電腦網路秘密分享機率模型之研究

The Study of Probability Modeling in a Secret Sharing Computing Environment

計畫編號：NSC89-2213-E009-198
執行期限：89 年 8 月 1 日至 89 年 7 月 31 日
主持人：陳登吉 交通大學資訊工程系教授
共同主持人：李清雲 交通大學資訊工程研究所

一、摘要

中文摘要

由於資源共享、相互通連等特性，造成資訊網路的驚人成長與廣泛應用，但也潛在著安全威脅等問題，那就是當使用者可以很方便的透過電腦網路，隨時隨地存取連接在網路上之其他電腦資訊時，儲存在本身電腦的機密資料及當一些重要資料在電腦網路傳輸時，會受到什麼樣的威脅且該如何的保護？對於此一發展趨勢，資訊保密與網路安全已成為很重要的課題。本計畫探討密鑰分享方式，以確保資料儲存與傳輸的安全性。首先，在開放式的電腦網路環境中，我們嘗試提出新的機率模型來評估密鑰恢復的或然率，並提出演算法來計算在不可靠的網路系統中密鑰恢復之或然率。

其次，針對階層式授權及團體導向的密鑰分享策略應用，提出兩個密鑰分享方法，稱為複式分配法和複式密鑰分享方法，是廣義的密鑰分享方式，不受限於一個固定的門檻值且可實現預定的分享策略；同時，配合上述密鑰分享方法，我們提出次密鑰配置法則，利用次密鑰加權衡量及參與者的重要性等觀念，可獲得密鑰恢復或然率最佳解之逼近值，由模擬結果得到其平均絕對誤差小於 0.01。最後，將此計畫所發展的模型計算、秘密分享方法與密碼技術提供給系統開發與網路管理人員，使其能夠應用在實際的網路系統，作為提高系統效率與系統安全性能之參考。

關鍵字詞：網際網路；秘密分享；或然率；網路安全；密碼技術

Abstract

Information technologies have ushered in a new era for computer-related communications. Use of the Internet for

commercial applications and resource sharing has accelerated in recent years as well. Individuals can use the Internet to instantly access information from anywhere in the world. Owing to such developments, computer security has become a critical issue nowadays. Much research has been conducted on areas involving network security such as user authentication, data confidentiality, and data integrity. In some applications, a critical message can be divided into pieces and allocated at several different sites over the Internet for security access concern. To secure the applications and data transmission over the Internet, we examine the secret sharing schemes. A secret sharing scheme could be very helpful in the management of secret messages. In this project, we first attempt to present a novel probability model for reconstructing a secret in a computer environment. Algorithm to estimate the probability of secret sharing reconstruction is presented as well.

Next, we propose two secret sharing schemes called multiple assignment scheme and multiple secret sharing scheme for sharing a secret. These schemes provide generalized secret sharing which allow multiple threshold access structure for a shared secret and can realize predefined sharing policies. We also propose two assignment methods, called WSA (weighted share assignment) and RSHA (ranked share-holder assignment), for assigning shares on hosts in such a way that the probability to be able to reconstruct the secret becomes the highest with regards to failure in unreliable computer networks. From the simulation results, we can see that in almost each case the proposed algorithms find suboptimal solution efficiently.

Keywords: Internet; Secret Sharing; Probability; Security; Cryptology

二、緣由與目的

資訊技術的精進，將電腦通訊帶入一個新的紀元，它促使資訊的流通與存取更為快速與便捷，而資源共享、相互通連等特性，造成資訊網路的驚人成長。電腦網路的廣泛應用，縮短了人與人之間的距離，但相隨的也激起了人們的危機意識，那就是當使用者可以很方便的透過電腦網路，隨時隨地挖取連接在網路上之其他電腦資訊時，儲存在本身電腦的機密資料會受到什麼樣的威脅且該如何的保護？尤其是當一些重要的機密資料在電腦網路上傳輸時，該如何的處理才不會讓這些資料輕易曝光，而讓資料擁有者免於蒙受重大的損失。安全保護有許多不同的研究主題，包括: **實體備份**(Backup)**、存取控制**(Access

Control)、認證措施(Authentication)、架設防火牆(Firewall)，對資料的加密機制(Encryption Mechanisms)、數位簽章(Digital Signature)及密鑰管理(Key Management)等。這些研究主題對網路系統與資訊安全都很重要。本研究計畫主要是針對網際網路中秘密分享的應用與資訊的安全性做探討。

由於資源共享、相互通連等特性，資訊網路的驚人成長使得網路彼此相連已成為未來發展的重要趨勢，但也潛在著安全威脅等問題；如何提升資訊網路的可靠性與安全性是一重要課題，尤其在現代軍事運用上更是成敗的關鍵。網際網路將各區域的網路互相連接在一起，是最大也是成長最快速的全球性電腦網路；而資訊技術的蓬勃發展，促使資訊之流通與存取更為快速與便捷。自從 1990 年網際網路開放商業服務, 以及 1994 年全球資訊網（World Wide Web, WWW）在個人電腦視窗用戶端瀏覽器（如 Netscape 及 Explorer）的成熟後，使得網際網路的使用者呈倍數成長；網際網路是一開放性的計算機架構，經由網際網路的廣泛應用，縮短了人與人之間的距離，淡化了國與國之間的界限。對於此一發展趨勢，資訊高速公路的時代即將來臨，資訊保密與網際網路的安全性愈來愈受各界的重視。在某些管理系統與應用中，為了安全因素考量，我們將一重要的主密鑰分割成多份不同的次密鑰，交給多位參與者保管或存放在不同的網站上；要恢復此一重要的密鑰，我們需將多份次密鑰聚集以導出主密鑰。在網際網路的環境下，我們提出新的模型計算來評估密鑰恢復之或然率，並分析次密鑰配置方式；同時探討秘密分享方法以實現任意的分享策略，配合資料加密技術，以提供系統設計與管理人員，作為規劃出有效率且不失安全性密鑰管理系統之參考。

本計畫的目的是希望對網際網路上秘密分享的策略與應用，資料加密標準及網路安全方面提出一完整的研究與探討。首先對各種不同的秘密分享方法做一專研，分析找出不同的次密鑰配置方式；接著再對網路系統做風險分析和瞭解安全裝置如何工作及如何被實行，以決定計算機系統與網路系統的安全功能及如何適度的改善系統的安全措施。我們在不可靠的網路建構模型計算，利用單一配置與多重配置混合，加上次密鑰權衡方式提出較佳的次密鑰配置方式，並分析問題計算的複雜度。最後，希望能夠將我們所提出的模型計算應用在實際的網路系統中，並且提供系統規劃與網路管理人員，建構安全的系統裝置並設計出有效率且不失安全性的密鑰管理系統，因而能夠降低因網站或通信網路線路被入侵時所造成的損失，及無法即時恢復密鑰以獲得重要資料之風險。

三、研究方法

我們探討各種秘密分享方法及分散

式計算機系統可靠度之研究文獻，並且加以分析歸納。由於現有之秘密分享方法，無法實現任意的分享策略，所以必須尋求其他解決之道。除了前述利用單向赫序(Hash)函數及分割藏寶圖的觀念來建構秘密分享方法外，我們亦考慮到利用單一次秘密配置、多重次秘密配置及次秘密的複製的混合使用方式來實現任意的秘密分享機能。

所謂單一次秘密配置是指每位參與者只擁有一個次秘密，而多重次秘密配置是指按照參與者重要性的不同給予不同數目的次秘密，如此可實現階層式授權的秘密分享策略。

同時，為確保重要資料在儲存、傳輸及使用上的安全性，我們探討在開放式網路系統的秘密分享方式。那就是，將一重要的秘密分割成多份次秘密並將其存放在不同的網路站台，要恢復此一重要秘密，我們需將多份次秘密取回以導出主秘密。在不可靠網路環境，我們構思建立新的模型計算及演算法來評估秘密恢復之或然率。

當我們在建立模型計算時，考慮到由各個站台取回所需之次秘密以導出主秘密的或然率。如何將次秘密配置到不同站台，才能使得秘密恢復之或然率最佳化，是我們所重視的。我們構思利用優先搜尋將圖形網路系統轉化為樹狀結構，並提出加權衡量等觀念將次秘密(包括單一及多重次秘密)依其重要性給予不同的權數；然後將較重要之次秘密依序配置到由優先搜尋所得之網路樹狀結構。我們期望獲得秘密恢復或然率之最佳解，或近似的答案並且是在容許的誤差範圍之內。

最後，將以上的研究結果整合成一完整之計算機網路系統之或然率分析工具，再利用這套或然率的分析工具，以不同的網路結構與配置方式來進行測試，以評估其性能與實用性。

四、成果及結論

首先，在開放式的電腦網路環境中，我們提出機率模型來評估密鑰恢復的或然率，我們考慮站台與通訊連線是 Imperfect 的情形及應用環境參數的不同，設計出適用於秘密或然率的計算分析之演算法，以用來計算在不可靠的網路系統中密鑰恢復之或然率。

其次，針對開放式網路系統易遭受有意者的入侵，及一些不可預知的因素常造成通信網路的中斷，同時考慮到次秘密配置、傳輸、恢復等因素，我們探討網路秘密分享方式，以確保機密資料儲存與傳輸的安全性。對階層式授權及團體導向的密鑰分享策略應用，提出兩個密鑰分享方法，稱為複式分配法和複式密鑰分享方法，是廣義的密鑰分享方式，不受限於一個固定的門檻值且可實現預定的分享策略。

不同的次秘密配置方式，系統會得不同的恢復或然率。次秘密配置問題是指找出一配置方式，將次秘密分配到不同的網站，使得在要恢復此秘密時，經

由各站台取回次秘密並導出主秘密的或然率能最大化。我們提出啟發式秘密配置法則(Heuristic Share Assignment)**，可快速獲得最佳解之逼近值；同時，配合上述密鑰分享方法，我們提出次密鑰配置法則，利用次密鑰加權衡量及參與者的重要性等觀念，提出**(WSA, weighted share assignment) **與** (RSHA, ranked share-holder assignment)**兩種次密鑰配置法則，可獲得密鑰恢復或然率最佳解之逼近值，由模擬結果得到其平均絕對誤差小於** 0.01**。最後，將此計畫所發展的模型計算、秘密分享方法與次密鑰配置法則，整合成一完整的計算機通信網路之或然率分析工具，利用此或然率分析工具來設計一高或然率之電腦網路秘密分享的應用，以降低因網站或通信線路故障所造成無法恢復秘密之風險。**

五、參考文獻

[1] G. R. Blakley, "Safeguarding Cryptographic Keys," Proceedings AFIPS 1979 National Computer Conference, vol. 48, June 1979, pp. 313-317.

[2] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, 1979, pp. 612-613.

[3] E. D. Karnin, J. W. Greene and M. E. Hellman, "On Secret Sharing Systems," IEEE Trans. on Information Theory, vol. IT-29, no. 1, Jan. 1983, pp. 35-41.

[4] G. J. Simmons, "Geometric Shared Secret and/or Shared Control Schemes," Advances in Cryptology - CRYPTO '90, Springer-Verlag, 1991, pp. 216-241.

[5] D. R. Stinson, "An Explication of Secret Sharing Schemes," Design, Codes and Cryptography, vol. 2, 1992, pp. 357-390.

[6] G. J. Simmons, An Introduction to Shared Secret and/or Shared Control Schemes and their Application, Contemporary Cryptology, IEEE Press, New York, 1991, pp. 441-497.

[7] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons, Inc., 1996.

[8] S. C. Kothari, "Generalized Linear Threshold Scheme," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 231-241.

[9] H. M. Sun and S. P. Shieh, "On Dynamic Threshold Schemes," Information Processing Letters, 52, 1994, pp. 201-206.

[10] T. C. Wu and W. H. He "A Geometric Approach for Sharing Secrets," Computer & Security, vol. 14, 1995, pp. 135-145.

[11] M. Ito, A. Saito and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," Proc. IEEE Globecom'87, Tokyo, 1987, pp. 99-102.

[12] K. Koyama, "Cryptographic Key Sharing Methods for Multi-groups

and Security Analysis," Trans. IECE Japan, E66, vol. 1, 1983, pp. 13-20.

[13] J. Benaloh and J. Leichter, "Generalized Secret Sharing and Monotone Functions," Advances in Cryptology - CRYPTO '88, vol. 403, Springer-Verlag, 1989, pp. 27-35.

[14] C. C. Chang and H. M. Tsai, "A Generalized Secret Sharing Scheme," J. Systems Software, vol. 36, 1997, pp. 267-272.

[15] V. K. Prasanna Kumar, S. Hariri, and C. S. Raghavendra, " Distributed Program Reliability Analysis," IEEE Trans. Software Eng., vol. SE-12, Jan. 1986, pp. 42-50.

[16] S. Hariri and C. S. Raghavendra, "SYREL: A Symbolic Reliability Algorithm Based on Path and Cutset Methods," IEEE Trans. Computers, vol. 36, Oct. 1987, pp. 1224-1232.

[17] D. J. Chen and T. H. Huang, "Reliability Analysis of Distributed Systems Based on a Fast Reliability Algorithm," IEEE Trans. on Parallel and Distributed Systems, vol. 3, no. 2, Mar. 1992, pp. 139-154.

[18] M. S. Lin and D. J. Chen, "New Reliability Evaluation Algorithms for Distributed Computing Systems," Journal of Info. Science and Eng. 8, 1992, pp. 353-391.

[19] A. Satyanarayana and M. K. Chang, "Network Reliability and the Factoring Theorem," Networks, vol. 13, 1983, pp. 107-120.

[20] O. R. Theologou and J. G. Carlier, "Factoring and Reductions for Network with Imperfect Vertices," IEEE Trans. on Reliability, vol. 40, June 1991, pp. 210-217.

[21] M. O. Ball, "The Complexity of network Reliability Computation," Network, vol. 10, Summer 1980, pp. 153-165.

[22] L. G. Valiant, "The Complexity of Enumeration and Reliability Problems," SIAM J. Computing, vol. 8, 1979, pp. 410-421.

[23] M. O. Ball, "Computational Complexity of Network Reliability Analysis: An Overview," IEEE Trans. on Reliability, vol. R-35, Aug. 1986, pp. 230-239.

[24] Ching-Yun Lee, Yi-Shiung Yeh, D. J. Chen and K. L Ku, "A Probability Model for Reconstructing Secret Sharing under the Internet Environment," Information Science, vol. 116, no. 2-4, June 1999, pp. 109-127.

[25] Ching-Yun Lee, Yi-Shiung Yeh, D. J. Chen and K. L Ku, "A Share Assignment Method to Method to Maximize the probability of Secret Sharing Reconstruction under the Internet," IEICE Trans. Inf.&Syst., vol. E83-D, no. 2, Feb. 2000, pp. 190-199.