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

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	$A \models A \overset{K}{\leftrightarrow} B$	$B \models A \overset{K}{\leftrightarrow} B$
key confirmation	$A \models B \models A \overset{K}{\leftrightarrow} B$	$B \models A \models A \overset{K}{\leftrightarrow} B$
key freshness	$A \models \sharp\left(A \overset{K}{\leftrightarrow} B\right)$	$B \models \sharp\left(A \overset{K}{\leftrightarrow} B\right)$

1.2 Protocollo idealizzato

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

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

$$M2 : A \leftarrow B \quad \left\{ \overset{K_B{}^+}{\mapsto} B,\ L_B \right\}_{K_T{}^-}$$

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

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

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

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	$A \models \overset{K_T^+}{\mapsto} T$ $A \models T \Rightarrow \overset{K_X^+}{\mapsto} X$	$B \models \overset{K_T^+}{\mapsto} T$ $B \models T \Rightarrow \overset{K_X^+}{\mapsto} X$
freshness	$A \models \sharp(n_A)$ $A \models \sharp(L_A)$ $A \models \sharp(L_B)$	$B \models \sharp(n_B)$ $A \models \sharp(L_A)$ $A \models \sharp(L_B)$

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 $M1$:

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

per la *meaning rule*

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

e poiché

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

allora, per la *nonce verification rule*

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

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 $M3$:

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

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

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

1.4.4 Messaggio $M4$

Messaggio $M4$:

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

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

$$B \models A \xleftrightarrow{\langle n_A \rangle_{n_B}} B \qquad B \textit{ ottiene key authentication}$$

inoltre,

$$\frac{B \models \sharp\,(n_B)}{B \models \sharp \left(A \xleftrightarrow{\langle n_A \rangle_{n_B}} B \right)} \qquad B \textit{ ottiene key freshness}$$

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

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

per quanto riguarda A, invece, otteniamo

$$\frac{A \models \sharp\,(n_A)}{A \models \sharp\left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}$$

e poiché, per la *meaning rule*

$$\frac{A \models A \overset{n_A}{\rightleftharpoons} B,\ A \triangleleft \left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}{A \models B \mid\sim \left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}$$

allora, per la *nonce verification rule*

$$\frac{A \models B \mid\sim \left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right),\ A \models \sharp\left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}{A \models B \models \left(n_A,\ n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}$$

e in particolare

$$A \models B \models A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \qquad A \textit{ ottiene key confirmation}$$

1.4.5 Messaggio $M5$

Messaggio $M5$:

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

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

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

inoltre,

$$\frac{A \models \sharp\,(n_A)}{A \models \sharp\left(A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)} \qquad A \textit{ ottiene key freshness}$$

per quanto riguarda B, invece, otteniamo

$$\frac{B \models \sharp\,(n_B)}{B \models \sharp\left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B\right)}$$

e poiché, per la *meaning rule*

$$\frac{B \models A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B,\ B \triangleleft \left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right)}{B \models A \mid\sim \left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right)}$$

allora, per la *nonce verification rule*

$$\frac{B \models A \mid\sim \left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right),\ B \models \sharp \left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right)}{B \models A \models \left(n_B,\ A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \right)}$$

e in particolare

$$B \models A \models A \overset{\langle n_A \rangle_{n_B}}{\longleftrightarrow} B \qquad B \textit{ ottiene key confirmation}$$