基於身分認證的密碼分析

楊伏夷　　楊庭綸
朝陽科技大學資訊工程系　朝陽科技大學資訊工程系
yangfy@cyut.edu.tw　　s9927639@cyut.edu.tw

摘要

密碼學者所提出的身分驗證系統，廣泛應用於網路環境的遠端認證。為了解決發生在傳統遠端認證系統上的安全以及管理問題，在最近十年內，眾多學者提出了許多使用智慧卡的遠端認證協定來改善安全上的問題。在 2010 年 Ronggong Song 所提出改進方案試圖改進 Xu-Zhu-Feng 方案的弱點，但是我們發現 Ronggong Song 的方案仍然會遭受到密碼猜測攻擊。在本篇文章，我們分析他們的協定，並描述其弱點與攻擊方法。

關鍵詞：智慧卡、身分認證、交互認證。

Abstract

Cryptographers proposed the identity authentication scheme which is widely used in the remote authentication of the network environment. In the last decade, many researchers proposed the remote authentication scheme to deal with the security and the management problem of the traditional remote authentication system. In 2010, Ronggong Song proposed the improvement to improve the flaws of Xu et al.'s scheme. Unfortunately, we found out the Ronggong Song's scheme is vulnerable to password-guessing attack. In this paper, we analyze their scheme and depict the weaknesses and how to attack.

Keywords: Smart card, identity authentication, mutual authentication.

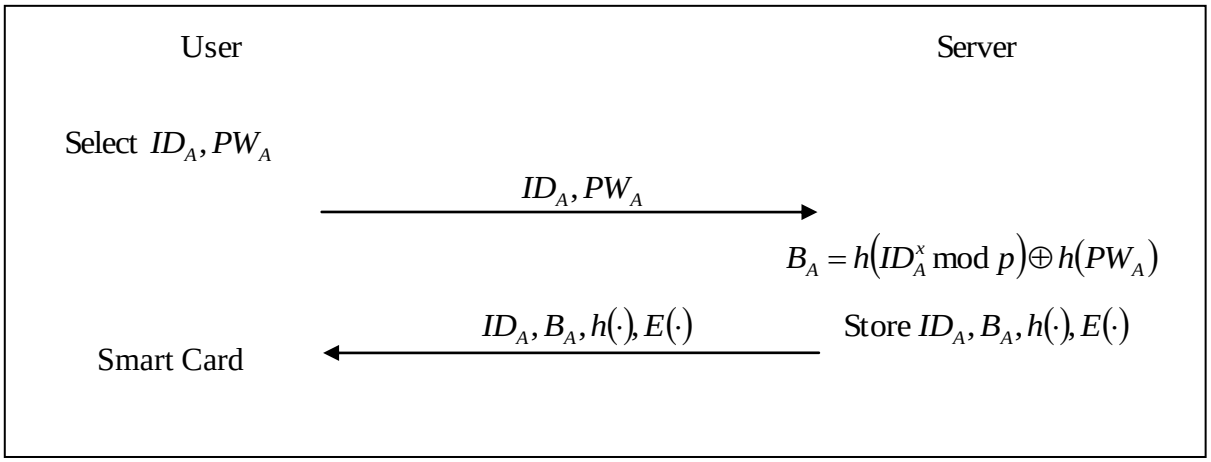
1. 前言

現今遠端認證系統普遍採用密碼認證的方式，但是密碼認證的方式仍然不夠安全，因為攻擊者能透過一些方法來猜測使用者的密碼或是模擬使用者登入。

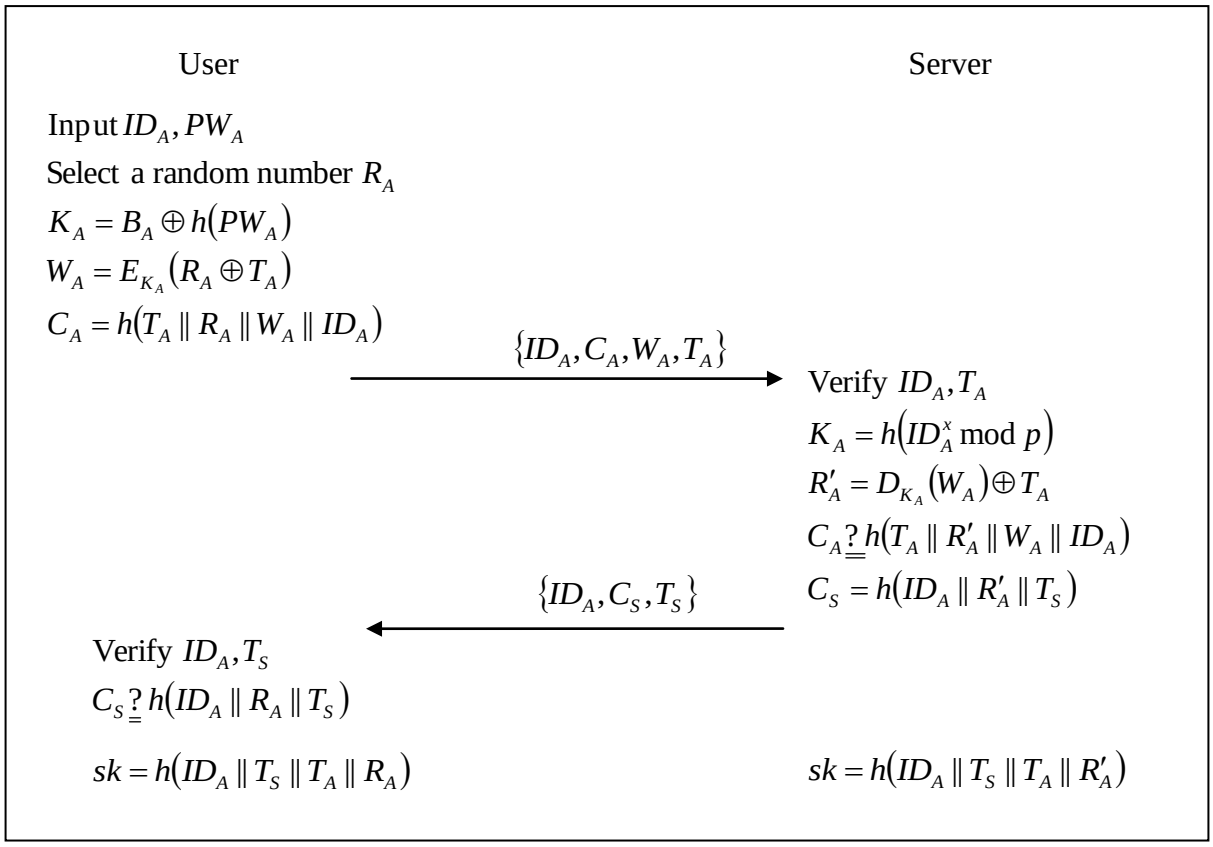
在 1981 年，首先由 Lamport[1]提出了基於密碼的遠端認證方案，但這個方案會受到關於密碼部分的攻擊，例如離線密碼猜測攻擊，之後密碼學者為了提高安全性相繼提出了許多改進的方案。在 2009 年，Xu–Zhu–Feng[2]指出 Lee–Chiu[3]的方案會遭受偽造攻擊，還有 Lee–Kim–Yoo[4]的方案會遭受到密碼字典攻擊，字典攻擊就是攻擊者將部分常被使用到的密碼或是其它常被當成密碼的資料整理成一本類似字典的檔案，再利用這份檔案去猜測對方的密碼；因此，Xu–Zhu–Feng 提出了一個基於智能卡的密碼認證方案，這個方案達到了下列三個條件（1）保護系統抵擋離線密碼字典攻擊，（2）伺服器端可以減輕密碼相關的攻擊，和（3）可以保護伺服器不會遭受合法使用者攻擊。但是，Ronggong Song[5] 發現 Xu–Zhu–Feng 的方案會遭受到模擬攻擊，並且提出一個更有效率且能進行相互認證的方案。然而我們發現 Ronggong Song 改善的方案，仍然會遭受到密碼猜測攻擊，所以在本篇文章我們先回顧 Ronggong Song 的方案，接著在安全性分析會提出 Ronggong Song 方案會遭受的攻擊。

2. 回顧 Song 的方案

Ronggong Song 的方案中分為五個階段: 初始階段，註冊階段，登入階段，認證階段，密碼變更。



圖一、註冊階段



圖二、登入和驗證階段

該方案的參數:

- ID_A，ID_B: 用戶A，B的身份;
- PW_A: 用戶A的密碼;
- R_A:用戶A產生的一次性亂數;
- T_A:用戶A的時戳;
- T_S:伺服器的時戳;
- $h(\cdot)$:安全的單向雜湊函數;
- $E_k(M)$:用交談密鑰K加密的訊息M;
- $\oplus$:互斥邏輯運算;
- $\|$:串接符號;
- p , q:兩個大質數滿足 $p = 2q + 1$;
- Z_q^*: Z_q 的乘法群;
- Z_q :加法群 q;

初始階段:

由伺服器選擇兩個大質數 p 跟 q，並且滿足 p=2q+1，接著選擇一把密鑰 $x \in Z_q^*$。

註冊階段:

用戶提交身份 ID_A 跟自己選擇的密碼 PW_A 透過安全通道傳給伺服器。

伺服器收到註冊訊息$\{ID_A, PW_A\}$後，首先計算$B_A = h(ID_A^x \bmod p) \oplus h(PW_A)$，之後將$\{ID_A, B_A, h(\cdot), E(\cdot)\}$存在用戶的智慧卡，流程如圖一所示。

登入階段:

用戶插入智慧卡到讀取裝置，並且輸入ID_A跟PW_A，再由智慧卡選擇隨機數R_A，並且使用用戶的時間產生時戳T_A後，執行下列計算：

$$K_A = B_A \oplus h(PW_A)$$
$$W_A = E_{K_A}(R_A \oplus T_A)$$
$$C_A = h(T_A \| R_A \| W_A \| ID_A)$$

其中E_{k_A}為對稱式加密演算法使用密鑰K_A,計算完畢後,將登入訊息$\{ID_A, C_A, W_A, T_A\}$傳送到伺服器，流程如圖二所示。

驗證階段:

伺服器在時間T^*收到登入訊息，會先驗證用戶身份ID_A是否已註冊，並透過$(T^* - T_A) \le \Delta T$，檢查時戳T_A是否在合法的登入時間內；設若正確，則計算$K_A = h(ID_A^x \bmod p)$和$R_A' = D_{K_A}(W_A) \oplus T_A$，並檢查$C_A$是否等於$h(T_A \| R_A' \| W_A \| ID_A)$,若驗證通過，伺服器會計算$C_S = h(ID_A \| R_A' \| T_S)$，並傳送$\{ID_A, C_S, T_S\}$給用戶，其中$C_S = h(ID_A \| R_A' \| T_S)$中的$T_S$是伺服器端的時戳。

用戶接收訊息後，對訊息進行驗證，並且檢查C_S是否等於$h(ID_A \| R_A \| T_S)$，如果相等則對伺服器驗證成功。

用戶和伺服器計算一把共同的交談密鑰

$$sk = h(ID_A \| T_S \| T_A \| R_A)$$
$$= h(ID_A \| T_S \| T_A \| R_A')$$

，流程如圖二所示。

密碼更改:

用戶需要更改密碼，要先經過上述認證過程，讓伺服器先驗證舊密碼PW_A，驗證成功會從伺服器端收到確認訊息，之後智慧卡讓用戶輸入新的PW_A'，計算$B_A' = B_A \oplus PW_A \oplus PW_A'$來取代舊的$B_A$。

3. 安全性分析

在本章節中，我們將討論 Ronggong Song 的方案雖然能夠抵擋模擬攻擊、重送攻擊、修改攻擊、平行攻擊，並且說明智慧卡中的資料無法幫助攻擊者猜測使用者密碼，但是我們證明攻擊者仍然可以利用 B_A 去進行密碼猜測攻擊，攻擊方式如下所述：

步驟 1:
假設攻擊者從使用者的智慧卡中取得B_A,並且竊取到登入訊息ID_A、C_A、W_A、T_A。

步驟 2:
之後攻擊者隨機選擇一個PW'當作是使用者的密碼。

步驟 3:
攻擊者利用從智慧卡中取得的 B_A 跟自己計算出的$h(PW')$計算K_A'。

步驟 4:
利用K_A'對竊取到的 W_A 進行解密，解出 $R_A \oplus T_A$，在取得$R_A' = W_A \oplus T_A$。

步驟 5:
利用取得的 C_A 比對重新產生的參數$C_A \stackrel{?}{=} h(T_A \| R_A' \| W_A \| ID_A)$，如果相等則代表$PW'$為使用者的密碼。

4. 結論

在本篇文章中，我們回顧 Ronggong Song 所提出的方案，發現他們的方案仍然會遭受到密碼猜測攻擊，Ronggong Song 提到智慧卡中所包含的資訊，就算被竊取也無法幫助攻擊者取得使用者的密碼，可是我們發現攻擊者仍然可以藉由智慧卡中的 B_A 以及利用竊取到的登入訊息去猜測使用者的密碼，因此 Ronggong Song 所提出的方案仍然不夠安全。

致謝

在作者感謝審稿委員們寶貴的評論與建議。本研究承蒙教育部補助技專校院建立特色典範計畫支持部分經費，謹此致謝，計畫編號：台技(一)字第 0990045921n 號。

參考文獻

[1] Lamport, L., "Password authentication with insecure communication," ***Communications of the ACM***, pp. 770 – 772,1981.

[2] Xu, J., Zhu, W. T. and Feng, D. G., "An improved smart card based password authentication scheme with provable security," ***Computer Standards & Interfaces***, pp. 723–728,2009.

[3] Lee, N.Y. and Chiu, Y.C., "Improved remote authentication scheme with smart card," ***Computer Standards & Interfaces***, pp. 177–180,2005.

[4] Lee, S.W., Kim, H.S. and Yoo, K.Y., "Improvement of Chien et al's remote user authentication scheme using smart cards," ***Computer Standards & Interfaces***, pp.181–183,2005.

[5] Ronggong Song, "Advanced smart card based password authentication protocol," ***Computer Standards & Interfaces***, pp. 321 – 325,2010.