2004-04-27

Group Key Manager on a Smart Card

Hamandi, Hani

Boston University Computer Science Department

http://hdl.handle.net/2144/3775

Boston University
Abstract:

Group communication is as an important functionality, which needs to be supported by various communication technologies. Applications of group communication include IP (or application-level) multicast, wireless and/or ad-hoc networks, broadcast, conference calling, pay-per-view, and even such seemingly unrelated to networks areas as copy protection. For many, if not all, of these applications, security and trust play an important role. Securing group communication typically requires confidentiality and authentication, which typically rely on secret keys. Thus key management issues must be addressed.

This paper describes an implementation of one approach to dynamic group key management, which is based on Logical Key Hierarchy or Subset-Cover approach [1,2].

Our approach achieves a dramatic reduction of the storage requirements for the Group Key Manager, and in particular allows all the secret key data to be stored on a smart-card. It also allows a number of subsequent improvements.