Computer Communications 22 (1999) 193–194

Research note

A note on breaking and repairing a secure broadcasting in large networks

Hung-Min Sun[a,*], Shiuh-Pyng Shieh[b], Hsin-Min Sun[c]

[a]Department of Information Management, Chaoyang University of Technology, Wufeng, Taichung County, Taiwan 413
[b]Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan 30050
[c]Chianan College of Science and Pharmacy, Tainan, Taiwan

Received 1 May 1998; received in revised form 24 September 1998; accepted 24 September 1998

Abstract

In this note, we show that a proposed secure broadcasting scheme is insecure. We also present a modified scheme to overcome this weakness. The modified scheme has the extra advantage that each participant can derive his group keys from group identities without the need of knowing other information.

Keywords: Secure system; Broadcasting; Network security; Cryptography; Computer network

1. Introduction

Recently, Sun and Shieh [1] proposed a secure broadcasting scheme (SS scheme in short) based on the assumption that users or hosts in a large network are partitioned and organized as a hierarchical tree where children of the common parent form a group. In this note, we show that SS scheme is insecure because those groups with the common parent have the same group key. We also present a modified scheme to overcome this weakness. The modified scheme has the extra advantage that each principal can derive his group keys from group identities without the need of knowing other information.

Basically, SS scheme contains two parts: a key management mechanism in a hierarchical tree of principals which is responsible for key generation and group key derivation, and a secure broadcasting protocol which is responsible for encryption by the sending principal and decryption by the legal receiving principals. In SS scheme, users or hosts in a large network are partitioned and organized as a hierarchical tree where children of the same parent form a group. A group may contain one or many principals. Every principal in a network system is regarded as a group and is represented by a leaf in a tree. Groups (children) sharing some characteristics form a sup-group (parent group), represented by a subtree. That is, the union of groups in a subtree forms their parent group. The root of the tree represents the universal group which is the group of all principals in the network system. Owing to the characteristics of the tree structure, SS scheme uses a key management mechanism to generate the corresponding group key for each group. Every principal in a group can recover the group key by using his secret-key, but principals outside this group cannot. SS scheme also uses a secure broadcasting protocol for encryption and decryption. The sending principal encrypts a message into a ciphertext by using the public-keys of the receiving groups and then broadcasts this ciphertext to the principals in these groups. Each principal in a legal group can derive his group key and then decrypt the ciphertext into the message, while illegal principals cannot. As the insecurity of SS scheme comes from the weakness of the key management mechanism, for simplicity, we describe only the key management mechanism here.

1.1. Key generation algorithm:

A center authority (CA) first selects two large prime numbers, p and q, satisfying the RSA assumption and then computes $N = p \cdot q$. CA travels the nodes in the tree of hierarchical principal groups from the root to leaves, and from left to right.

1. If the node is G_u which is the root of the tree, then CA assigns a random number k_u (mod N) as the group key of G_u and selects a pair of (T_u, S_u) such that $T_u \cdot S_u = 1$ (mod $\phi(N)$), where T_u is public and S_u is secret.
2. If the node G_i is not the root or a leaf, we assume that G_j is the parent of node G_i and the group key of G_j is k_j. CA computes $k_i = (k_j)^{S_j} (\text{mod} N)$ *as the group key of* G_i and

* Corresponding author. Tel.: 0886 4 3323000 7122; fax: 08864 3742337; e-mail: hmsun@mail.cyut.edu.tw; e-mail: ssp@csie.nctu.edu.tw; e-mail: sunhm@chna.chna.edu.tw

0140-3664/99/$ - see front matter
PII: S0140-3664(98)00253-9

selects a pair of (T_i, S_i) such that $T_i \cdot S_i = 1$ (mod $\phi(N)$), where T_i is public and S_i is secret.
3. If the node G_i is a leaf (the group contains only one principal) of the tree, we assume that node G_j is the parent of node G_i and the group key of G_j is k_j. CA computes $k_i = (k_j)^{S_j}(\mathrm{mod}N)$ as the group key of G_i (the secret key of the principal).

1.2. Key derivation algorithm:

Assume u_s is a principal in the group G_i, who wants to get the group key k_i of G_i. We assume that the principal corresponds to the group G_s, i.e., $G_s = \{u_s\}$, and G_f is the parent of G_s.

1. If $G_s = G_i$, then the group key k_i of G_i is equal to k_s (the secret key of the principal).
2. If $G_s \neq G_i$, then $G_s \subset G_f \subseteq G_i$. U_s who owns the group key k_s can compute the group key k_f of G_f by $k_f = (k_s)^{T_f}(\mathrm{mod}N)$. Upon the group key k_f of G_f is determined, the group key k_r of G_r can be computed by $k_r = (k_f)^{T_r}(\mathrm{mod}N)$ where node G_r is the parent of node G_f. The same processes are repeated until the group key k_i is derived.

2. Weakness of SS scheme

In [1], they considered only the security problem whether a principal outside the group G_i can derive the group key k_i of G_i. They ignored the possibility that a principal inside a group G_i but outside a group G_j, where $G_j \subset G_i$, can derive the group key k_j of G_j. We point out the details in the following.

In the key management mechanism of SS scheme, if node G_i is a child of G_j and the group key of G_j is k_j, CA will assign $k_i = (k_j)^{S_j}(\mathrm{mod}N)$ as the group key of G_i. If node G_h is another child of G_j, CA will assign $k_h = (k_j)^{S_j}(\mathrm{mod}N)$ as the group key of G_h. It is unfortunate that $k_i = k_h = (k_j)^{S_j}(\mathrm{mod}N)$.

Therefore, all groups with the common parent own the same group key. This leads SS scheme to be insecure because any principals in an illegal group can correctly decrypt the ciphertext into the message provided that the illegal group has the common parent with any legal groups.

3. A modified key management mechanism

We revise the key management mechanism of SS scheme as follows:

3.1. Key generation algorithm:

(1′) If the node is G_u which is the root of the tree, then CA assigns a random number k_u (mod N) as the group key of node G_u.
(2′) If the node G_i is not the root, we assume that node G_j is the parent of node G_i and the group key of node G_j is k_j. CA computes a value S_i satisfying $F(\mathrm{ID}_i) \cdot S_i = 1$ (mod $\phi(N)$), where ID_i is the group identity of G_i and F(k) is the function of the maximum prime number which is less than or equal to k. CA computes $k_i = (k_j)^{S_i}(\mathrm{mod}N)$ as the group key of node G_i. After k_i is computed, S_i shall be discarded. If a node G_i is a single principal, the group key k_i is the secret key of the principal.

3.2. Key derivation algorithm:

Step 2 in the previous key derivation algorithm is modified as follows:

(2′) If $G_s \neq G_i$, $G_s \subset G_f \subseteq G_i$, principal u_s computes the group key k_f of node G_f by $k_f = (k_s)^{F(ID_s)}(\mathrm{mod}N)$. Once the group key k_f of node G_f is determined, the group key k_r of node G_r can be also computed by $k_r = (k_f)^{F(ID_f)}(\mathrm{mod}N)$ where node G_r is the parent of node G_f. The same processes are repeated until the group key k_i is derived

.

The modified scheme can overcome the weakness of the previous key management mechanism. In addition, the modified scheme has the extra advantage that each principal can derive his group keys from group identities without the need of knowing other information.

Acknowledgements

This work was supported in part by the National Science Council, Taiwan, under contract NSC-87-2213-E324-003. The authors would like to thank anonymous reviewers for their useful comments.

References

[1] H.M. Sun, S.P. Shieh, Secure broadcasting in large networks, Computer Communications 21 (3) (1998) 279–283.