Cryptology ePrint Archive: Report 2013/100

Attacks and Comments on Several Recently Proposed Key Management Schemes

Niu Liu and Shaohua Tang and Lingling Xu

Abstract: In this paper, we review three problematic key management(KM) schemes recently proposed, including Kayam's scheme for groups with hierarchy [9], Piao's group KM scheme [13], Purushothama's group KM schemes [15]. We point out the problems in each scheme. Kayam's scheme is not secure to collusion attack. Piao's group KM scheme is not secure and has a bad primitive. The hard problem it bases is not really hard. Purushothama's scheme has a redundant design that costs lots of resources and doesn't give an advantage to the security evel and dynamic efficiency of it. We also briefly analyze the underlying reasons why these problem emerge.

Category / Keywords: cryptographic protocols / key management schemes; hierarchical access control;collusion attack;

Date: received 22 Feb 2013, last revised 11 Mar 2013

Contact author: niuliu83 at gmail com