The Study of Dynamic Access Control in a User Hierarchy

聞士林、翁永昌 ; 陳澤雄

E-mail: 8919400@mail.dyu.edu.tw

ABSTRACT

In this thesis, three cryptographic key assignment schemes were proposed to solve the dynamic access control problems in a user hierarchy. The first scheme is an extension of Chen?s scheme that is based on Chinese Remainder Theorem, and the extended scheme is more efficient than the original scheme. The second scheme was proposed to improve the Lin?s scheme that is weak in some attack. The third scheme is a new scheme that is more efficient than the earlier schemes. The dynamic access control problems, such as adding/ deleting classes, adding/deleting relationships, and changing secret keys, are considered. Moreover, no modification of the secret keys for existing classes is needed.

Keywords : user hierarchy ; dynamic access control ; key management

Table of Contents

REFERENCES

[1] AKL, S.G., and TAYLOR, P.D., ‘ Cryptographic solution to a problem of problem of access control in a hierarchy ’ , ACM Trans. Comput. Syst., 1, (3), 1983, pp. 239-247 [2] Mackinnon, S.T., Taylor, P.D., Meijer, H., and Akl, S.G. ‘ An optimal algorithm for assigning cryptographic keys to control access in a hierarchy ’ , IEEE Trans. Comput., C-34, (9), 1985, pp. 797-802 [3] HARN, L., and LIN, H.Y., ‘ A cryptographic key generation scheme for multilevel data security ’ , Comput. Secur., 9, 1990, pp. 539-546 [4] Kuo, F.H., Shen, V.R.L., Chen, T.S., and Lai, F, ‘ Cryptographic key assignment scheme for dynamic access control in a user hierarcy ’ , IEE Proc.-Computers & Digital Techniques, Vol. 146, No.5, Sept. 1999, pp. 235-240