Cryptology ePrint Archive: Report 2011/575

Exclusive Key-Based Group Rekeying

Jing Liu, Changji Wang

Abstract: Group rekeying protocols are intended to support private group communications for large and dynamic groups. Given a group of users, an exclusive key for a user i is a key shared by all users in this group except i, and thus can be used to exclude i from this group. In this paper, we present three personal key assignment algorithms based on this idea. The first algorithm is based on the so-called independent exclusive keys, and thus has a great storage requirement. The other two are based on functional-dependent exclusive keys which are derived using dual hash chains and a binary hash tree, respectively, and thus greatly reduce the storage requirement. Basing on each of these personal key assignment algorithms, we propose a stateful group rekeying protocol and a stateless group rekeying protocol. We prove that all six protocols are secure against single-user attacks (i.e., 1-resilient) in a symbolic security model. We also give a performance comparison between our stateful protocols and existing 1-resilient stateful group rekeying protocols, and a comparison between our stateless protocols and existing 1-resilient stateless group rekeying protocols. To the best of our knowledge, the proposed Protocol III is the most efficient 1-resilient stateful group rekeying protocol to date.

Category / Keywords: applications / multicast key distribution, group rekeying, 1-resilient

Date: received 25 Oct 2011

Contact author: liujing3 at mail sysu edu cn

Available formats: PDF | BibTeX Citation

Version: 20111025:171405 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]