ESIMS - An Efficient Key Predistribution Scheme

Mahalingam Ramkumar, Nasir Memon
Department of Computer and Information Science
Polytechnic University, Brooklyn, NY 11201.

Abstract

SIMS (Secure Interaction of Mobile Strangers) [1] is a highly scalable, renewable, key predistribution scheme suitable for resource constrained nodes that need to operate without a trusted authority (TA) for extended periods. In a subsequent work [2] SIMS was extended for multicast and broadcast communications. Like any key predistribution scheme however, SIMS can be compromised by a collusion of a certain number of nodes. We are currently investigating an extension of SIMS (ESIMS), which significantly reduces the vulnerability of SIMS to collusion. ESIMS is infact a generalization of both SIMS and a scheme proposed by Leighton and Micali (LM) in [3].

In SIMS (characterized by P, k), k preloaded keys in each node are chosen from a larger (indexed) pool of P $(K_1 \cdots K_P)$ keys in a pseudo-random fashion. Every node has a unique ID, and the indices of the k keys preloaded in a node is obtained from a public function $F_1(ID)$. Let $F_1(ID_i) = x_{1_i} \cdots x_{k_i}$, $1 \leq x_{j_i} \leq P \forall j, i$. Now $K_{x_{1_i}} \cdots K_{x_{k_i}}$ are the k distinct keys assigned to (or preloaded in) node i. Any two nodes (i and j) wishing to communicate securely, just need to know each other's IDs. From the IDs the two nodes i and j can independently calculate the keys they share (if any) using the public function $F_1()$ as $F_1(ID_i) \bigcap F_1(ID_j)$. The session key is then obtained as a function of *all* the shared keys. Similarly, multicasting between r nodes of a network can be achieved by using the intersection of the keys of all r nodes to get the session key (for unicasting $r = 2$).

In the LM key predistribution scheme [3] (characterized by k, L), the TA generates k keys, $M_1 \cdots M_k$. A user i is assigned a sequence of numbers $\alpha_{1_i} \cdots \alpha_{k_i}$, $1 \leq \alpha_{j_i} \leq L \forall j$ which serves as the "public key" of user i. The k keys $K_{i_1} \cdots K_{i_k}$ preloaded in node i is given by $K_{i_j} = h^{\alpha_{j_i}}(M_j), 1 \leq j \leq k$ (where, $h^0(x) = x, h^1(x) = h(x), h^2(x) = h(h(x))$ and so on). For communication between two nodes A and B, let $\alpha_{1_A} \cdots \alpha_{k_A}$ be the public key of node A, and $\alpha_{1_B} \cdots \alpha_{k_B}$ that of node B. Node A obtains the session key K_{AB} as follows. If $v_j = 0$ for $\alpha_{j_A} \geq \alpha_{j_B}$ and $v_j = \alpha_{j_B} - \alpha_{j_A}$ otherwise, and $w_j = \max(\alpha_{j_A}, \alpha_{j_B})$. the session key K_{AB} is obtained as

$$K_{AB} = h(h^{v_1}(K_{A_1})|h^{v_2}(K_{A_2})| \cdots |h^{v_k}(K_{A_k})) = h(h^{w_1}(M_1)|h^{w_2}(M_2)| \cdots |h^{w_k}(M_k)) \quad (1)$$

ESIMS, characterized by P, k, L, can be considered as a direct extension of both SIMS and the LM scheme. Like SIMS, ESIMS uses a set of $P > k$ keys in the pool. And like the LM scheme, a certain order (less than L) of hash of the keys is loaded in the nodes. In short, SIMS is special case of ESIMS with $L = 0$. LM is a special case of ESIMS with $P = k$.

The performance merit of SIMS, LM and ESIMS can be considered as a function of the probability of eavesdropping on a multicast communication between r nodes, by a collusion of n nodes. Lower the probability of eavesdropping, better the merit of the system. In general, SIMS is seen to outperform LM significantly (for a given k). ESIMS is seen to outperform both SIMS and LM significantly. Due to the "orthogonal" nature of SIMS and LM the obtainable merit in ESIMS is almost equal to the product of the merits of SIMS and LM.

References

[1] M. Ramkumar, N. Memon, R. Simha, "SIMS - Secure Interaction of Mobile Strangers," submitted to ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, Boston, MA, July 2003.

[2] M. Ramkumar, N. Memon, "Pre-Loaded Key Based Multicast and Broadcast Authentication in Mobile Ad-Hoc Networks," submitted to Globecom-03.

[3] T. Leighton, S. Micali, "Secret-key Agreement without Public-Key Cryptography,"*Advances in Cryptology* - CRYPTO 1993, pp 456-479, 1994.