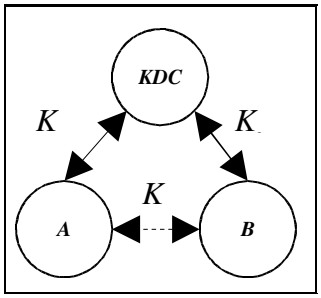
PROVA SCRITTA DEL 7 Luglio 2009 (10 PT)



A e *B* stabiliscono una chiave di sessione K_{ab} per mezzo del protocollo Diffie-Hellman (DHP), con parametri pubblici *p* e *g*. Per evitare l'attacco dell'uomo nel mezzo, il protocollo DH viene esteso per mezzo di un Key Distribution Center (KDC), on-line, con cui *A* e *B* condividono un cifrario simmetrico (*E*, *D*) ed una chiave simmetrica segreta. Siano K_a e K_b le chiavi simmetriche segrete che *A* e *B* condividono con KDC, rispettivamente.

Quesito 1. Progettare il protocollo DH-esteso (E-DHP) in modo che soddisfi i seguenti requisiti: a) il protocollo non è soggetto all'uomo nel mezzo; b) al termine del protocollo, *A* ha la prova che *B* dispone di K_{ab} e viceversa.

Quesito 2. Valutare se nell'interazione tra *A*, *B* e *KDC* è possibile sostituire il cifrario (*E*, *D*) con un *message authetication code* $h_K()$. Motivare la risposta.

Quesito 3. Si assuma che un avversario disponga di una Kab passata ed abbia registrato tutti i messaggi dell'istanza di protocollo che l'ha stabilita. Tramite un replay attack, l'avversario può indurre A (o B) a stabilire ancora Kab come chiave condivisa? Motivare la risposta.

Soluzione

Quesito 1 (4 pt)

M1 A -> KDC: A, B, {A, B, Xa}Ka
M2 KDC->B: A, B, {A, B, Xa}Kb
M3 B -> KDC: B, A, {B, A, Xb}Kb
M4 KDC->A: B, A, {B, A, Xb}Ka
M5 A->B: {A}Kab
M6 B->A: {B}Kab

Quesito 2 (3 pt)

{Z}Kx può essere sostituito con hKx(Z)

Quesito 3 (3 pt)

No, l'avversario non può indurre A (o B) a stabilire ancora Kab. Infatti, il protocollo DH richiede che ad ogni istanza di esecuzione, ciascuno dei peer generi una nuova chiave segreta in modo random. Per cui, anche se l'avversario riusa Xb, A genererà una nuova chiave segreta a' e perciò l'a nuova chiave sarebbe kba'. Per poter stabilire tale chiave l'avversario dovrebbe ricavare b da Xb ma ciò richiede di risolver il DLP.