

## MPS<sup>1</sup> Protocol – BAN logic

### Sign Up Real Protocol

$$M_1: A \rightarrow S: K_a, E_{k_s}(A, N_a, S(K_a)) || S(A, N_a)$$

$$M_2: S \rightarrow A: E_{k_a}(N_a, N_s) || E_{k_s}^{-1}(S(E_{k_a}(N_a, N_s)))$$

$$M_3: A \rightarrow S: E_{k_s}(N_s, g_a, p_a) || E_{k_a}^{-1}(S(E_{k_a}(N_s, g_a, p_a)))$$

$$M_4: S \rightarrow A: E_{k_a}(S(N_s, g_a, p_a)) || E_{k_s}^{-1}(S(E_{k_a}(S(N_s, g_a, p_a))))$$

### Sign Up Idealized Protocol

$$M_1: A \rightarrow S: \{A, N_a\}_{k_s}$$

$$M_2: S \rightarrow A: \{N_a, \#(N_a), N_s\}_{k_a} || \{S(\{N_a, \#(N_a), N_s\}_{k_a})\}_{k_s}^{-1}$$

$$M_3: A \rightarrow S: \{N_s, \#(N_s), g_a, p_a\}_{k_s} || \{S(\{N_s, \#(N_s), g_a, p_a\}_{k_s})\}_{k_a}^{-1}$$

$$M_4: S \rightarrow A: \{S(N_s, \#(N_s), g_a, p_a)\}_{k_a} || \{S(\{S(N_s, \#(N_s), g_a, p_a)\}_{k_a})\}_{k_s}^{-1}$$

### Sign Up Protocol Analysis

Objectives

$$S \models (g_a, p_a)$$

# Diffie Hellman Parameters

$$A \models S \models (g_a, p_a)$$

# DH Parameters confirmation

Assumptions

$$A \xrightarrow{k_s} S$$

# Hardcoded Server's Public Key

$$S \xrightarrow{k_a} A$$

# Alice's Public Key sent in plaintext in the first message

$$S \models A \Rightarrow g_a, p_a$$

After  $M_1$ :

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

After  $M_2$ :

$$\frac{A \xrightarrow{k_s} S, A \triangleleft \{N_a, \#(N_a), N_s\}_{k_s}^{-1}}{A \models S \mid \sim (N_a, \#(N_a), N_s)}$$

<sup>1</sup> Magherini – Pochiero – Sieni (MPS)

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

After  $M_3$ :

$$\frac{S \xrightarrow{k_a} A, S \triangleleft \{N_s, \#(N_s), g_a, p_a\}_{k_a^-}}{S \models A \mid \sim (N_s, \#(N_s), g_a, p_a)}$$

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

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

After  $M_4$ :

$$\frac{A \xrightarrow{k_s} S, A \triangleleft \{S(N_s, \#(N_s), g_a, p_a)\}_{k_s^-}}{A \models S \mid \sim (S(N_s, \#(N_s), g_a, p_a))}$$

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

## Authentication Real Protocol

$$M_1: A \rightarrow S: E_{k_s}(A, N_a) \parallel E_{k_a^-}(S(E_{k_s}(A, N_a)))$$

$$M_2: S \rightarrow A: E_{k_a}(N_a, N_s, K_{as}) \parallel E_{k_s^-}(S(E_{k_a}(N_a, N_s, K_{as})))$$

$$M_3: A \rightarrow S: E_{k_{as}}(N_s)$$

## Authentication Idealized Protocol

$$M_1: A \rightarrow S: \{A, N_a\}_{k_s} \parallel \{S(\{A, N_a\}_{k_s})\}_{k_a^-}$$

$$M_2: S \rightarrow A: \left\{ N_a, \#(N_a), N_s, (A \xleftrightarrow{k_{as}} S) \right\}_{k_a} \parallel \left\{ S(\{ N_a, \#(N_a), N_s, (A \xleftrightarrow{k_{as}} S) \}_{k_a}) \right\}_{k_s^-}$$

$$M_3: A \rightarrow S: \left\{ N_s, \#(N_s), (A \xleftrightarrow{k_{as}} S) \right\}_{k_{as}}$$

## Authentication Analysis

Objectives

$$A \models \#(N_s), \quad S \models A \models \#(N_s)$$

# Session ID

$$A \models A \xleftrightarrow{k_{as}} S \quad A \models \#(A \xleftrightarrow{k_{as}} S)$$

# Session Key

$$S \models A \models A \xleftrightarrow{k_{as}} S$$

# Session Key confirmation

Assumptions

$$S \models A \xleftrightarrow{k_{as}} S$$

# Session Key

$$A \models \rightarrow S$$

# Hardcoded Server's Public Key

$$S \models \xrightarrow{k_a} A$$

# Alice's Public Key

$$A \models S \Rightarrow N_s$$

# Nonce Authority

$$A \models S \Rightarrow A \xleftrightarrow{k_{as}} S$$

# Session Key Authority

After  $M_1$ :

$$\frac{S \models \xrightarrow{k_a} A, S \triangleleft \{A, N_a\}_{k_a^-}}{S \models A \mid \sim (A, N_a)}$$

After  $M_2$ :

$$\frac{A \models \xrightarrow{k_s} S, A \triangleleft \{N_a, \#(N_a), N_s, (A \xleftrightarrow{k_{as}} S)\}_{k_s^-}}{A \models S \mid \sim (N_a, \#(N_a), N_s, (A \xleftrightarrow{k_{as}} S))}$$

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

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

$$\frac{A \models S \models (A \xleftrightarrow{k_{as}} S), A \models S \Rightarrow (A \xleftrightarrow{k_{as}} S)}{A \models (A \xleftrightarrow{k_{as}} S)}$$

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

$$\frac{A \models A \xleftrightarrow{k_{as}} S, A \models \#(A \xleftrightarrow{k_{as}} S)}{A \models \#(A \xleftrightarrow{k_{as}} S)}$$

After  $M_3$ :

$$\frac{S \models A \xleftrightarrow{k_{as}} S, S \triangleleft \{N_s, \#(N_s), (A \xleftrightarrow{k_{as}} S)\}_{k_{as}}}{S \models A \mid \sim (N_s, \#(N_s), (A \xleftrightarrow{k_{as}} S))}$$

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

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

## Online Key Exchange Real Protocol

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

$$M_2: S \rightarrow A: E_{k_{as}}(N_{sa}, g_b, p_b, k_b, E_{k_{bs}}(k_a, N_{sb}, N_{sa}))$$

$$M_3: A \rightarrow B: E_{k_b}(A, B, Y_A, E_{k_{bs}}(k_a, N_{sb}, N_{sa})) \parallel E_{k_a^-}(S(E_{k_b}(A, B, Y_A, E_{k_{bs}}(k_a, N_{sb})))))$$

$$M_4: B \rightarrow A: E_{k_a}(Y_B, N_{sa}, E_{k_{ab}}(N_b)) \parallel E_{k_b^-}(S(E_{k_a}(Y_B, N_{sa}, E_{k_{ab}}(N_b))))$$

$$M_5: A \rightarrow B: E_{k_{ab}}(N_b)$$

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

## Online Key Exchange Idealized Protocol

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

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

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

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

$$M_5: A \rightarrow B: \{N_b\}_{k_{ab}}$$

## Online Key Exchange Analysis

Objectives

$$A \models A \xleftrightarrow{k_{ab}} B, \quad B \models A \xleftrightarrow{k_{ab}} B \quad \# \text{ Key Authentication}$$

$$A \models B \models A \xleftrightarrow{k_{ab}} B, \quad B \models A \models A \xleftrightarrow{k_{ab}} B \quad \# \text{ Key Confirmation}$$

## Assumptions

$A \models A \xleftrightarrow{k_{as}} S, \quad S \models A \xleftrightarrow{k_{as}} S$	# A-S Session keys (authentication protocol)
$B \models B \xleftrightarrow{k_{bs}} S, \quad S \models B \xleftrightarrow{k_{bs}} S$	# B-S Session keys (authentication protocol)
$S \models \#(N_{sa}), \quad A \models \#(N_{sa}), \quad B \models \#(N_{sb})$	# Freshness session ids (authentication protocol)
$S \models (g_b, p_b)$	# Diffie Hellman's parameters
$A \models B \Rightarrow Y_B, \quad B \models A \Rightarrow Y_A$	# Authority on Y parameters

After  $M_1$ :

$$\frac{S \models A \xleftrightarrow{k_{as}} S, \quad S \triangleleft \{A, B, N_{sa}\}_{k_{as}}}{S \models A \mid \sim (A, B, N_{sa})}$$

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

After  $M_2$ :

$$\frac{A \models A \xleftrightarrow{k_{as}} S, \quad A \triangleleft \left\{ N_{sa}, g_b, p_b, \xrightarrow{k_b} B, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sa}) \right\}_{k_{as}}}{A \models S \mid \sim (N_{sa}, g_b, p_b, \xrightarrow{k_b} B, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sa}))}$$

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

$$\frac{A \models S \models \xrightarrow{k_b} B, \quad A \text{ trusts } S \text{ on } k_b}{A \models \xrightarrow{k_b} B}$$

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

After  $M_3$ :

$$\frac{B \models B \xleftrightarrow{k_{bs}} S, \quad B \triangleleft \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}}{B \models S \mid \sim \left( \xrightarrow{k_a} A, N_{sb}, N_{sa} \right)}$$

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

$$\begin{array}{c}
\frac{B \models S \models \xrightarrow{k_a} A, \text{ } B \text{ trusts } S \text{ on } k_a}{B \models \xrightarrow{k_a} A} \\
\\
\frac{B \models \xrightarrow{k_a} A, \text{ } B \triangleleft \left\{ A, B, Y_A, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sb}) \right\}_{k_a^-}}{B \models A \mid \sim (A, B, Y_A, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sb}))} \\
\\
\frac{B \models A \mid \sim (A, B, Y_A, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sb})), \text{ } B \models \#(N_{sb})}{B \models A \models (A, B, Y_A, \left\{ \xrightarrow{k_a} A, N_{sb}, N_{sa} \right\}_{k_{bs}}, \#(N_{sb}))} \\
\\
\frac{B \models A \models Y_A, \text{ } B \models A \Rightarrow Y_A}{B \models Y_A} \\
\\
\frac{B \models Y_A, \text{ } B \Rightarrow Y_B}{B \models A \xleftrightarrow{k_{ab}} B}
\end{array}$$

After  $M_4$ :

$$\begin{array}{c}
\frac{A \models \xrightarrow{k_b} B, \text{ } A \triangleleft \{ Y_b, N_{sa}, \{N_b\}_{k_{ab}} \}_{k_b^-}}{A \models B \mid \sim (Y_b, N_{sa}, \{N_b\}_{k_{ab}})} \\
\\
\frac{A \models B \mid \sim (Y_b, N_{sa}, \{N_b\}_{k_{ab}}), \text{ } A \models \#(N_{sa})}{A \models B \models (Y_b, N_{sa}, \{N_b\}_{k_{ab}})} \\
\\
\frac{A \models B \models Y_B, \text{ } A \models B \Rightarrow Y_B}{A \models Y_B} \\
\\
\frac{A \models Y_B, \text{ } A \Rightarrow Y_A}{A \models A \xleftrightarrow{k_{ab}} B} \\
\\
\frac{A \models A \xleftrightarrow{k_{ab}} B, \text{ } A \triangleleft \{N_b\}_{k_{ab}}}{A \models B \mid \sim (N_b)} \\
\\
\frac{A \models B \mid \sim (N_b), \text{ } A \models \#(N_{sa})}{A \models B \models A \xleftrightarrow{k_{ab}} B}
\end{array}$$

After  $M_5$ :

$$\begin{array}{c}
\frac{B \models A \xleftrightarrow{k_{ab}} B, \text{ } B \triangleleft \{N_b\}_{k_{ab}}}{B \models A \mid \sim (N_b)} \\
\\
\frac{B \models A \mid \sim (N_b), \text{ } B \models \#(N_b)}{B \models A \models A \xleftrightarrow{k_{ab}} B}
\end{array}$$

## Offline Communication Real Protocol

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

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

$$M_x: A \rightarrow S: E_{k_b} \left( data, SeqNum, E_{k_a^-}(S(data, SeqNum)) \right) \quad || \\ E_{k_a^-}(S(data, SeqNum, E_{k_a^-}(S(data, SeqNum))))$$

## Offline Communication Idealized Protocol

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

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

## Offline Communication Analysis

Objective

$$A \models \xrightarrow{k_b} B$$

# Bob's Public Key

Assumptions

$$A \models A \leftrightarrow^{k_{as}} S, \quad S \models A \leftrightarrow^{k_{as}} S$$

# Session key (authentication protocol)

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

# Freshness session ids (authentication protocol)

After  $M_1$ :

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

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

After  $M_2$ :

$$\frac{A \models A \leftrightarrow^{k_{as}} S, \quad A \triangleleft \left\{ N_{sa}, \xrightarrow{k_b} B, \#(N_{sa}) \right\}_{k_{as}}}{A \models S \mid \sim (N_{sa}, \xrightarrow{k_b} B, \#(N_{sa}))}$$

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

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