具有弱金匙保護的可認証金匙分配協定之研究

劉孟宗、顏嵩銘

E-mail: 8515743@mail.dyu.edu.tw

摘 要

網際網路的連接四通八達，沒有國界之分，只要坐在終端機前面便可 以和位於全球各個角落的人互通訊息。科技的發展為我們帶來相當大的便 利，同樣的也伴隨著許多的問題。電腦網路雖然縮短了人與人之間的距離 ，但是畢竟不同於傳統面對面的交談，要如何去識別對方的身份成為首要 之務。而且，如何使資料能在開放式的網路架構下安全的傳輸，以及隱私權的保護，也是相當的重要。我們必須體認到：任何人都有可能正在監聽 著我們在網路上所傳輸的資料。為了確保網路通訊的安全，我們必須做到 下列兩點：1.身份的驗証，2.資料的保密。對於資料的保密，只要會議金 匙選取得宜，這個問題較易解決。至於身份的驗証，以使用者的密碼來辨 識身份，是最普遍的一種做法。然而，絕大多數的密碼皆屬於弱金匙（weak key），難以抵擋字典攻擊法（dictionary attack）的侵襲。在本 論文中，針對弱金匙保護的問題，做了一系列的討論。文中除了介紹弱金 匙可能遭遇到的一些攻擊之外，同時也提供了在設計通訊協定時應注意的 事項。在論文的最後，提出了一套可立即實現的弱金匙保護架構，以彌補 現今身份驗証系統的一大漏洞。

關鍵詞 : 弱金匙保護 ; 密碼學 ; 資訊安全

目錄

參考文獻

0