SEMPRE: SECURE MULTICAST ARCHITECTURE USING PROXY RE-ENCRYPTION

YUN-PENG CHIU¹, CHUN-YING HUANG² AND CHIN-LAUNG LEI¹

¹Department of Electrical Engineering
National Taiwan University
No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan
frank@fractal.ee.ntu.edu.tw; lei@cc.ee.ntu.edu.tw

²Department of Computer Science and Engineering
National Taiwan Ocean University
No. 2, Peining Rd., Keelung 20224, Taiwan
chuang@ntou.edu.tw

Received February 2011; revised June 2011

ABSTRACT. The goal of a secure multicast communication environment is to ensure that only valid members belonging to the multicast group can decrypt data. A simple solution adopted by many previous studies is to use a “group key” that is shared by all group members. The sender uses the group key to encrypt the multicast data, and the receivers decrypt the data with the same key. However, the procedure may incur the so-called “1 affects n problem”, whereby the action of one member affects the whole group. This is the source of scalability problems. Moreover, from an administrative perspective, it is desirable to confine the impact of membership changes to a local area. In this paper, we propose a novel secure multicast architecture that reduces the impact of the 1 affects n problem significantly by exploiting a cryptographic primitive, “proxy re-encryption”. Therefore, we call the proposed secure multicast architecture Sempre (SEcure Multicast architecture using Proxy Re-Encryption). Proxy re-encryption allows intermediate routers to convert the ciphertext encrypted with one key to ciphertext encrypted with another key, without revealing the private key or the plaintext. If the intermediate routers are given proper keys, they can provide separation between subgroups and thereby achieve the goals of scalability and containment. Successful containment reduces the 1 affects n problem significantly. We also compare several related schemes, and discuss some security problems that we identified in them. Existing schemes that use similar techniques only use asymmetric-key algorithms, but the computational costs of the algorithms mean that the schemes are infeasible in practice. Our scheme combines asymmetric-key and symmetric-key algorithms, so it is practical for real-world applications.

Keywords: Secure multicast, Multicast key management, Proxy re-encryption

1. Introduction. Since the emergence of multicast communications in the late 1980s [1, 2], the issue of secure multicast communications has been addressed frequently in the literature. Rafaeli and Hutchison provide a detailed survey of works on secure multicast [3].

Several approaches utilize a group key that is shared by all group members. The sender uses the group key to encrypt the multicast data, and all valid members use the same group key to decrypt the data. However, the group-wise key may incur the so-called “1 affects n problem” [4], which means that the action of one member affects the whole group. More specifically, because the group key is known by all members, whenever a member joins or leaves the group, the remaining members of the group must acquire a new group key.