Secure, Scalable Few-to-Many Group Communication*

Nathalie Weiler <weiler@acm.org>
Swiss Federal Institute of Technology ETH Zürich, Switzerland

Abstract

News distribution and service discovery protocols are examples of applications that typically involve more than one sender for performance reasons in the distribution process. Few-to-Many Semsomm – presented below – proposes a secure and scalable group key management scheme for this purpose.

1 Introduction

Many Internet multi-party applications require a **scalable and secure group communication infrastructure**. Existing communication protocols are moderately suited for dynamic groups as they require the key used for data encryption (a session key) to be changed at every membership change in the group. This is because perfect forward secrecy must be ensured, i.e. only actual members of the group should be able to decrypt the multicast traffic. Most proposed approaches are either scalable (Ex.: [2]) or ensure perfect forward secrecy (Ex.: [1]).

In [3], we proposed Semsomm, a new generation means for **scalable, perfect forward secure group communication** for a classical one-to-many scenario with one sender and a huge number of receivers. Therefore, we combined the idea of periodic re-keying with a double encryption scheme involving internal nodes of the multicast distribution scheme. This poster describes extensions of Semsomm to **few-to-many scenarios**, i.e. to applications involving a huge number of receivers, but only few senders.

2 Few-to-Many Semsomm: Data Distribution

S	: Sender
R_i	: Receiver Number i
N_j	: Intermediate Node Number j
KD_k	: Key Distributer Number k
SR	: Encryption Key for multicast traffic used between Sender and Receivers
SN_k	: Encryption Key used between Sender and intermediate Nodes at the same location
N_jR	: Encryption Key used between Node N_j and its adjacent Receivers
SR_{KD_k,R_i}	: Encryption Key used during the re-keying, known only to KD_k and R_i
f	: One-Way Hash Function

Table 1. Notation.

*This handout is a description of the poster presented at CMS'02.

The general data protocol illustrated below shows how the multiple encryption scheme of Semsomm is applied. The notation are explained in Table 1.

- The data payload is encrypted by the senders with SR.
- Additionally, the senders also perform a second encryption with the keys SN_1 and SN_2 known only to them and the intermediate nodes.
- Finally, the node N_x decrypts the packet for its receivers and forwards it to them after encrypting it with a key N_xR known to itself and its receivers.

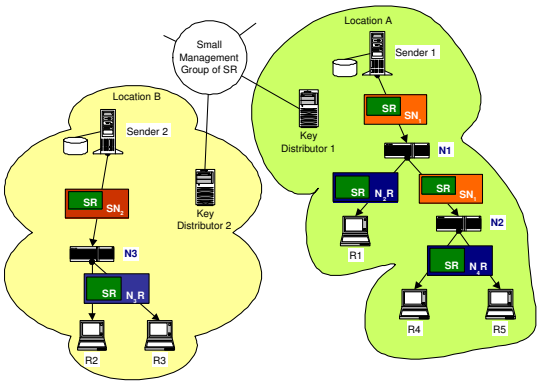

Figure 1. Key Usage in Few-to-Many Scenario.

As the knowledge of the keys is distributed, only legitimate receivers knowing SR can decrypt the original message. The intermediate nodes are only trusted for forwarding and, if necessary, re-encrypting these encrypted messages. They cannot read the original message because they do not know SR.

2.1 Join

The join process is performed in five steps:

(1) The new participant R_6 requests SR from the key distributor the present location presenting its credentials – e.g. some kind of payment – to join the group.

(2) The key distributor verifies the credentials. In case of a successful verification, it computes the result of $f(SN_1)$ [1] and transmits both $f(SN_1)$ and SR together with an additional key SR_{KD_1,R_6} through a secure channel to R_6.

(3) R_6 asks N_3 for N_3R presenting $f(SN_1)$ as credential.

[1] f is a defined one way function known at least to all sender and intermediate nodes, but others may also know f.

(4) N_3 generates a new N_3R and distributes it to the subscribed receivers R_2, R_3 and R_6 upon successful verification of $f(SN_1)$.
(5) From this point in time on, the N_3R_{new} is used as encryption key by N_3.

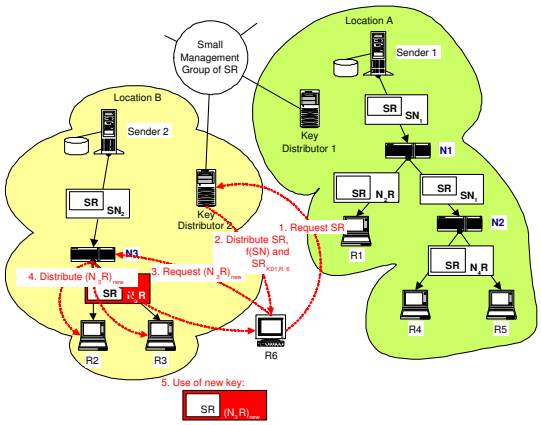

Figure 2. Join of R_6.

2.2 Leave

Assuming R_3 leaves the group – voluntarily or forced. The leave operation is straightforward as depicted below: We only need a new N_3R_{new}.

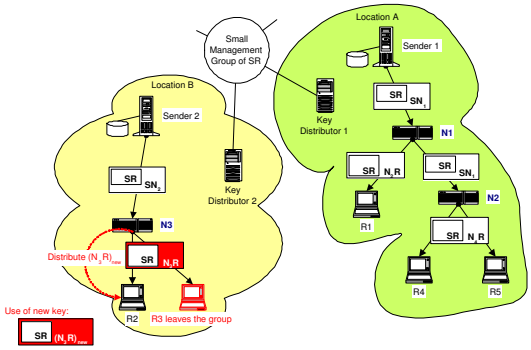

Figure 3. Leave of R_3.

2.3 Periodic Re-Keying

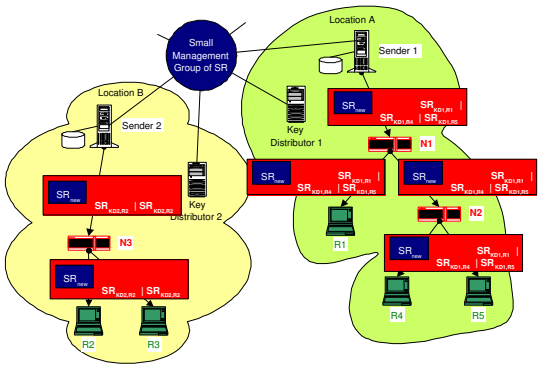

Figure 4. Re-keying of SR.

SR and SN are replaced by newly generated keys at regular time intervals as show beneath for SR. Thereby,

- infinite lifetimes of the keys are avoided, and
- the overhead involved is predictable, an important feature especially for applications running on limited resources.

3 Performance

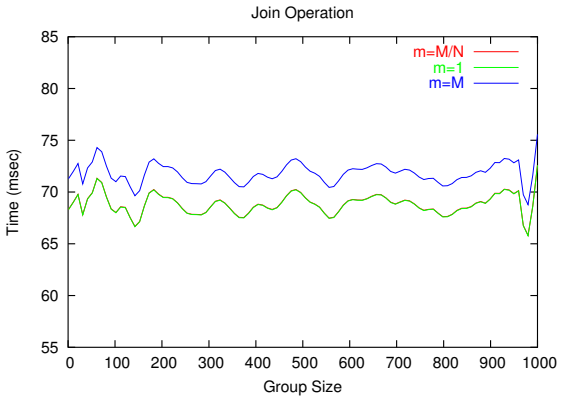

Figure 5. Join Performance

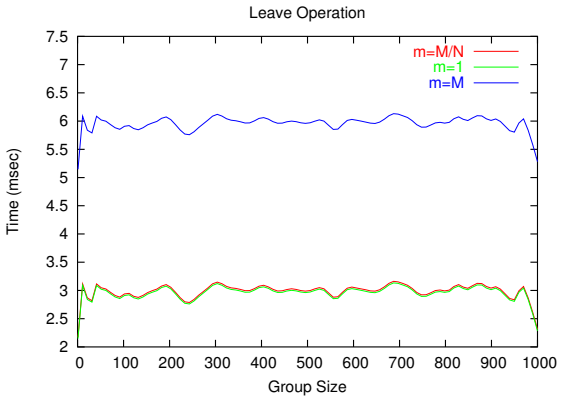

Figure 6. Leave Performance

4 Conclusion

Few-to-many Semsomm is a new scalable, secure group communication solution for applications involving few senders and a large number of receivers. The approach proved to be collusion resistant. Furthermore, the computational and communication overheads depend only on the number of receivers per node. One promising future application area is a service discovery protocol in ad hoc networks.

References

[1] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm. Group key management architecture. Internet Draft: draft-ietf-msec-gkmarch-02.txt, February 2002.

[2] S. Setia, S. Loussih, S. Jajodia, and E. Harder. Kronos: A scalable group re-keying approach for secure multicast. In *IEEE SSP*, 2000.

[3] N. Weiler. SEMSOMM - A Scalable Multiple Encryption Scheme for One-To-Many Multicast. In *Proceedings of the WET ICE '01*, June 2001.