行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 在沒有公信第三者的動態群體中 ※
※ 產生群體共用秘密金匙技術之研究 ※
※ ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號：NSC　90-2213-E-032-017

執行期間：九十年八月一日至九十一年七月卅一日

計畫主持人：黃仁俊

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：淡江大學資訊工程學系

中　華　民　國　九十一年 八月　二十日

行政院國家科學委員會專題研究計畫成果報告

在沒有公信第三者的動態群體中產生群體共用秘密金匙技術之研究

The Study of Key Agreement in Dynamic Groups without Trusted Third Party

計畫編號：NSC 90-2213-E-032-017
執行期限：九十年八月一日至九十一年七月卅一日
主持人：黃仁俊 淡江大學資訊工程學系

一、中文摘要

資訊安全技術在數位網路之新世紀中是一項非常重要的技術，它是數位網路世界安全之憑藉與基石。在資訊安全技術中，常常使用金匙（Secret key）來做為管制的憑藉，因此金匙如何產生和傳遞是資訊安全技術非常重要的主題，這也使得國內外許多專家學者均致力於所謂金匙分配（key distribution）、金匙交換（key exchange）、金匙一致性（key agreement）和會議金匙（conference key）等與金匙傳遞和產生有關的研究工作。在今日網路技術與應用已蓬勃發展且已非常普及的時代，網路的通訊方式已由早期一對一的兩點通聯模式，提昇為群體的多點通訊或廣播模式，然而群體的通聯方式所面臨的相關技術絕非單純的將兩點通聯模式擴充即可，尤其以資訊安全技術來看，其整體系統要安全考量的因素更為複雜，故本計畫研究一新技術來解決資訊安全技術中，產生和傳遞一群體共用秘密金匙的問題，我們所發展之技術有別於先前許多學者利用公信第三者或金匙分配中心產生群體共用秘密金匙，再傳遞給所有成員之做法；本計畫發展的技術不需公信的第三者存在，藉以提高系統的安全行及可行性；在所發展的技術中，群體中每位成員權利義務都相等，他們的共用秘密金匙是群體成員必需全部一起合作才能產生，而為提高我們所發展之技術的應用層面，我們也進一步考慮研發的技術必須容許群體成員可以彈性地動態增加或減少，使縱然經過動態變化之新群體，在不必重置的條件下很快地產生新群體共用秘密金匙，繼續維護群體通訊之秘密與安全。另外，為增強安全性，我們的技術可以使同一群體在不同次的群體通訊產生不同的共用秘密金匙。綜合而論，相信本計畫所發展的技術，對於目前網路的群體通訊和廣播應用模式之安全有所貢獻與助益，對於維繫 e 時代數位網路機制之安全有正面幫助與提昇。

關鍵詞：資訊安全、電腦密碼學、群體共用秘密金匙、群體通訊

Abstract

The technologies of information security are very important in the Digital Network Age. The secret key is an important component of many information security technologies. “How to establish and distribute the secret key?” is a significant research topic. There are many scientists focus on the research of key distribution、key exchange、key agreement and conference key. The communication model of network upgrades to group communication by the rapid progress of network technology. While peer-to-peer security is a mature and well-developed field, secure group communication remains relatively unexplored. The secure group communication is not a simple extension of secure two-party communication. It is more complexity. This project devises a new technology to establish a group secret key for the dynamic group communication. There are three significant differences between the technology that we want to devise and the previous results of the other researchers. First, the new technology does not need the assistance of the trusted third party. Second, the member of the group can add or leave dynamically. Third, the group secret key can be altered easily in different cooperation of the same group.

The technology that the project devised will advance the security of group communication and multicasting. It is helpful to advance the security of the network environment.

Keywords ： Information Security 、 Cryptography 、 Key agreement 、 Group communication

二、緣由與目的

With fast growth of the Internet and the shift of communication services to the network, group communication becomes increasingly important. Modern group-oriented applications include IP-telephony, video-conferencing and collaborative workspaces etc… Simultaneously, security and privacy become necessary. The security requirement of these applications can be addressed by building upon a secret key.

Group key agreement means that several parties want to create a common secret to be used in exchanging information covertly. For example, a group of people that is coming together in a closed meeting and wants to from a private wireless network with their laptop computers for duration of the ad hoc meeting. They want to share information security so that no one outside of the room can eavesdrop during their communication.

Ad hoc networks are dynamic, peer-to-peer network with little or no supporting infrastructure. The members of ad hoc networks may be PDA, mobile phone or notebook and so forth. These equipments are hardware-limited lack of storage devices and due to the security problems caused by ad hoc networks, we consider a small group in a closed meeting. Members in this group know each other but can not digitally identifying and authenticating each another. Group members cannot provide or access third party key management service. They need a group shared key establishment protocol to construct a secure communication channel.

In general group key management protocols come in two different flavors: contributory key agreement protocols for small groups and centralized, server-based key distribution protocols for large groups. Becker and Wille [5] analyze the minimal communication complexity of group key distribution protocol and propose two protocols: *hypercube* and *octopus*. They proposed a method using Diffie-Hellman Key exchange protocol to construct a common group key. This protocol handles join and merge operations efficiently, but it is inefficient when the group member leave. Becker and Wille [5] proposed the *hypercube* protocol for the number of group member is just equal to the exponents of 2; otherwise, the efficiency to decrease. Steiner et al. [2] address dynamic membership issues of group key agreement based on the two-party Diffie-Hellman Key exchange [12]. The method named Group Diffie Hellman (GDH) protocols. GDH provides contributory authenticated key agreement and key independence. It requires one broadcast message at the end of each protocol run. The GDH protocol should be implemented on linear chain network topology where the last node has broadcast capabilities. The scheme uses a group controller and need n protocol rounds to establish a common key in a group of n members.

In this project, we develop a key agreement protocol based on XOR operation [14]. The group members share a conference password. Each group member contributes its share to derive a common session key in a general ad hoc network environment without making additional assumptions about the availability of any support infrastructure. By the proposed method, the member generate group shared key more efficient then the previous methods.

三、結果與討論

This section introduces our key agreement protocol. Subsection 3.1 describes a key tree structure that we

construct based on the member numbers. The proposed protocol based this tree structure will be introduced in Subsection 3.2. Subsection 3.3 discusses the cases when some members joint or leave the conference.

3.1 The key tree of the key agreement protocol

We assume that there are n members, M_1, M_2,…,M_n, want to hold a closed conference base on ad hoc network without network infrastructure. Each member of this group keeps a unique number over [1, n]. These members cooperate based on a *complete binary tree*. We assign the member M_n be "Checker". The checker is just a group member, but with an additional role to confirm the session key correctness. The member M_{n-1} is named "Candidate", who arranges replacement of member number after the member leave the conference meeting.

3.2 Two phases of the proposed protocol

This subsection introduces our key agreement protocol based on XOR operation. In our scenario, there are n members sharing a password P. Our goal is that at the end of the protocol all members who know P will get a shared session key $K = S_1 \oplus S_2 \oplus \ldots \oplus S_n$, where S_i is contributed by M_i. M_i selects S_i randomly. The protocol is divided into two phases. In the first phases, M_1, M_2,…,M_{n-1} cooperate to construct a subkey $\pi = S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1}$ secretly. In the second phases, each M_i (i = 1, 2, …,n-1) engages in a separate exchange with M_n, all members have sufficient information to compute the session key K. He also verifies that the other members generated the same session key K. We introduce our method in detail as the following two phases:

Phase 1:

Each member M_i chooses a random quantity S_i, i is the node number that M_i located in the key tree. If the member M_i locates at leaf node (i.e. $2i > n$) of the key tree, he assigns his intermediate key K'_i as S_i. He sends intermediate key K'_i and verification message, F_i ($=f(P||K'_i)$, where $f(\bullet)$ is a public one-way hash function) to his parent node. The parent concatenates K'_i with P and generates a verification message F_i' by hash function $f(\bullet)$. If $F=F'$, the parent node authenticates the child note's identity and his S_i because they share the same P. The parent node records children's intermediate keys. If the member M_i locates at internal node (i.e. $2i \le n$), he authenticates the children nodes' identities and their intermediate keys (e. g. K'_{2i} and K'_{2i+1}) by using verification messages $F_{2i}(=f(P||K'_{2i})$ and $F_{2i+1}(=f(P||K'_{2i+1}))$ separately. The M_i randomly selects a number S_i and generates intermediate key $K'_i = S_i \oplus K'_{2i} \oplus K'_{2i+1}$, where "$\oplus$" denotes the XOR operation. He also generate the verification message $F_i(=f(P||K'_i))$. Furthermore, he sends the intermediate key and verification message to his parent node. If the member is the root node (i.e. i = 1), who has to collect his children nodes' intermediate keys and use his random number S_1 to compute the subkey π ($=K'_1=S_1 \oplus K'_2 \oplus K'_3$). Note that the members perform the previous simultaneously when they locate on the same level of the key tree.

Phase 2:

At the end of Phase 1, the member M_1 generates a subkey $\pi(= S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1})$. In Step1 of this phase, the member M_1 broadcasts subkey π to each member, except the member M_n. In Step2, each member M_i (i = 1,2,…,n-1) removes its contribution from π and inserts a randomly chosen blinding factor S_i'. The resulting quantity, C_i, is equal to $\pi \oplus S_i \oplus S_i'$. Each member M_i (i = 1,2,…,n-1) sends C_i and the verification message $f(P||C_i)$ to member M_n. M_n verifies the message sent by each member. In Step3, M_n computes and sends $E_{P \oplus C_i}(C_i \oplus S_n)$ to each member M_i. He encrypted the message $C_i \oplus S_n$ by using the symmetric encryption function with key $P \oplus C_i$. The legal member decrypts the received messages to extract S_n. A this point, M_i (i = 1,2,…,n-1) unbinds the

quantity received from M_n and constructs a session key $K_i = \pi \oplus S_n$. In Step4, each member M_i (for i=1, 2, …, n-1) sends the key confirmation message of K_i as $E_{P \oplus S_n}(K_i)$ to member M_n, where $E_{P \oplus S_n}(K_i)$ denotes encrypting K_i with a symmetric encryption function and key $P \oplus S_n$. In Step5, the member M_n verifies that each member generated the same session key $K(=K_1=K_2=\ldots=K_{n-1})$. M_n notifies all members the conference that the session key is established successfully.

3.3 Membership events

In our scenario, the conference members are not always fixed. Some times there are new members joint the conference, after the session key is generated. This new member does not authorize to know the messages of this conference before he joins this conference. The conference should change their session key and the shared password. Some times there are some members leave. They do not authorize to get the messages after they leave. This conference should change the session key and the shared password, too.

四、計畫成果自評

This project devises a new protocol for password-based key agreement in ad hoc networks. The environment does not provide additional infrastructure and physically secures communication channels. In our protocol, the legal conference member use password to authenticate participants and lower computing operations for the session key generation. In addition, this protocol supports dynamic conference member events. The proposed protocol is more efficient than the others. Table 1 shows the comparisons among GDH.2 [2], hypercube [5], octopus protocols [5] and our protocols. It is clear that our protocol is more efficient than the others. Thus, this result achieves the subject of this project. It is success. This result is submitted to the 2002 International Computer Symposium.

Table 1: Protocols comparison

Items \ Methods	GDH.2	Hypercube	Octopus	Our method
The number of messages send via the communication	n	$n\log_2 n$	$3n$-4	n
DH-Key Exchanges	n	$\frac{n\log_2 n}{2}$	$2n$-4	0
Simple Rounds	n	$\log_2 n$	$2\left\lceil \frac{n-4}{4} \right\rceil + 2$	$\log_2 n$+1
Broadcast	Yes	No	No	Yes

五、參考文獻

[1] N. Asokan and Philip Ginzboorg. “Key-agreement in ad hoc networks”, *Computer Communications,* Vol. 23, No. 17, Nov. 2000, pp. 1627-1637.

[2] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. “Authenticated group key agreement and friends”, In *Proc. 5th ACM Conference on Computer and Communications Security*, Nov. 1998, pp. 17-26.

[3] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. “New multiparty authentication services and key agreement protocols”, *IEEE Journal on Selected Areas in Communications*, Vol. 8, No. 4, Apr. 2001, pp. 628-640.

[4] Giuseppe Ateniese and Gene Tsudik. “Some open issues and new directions in group signatures”, In *Proc. 3rd International Conference on Financial Cryptography (FC’99)*, Vol. 1648 of *LNCS*, Feb. 1999, pp. 196-211.

[5] Klaus Becker and Uta Wille. “Communication complexity of group key distribution”, In Proc. *5th ACM Conference on Computer and Communications Security*, Nov. 1998, pp. 1-6.

[6] M. Bellare, D. Pointcheval and P. Rogaway, “Authenticated key exchange secure against dictionary attack”, *Proceeding of Advances in Cryptology – Eurocypt 2000*, pp. 139-155.

[7] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attack", *IEEE Symposium on Research in Security and Privacy*, 1992, pp. 72-84.

[8] S. Bellovin and M. Merritt, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-life compromise", *ACM Conference on Computer and Communications Security*, 1993, pp. 244-250.

[9] M. Boyarsky, "Public-key cryptography and password protocols: the multi-user case", *ACM Conference on Computer and Communications Security*, Sep.1999, pp. 63-72.

[10] V. Boyko, P. Mackenzie and S. Patel, "Provably secure password authenticated key exchange using Diffie-Hellman", *Proceedings of Advances in Cryptology-Eurocrypt 2000*, 1998, pp. 156-171.

[11] Mike Burmester and Yvo Desmedt. "A secure and efficient conference key distribution system", In *Advances in Cryptology - EUROCRYPT '94*, Vol. 950 of *LNCS*, May 1994, pp. 275-286.

[12] W. Diffie, and M.E. Hellman, "New directions in cryptography", *IEEE Trans. On Information Theory*, Vol. IT-22, No.6, 1976, pp. 644-654.

[13] D. Jablon, "Extended password key exchange protocols", *WETICE Workshop on Enterprise Security*, 1997.

[14] Sahar M. Ghanem, Hussein Abdel-Wahab, "A simple XOR-based technique for distributing group key in secure multicasting", In Proc. *The Fifth IEEE Symposium on Computers and Communications*, pp. 166-171, 2000.

[15] Ingemar Ingemarsson, Donald T. Tang, and C. K. Wong. "A conference key distribution system", *IEEE Transactions on Information Theory*, Vol. IT-28, No. 5, Sep. 1982, pp. 714-720.

[16] Y. Kim, A. Perrig, and G. Tsudik. "Simple and fault-tolerant key agreement for dynamic collaborative group", In *7th ACM conference on Computer and communications*, Nov. 2000, pp. 235-244.

[17] Silja Mäki, Maarit Hietalahti, and Tuomas Aura. "A survey of ad-hoc network security", Interim report of project 007- security of mobile agents and ad-hoc societies, *Helsinki University of Technology, Laboratory for Theoretical Computer Science*, Sep. 2000.

[18] Michael Steiner, Gene Tsudik, and Michael Waidner. "Diffie-Hellman key distribution extended to group communication", In *3rd ACM Conference on Computer and Communications Security*, Mar. 1996, pp. 31-37.

[19] Michael Steiner, Gene Tsudik, and Michael Waidner. "CLIQUES: a new approach to group key agreement", In *Proc. 18th International Conference on Distributed Computing Systems (ICDCS'98)*, May 1998, pp. 380-387.

[20] Michael Steiner, Gene Tsudik, and Michael Waidner. "Key agreement in dynamic peer groups", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 11, No. 8, Aug. 2000, pp. 769-780.