基於代理簽章的多伺服器認證方案

楊伏夷　　林威廷
朝陽科技大學資訊工程系　朝陽科技大學資訊工程系
副教授　　研究生
yangfy@cyut.edu.tw　s10027634@cyut.edu.tw

摘要

在電子商務中，使用者通常會去多個服務伺服器註冊進而獲得服務。因此多伺服器環境上安全的身分認證方案是很重要的議題。

在 2012 年，廖學者等人指出曾學者等人的方案會遭受到內部攻擊與離線密碼猜測攻擊，以及沒有提供相互認證。因此，他們提出了一個新穎的多伺服器認證方案。而廖學者所提出的方案中，服務伺服器在加入多伺服器環境後，服務伺服器會得到註冊中心所發配的驗證公鑰。

一般而言，服務伺服器在加入多伺服器環境前，它通常已經擁有了在其他環境所發配的驗證公開金鑰。為了減少服務伺服器存放公開金鑰的成本，在本篇文章中，我們提出了基於代理簽章的多伺服器認證方案，並且對我們提出的方案作安全性分析以及結論。

關鍵詞：電子商務、代理簽章、相互認證。

Abstract

In e-commerce, users often register at different service servers and receive the services; thus, secure authentication of multi-server environment is an important issue.

In 2012, Liao et al. pointed that the scheme proposed by Tzeng et al. would encounter insider attack and offline password guessing attack, while also lacked mutual authentication. Therefore, they proposed a multi-server authentication scheme. In that scheme, after joining in multi-server environment, service servers will obtain public keys of issued by registration center.

Generally speaking, before joining multi-server environment, service servers usually have public keys issued by other environments. In order to lower the cost for service servers to save public keys, this study proposed a multi-server authentication scheme based on proxy signature, conducted security analysis on the scheme, and offered conclusions**.**

Keywords: electronic commerce, proxy signature, mutual authentication

1. 前言

隨著網際網路的快速發展，很多使用者利用網路交換知識、取得資訊、以及進行交易活動和相關的服務活動。因此，如何在網路上進行安全的交易是非常重要的課題。由於電子商務的方便性，使用者可能會向許多服務伺服器註冊進而得到服務。在這樣的環境下，使用者必須向多個服務伺服器分別進行註冊，而且使用者必須記住多個密碼，這樣一來會造成使用者的不方便性。有鑑於上述的問題，所以最近很多學者提出了多伺服器環境下安全認證方案[7,8,9,15,17]來解決多次註冊以及記住多個密碼的問題。目前所提出的多伺服器認證方案中，可區分為基於雜湊函數的認證方案與基於公開金鑰密碼系統的認證方案。由於目前行動裝置的普及化，使用者可以利用行動裝置來取得服務，而考慮行動裝置在計算能力的限制，因此，如何設計出一個高效率與安全的方案是目前非常重要的議題。

一般而言，一個健全的多伺服器網路環境的遠端使用者驗證方案必須滿足下列需求[7]:

1. 服務伺服器不需儲存任何的驗證表與密碼表。
2. 使用者變更密碼時不需要第三者的協助。
3. 使用者與服務伺服器允許相互驗證並協議出用來通訊的會議金鑰。
4. 由於智慧卡計算能力上的限制，因此必須有效率的計算。
5. 使用者只需要在註冊中心註冊一次，並可使用合法服務伺服器所提供的服務。
6. 不需要利用時間戳記防止重送攻擊，以解決時間同步的問題。
7. 可以抵擋各種可能的攻擊。

在 2012 年，廖學者等人提出了一個基於雙線性配對的多伺服器認證方案[8]，並表示該

方案計算的效率，比起其他之前學者所提出的基於公開金鑰密碼系統的認證方案而言，有更好的計算效率。但我們發現該方案仍然需要比較大的計算量。一般而言，雙線性配對的計算量是橢圓曲線乘法的數倍[1,5]，以運作於橢圓曲線 E/F_3^{97} 短簽章技術協定[2]為例，簽章階段包括雜湊至橢圓曲線元素及橢圓曲線乘法各一次的運算，驗證階段包括兩次雙線性配對的計算，在 PIII 1 GHz 的平台上，耗費時間分別為 3.57 ms 和 53 ms[1]。因此我們提出了一個使用橢圓曲線公開金鑰密碼系統的多伺服器認證方案，免除雙線性配對運算，可以大幅減少計算成本，因此更適合用於計算能力有限的行動裝置上面。

一般來說，在服務伺服器要加入多伺服系統環境之前，服務伺服器通常已經擁有在其他系統環境所發配的驗證公開金鑰。因此，如果服務伺服器向註冊中心進行註冊後，又獲得由註冊中心發配的公開金鑰，這樣會增加服務伺服器在存放與管理多個驗證公開金鑰的成本。為了解決上述的問題，因此我們提出了一個基於代理簽章的多伺服器認證方案，當特定服務伺服器要向註冊中心註冊，來加入多伺服器環境時，註冊中心會發配代理金鑰給特定服務伺服器。而使用者可由服務伺服器利用代理金鑰對訊息簽署產生的代理簽章，來驗證服務伺服器的合法性。

2. 我們的方案

在廖學者等人的方案中[8]，特定服務伺服器向註冊中心註冊時，會得到由註冊中心所發配的驗證公鑰。一般而言，當服務伺服器加入多伺服器系統環境時，它通常已經擁有在其他環境所發配的驗證公鑰，為了減少服務伺服器存放與管理公開金鑰的成本，因此我們提出了基於代理簽章的多伺服認證方案來改善廖學者等人的方案。我們的方案共有四個階段：伺服器註冊階段，使用者註冊階段，使用者登入階段，相互驗證階段。

本方案的參數設置:

U_i: 第 i 個使用者
SS_j: 第 j 個服務伺服器
ID_i: 使用者 U_i 的身分
SID_j: 服務伺服器 SS_j 的身分
PW_i: 使用者 U_i 的密碼
RC: 可信任的註冊中心
m_{wj}: 註冊中心頒給服務伺服器 SS_j 的授權書、其中包含了服務伺服器的身分、服務伺服器的公開金鑰、以及有效條款
G_1: 加法循環群其序為質數 q
P: G_1 群的生成元
(s_{RC}, PK_{RC}):註冊中心的私鑰與公鑰, $PK_{RC} = s_{RC}P$
(s_j, PK_j): 服務伺服器原始的私鑰與公鑰 $PK_j = s_jP$
(s_i, PK_i): 使用者的私鑰與公鑰
$h(.)$:單向雜湊函數,
$\|$: 串接運算

2.1 伺服器註冊階段:

本階段採用代理簽章技術[11,16]，由註冊中心授權服務伺服器，在使用者登入伺服器時相互認證。

當服務伺服器 SS_j 要加入多伺服器系統時，它會先傳送公開金鑰與憑證給 RC 進行註冊，註冊中心驗證身分與憑證後，會核定服務授權書 m_{wj}，m_{wj} 包含了服務伺服器的身分 SID_j、公開金鑰 PK_j、以及有效條款，然後註冊中心會產生一個隨機亂數 $r \in Z_q^*$，並且計算 $R = rP$，以及 $m_j = h(m_{wj}, R)$，接著使用自己的私鑰計算 $w_j' = r + m_j s_{RC} \pmod q$，接著透過安全通道將$(R, m_j, w_j')$傳送給服務伺服器。服務伺服器收到後，會去驗證它的有效性:

$m_j = h(m_{wj}, R)$
$w_j'P \stackrel{?}{=} R + m_j PK_{RC}$

服務伺服器驗證有效性後，會利用自己的私鑰計算 $w_j = w_j' + s_j \pmod q$。

2.2 使用者註冊階段:

傳統簽章技術[3, 13]必需驗證簽署者的簽章與簽署者的公開金鑰，身分鑑別(ID-based)簽章技術[6, 14]固然免除驗證簽署者的的公開金鑰，但也產生了授權機構知道使用者私密簽章金鑰的問題(Key escrow problem)[18]，自我驗證(Self-certified public keys)公開金鑰技術[4, 10, 12]，則同時解決上述問題，本研究使用者註冊階段採用文獻[10]的自我驗證簽章技術。

當使用者 U_i 想要存取多伺服器環境系統時，會先選擇身分 ID_i 以及密碼 PW_i，且產生一個隨機亂數 $c \in Z_q^*$計算 $C_i = cP$，之後透過安全通道將(ID_i, PW_i, C_i)傳送給註冊中心來進行註冊。註冊中心收到後，會產生一個隨機亂數 $d \in Z_q^*$，計算 $D_i = dP + C_i$，然後註冊中心會利用私鑰計算 $s_i' = h(ID_i \| D_i)s_{RC} + d \pmod q$，並

且計算要存放在智慧卡的參數:

$E_i = s_i' + h(PW_i \| C_i)$

$PK_i = h(ID_i \| D_i)PK_{RC} + D_i$

接著註冊中心將$\{E_i, C_i, D_i, PK_i, h(.)\}$這些私密參數存放在智慧卡中，並透過安全通道將智慧卡交付給使用者。使用者收到智慧卡後，將智慧卡插入讀取裝置，接著使用者輸入 ID_i，PW_i 以及 c，之後智慧卡執行下列的運算：

$s_i' = E_i - h(PW_i \| C_i)$

$s_i = s_i' + c \pmod q$

接著智慧卡會驗證 $s_iP \stackrel{?}{=} PK_i$，如果相等，則計算 $E_i^{new} = E_i + c \pmod q$，並更換存放在智慧卡中的 E_i；否則，則取消請求。

2.3 使用者登入階段:

當使用者 U_i 想要登入服務伺服器 SS_j 時，會先輸入 ID_i 與 PW_i，接著智慧卡會計算使用者的私鑰:

$s_i = E_i - h(PW_i \| C_i) \pmod q$

之後產生一個隨機亂數 $a \in Z_q^*$，計算 $A_i = aP$，並將(ID_i, D_i, A_i)傳送給服務伺服器。

2.4 相互驗證階段:

當服務伺服器 SS_j 接收到使用者 U_i 所傳送的登入訊息(ID_i, D_i, A_i)後，會先計算使用者的公開金鑰 $PK_i = h(ID_i \| D_i)PK_{RC} + D_i$，產生隨機亂數 $b \in Z_q^*$，並計算 $B_j = bP$ 與短期私鑰 $K_{ji} = bA_i$，接著服務伺服器計算驗證訊息 $d_{ji} = h(ID_i \| SID_j \| K_{ji} \| B_j \| A_i)$，之後服務伺服器會利用代理金鑰對驗證訊息進行簽署而產生代理簽章 t:

$t = b + w_j d_{ji} \pmod q$

接著服務伺服器會將(R, B_j, m_{wj}, t)傳送給使用者。當使用者收到(R, B_j, m_{wj}, t)，會先利用服務伺服器的公鑰與註冊中心的公鑰檢查代理簽章的有效性:

$m_j = h(m_{wj}, R)$

$PK_{SIDj} = R + m_j PK_{RC} + PK_j$

$K_{ij} = aB_j$

$d_{ij} = h(ID_i \| SID_j \| K_{ij} \| B_j \| A_i)$

$tP \stackrel{?}{=} B_j + d_{ij}PK_{SIDj}$

如果驗證通過，則代表服務伺服器為有效的；接著使用者會利用自己的私鑰計算簽章:

$u = a + d_{ij}s_i \pmod q$

接著使用者會將簽章 u 傳送給服務伺服器進行認證，服務伺服器收到後，會先驗證簽章的有效性:

$uP \stackrel{?}{=} A_i + d_{ji}PK_i$

如果相等，則表示使用者為有效的；雙方完成相互認證後，使用者和服務伺服器的會議金鑰分別為 $SK_i = h(K_{ij})$以及 $SK_j = h(K_{ji})$。

3. 安全性分析

在本章節中，我們將討論提出的多伺服器認證方案，能夠抵擋各種可能的攻擊。包含了代理簽章的正確性，可以抵擋重送攻擊、假冒伺服器攻擊、內部攻擊、已知金鑰攻擊、假冒攻擊，達到完美前推私密性，並且在我們的方案中，伺服器不需要儲存驗證表。

3.1 代理簽章正確性

由服務伺服器所簽署的代理簽章傳送給使用者，使用者可以驗證代理簽章的正確性。

$$\begin{aligned} tP &= (b + w_j d_{ij})P \\ &= B_j + (w_j d_{ij} P) \\ &= B_j + [(w_j' + s_j)d_{ij}P] \\ &= B_j + [(r + m_j s_{RC} + s_j)d_{ij}P] \\ &= B_j + d_{ij}R + (d_{ij}m_j)PK_{RC} + d_{ij}PK_j \\ &= B_j + d_{ij}PK_{SIDj} \end{aligned}$$

3.2 重送攻擊

在我們的方案中，使用者每次登入同時啟用金鑰協商，使用了使用者和服務伺服器各自產生的亂數 A_i 和 B_j 來抵擋重送攻擊，因此，如果攻擊者攔截到使用者所傳送的登入訊息(ID_i, D_i, A_i)以及簽章 u，然後傳送給服務伺服器來假冒使用者，並無法通過服務伺服器的驗證，所以我們的方案可以防止重送攻擊。

3.3 假冒伺服器攻擊

此種攻擊方式是假冒遠端伺服器，而使用者卻不知道此伺服器是偽造的，而傳送相關的秘密資料給假冒的伺服器，使得重要的資料被竊取。在我們提出的方案中，假設攻擊者想要假冒伺服器，計算出有效的訊息(R, B_j, m_{wj}, t)給使用者進行驗證，由於攻擊者沒有服務伺服器 SS_j 的代理金鑰 w_j，因此無法成功假冒合法的服務伺服器。

3.4 假冒攻擊

如果攻擊者假冒使用者傳送訊息(ID_i, D_i, A_i)給服務伺服器，雖然會獲得服務伺服器所傳送的訊息(R, B_j, m_{wj}, t)，但由於攻擊者無法得知使用者的私鑰，因此攻擊者無法計算有效的簽章 u 給服務伺服器來進行驗證。

3.5 已知金鑰安全

在我們的方案中，會議金鑰是由短期私鑰(K_{ij} or K_{ji})所產生的，而短期私鑰則由隨機數(a,b)所計算的，假設攻擊者獲得目前回合的會議金鑰，也無法推導出未來所使用的會議金鑰。

3.6 完美前推私密性

完美前推私密性是指假如通訊雙方的私鑰洩漏，攻擊者也無法推導出通訊雙方之前所產生的會議金鑰。在我們的方案中，雙方通訊的會議金鑰是由短期私鑰(K_{ij})所產生的，而短期私鑰是由隨機數(a, b)產生的，而無關於通訊雙方的私鑰，因此我們的方案達到完美前推私密性。

3.7 內部攻擊與驗證表竊取攻擊

在我們的方案裡，使用者私鑰產生過程是先由註冊中心產生部分私鑰並傳給使用者，接著使用者再產生完整私鑰，因此假設註冊中心的私鑰洩漏，攻擊者也無法推導出使用者的私鑰。並且在我們的方案中，註冊中心與服務伺服器並沒有儲存任何的驗證表與密碼表，因此我們的方案沒有驗證表被竊取的風險。

4. 結論

在本研究中，我們提出了一個基於代理簽章的多伺服器環境的遠端使用者認證方案，來改善先前學者所提出的方案。當服務伺服器加入本系統後，可使用原始的公鑰供使用者進行驗證，因此減少了服務伺服器儲存與管理多個驗證公鑰的成本。以及我們的方案，可以抵擋在多伺服器環境下可能的攻擊，並且使用者與服務伺服器相互認證會協商出共同通訊的會議金鑰。因此我們所提出的方案，可以更適用於多伺服器系統環境中。

致謝

審稿委員們寶貴的評論與建議以及國科會專案研究計畫補助部分經費，謹此致謝，計畫編號：NSC 101-2221-E-324-047。

參考文獻

[1] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," ***in: Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science 2442, Springer-Verlag, New York***, pp. 354-368, 2002.

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," ***in***: ***Advances in Cryptology – Asiacrypt'2001, Lecture Notes in Computer Science 2248***, ***Springer-Verlag***, ***New York***, pp. 514-532, 2002.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," ***IEEE " IEEE Transactions on Information Theory***, Vol. 31, Issue 4, pp. 469-472, 1985.

[4] M. Girault, "Self-certified public keys," ***Advances in Cryptology - EUROCRYPT'91, LNCS 547***, pp. 490-497, 1991.

[5] S. D. Galbraith , K. Harrison and D. Soldera, "Implementing the Tate Pairing," ***Proceedings of the 5th International Symposium on Algorithmic Number Theory***, pp. 324-337, July 07-12, 2002.

[6] F Hess, "Efficient identity based signature schemes based on pairings," ***Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography (SAC2002), Lecture Notes in Computer Science 2595***, ***Springer-Verlag***, ***New York***, pp. 310-324, 2003.

[7] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," ***IEEE Transactions on Consumer Electronic***, pp.251 – 255,2004.

[8] Y. P. Liao, C. M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," ***Future Generation Computer Systems***, Vol.29, Issue 3, pp.

886-900,2012.

[9] Y. P. Liao, S. S. Wang, "A secure dynamic ID-based remote user authentication scheme for multi-server environment," ***Computer Standards & Interfaces***, pp.24 – 29, 2009.

[10] Y. P. Liao, S. S. Wang, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves," ***Computer Communications***, Vol.33, Issue 3, pp.372-380,2009.

[11] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," ***IEICE Transaction on Fundamentals***, Vol. E79-A, No.9, pp. 1338-1354, 1996.

[12] H. Petersen and P. Hoster, "Self-certified keys – concept and application," ***Proceedings of the Communication and Multimedia security'97***, pp. 102-116, 1997.

[13] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," ***Communications of the ACM***, Vol. 21, No. 2, pp. 120-126, 1978.

[14] Shamir, "Identity-based cryptosystems and signature schemes," ***in***: ***Advances in Cryptology – Crypto'84, Lecture Notes in Computer Science 196***, ***Springer-Verlag***, ***New York***, pp. 47-53, 1984.

[15] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," ***Computers & Security***, Vol. 27, Issue 3–4, pp. 115-121,2008.

[16] W. J. Tsaur, "Secure communication for electronic business applications in mobile agent networks," "***Expert Systems with Applications***, Vol.39, Issue1, pp. 1046-1054, 2012.

[17] W. J. Tsaur, J. H. Li, W. B Lee., "An efficient and secure multi-server authentication scheme with key agreement," ***Journal of Systems and Software***, Vol. 85, Issue 4, pp. 876 – 882,2012.

[18] T. H. Yuen, W. Susilo and Y. Mu, "How to Construct Identity-Based Signatures without the Key Escrow Problem," ***International Journal of Information Security***, Vol. 9, No. 4, pp. 297-311, 2010.