代理匿名機制達到訊息請求之可追溯性

莊梅櫻　　**蔡敦仁**
中國文化大學資訊管理研究所　**中國文化大學資訊科學系**
Mychung0112@yahoo.com.tw　**drtt@mail.pccu.edu.tw**

摘要

資訊系統發達中，一個使用者常會擁有相關資訊，並且於存放各個不同的單位機構或儲存在不同資料庫之中；有些單位機構或資料庫是屬於獨立性且資訊互不相通的，這可造成了資料無法整合使用，例如：個人資訊可能會存放於醫療機構、金融體系…等等系統中，在資訊的傳送中，有些訊息是需要被保護且不被其第三單位知道，但當有任何司法糾紛時，又可透過其機制達到訊息的鑑別性其真確性。本論提出一個有別於 Kerberos 機制的代理匿名授權的新機制，來解決單一的使用者在不同機構的分散資料，透過此新的機制架構，讓使用者的資料能透過獨立且不相關的伺服器共享彼此交換，而代理匿名使用者所提出的訊息，達到資料的可追溯性。

關鍵詞：票證(Ticket)、鑑別性(Authentication)、機密性(Confidentiality)、完整性(Integrity)、匿名(Anonymity)、可追溯性(Traceability)、Kerberos、盲簽章(Blind Signature)

1. 前言

在資訊科技發達的社會中，每個人身邊都充滿了一堆的帳號與密碼，不論是金融卡、門禁管理系統或資訊系統，一個人即擁有好幾組的帳號與密碼，這也造成了管理的問題，所以有學者提出了單一簽入(Single Sign-On，SSO)的鑑別(Authentication)機制，希望解決一個人必須要記得數組的帳號與密碼的不方便性。

但是除了上述的單一簽入的鑑別機制之外，尚有使用票證為基礎的機制[1,3]，來減少使用者多次存取同一系統服務必須重複輸入帳號與密碼的情況。不過在解決個人重複登入的不便性之外，另一更重要的事情，是在個人資訊散佈於獨立的不同機構的情形下，如何能透過有效電子化作業來完成資料的交換，達到個人及獨立單位的鑑別性(Authentication)、資料傳送中的機密性(Confidentiality)、資料本身的完整性(Integrity)、使用者的匿名性(Anonymity) [4,5,6]或變動識別碼(Dynamic ID-based)[8]來隱藏身份、以及對該資訊系統的存取控制權(Access Control)、和對事後糾紛產生時匿名使用者請求的可追溯性(Traceability)。本論文除了基於票證為基礎的鑑別機制外，另將使用者於票證伺服器的票證申請中，採用匿名方式進行，提出一個新的架構及方法，達成上述的各項安全需求，並達成票證伺服核發匿名票證。

2. 票證為基礎的鑑別機制

在傳統的使用者鑑別系統(Authentication System)，通常會以使用者的帳號及密碼來做簡單查證，例如 Unix 系統即是將使用者的查證表(Verification Table)儲存於系統之中，藉由使用者輸入的資訊再與系統中的查證表比對。為避免使用者的密碼以明文方式儲存，可經過某種的函數運算，例如安全單向的雜湊函數(Secure On-Way Hash Function)，再將經運算後的雜湊值儲存於查證表中。但是，對於複雜的環境中，一位使用者可能必須要使用數個設備或工作站，這將造成管理者對使用者管理上的不便，使用者更需要記得每一個工作站不同的帳號與密碼，倘若要更改密碼時，便要將全部資料都更改。因此有中央鑑別伺服器(Authentication Server)的概念產生，將所有的使用

者帳號與密碼全部儲存與此部鑑別伺服器，以達到一人一個帳號的單一簽入(Single Sign-On)目的。

票證為基礎的鑑別機制，主要目的在於分散系統之中，被鑑別的使用者或許在某些工作站上並未被授權使用，或是沒有個人的帳號與密碼儲存於該工作站時，可透過第三者票證核發單位(Ticket-Granting Server)事先與該工作站建議彼此信賴關係，以公正立場來核發授權票證，當該工作站收到此授權票證，並查證屬於該公正的第三者票證核發單位，即可接受使用者登入使用。

票證為基礎的存取服務亦可使用於無線通訊中的移動使用者[1,3]，當使用者從某一個基地台移動到另一個不屬該使用者的基地台，假設基地台間有事先建立的彼此信賴協定，使用者即可使用票證為基礎的鑑別機制來達到行動之間彼此授權，便於使用於彼此之間的帳務(Accounting)及費用拆帳比例問題的解決。

3. Kerberos 的簡介

Kerberos V4[7,9,10]的基本架構可參考圖 1，使用者鑑別及服務請求的流程可分為三個階段，第一階段為鑑別性服務的訊息交換，主要目的在於使用者向鑑別伺服器請求登入票證授權伺服器(TGS)的票證；第二階段為門票核准服務的訊息交換，主要目的在於取得服務授權的門票；第三階段為客戶端/伺服端互相確認的訊息交換階段，主要目的在於取得伺服器的服務，其各階段的訊息交換略述如下：

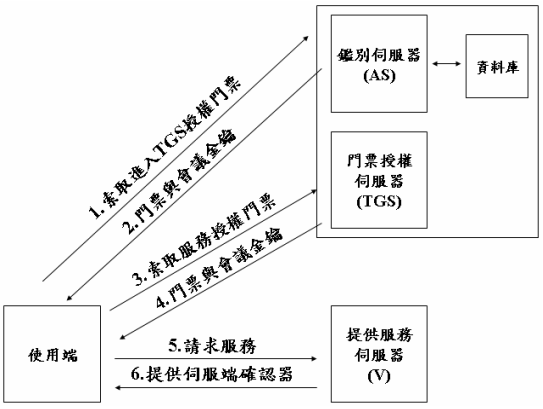

圖 1：Kerberos V4 的基本架構

鑑別性服務的訊息交換階

$C->AS$：$ID_C \| ID_{TGS} \| TS_1$

$AS->C$：

$E_{K(C)}[K_{C,TGS} \| ID_{TGS} \| TS_2 \| lifetime_2 \| Ticket_{TGS}]$

門票核准服務的訊息交換階段

$C->TGS$：$ID_V \| Ticket_{TGS} \| Authenticator3_C$

$TGS->C$：

$E_{K(C,TGS)}[K_{C,v} \| ID_V \| TS_4 \| Ticket_V]$

客戶端/伺服端互相確認的訊息交換階段

$C->V$：$Ticket_V \| Authenticator5_C$

$V->C$：$E_{K(C,V)}[TS_5+1]$

其中

$Ticket_{TGS} =$

$E_{K(TGS)}[K_{C,TGS} \| ID_C \| AD_C \| ID_{TGS} \| TS_2 \| lifetime_2]$

$Ticket_V =$

$E_{K(V)}[K_{C,V} \| ID_C \| AD_C \| ID_V \| TS_4 \| lifetime_4]$

$Authenticator3_C = E_{K(C,TGS)}[ID_C \| AD_C \| TS_3]$

$Authenticator5_C = E_{K(C,V)}[ID_C \| AD_C \| TS_5]$

在第一階段中，使用者傳送自己的識別碼 ID_C、票證授權伺服器識別碼 ID_{TGS} 及時戳 TS_1 給鑑別伺服器，鑑別伺服器則利用該使用者儲存於密

碼資料庫中的密碼產生票證授權伺服器與使用者之間共用的對稱金鑰 $E_{K(C)}$，及隨機產生使用者與票證授權伺服器 TGS 之間共用的會期金鑰 $K_{C,TGS}$，並利用 $E_{K(C)}$ 將 $K_{C,TGS}$ 及票證授權伺服器識別碼 ID_{TGS}、時戳 TS_2、生命週期 $lifetime_2$ 和進入 TGS 的票證 $Ticket_{TGS}$ 加密後送回給使用端。

在第二階段中，使用者端將欲連線的伺服器識別碼 ID_V 及從鑑別伺服器取得的票證 $Ticket_{TGS}$ 和鑑別子 $Authenticator3_C$ 傳送給 TGS，TGS 再利用使用者端和 TGS 共用的會期金鑰 $K_{(C,TGS)}$ 將 TGS 隨機產生的會期金鑰 $K_{C,V}$、伺服器 V 的識別碼 ID_V、時戳 TS_4 和進入伺服器 V 的授權票證 $Ticket_V$ 加密傳回給使用者端。

在第三階段中，使用者端將 TGS 傳回的 $Ticket_V$ 及鑑別子 $Authenticator5_C$ 傳送給伺服器 V 以請求提供服務授權，伺服器 V 則將時戳 TS_5 累計後，利用使用者端和伺服端共用的會期金鑰 $K(C,V)$ 將其加密後，回送給使用者端做為鑑別依據。

4. David Chaum 的盲簽章

David Chaum[2] 所提出的盲簽章(Blind Signature)是利用 RSA 演算法所導出，先選擇兩個很大的質數 p、q，計算 $n=p\times q$、$\phi(n)=(p-1)(q-1)$，找出 e 使得 $\gcd(\phi(n),e)=1$，再計算出 $d=e^{-1}\bmod\phi(n)$，其中的 (d,n) 為私鑰，(e,n) 為公鑰，整體計算流程如下

- 使用者：選定一訊息 m，再任選一亂數 R，計算 $C=R^e m \bmod n$，並送給簽署者。
- 簽署者：計算 $T' \equiv C^d \bmod n$，將 T' 送還給使用者。
- 使用者：計算 $T \equiv R^{-1}T' \bmod n$

$$\equiv R^{-1}(C^d \bmod n)\bmod n$$
$$\equiv R^{-1}(R^{ed}m^d \bmod n)\bmod n$$
$$\equiv R^{-1}Rm^d \bmod n$$
$$\equiv m^d \bmod n$$

使用者驗證 T 是否為 m 的數位簽章方式如下：

$$T^e \bmod n \equiv m^{ed} \bmod n \equiv m$$

5. 提出新的匿名票證機制

本論文所提出的新架構如圖 2 所示，共分為三個階段處理，第一階段使用者登入階段，處理使用者輸入個人相關資訊，第二階段匿名票證申請階段，處理使用者的識別碼和請求資訊的匿名申請處理，第三階段訊息請求及回應階段，是將提供資訊伺服器回傳的被加密資訊請求與回應，本篇以下的使用符號表示成如下。

ID_C：使用者的識別碼

ID_{PS}：PS 的識別碼

ID_{PSS}：PSS 的識別碼

$m = ID_c \| REQ$：使用者的識別碼與請求資訊

R：PS 產生的亂數值

$C = R^e m \bmod n$

$T' \equiv C^d \bmod n$

$T \equiv R^{-1}T' \bmod n \equiv m^d \bmod n$

PS：代理伺服器(Proxy Server)

PSS：提供服務伺服器(Providing Service Server)

TGS：票證授權伺服器(Ticket Granting Server)

$$Ticket_{PSS} = E_{K(PSS,TGS)}[T' \| ID_{PS} \| ID_{TGS} \| K_{PS,PSS} \| TS_1 \| Sig_{C,PS,TGS}]$$

$Sig_C = E_{KR(C)}(h(m \| TS_1))$

$Sig_{C,PS} = E_{KR(PS)}[E_{KR(C)}(h(m \| TS_1))]$

$$Sig_{C,PS,TGS} = E_{KR(TGS)}[E_{KR(PS)}[E_{KR(C)}(h(m))]]$$

$K_{(PS,TGS)}$：由 PS 與 TGS 共用的主金鑰(Master Key)

$K_{(PSS,TGS)}$：由 PSS 與 TGS 共用的主金鑰(Master Key)

$K_{(PS,PSS)}$：由 TGS 隨機產生 PS、PSS 共用會期金鑰(Session Key)

$KU_{(C)}, KR_{(C)}$：使用者的公鑰(Public Key)、私鑰(Private Key)

$KU_{(PS)}, KR_{(PS)}$：PS 的公鑰(Public Key)、私鑰(Private Key)

$KU_{(TGS)}, KR_{(TGS)}$：TGS 的公鑰(Public Key)、私鑰(Private Key)

E_K, D_K：利用金鑰 K 加密(Decrypt)、解密(Encrypt)

第一階段是使用者利用代理伺服器的使用，並輸入使用者的識別碼 ID_C 及請求資訊 REQ，並將 ID_C 與 REQ 合併後加簽送出，完整訊息如下所示，。

第一階段使用者登入階段的訊息

(1) $C->PS$：

$$ID_C \| REQ \| TS_1 \| Sig_C$$

第二階段是將使用者的識別碼 ID_C 及請求資訊 REQ 利用 David Chaum 所提出的盲簽章方式來將 $m = ID_c \| REQ$ 與代理伺服器隨機產生的亂數 R，並利用票證伺服器的公鑰 (e,n) 將 R 加密後的乘積 $C = R^e m \bmod n$、代理伺服器識別碼 ID_{PS}、服務提供伺服器識別碼 ID_{PSS}、時戳 TS_1 及使用者與代理伺服器的簽章 $Sig_{C,PS}$ 傳送給票證伺服器。當票證伺服器 (TGS) 收到訊息後，會使用票證伺服器的私鑰 (d,n) 將 C 加簽，如 $T' \equiv C^d \bmod n$，並將 T' 置於服務提供伺服器 (PSS) 的票證中後傳回給代理伺服器 (PS)，以達到盲簽章目的，如下

$$Ticket_{PSS} = E_{K(PSS,TGS)}[T' \| ID_{PS} \| ID_{TGS} \| K_{PS,PSS} \| Sig_{C,PS,TGS}]$$

第二階段：匿名票證申請階段的訊息

(2) $PS->TGS$：

$$E_{K(PS,TGS)}[C \| ID_{PS} \| ID_{PSS} \| TS_1 \| Sig_{C,PS}]$$

(3) $TGS->PS$：

$$E_{K(PS,TGS)}[K_{(PS,PSS)} \| TS_2 \| Ticket_{PSS}]$$

第三階段是利用票證伺服器 (TGS) 所核發的票證向服務提供伺服器 (PSS) 請求相關資訊，所以直接將所取得的票證、所產生的亂數 R、時戳 TS_2 及其雜湊值，利用票證伺服器 (TGS) 所提供的會期金鑰 $K_{(PS,PSS)}$ 加密後送出給服務提供伺服器 (PSS)。服務提供伺服器 (PSS) 收到資訊後將會利用票證內的 $T' \equiv C^d \bmod n$，透過 $T \equiv R^{-1}T' \bmod n \equiv m^d \bmod n$ 的計算後，便可得到使用者的 $m = ID_c \| REQ$ 簽體，此時只要使用票證伺服器的公鑰 (e,n) 便可解出使用者的識別碼 ID_c 和請求資訊 REQ，再依請求的資訊回覆，並使用票證內的會期金鑰 $K_{(PS,PSS)}$ 加密回覆資訊 $REPLY$，完整訊息如下所示。

第三階段：訊息請求及回應階段的訊息

$PS->PSS$：

$$E_{K(PS,PSS)}[Ticket_{PSS} \| R \| TS_2 \| E_{KR(PS)} [h(Ticket_{PSS} \| R \| TS_2)]]$$

$PSS->PS$：

$$E_{K(PS,PSS)}[REPLY \| E_{KR(PSS)}(h(REPLY))]$$

當服務提供伺服器 (PSS) 處理以上資訊的同時，會將所接受到的 $h(m \| TS_1)$、TS_1、R 及 T' 儲存於資料庫內，以便日後若有任何爭議，可達可追溯性，驗證方式如下：

透過下列計算式，可得使用識別碼 ID_c 及請求的資訊 REQ

$$h(R^{-1}T')^e = m = ID_c \| REQ$$

透過下列計算式是否成立來判定此資訊的完整及不可否認性

$$h(m \| TS_1) = ? h((R^{-1}T')^e \| TS_1)$$

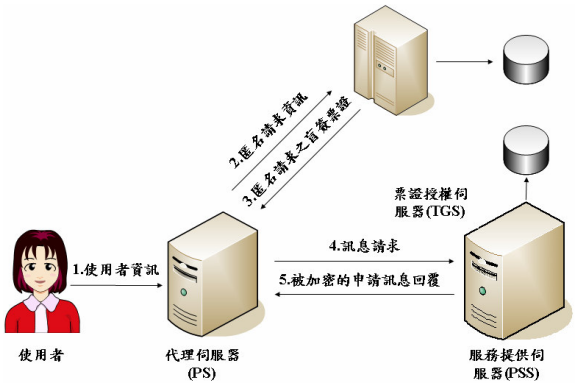

圖 2：匿名票證授權機制

也由於此機制中所使用的是代理匿名方式，所以在票證伺服器並無法驗證使用者的簽章，必須要到最後的服務提供伺服器方能解出使用者的識別碼，所以在最後的驗證過程如圖 3 所示。

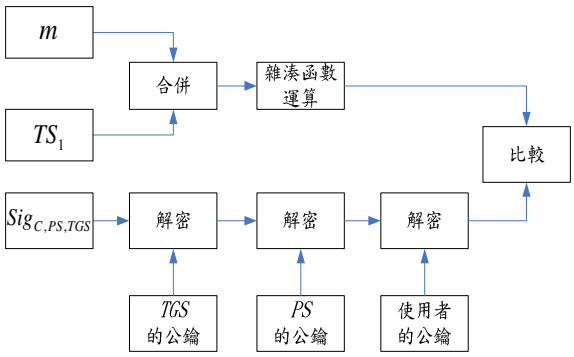

圖 3：$Sig_{C,PS,TGS}$ 的查證流程

6. 安全性探討

在本架構下，主要是藉由使用者 ID_c 、*PS* 和 *TGS* 三者的簽章，由服務提供伺服器 *PSS* 來認定該請求使用者的 ID_c 及所請求的資訊 *REQ* ，確實是經由使用者所提出、代理伺服器 *PS* 所代理及票證伺服器 *PSS* 所核發的匿名票證。

藉由 *PS* 向 *TGS* 合法取得匿名的授權票證再向 *PSS* 正式提出資訊的請求，整個過程當中，透過第三者的盲簽章以達到對服務提供伺服器 *PSS* 的授權之外，主要的身份鑑別(Authentication)是透過最後的服務提供伺服器 *PSS* 將盲簽章的資訊解開核對無誤後，再傳回所請求的資訊，其中所傳送的任何資訊，利用兩兩信賴關係所共用的主金鑰(Master Key)加密，並使用由 *TGS* 所核發的臨時性會期金鑰(Session Key) $K_{(PS,PSS)}$，來進行資料的加密處理和達成機密性的要求，更能透過彼此的主要金鑰來確認彼此雙方的身份，而在獨立鑑別伺服器之間的資料傳輸，則透過合法第三者的 *TGS* 核發票證中的會議金鑰(Session Key)來完成該次交易的安全通道金鑰。

本論文對資料傳送過程也導入了時戳的概念，時戳的目的除了能記錄該次請求的實際時間，提供做為後續的追溯依據，更能透過 Client 端的時戳與伺服端的時間做比對，使得 $T_1 - T_2 < \Delta T$ ，可避免掉有心人士的重送攻擊法(Replay Attack)。

最後，在機制中由於是使用匿名申請，除非是服務提供伺服器 *PSS* 可以識別出使用者識別碼，所以服務提供伺服器 *PSS* 必須將相關的資訊儲存於資料庫內，而票證伺服器在此扮演公正單位，所以也必須將盲簽章的資訊儲存於資料庫內，做為後續能達到資料請求之可追溯性。

7. 結論

本論文提出新的匿名票證機制架構，主要是要解決單一使用者可能有數組的帳號、密碼，以及有多個同質性甚高資訊散佈在不同的彼此獨立的單位，例如銀行的存款資訊、個人金融信用資訊及個人的醫療服務紀錄，的不共享性的問題。但為求能透過第三者(如本文提到的 *TGS*)來達到公正的裁決作用，透過盲簽章機制，來達到匿名且可追溯性，整個請求過程必須同時能達到鑑別性(Authentication)、完整性(Integrity)、機密性(Confidentiality)和存取控制權(Access Control)，從不同單位取得同一使用者個人資料彙整的資訊，減少資源成本，達到安全的資訊共享。

8.參考文獻

[1] Bhrat Patel, Jon Crowcroft(1997), "Ticket Based Service Access for the Mobile User", *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*, pp223-233, Budapest, Hungary, September.

[2] Chaum, D., "Blind signature for untraceable payments" in : Advances in cryptology: Proc. Crypto 82 (Plenum Press, New York, 1983). pp. 199-203

[3] Hua Wang, Jinli Cao, Yanchuan Zhang(2002), "Ticket-based service access scheme for mobile users" *The Twenty-Fifth Australian Computer Science Conference* (ACSC2002), Conferences in Research and Practice in Information Technology, Vol. 4, pp285-292, Melbourne, Australia.

[4] Hung-Yu Chien and Che-Hao Chen, "A Remote Authentication Scheme Preserving User Anonymity", *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)*, IEEE, 2005.

[5] Jaeseung Go, Kwangjo Kim. "Wireless Authentication Protocol Preserving User Anonymity", *SCIS2001, Japan*, January, pp. 23-26, 2001.

[6] Jianming Zhu and Jianfeng Ma, "A New Authentication Scheme with Anonymity for Wireless Environments", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, February, 2004.

[7] Kohl, J., Neuman, B., Ts'o, T."The Evolution of the Kerberos Authentication Service." In Brazier, F., and Johansen, D., *Distributed Open Systems*. Los Alamitos, CA: IEEE Computer Society Press, 1994. Available at http://web.mit.edu/kerberos/www/papers.html

[8] Manik Lal Das, Ashutosh Saxena and Ved P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2 May 2004.

[9] RFC1510, The Kerberos Network Authentication Service (V5)

[10] William Stallings(2002), "Cryptography and Network Security : Principles and Practice 3rd ", ISBN 0-13-091429-0, Prentice Hall.