Information and Management Sciences
Vol. 5, No. 2, pp.73-85, 1994

Cryptographic Implementation of Dynamic Access Control in User Hierarchy

Tzong-Chen Wu
National Taiwan Institute of Technology
R.O.C.

Abstract

This paper presents a cryptographic key assignment scheme for the access control in an arbitrary partially ordered user hierarchy. In our scheme, each user U_i in the hierarchy is assigned a secret key k_i. Associated with all the secret keys for users in the hierarchy, a public interpolating polynomial $Q(x)$ is constructed. The information items held by U_i are enciphered with the key k_i. By using the secret key k_i along with the $Q(x)$, U_i can derive any of his successor's secret key and then read the information items held by the successor. The proposed scheme is rather simple and flexible to handle the dynamic access control, such as change secret keys for users, add/delete immediate relationships between users, and add/delete users. Besides any user in the hierarchy can freely change his secret key for some security considerations without altering the existing secret keys for his successors.

Keywords: Access Control, User Hierarchy, Partially Ordered Hierarchy, Key Assignment, Dynamic Access Control