行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　線上金鑰更新與其相關密碼系統研究　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：■個別型計畫　　□整合型計畫
計畫編號：NSC 89-2213-E-008-049
執行期間： 88年8月1日 至 89年7月31日

計畫主持人：顏嵩銘
共同主持人：

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位： 國立中央大學 資訊工程系

中 華 民 國 89年 10月 25日

行政院國家科學委員會專題研究計畫成果報告

線上金鑰更新與其相關密碼系統研究
On-line Key Renew and Its Related Cryptographic Study

計畫編號：NSC89-2213-E-008-049
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日

主持人：顏嵩銘　國立中央大學 資訊工程系
e-mail address:　yensm@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/

一、中文摘要

自從人們開始大量採用電腦系統進行各項資料處理並透過網路來傳送經過處理之重要訊息，網路安全與密碼學成為極重要之研究課題，不論在學術界或產業界，不論在理論層次或實用觀點都得到極大之重視並進行全面之研究。透過過去近二十年來研發所得之各項資訊安全與保密系統，人們逐漸可以保障其經由網路傳送資料之安全性、完整性及隱私性，並有愈來愈多之實用系統呈現在人們眼前，以上之發展為人們帶來諸多生活上之方便乃至於生活型態之改變。

為使每項資訊安全系統得以安全而正確之運作，每項系統皆需配合一個唯一之密碼(或稱金鑰)以進行資料加密、數位簽章或身份驗證等目的。然而基於某些安全需求之原因或系統設計架構之理由，某些金鑰必須定期予以更新，這將造成某些程度之不變。以往之系統為求安全起見均要求使用者回到遠端伺服者之地點，以離線面對面之方式進行金鑰更新。在本計畫中我們針對此日趨重要之研究課題進行全面性研究，提出可行且極具效率之方案，同時研究與此主題相關之基礎密碼系統。

事實上，線上金鑰更新之研究在國際上仍為一新興之研究主題，然其重要性就如同金鑰管理(key management)一樣不可或缺。本計畫的目標是針對此新穎且極具實用價值之主題邁進一步，徹底研究其特性與相關密碼系統並提出具體之解決方案。

關鍵詞：網路安全、資訊安全、密碼學、金鑰更新、線上協定、身份驗證、單次密碼

Abstract

In the secret key or called symmetric key cryptographic systems, private relationship binding between any two parties is achieved via holding the knowledge of a shared common secret information, i.e., the key, under a related cryptographic construction. The symmetric key systems have the main advantages of easy implementation and good performance, while suffer from the intrinsic disadvantages of inconvenient key distribution and key management. The above two requirements can be achieved more easily using the counter technology named the public key cryptography subject to that a trustworthy public key certification service can be accessed easily. X.509, the directory authentication framework, is one of the most popular public key certification protocols using public key digital signature scheme as the fundamental.

Conventionally, in the symmetric key

systems, each time to achieve the common key sharing or the key renewing owing to possible disclosure of the present shared key or after a long time of using the present shared key requires both the parties to negotiate the new common key through a secure channel of any form or to meet each other face to face. Both the above two approaches make the key distribution problem be inflexible or even be impossible because there is no more shared common secret information between the two parties to form a secure channel.

Basically, the following three approaches can be used to negotiate a new common secret key between both parties A and B: (1) face-to-face physical authentication and key exchange; (2) key exchange via the help of a trustworthy carrier or server; (3) on-line key renewal process initiated by one party, say A. It is obvious that the first approach is the most secure but the least convenient design. On the contrary, the third approach (when not under well developed protection) is the least secure but the most convenient way. In this research, a new model called the authenticated on-line key renewal process is proposed and studied which is not only convenient but also secure. Protocols developed under this model can be used to overcome the difficulty of common key re-distribution problem in the symmetric key systems. Finally, practical applications of the proposed model on two famous systems, the Kerberos authentication system and the S/KEY one-time password system, are introduced in this project.

The topic is not only new but also practical. In this project, we also considered some related problem about key renewing.

Keywords: Network security, Information security, Cryptography, Key renewing, On-line protocol, Identification, One-time password.

二、緣由與目的

如何於廣域之開放式計算機網路下進行使用者身份確認幾乎可說是計算機網路安全的第一道防線，也可說是所有資訊系統必備的安全元件。在網路大幅朝向廣域化與開放化之際，如何使得客戶端（client）可向遠方的服務伺服器（server）證明自己的身份及合法使用權，而不會於驗證過程中使得自己的秘密洩露出來成為首要之務。在達成上述目的之過程中，幾乎大部份之系統均假設於客戶端及伺服器端存有一共享之秘密金鑰。

不論是何種安全機制，金鑰管理皆是最基本而且也是最重要的一項工作。金鑰的安全程度會隨著時間的增長而逐漸遞減。即使是再安全的金鑰，也會隨著系統使用的次數漸增相對的於網路上傳輸之資訊量亦漸增，總會有被猜出來的一天。因此，我們必須根據所使用系統(或其相對之金鑰)的安全程度，來訂定合理的金鑰生命週期。當金鑰的生命週期將屆之時，我們必須更換舊的金鑰，以確保通訊的安全性，此即所謂之金鑰更新。

本研究計畫形成之緣由與目的如前摘要所述乃為針對此一新穎且極具實用價值之主題邁進一步，徹底研究其特性與相關密碼系統並提出具體之解決方案。

三、結果與討論

理論上而言，金鑰更新的方法一般可歸類為下列三種情形：

(1)親自前往更新 --- 由使用者本人親自到伺服器端申請一把新的金鑰。這是最安全，卻也是最不方便的一種做法。如果是在金鑰外洩的情況下，若不能即時抽空前往更換舊的金鑰，安全機制將一直地癱瘓下去。

(2)委託快遞公司 --- 新的金鑰經由快遞服務業者的協助，達到金鑰更新的目的。但是，我們很難保証說，新的金鑰在送至伺服器端的途中，是否被偷窺或

是遭到篡改，也就是面臨了傳遞者可信賴度的問題。

(3)線上更新 --- 在線上直接更換新的金鑰，有著快速且便利的特性。這是最為大家普遍接受的一種方式，但卻也是最不安全的一種做法。因為在舊金鑰外洩的情形下，根本不可能做到線上身份的驗証。例如Unix作業系統所提供之passwd指令即是提供使者進行線上金鑰更新，然其系統安全性卻蕩然無存。

事實上，線上金鑰更新之研究在國際上仍為一新興之研究主題，遍尋各項公開文獻，可發現之文章極其有限。Hauser, Janson,及 Tsudik 三人於 1996 年所發表之著作[3]曾討論與此相關之主題，然其系統假設需有一可信賴之第三者存(如 Kerberos 系統模式[4])在且只適用於區域性網路中。Yen 及 Liu[1,2]也於 1996 年發展出另一項適合用於線上金鑰更新之技術，然使用者需隨時針對每個伺服器端記憶兩個金鑰，增加了使用者之負擔。

上述兩項系統之設計均使用到加密器(encryptor)例如 DES [9]，這對某些應用環境而言或將造成不便，因為某些國家至今仍未承認使用加密器之合法性。為了能設計出具一般性可適用於任何資訊安全系統進行線上金鑰更新之需求，於金鑰更新協定中免除加密器之使用是必要之條件，此為本計畫所將設計之系統強調重點之一。

Wu 及 Sung 二人也曾於 1996 年發表一項相關於可在線上更換密碼之系統[5]，然其方法只能適用於極為特殊之系統中，例如類似 Lamport[6]與 S/Key[7]之單次密碼系統(one-time password)。同時，此系統之效能有待改善，且其安全性與系統運作正確性亦有待商榷。

如同前述，線上金鑰更新之研究在國際上仍為一新興之研究主題，然其重要性就如同金鑰管理(key management)一樣不可或缺。舉一典型之應用實例，於單次密碼系統之使用中，使用者得經常回到遠端電腦伺服器處更新其密碼以便能夠繼續進行遠端身份認證，安全而具效率之線上金鑰更新協定將為此帶來極大之幫助。

由於計畫主持人於計畫執行前已進行相當程度之規劃與探討，且於計畫執行過程中針對進度予以適宜之控制，本計畫如期完成以下之研究主題。

(一) 設計出具一般性可適用於任何資訊安全系統進行線上金鑰更新需求之系統，於此類金鑰更新協定中免除加密器之使用，而僅採用如 one-way hash 函數及基於公開金鑰之驗證協定。我們設計出兩類線上金鑰更新協定，其中一種可適用於更新"*亂數型式*"(註:此亂數一般均假設不是由使用者隨意選擇)之密碼，另一種系統則可適用於更新"*使用者隨意選擇型式*"之密碼。此二型式之系統皆有其適用對象。

(二) 研究應用上述基本型式線上金鑰更新協定於單次密碼(one-time password)系統，於此系統中使用者不必經常回到遠端電腦伺服器處更新其密碼以便能夠繼續進行遠端身份認證。

(三) 針對簡單而具效率之 Schnorr 驗證協定，進行改良型 Schnorr 驗證協定之設計及研究，初步完成 Two-step Schnorr 驗證協定之研究。目前一般均以為 two-step Schnorr 驗證協定無法達到安全之需求，但於本研究中我們證明基於 Schnorr 系統之安全 two-step 驗證協定存在。進而嘗試設計基於 Schnorr 系統之 three-step mutual authentication 協定設計與研究，並利用此改良型 Schnorr 驗證協定所提供之可驗證性，加上其他設計技巧所將提供之安性而設計出安全且具效率之線上金鑰更新協定。

(四) 針對其他與線上金鑰更新相關之系統研究：

4.1 針對 Yen-Liu 之基於私密金鑰密碼系統的線上金鑰更新協定[1,2]分析。

4.2 針對 Wu-Sung 之可更新單次密碼協

定[5]進行相關分析，指出此系統之效能有待改善，並且發現其安全性之缺失，及可能之改善措施。

四、計畫成果自評

綜觀以上 *計畫緣由與目的* 及 *結果與討論* 可以清楚地看出本研究計畫確實有其價值。

整體而言，本研究計畫在進度控制、研究內容、預期達成目標各方面均與原計畫相符。研究成果之內容已完成數篇技術報告，一部分並發表於該領域相關之學術會議，列舉如下。

五、參考文獻

[1] S.M. Yen, R.L. Oyan, and Y.Y. Lee, "Improved Private Information Download Protocol," Proc. of the 2000 International Computer Symposium, Workshop on Cryptography and Information Security, December 6-8 2000 (to appear).

[2] S.M. Yen and M.T. Liu, "Cryptographically Strong On-Line Key Renewal Protocol," Proc. of the 9th National Conference on Information Security, May 1999.

[3] Sung-Ming Yen and Ray-Lin Oyan, Remarks on the SRP Password-based Key Exchange Protocol. LCIS Tech. Report TR-99-12, National Central University, October 1999.

[4] Sung-Ming Yen and Meng-Tzung Liu, Communication Optimized Variations of Schnorr Authentication Protocol (under developed). LCIS Tech. Report TR-99-9, National Central University, September 1999.

[5] 顏嵩銘, "免用加密器之線上金鑰更新系統", 已向國科會提出中華民國專利申請(同意申請).

[1] S.M. Yen and M.T. Liu, "Cryptographically strong on-line key renewal protocol", Technical Research Report, 1996.

[2] M.T. Liu, "A study on weak key protectable authenticated key exchange protocols", MS thesis, Da-Yeh University, Dept. of Electrical Eng., 1996.

[3] R. Hauser, P. Janson, and G. Tsudik, "Robust and secure password and key change method", Journal of Computer Security, Vol.4, No.1, pp.97-111, 1996.

[4] J.G. Steiner, B.C. Neuman, and J.I. Schiller, "Kerberos: An authentication service for open network systems", Usenix Conference Proceedings, Dallas, Texas, pp.191-202, February 1988.

[5] T.C. Wu and H.S. Sung, "Authenticating passwords over an insecure channel", Computers & Security, Vol.15, No.5, pp.431-439, 1996.

[6] L. Lamport, "Password authentication with insecure communication", Commun. of ACM, Vol.24, No.11, pp.770-772, 1981.

[7] N.M. Haller, "The S/KEY one-time password system", Proceedings of the ISOC Symposium on Network and Distributed System Security, San Diego, CA, Feb. 1994.

[8] C.P. Schnorr, "Efficient signature generation for smart cards", Journal of Cryptology, Vol.4, No.3, pp.161-174, 1991.

[9] NBS FIPS PUB 46, "Data Encryption Standard", National Bureau of Standard, U.S. Department of Commerce, Jan. 1977.

[10] R. Rivest, "The MD5 message digest algorithm", RFC 1321, Apr. 1992.

[11] FIPS 180-1, "Secure Hash Standard", NIST, US Department of Commerce, Washington D.C., April 1995.