以延伸帳號紓解區域網路中心開放電話撥接服務的帳號管理問題

陳奕明　曾黎明*

國立中央大學資訊管理學系所
臺灣省桃園縣中壢市
E_mail: cym@im.mgt.ncu.edu.tw

*國立中央大學資訊工程學系所
臺灣省桃園縣中壢市
E_mail: t341727@ncu865.ncu.edu.tw

摘要

如何減輕帳號管理負擔以讓有限的人力投入到更具創造性的服務工作上，一直是許多學校電算中心的期望，近年來雖然有許多方法被提出來，但大多僅適用於區域網路上，對於廣域網路上的帳號管理問題，例如各區域網路中心在開放電話撥接服務後常常需要額外管理許多的終端機伺服器使用者帳號，卻仍缺少一套簡單有效的方法。為解決此問題，本文提出一個延伸帳號(extended account)的方法，此方法的特色是將建帳號的工作由系統管理者轉變成由系統管理者、使用者及電腦程式來共同負擔。電腦程式負責一切例行性的帳號建立工作，系統管理者負責帳號開放政策的制定，至於帳號建立中最困難的身份辨認問題，則交由使用者來自行證明。我們利用挑戰__回應(Challenge--Response)的原理，由使用者自行回答系統提出的問題，若回答正確，帳號才會被自動建立成功。整個過程中，不須更改系統程式或通信協定，也不受機器型態或作業系統版本的影響，使用者只要事先擁有一個合法的TANET使用帳號並且會基本的e-mail能力即可。文中除介紹延伸帳號的觀念和原理外，對於其設計和應用也將一一說明。

1. 簡介

如何減輕帳號管理負擔以讓有限的人力投入到更具創造性的服務工作上，一直是許多學校電算中心的期望，此種期望隨著TANET的日漸普及更顯得明顯。近年來，由於TANET推行成功，許多老師及學生已經相當依賴TANET來從事學術活動，即使回到家也希望透過電話線和學校主機連線。因為長途電話所費不貲，所以大部分人都會先連到附近區域網路中心的終端機伺服器（terminal serve,TS），但這時往往會遇到一個問題就是各區域網路中心為了避免非TANET使用者(例如使用Hinet的一般社會人士)經由區域網路中心的TS連上Internet,通常都會將其TS設定成只能連上校內主機或要求使用者於連線時就輸入帳號。無論是上述那一種情形，對於非本校的學生都會造成不便，因為需要特地向區域網路中心申請一個TS帳號。對於各區域網路中心而言，要管理這些帳號也會形成額外的負擔。因此如果能讓此類帳號交由使用者自行建立（當然，使用者能自行建立帳號的前提是他在其所屬學校的機器上已有帳號，我們稱此種帳號為信任帳號,trusted account，使用者自行建立的帳號則稱為延伸帳號,extended account），則不僅可紓解TANET使用者不在校園時使用網路不便的問題，學生在校園裡要申請一台以上電腦的帳號時，也可依此方法自行建立，大幅減少系統管理者管理帳號的負擔。

帳號管理最關鍵的問題就是帳號申請者的身分認證問題。為了簡單易推廣起見，我們不擬採用複雜的安全協定或依賴某種商業產品，相反地，我們採用半自動的方式，讓使用者自行證明其具有TANET的合法使用者身分；管理者只要制定安全政策，如帳號可開放給那一類的使用者、有效期限是多久等參數即可，如此可大幅減少建立帳號的步驟及使用者申請帳號的不便。

本文分為五節。下一節我們將回顧帳號管理的相關研究，第三節將介紹延伸帳號的技術和其實現方法，第四節說明延伸帳號的應用，最後做一簡短結論。

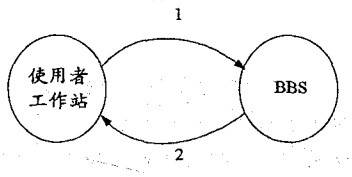
2.相關研究

在帳號管理上，目前有兩類方法可以最少的帳號建立成本，讓最大數目的使用者進入一部以上的電腦：共用帳號(common account)和公開帳號(public account)法。所謂共用帳號是指在一個網路範圍內，所有的電腦都可共用一使用者密碼檔，使用者不論在網路上的那一台電腦上簽入(login)，都可使用相同的帳號和密碼，目前在技術上已有 Sun Microsystems 的 NIS(Network Information System)[1]、美國MIT Athena計劃的Hesiod service[2]及中央大學曾黎明的共用密碼檔[3]等三種方法可實現此功能。此方法的優點是簡單方便，缺點是不論那一種技術，都需要依賴系統軟體的支援才可使用，對於大範圍的廣域網路而言，要求每一部電腦都具有相類似的系統軟體並不容易做到。至於公開帳號法，是指每一台機器上都提供一個公開的帳號（例如GUEST，此帳號可在login畫面上出現，或以其他管道公佈出來），此方式的優點是不須修改任何系統軟體就可達到網路資源共享的目的，每個人都可利用此帳號簽入系統，其缺點則是無法事先查核使用者身分，對於有使用資格限制的情況（例如區域網路中心的終端機伺服器只限TANET使用者使用）就不適合。

帳號建立的過程中，關鍵性的一個步驟就是事先要過濾使用者的身份，所以目前的帳號申請程序都是填寫申請表格，附上學生證影印本之類的證明文件然後交給系統管理者統一建立帳號。延伸帳號的挑戰就是如何在省略申請過程中的身分證明書面文件後，還能驗證使用者的身份以讓系統自動為使用者建立帳號？目前在TANET上有一個類似的解法就是BBS帳號的申請。

BBS的特色之一就是由使用者自行建立其帳號和密碼。好處是BBS管理者幾乎不須花費精力在帳號管理上，缺點則是若有人濫用此項權利，在BBS上做出謾罵，人身攻擊等違反網路禮節行為時，BBS管理者除了消極地砍掉此帳號外，難以追查出該帳號使用者的眞正身份于以處罰。為解決此問題，目前許多BBS站都要求申請者要在TANET上擁有一個e-mail address後才能申請帳號。這樣，萬一日後有需要時，至少有e-mail address這條線索可以去追查。BBS如何驗證使用者所提出的e-mail address是正確的呢？其原理如圖一所示。首先申請者在申請註冊的畫面上便須輸入一個e-mail address,之後申請者還須利用此e-mail address送封特定內容（包括申請者在註冊畫面所自取的帳號和密碼）的mail到BBS去。BBS若能收到此mail並檢查其帳號和密碼和原註冊的符合後，此帳號才算眞正生效。

上述BBS 的方法保留了使用者自行建立帳號的優點，也略微達到使用者身份認證的功能，但其基本假設是e-mail 上的sender欄位不會被竄改。但事實上利用sendmail protocol的漏洞[4]，一個稍具網路知識的不法者便可冒充別人的名義註冊，再冒用別人的e-mail address發出mail,而達到隱藏自己身分的目的。 因此，我們固然一方面要達到像BBS般允許使用者自行設立帳號和密碼，一方面也要設法改善上述BBS在身分驗證上的安全缺失。



說明：
step1. 使用者於註冊時輸入帳號密碼及 E-MAIL ADDRESS
step2. 使用者發 E-MAIL 至 BBS

圖一：使用者申請 BBS 帳號動作示意圖

3.延伸帳號的建立

所謂延伸帳號，是指使用者已有一個合法的TANET帳號（我們稱此帳號為信任帳號，trusted account）後再自行申請建立的帳號。因為此種帳號通常是為了方便或臨時需要而申請的（例如學生寒暑假回家後，須申請他校區域網路中心的終端機伺服器帳號等），因此這類帳號的建立方法有下列幾個原則：

(1)簡單：意指不需要更改系統程式，容易實現，這樣才有可能在TANET上普遍使用

(2)有效：每個人都會用，如此才能要求每一個帳號申請者都採用此種程序而確實達到減少帳號管理負擔的目的

(3)可靠：穩定性高，不會因作業系統或環境參數改變而有不同表現

為了達到上述三個設計原則，我們首先決定不採共用帳號而採用公開帳號的方法以求簡單易實現，接著參考BBS的做法，以e-mail來驗證申請者的身份，整個系統和使用者之間的動作流程如圖二所示。

圖二的動作說明如下：

(1)使用者用Modem連上區域網路中心的終端機伺服器(Terminal Server,TS)

(2)此TS被設定只能連到一台特定的工作站，此工作站上並提供一個公開帳號（例如public）.此公開帳號被設定成一login便執行一個帳號建立代理人(account agent)程式

(3)account agent程式顯示註冊表格，要求使用者自行填入帳號、密碼和信任帳號（亦即使用者的e-mail address)

(4)account agent首先檢查已存在的帳號中是否有同名者？若有，則顯示錯誤訊息，要求使用者重新取名，否則自動送一封mail至使用者所指定的e-mail address去

(5)使用者利用其他方法進入其e-mail address所在的主機並回答該封e-mail

(6)account agent收到e-mail回信並確定無誤後，依照使用者原先所輸入的延伸帳號和密碼建立一個密碼表（其中密碼經加密過），以供添加到 TS上的密碼表上去。

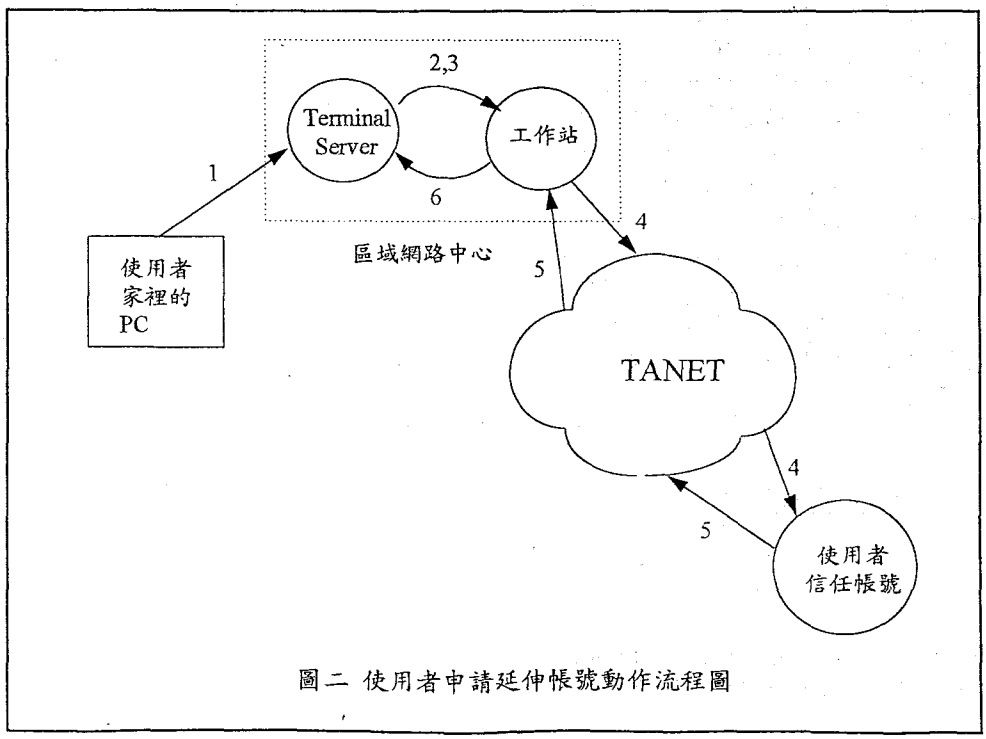
3.2 延伸帳號的安全性設計

為了避免延伸帳號像BBS的帳號申請一樣，每個人都可冒用他人名義來申請帳號（只要他知道怎樣利用sendmail protocol的漏洞來改sender欄位），在上述動作流程中，我們多了三項安全性設計：

(1)account agent主動mail至使用者的mail box並要求回信，使用者若能回信至少證明其擁有某個帳號的名稱和密碼。所以不法者即使知道某人的帳號，但因不知其密碼而無法冒充後者來申請延伸帳號。

(2)account agent可被設定成只承認某些TANET節點上的帳號才是信任帳號（例如各校電算中心管理的主機），如此可避免有人在PC上隨意建立帳號後再向他校申請延伸帳號。

(3)採用挑戰__回應的方法，account agent在發信時，每一封信的內容都不同（例如在信中附上一個隨機亂數），並要求使用者依內容回信（例如將該亂數值加一後傳回）。如此，當account agent收到e-mail回信時，除檢查回信的日期外（譬如發信和回信的間隔日期須在三天以內），還要檢查信件內容。由於每一位使用者所需回答的信件內容都不同，除非不法者可看到信件內容，否則無法正確回信，account agent收不到正確回信也就不會真正建立帳號。當然，如果



圖二 使用者申請延伸帳號動作流程圖

有人用tcpdump等工具在網路上擷取所有的e-mail後，再冒用別人名義回信，則因e-mail內容皆屬明文，所以無法避免這類的安全漏洞。

4. 應用：中小學老師學生上TANET的帳號管理

使全國各國中小老師學生能利用到TANET各項服務，是TANET建設的重要目標。由於人員設備等各種限制，上述學校不易維持一個網路中心，較合理的作法是透過現有各區域網路中心的電話撥接來連上TANET，但國中小學生老師人數眾多，各區域網路中心勢必不可能為每一位國中小學生老師建立帳號。一個較可行的做法是各校自行管理一台UNIX 機器（例如以486 PC 建置 Linux 或FreeBSD),上面建有該校老師學生的帳號，這樣，再利用本文所提的方法，需要利用各區域網路中心的TS上TANET的國中小學生老師可自行建立延伸帳號，如此可將帳號管理的工作分散到各校及使用者身上，不但可使國中小學生老師上TANET更方便，各區域網路中心也可節約帳號管理的人力來提供更有價值的網路服務。

5.結論

本文介紹了一個簡單的方法來將帳號建立的工作分散給使用者自行來做。此方法的要領是採用刺激__回應的原理，使用者只要會使用簡單的e-mail功能，就可以採用這套系統來自行建立帳號，預定開放帳號的機器只要執行一個account agent程式即可，不須額外的通信協定或軟體。文中我們分析了此方法的安全性，並對其應用也做了說明。因為延伸帳號的設計都是採用現成的技術，不須修改任何系統程式，所以應用於TANET上，應沒有技術上的困難。若能普遍應用，相信可以減少各區域網路中心管理終端機伺服器帳號的負擔。

6.參考文獻

1.SunOS User's Guide, SUN microsystems, 1990.

2.S.P. Dyer,"The Hesiod Name Server", Project Athena Document, Internet Draft,1988

3.曾黎明，ＰＣ小型網路伺服群系統，教育部專題研究計劃期末報告，民國八十二年六月

4. 王清佑，洞悉UNIX,網路與系統安全篇，和碩公司出版，民國八十三年三月，頁108-112