

UNIVERSITÀ DEGLI STUDI DI PISA

FACOLTÀ DI INGEGNERIA

Laurea Magistrale in

INGEGNERIA INFORMATICA

SICUREZZA NEI SISTEMI INFORMATICI

**Progetto di una applicazione peer-to-peer
con comunicazione sicura**

Implementazione in Java

a cura di

Sacco Cosimo e Silvestri Davide

Anno Accademico 2010/2011

Indice

1	Analisi del protocollo di scambio chiavi	1
1.1	<i>Beliefs</i> da ottenere	1
1.2	Protocollo idealizzato	1
1.3	Ipotesi	2
1.4	Analisi dei <i>beliefs</i>	2
1.4.1	Messaggio <i>M1</i>	2
1.4.2	Messaggio <i>M2</i>	3
1.4.3	Messaggio <i>M3</i>	3
1.4.4	Messaggio <i>M4</i>	3
1.4.5	Messaggio <i>M5</i>	4

Capitolo 1

Analisi del protocollo di scambio chiavi

1.1 *Beliefs* da ottenere

Procediamo ad analizzare il protocollo esposto nel capitolo (RIFERIMENTO). Si vuole provare che il protocollo produce, in ciascuna delle parti, i seguenti *beliefs*:

	A	B
key authentication	$A \models A \xleftrightarrow{K} B$	$B \models A \xleftrightarrow{K} B$
key confirmation	$A \models B \models A \xleftrightarrow{K} B$	$B \models A \models A \xleftrightarrow{K} B$
key freshness	$A \models \# \left(A \xleftrightarrow{K} B \right)$	$B \models \# \left(A \xleftrightarrow{K} B \right)$

1.2 Protocollo idealizzato

Viene riportato, qui di seguito, il *protocollo idealizzato* relativo al protocollo di scambio delle chiavi esposto nel capitolo (RIFERIMENTO).

$$\begin{aligned}
 M1 : A \rightarrow B & \quad \left\{ \overset{K_A^+}{\mapsto} A, L_A \right\}_{K_T^-} \\
 M2 : A \leftarrow B & \quad \left\{ \overset{K_B^+}{\mapsto} B, L_B \right\}_{K_T^-} \\
 M3 : A \rightarrow B & \quad \left\{ n_A, A \xleftrightarrow{n_A} B \right\}_{K_B^+} \\
 M4 : A \leftarrow B & \quad \left\{ n_A, n_B, A \xleftrightarrow{\langle n_A \rangle n_B} B \right\}_{K_A^+} \\
 M5 : A \rightarrow B & \quad \left\{ n_B, A \xleftrightarrow{\langle n_A \rangle n_B} B \right\}_{K_B^+}
 \end{aligned}$$

1.3 Ipotesi

Vengono esplicitate, qui di seguito, le ipotesi sotto le quali il protocollo viene eseguito.

	A	B
public keys	$A \models \overset{K_A^+}{\mapsto} A$	$B \models \overset{K_B^+}{\mapsto} B$
third party	$A \models \overset{K_T^+}{\mapsto} T$	$B \models \overset{K_T^+}{\mapsto} T$
	$A \models T \Rightarrow \overset{K_X^+}{\mapsto} X$	$B \models T \Rightarrow \overset{K_X^+}{\mapsto} X$
freshness	$A \models \#(n_A)$	$B \models \#(n_B)$
	$A \models \#(L_B)$	$B \models \#(L_A)$

1.4 Analisi dei *beliefs*

Procediamo, ora, con l'analisi dei singoli messaggi. Partendo dalle ipotesi esposte nella sezione 1.3 e applicando le *regole di inferenza* della logica BAN, ciascuna parte può ampliare l'insieme dei propri *beliefs*. Se, tra i beliefs finali, compaiono quelli elencati nella sezione 1.1, allora possiamo affermare che il protocollo esposto è corretto.

1.4.1 Messaggio *M1*

Messaggio *M1*:

$$M1 : A \rightarrow B \quad \left\{ \overset{K_A^+}{\mapsto} A, L_A \right\}_{K_T^-}$$

per la *meaning rule*

$$\frac{B \models \overset{K_T^+}{\mapsto} T, B \triangleleft \left\{ \overset{K_A^+}{\mapsto} A, L_A \right\}_{K_T^-}}{B \models T \sim \left(\overset{K_A^+}{\mapsto} A, L_A \right)}$$

e poiché

$$\frac{B \models \#(L_A)}{B \models \# \left(\overset{K_A^+}{\mapsto} A, L_A \right)}$$

allora, per la *nonce verification rule*

$$\frac{B \models T \sim \left(\overset{K_A^+}{\mapsto} A, L_A \right), B \models \# \left(\overset{K_A^+}{\mapsto} A, L_A \right)}{B \models T \models \left(\overset{K_A^+}{\mapsto} A, L_A \right)}$$

e, in particolare,

$$B \models T \models \overset{K_A^+}{\mapsto} A$$

infine, per la *jurisdiction rule*

$$\frac{B \models T \models \overset{K_A^+}{\mapsto} A, B \models T \Rightarrow \overset{K_A^+}{\mapsto} A}{B \models \overset{K_A^+}{\mapsto} A}$$

1.4.2 Messaggio M2

In maniera del tutto analoga a quanto visto per il messaggio M1, il *belief* ottenuto da A dopo aver ricevuto il messaggio M2 è

$$A \models \overset{K_B^+}{\mapsto} B$$

1.4.3 Messaggio M3

Messaggio M3:

$$M3 : A \rightarrow B \quad \left\{ n_A, A \overset{n_A}{\rightleftharpoons} B \right\}_{K_B^+}$$

L' applicazione delle regole di inferenza non porta, su B, alla realizzazione di alcun nuovo belief. Tuttavia, poiché l' unica entità in grado di leggere il nonce n_A è B^1 , A può ritenere che

$$A \models A \overset{n_A}{\rightleftharpoons} B$$

1.4.4 Messaggio M4

Messaggio M4:

$$M4 : A \leftarrow B \quad \left\{ n_A, n_B, A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right\}_{K_A^+}$$

L' unica entità in grado di leggere il messaggio M4 è A^2 . Pertanto, B può ritenere che

$$B \models A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \quad B \text{ ottiene key authentication}$$

inoltre,

$$\frac{B \models \#(n_B)}{B \models \# \left(A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right)} \quad B \text{ ottiene key freshness}$$

¹B, infatti, è l' unica entità a possedere la chiave K_B^- necessaria per decifrare i messaggi cifrati con K_B^+ .

²A, infatti, è l' unica entità a possedere la chiave K_A^- necessaria per decifrare i messaggi cifrati con K_A^+ .

4 CAPITOLO 1. ANALISI DEL PROTOCOLLO DI SCAMBIO CHIAVI

per quanto riguarda A , invece, otteniamo

$$\frac{A \models \#(n_A)}{A \models \# \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}$$

e poiché, per la *meaning rule*

$$\frac{A \models A \xrightarrow{n_A} B, A \triangleleft \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}{A \models B \sim \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}$$

allora, per la *nonce verification rule*

$$\frac{A \models B \sim \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right), A \models \# \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}{A \models B \models \left(n_A, n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}$$

e in particolare

$$A \models B \models A \xleftarrow{\langle n_A \rangle_{n_B}} B \quad A \text{ ottiene key confirmation}$$

1.4.5 Messaggio $M5$

Messaggio $M5$:

$$M5 : A \rightarrow B \quad \left\{ n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right\}_{K_B^+}$$

L' unica entità in grado di leggere il messaggio $M5$ è B . Pertanto, A può ritenere che

$$A \models A \xleftarrow{\langle n_A \rangle_{n_B}} B \quad A \text{ ottiene key authentication}$$

inoltre,

$$\frac{A \models \#(n_A)}{A \models \# \left(A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)} \quad A \text{ ottiene key freshness}$$

per quanto riguarda B , invece, otteniamo

$$\frac{B \models \#(n_B)}{B \models \# \left(n_B, A \xleftarrow{\langle n_A \rangle_{n_B}} B \right)}$$

e poiché, per la *meaning rule*

$$\frac{B \models A \xrightarrow{\langle n_A \rangle_{n_B}} B, \quad B \triangleleft \left(n_B, A \xrightarrow{\langle n_A \rangle_{n_B}} B \right)}{B \models A \sim \left(n_B, A \xrightarrow{\langle n_A \rangle_{n_B}} B \right)}$$

allora, per la *nonce verification rule*

$$\frac{B \models A \sim \left(n_B, A \xrightarrow{\langle n_A \rangle_{n_B}} B \right), \quad B \models \# \left(n_B, A \xrightarrow{\langle n_A \rangle_{n_B}} B \right)}{B \models A \models \left(n_B, A \xrightarrow{\langle n_A \rangle_{n_B}} B \right)}$$

e in particolare

$$B \models A \models A \xrightarrow{\langle n_A \rangle_{n_B}} B \quad B \text{ ottiene key confirmation}$$