{N_b\}_{k_{ab}}\right\}_{k_a})\right\}_{k_b^-}$

M_5: A → B: $\{N_b\}_{k_{ab}}$

Online Key Exchange Analysis

Objectives

$A \models A \overset{k_{ab}}{\leftrightarrow} B$, $B \models A \overset{k_{ab}}{\leftrightarrow} B$ # Key Authentication

$A \models B \ \models A \overset{k_{ab}}{\leftrightarrow} B,$ $B \models A \ \models A \overset{k_{ab}}{\leftrightarrow} B$ # Key Confirmation

Assumptions

$A \ \models A \overset{k_{as}}{\leftrightarrow} S\,,$ $S \ \models A \overset{k_{as}}{\leftrightarrow} S$ # Symmetric keys

$B \ \models B \overset{k_{bs}}{\leftrightarrow} S\,,$ $S \ \models B \overset{k_{bs}}{\leftrightarrow} S$ # Symmetric keys

Freshness of the session ids used during the authentication protocol

$S \ \models \#(N_{sa}),$ $A \ \models \#(N_{sa}), B \ \models \#(N_{sb})$

$S \ \models (g_b, p_b)$ # Diffie Hellman's parameters

$A \models B \ \Rightarrow Y_B\,,$ $B \ \models A \Rightarrow \ Y_A$ # Authority on Y parameters

After M_1:

$$\frac{S \ \models A \overset{k_{as}}{\leftrightarrow} S \ , \ S \ \lhd \ \{A, B, N_{sa}\}_{k_{as}}}{S \ \models A \mid\sim (A, B, N_{sa})}$$

$$\frac{S \ \models A \mid\sim (A, B, N_{sa}), \ S \models \#(N_{sa})}{S \ \models A \models (A, B, N_{sa})}$$

After M_2:

$$\frac{A \ \models A \overset{k_{as}}{\leftrightarrow} S \ , \ A \ \lhd \left\{A, B, N_{sa}, g_b, p_{b,} \overset{k_b}{\rightarrow} B, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sa})\right\}_{k_{as}}}{A \ \models S \mid\sim (A, B, N_{sa}, g_b, p_{b,} \overset{k_b}{\rightarrow} B, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sa}))}$$

$$\frac{A \ \models S \mid\sim (X), \ A \ \models \#(N_{sa})}{A \ \models S \models (X)}$$

$$\frac{A \ \models S \ \models \overset{k_b}{\rightarrow} B \ , \ A \ trusts \ S \ on \ k_b}{A \ \models \overset{k_b}{\rightarrow} B}$$

$$\frac{A \ \models S \ \models (g_b, p_b) \ , \ A \ trusts \ S \ on \ (g_b, p_b)}{A \ \models (g_b, p_b)}$$

After M_3:

$$\frac{B \ \models B \overset{k_{bs}}{\leftrightarrow} S \ , \ B \lhd \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}}{B \ \models S \mid\sim \left(\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa} \ \right)}$$

$$\frac{B \models S \mid\sim \left(\overset{k_a}{\rightarrow} A\right),\ B \models \#(N_{sb})}{B \models S \models \left(\overset{k_a}{\rightarrow} A\right)}$$

$$\frac{B \models S \models \overset{k_a}{\rightarrow} A,\ B \text{ trusts } S \text{ on } k_a}{B \models \overset{k_a}{\rightarrow} A}$$

$$\frac{B \models \overset{k_a}{\rightarrow} A,\ B \lhd \left\{A, B,\ Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sb})\right\}_{k_a^-}}{B \models A \mid\sim (A, B,\ Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sb}))}$$

$$\frac{B \models A \mid\sim (A, B,\ Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sb})),\ B \models \#(N_{sb})}{B \models A \models (A, B,\ Y_A, \left\{\overset{k_a}{\rightarrow} A, N_{sb}, N_{sa}\right\}_{k_{bs}}, \#(N_{sb}))}$$

$$\frac{B \models A \models Y_A,\ B \models A \Rightarrow Y_A}{B \models Y_A}$$

$$\frac{B \models Y_A,\ B \Rightarrow Y_B}{B \models A \overset{k_{ab}}{\leftrightarrow} B}$$

After M_4:

$$\frac{A \models \overset{k_b}{\rightarrow} B,\ A \lhd \left\{A, B, Y_b, N_{sa}, \{N_b\}_{k_{ab}}\right\}_{k_b^-}}{A \models B \mid\sim (A, B, Y_b, N_{sa}, \{N_b\}_{k_{ab}})}$$

$$\frac{A \models B \mid\sim \left(A, B, Y_b, N_{sa}, \{N_b\}_{k_{ab}}\right),\ A \models \#(N_{sa})}{A \models B \models \left(A, B, Y_b, N_{sa}, \{N_b\}_{k_{ab}}\right)}$$

$$\frac{A \models B \models Y_B,\ A \models B \Rightarrow Y_B}{A \models Y_B}$$

$$\frac{A \models Y_B,\ A \Rightarrow Y_A}{A \models A \overset{k_{ab}}{\leftrightarrow} B}$$

$$\frac{A \models A \overset{k_{ab}}{\leftrightarrow} B,\ A \lhd \{N_b\}_{k_{ab}}}{A \models B \mid\sim (N_b)}$$

$$\frac{A \models B \mid\sim (N_b),\ A \models \#(N_{sa})}{A \models B \models A \overset{k_{ab}}{\leftrightarrow} B}$$

After M_5:

$$\frac{B \models A \overset{k_{ab}}{\leftrightarrow} B,\ B \lhd \{N_b\}_{k_{ab}}}{B \models A \mid\sim (N_b)}$$

$$\frac{B \models A \mid\sim (N_b),\ \ B \models \#(N_b)}{B \models A \models A \overset{k_{ab}}{\longleftrightarrow} B}$$

Offline Communication Real Protocol

M_1: A → S: $E_{k_{as}}(A, B, N_{sa})$

M_2: S → A: $E_{k_{as}}(A, B, N_{sa}, k_b)$

M_x: A → S: $E_{k_b}\Big(data, SeqNum,\ E_{k_a^-}(S(data, SeqNum))\Big) || E_{k_a^-}\big(S(data, SeqNum, E_{k_a^-}(S(data, SeqNum))\big)\big)$

Offline Communication Idealized Protocol

M_1: A → S: $\{A, B, N_{sa}\}_{k_{as}}$

M_2: S → A: $\left\{A, B, N_{sa}, \overset{k_b}{\rightarrow} B, \#(N_{sa})\right\}_{k_{as}}$

Offline Communication Analysis

Objective

$A \models \overset{k_b}{\rightarrow} B$ # Bob's Public Key

Assumptions

$A \models A \overset{k_{as}}{\longleftrightarrow} S$, $S \models A \overset{k_{as}}{\longleftrightarrow} S$ # Symmetric keys

Freshness of the session id used during the authentication protocol

$S \models \#(N_{sa}),\ \ A \models \#(N_{sa})$

After M_1:

$$\frac{S \models A \overset{k_{as}}{\longleftrightarrow} S,\ \ S \lhd \{A, B, N_{sa}\}_{k_{as}}}{S \models A \mid\sim (A, B, N_{sa})}$$

$$\frac{S \models A \mid\sim (A, B, N_{sa}),\ \ S \models \#(N_{sa})}{S \models A \models (A, B, N_{sa})}$$

After M_2:

$$\frac{A \models A \overset{k_{as}}{\leftrightarrow} S \ , \ A \lhd \left\{A, B, \ N_{sa}, \overset{k_b}{\rightarrow} B, \#(N_{sa})\right\}_{k_{as}}}{A \models S \mid\sim (A, B, N_{sa}, \overset{k_b}{\rightarrow} B, \#(N_{sa}))}$$

$$\frac{A \models S \mid\sim (X), \ A \models \#(N_{sa})}{A \models S \models (X)}$$

$$\frac{A \models S \models \overset{k_b}{\rightarrow} B \ , \ A \ trusts \ S \ on \ k_b}{A \models \overset{k_b}{\rightarrow} B}$$