Cryptology ePrint Archive: Report 2013/132

Yet Another Attack On the Chinese Remainder Theorem Based Hierarchical Access Control Scheme

Niu Liu and Shaohua Tang and Lingling Xu

Abstract: The hierarchical access control scheme based on Chinese Reminder Theorem [49] (CRTHACS) was supposed to be capable of hiding hierarchical structure, but Geiselmann et al. [18] showed practical attacks on CRTHACS to reveal the hierarchies it hides. Then, Zou et al. modified it, and gave a new CRTHACS [50] to resist those attacks. Nevertheless, we find that the modified version is still defective if it permits changes of structure, i.e. the scheme works in a dynamic scenario. In this paper, we describe our attack on the modified version of CRTHACS. We extend the description of the CRTHACS in a more proper form making it easier for us to look into the problem it has. We find the key character of the vulnerability which we name as double-invariance. We generalize our attack in an algebraic form and apply it to a series of hierarchical cryptographic access control schemes that share the same vulnerability with CRTHACS. We also give the countermeasure to fix this vulnerability.

Category / Keywords: cryptographic protocols / communication security, CRTHACS, Chinese remainder theorem,hierarchical access control, secure group communication

Date: received 6 Mar 2013

Contact author: niuliu83 at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130307:161852 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]