開放式網路之身份驗證=indentity anthentication for open network

廖國宏、顏嵩銘

E-mail: 8515721@mail.dyu.edu.tw

摘 要

在開放式的網路環境中，通訊節點是不被信任且所使用的通道是不安全的，導致意圖不軌的使用者有更多的機會來偽裝成別的使用者，因此必須有 更安全的身份驗證方法，才能滿足在開放式網路環境中的需求。因此研究 發展出一套開放式網路的身份驗證系統，實在是當務之急。密碼學的領域 中已有不少演算法可供身份驗證使用，其中尤以公開金匙密碼系統所具有 之特色為最適合。但使用公開金匙密碼系統的一大問題就在於如何確知所 拿到的公開金匙是屬於它所宣稱的擁有者所擁有。因此需要一些公信單位 的設置，證明該把公開金匙的確實性，這就是目前公開金匙密碼系統基礎 建設的研究，論文中的前段即對所需之基礎建設作一整合性之探討。由於 全面性的使用公開金匙密碼系統目前實屬不可能，需等公開金匙密碼系統 基礎建設完善後才行。因此類似於麻省理工學院Kerberos驗證系統為最切 合目前之需要，這系統是以一由使用者所共同信任的第三者為媒介來達到 身份驗證，但這系統仍有許多缺點及實際應用上的困難，因此於本篇論文 中我們提出一套身份驗證系統－宙斯，以與Kerberos相同的設計需求為前 提，來達到普及化的身份驗證，並避免掉Kerberos的一些缺點與問題。論 文的中段即對此實用化的身份驗證系統作探討及設計。在論文的後段中， 我們實作了一套於Unix作業系統上的安全性談話系統－PGPcTalk。目前 Unix上所使用的Talk系統沒有辦法判斷談話的那一方是否確是其人，亦無 法防止通訊的內容被人攔截解讀。PGPcTalk可解決這些安全上的問題。此 外PGPcTalk除了安全性方面的加強外，也因應中文本土化的需求，可以輸 入中文，讓使用中文之用者更為便利。此外使用者可透過實際使用此一系 統，來發覺並正視此一存在已久的網路安全問題，以期早日達成開放式網 路的全面安全化。

關鍵詞 : 公開金匙基礎建設 ; 雜湊函數 ; 對稱式密碼系統 ; 公開金匙密碼系統

目錄

參考文獻

0