

使用者階層中動態存取控制之研究

聞士林、翁永昌；陳澤雄

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

摘要

近幾年來，由於電腦網路的流行與電腦技術快速的發展，使得在一個開放及公開的多數使用者環境中，可以共同分享昂貴的電腦資源，諸如：電腦通訊網際網路、無線通訊等。然而，在階層式多數使用者共同分享資源的環境下，確保資料安全是一個非常重要的課題，因為可能出現一些不可期望的現象，諸如：未經授權的存取資料、或是存取資料的權力階層沒有相符的情形。因此，在階層式多數使用者的電腦網路環境中，如何控制存取系統的資源，將是一個非常重要的研究課題。在這篇論文中，我們提出三個金鑰管理的方法來解決動態存取控制的問題。

關鍵詞：使用者階層；動態存取控制；金鑰管理

目錄

Chapter 1. Introduction.....	1	Chapter 2. Background and Previous Research.....		
.....3	2.1 Basic Concepts of Cryptography	3	2.2 Previous Research.....	
.....10	Chapter 3. Extension of Chen's Scheme.....	13	3.1 Brief Review of Chen's Scheme	
.....13	3.2 Dynamic Access Control in Chen's Scheme.....	15	3.2 Dynamic Access Control in Chen's Scheme.....	
.....21	3.3 Extend Scheme.....		3.3 Extend Scheme.....	
.....29	3.4 Dynamic Access Control in Extended Scheme.....	23	3.4 Dynamic Access Control in Extended Scheme.....	
.....29	Security Analysis and Discussion	29	3.5 Security Analysis and Discussion	
.....30	Chapter 4. Modified Lin's Scheme		Chapter 4. Modified Lin's Scheme	
.....30	4.1 Brief Review of Lin's Scheme	30	4.1 Brief Review of Lin's Scheme	
.....32	4.2 Comments on Lin's Scheme		4.2 Comments on Lin's Scheme	
.....32	4.3 Modified Scheme.....	34	4.3 Modified Scheme.....	
.....36	4.4 Dynamic Access Control in		4.4 Dynamic Access Control in	
.....36	Modified Scheme.....	36	Modified Scheme.....	
.....40	4.5 Security Analysis and Discussion	40	4.5 Security Analysis and Discussion	
.....40	Chapter 5. A New Key		Chapter 5. A New Key	
.....43	Management Scheme	43	Management Scheme	
.....43	5.1 Key Managemetrn	43	5.1 Key Managemetrn	
.....44	5.2 Dynamic Access Control in the New Scheme	44	5.2 Dynamic Access Control in the New Scheme	
.....44	5.3 Security Analysis and Discussion		5.3 Security Analysis and Discussion	
.....49	Chapter 6. Conclusion and Future Research.....	53	Chapter 6. Conclusion and Future Research.....	
.....53				

參考文獻

- [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 hierarchy ', IEE Proc.-Computers & Digital Techniques, Vol. 146, No.5, Sept. 1999, pp. 235-240