Cryptoanalysis of a remote user authentication scheme without using smart cards

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

江承軒
朝陽科技大學資訊工程系
研究生
icemask@gmail.com

摘要

在 2009 年，Rhee-Kwon-Lee 等學者發表了一個不使用智慧卡的遠端使用者認證協定。這個協定是使用在現實環境中容易取得的儲存裝置，例如手機、PDA、USB 等，而不使用智慧卡，可以降低設備成本。在本篇文章中，我們認為 Rhee-Kwon-Lee 的協定是不安全的，並且指出協定會受到的簡易攻擊、密碼猜測攻擊，以及使用者和伺服器冒名攻擊。

關鍵字：智慧卡、密碼分析、簡易攻擊。

1 簡介

近年來，隨著資訊科技和網際網路的發展，人們可以輕易的登入到遠端伺服器來存取個人的資訊，但在不安全的網路環境下有著資訊洩漏的風險存在，使得遠端使用者認證成為了重要的問題。最近有多位學者發表了許多使用智慧卡(Smart card)的遠端伺服器認證的協定。使用者將註冊的智慧卡放入讀卡機並輸入使用者密碼，登入訊息經由不安全的通道傳送到遠端伺服器驗證，合法的使用者可存取遠端伺服器經授權的資訊。

在 2009 年，Rhee-Kwon-Lee 等學者發表一個遠端伺服器認證的協定[1]。這個協定是使用市面上的儲存裝置，例如 USB，PDA，手機等，來登入遠端伺服器，作者認為他們發表的協定在相同的安全等級下成本較智慧卡低。然而我們認為 Rhee-Kwon-Lee 的協定是不安全的，由於儲存裝置並沒有智慧卡和驗證表防止資訊洩漏的機制，攻擊者可以輕易取得儲存在儲存裝置內的資訊，便可進行簡易攻擊(Simple attack)、密碼猜測攻擊(Password guessing attack)、使用者冒名攻擊(User impersonation attack)，以及伺服器冒名攻擊(Server impersonation attack)等。

本篇文章結構，我們首先在第二章回顧 Rhee-Kwon-Lee 的協定，在第三章我們將會對 Rhee-Kwon-Lee 的協定做安全分析，並指出這個協定容易受到的攻擊，最後一個章節是我們的結論。

2 回顧 Rhee-Kwon-Lee 的協定

這個章節我們將回顧 Rhee-Kwon-Lee 的協定。這個協定由三個部分組成：註冊階段、登入階段和認證階段，底下首先說明協定的符號定義，再依次詳述各個階段的程序。

2.1. 符號定義

以下為協定使用之參數的定義。

- U_i：使用者。
- S：遠端伺服器。
- ID_i：使用者的身份。
- PW_i：使用者的密碼。
- $h(\cdot)$：一個單程函數，由 $\{0,1\}^*$ 對應至 $\{0,1\}^l$，l 為安全等級參數，例如 $l=160$。
- p：長度為 l-bit 的質數。
- G：序為 p 之乘法群。
- $H(\cdot)$：一個全域的雜湊函數，由 $\{0,1\}^*$ 對應至 G。
- x_s：伺服器的祕密金鑰。
- $\oplus$：為互斥運算符號。
- $\|$：為字串連結符號。
- T：時間戳章。

2.1 註冊階段

首先使用者 U_i 自行選取一組身份 ID_i 和

密碼PW_i傳給遠端伺服器S進行註冊，遠端伺服器S收到訊息 後，選擇亂數$r_i \in Z_p$，計算Y_i，Y_i包含$Y_{i,1} = ID_i^{r_i \cdot x_s} \cdot H(PW_i) \in G$，$Y_{i,2} = ID_i^{r_i} \in G$，並且將訊息$(H(\cdot), h(\cdot), p, Y_i)$傳送給使用者$U_i$，使用者$U_i$收到訊息後，將訊息存入 USB 儲存裝置中，以上動作都經由安全通道通訊，以上$Y_{i,1}$，$Y_{i,2}$之計算皆在乘法群之計算將省略符號$\in G$，以免方程式太複雜，以上註冊動作如圖一所示。

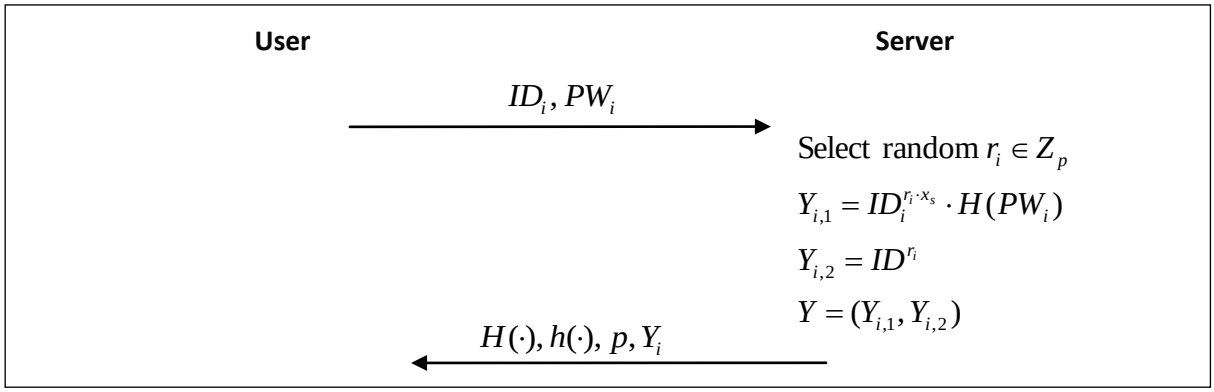
2.2 登入階段

使用者U_i將存在 USB 儲存裝置內的訊息讀入電腦，由Z_p群中選擇兩個隨機亂數a、b，計算登入訊息$Y_i' = Y_{i,1} / H(PW_i)$和$C_1 = (Y_{i,2})^a = (ID_i^{r_i})^a$以及$M = H(Y_i' \oplus T \oplus ID_i)$、$C_2 = (Y_i')^a \cdot M$和$C_3 = (Y_{i,2})^b = (ID_i^{r_i})^b$，並將登入訊息$C = (ID_i, Y_{i,2}, C_1, C_2, C_3, T)$傳送到遠端伺服器做驗證處理。$T$為使用者當下所抓取的時間戳章，以上登入動作如圖二所示。

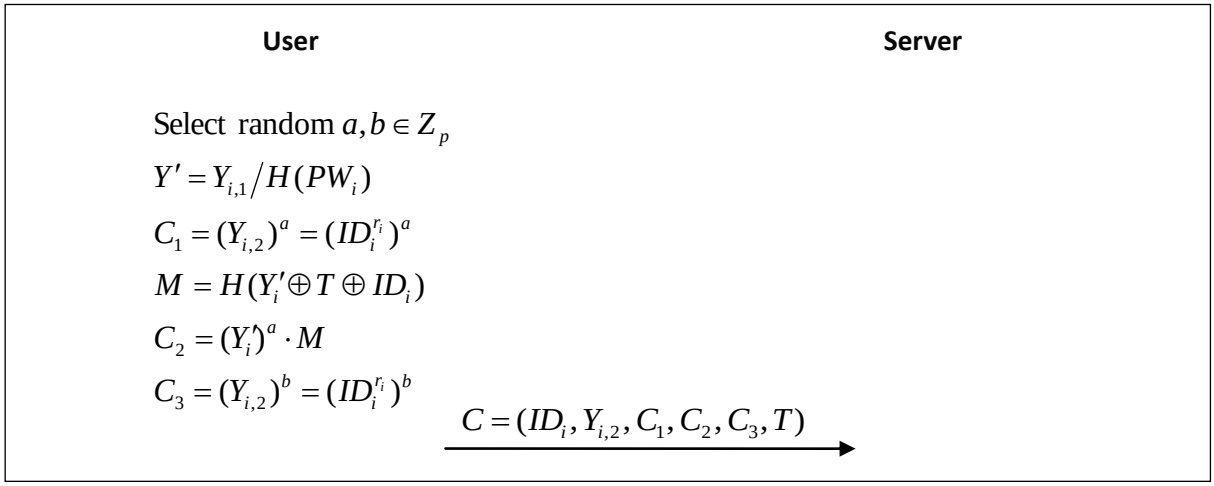
2.3 認證階段

遠端伺服器S在收到使用者U_i傳送的登入資訊，首先檢查ID_i的格式是否正確，如果格式不正確，則遠端伺服器S拒絕使用者登入。接著遠端伺服器S選取當下的時戳T'，並檢驗時戳$T' - T \le \Delta T$，確認使用者的登入訊息是否在合法時間內送達，如果超出合法時間範圍，遠端伺服器S拒絕驗證登入訊息，並要求使用者U_i重新傳送登入訊息，反之則確認$C_2 \cdot (C_1^{x_s})^{-1} \stackrel{?}{=} H((Y_{i,2})^{x_s} \oplus T \oplus ID_i)$是否相等，

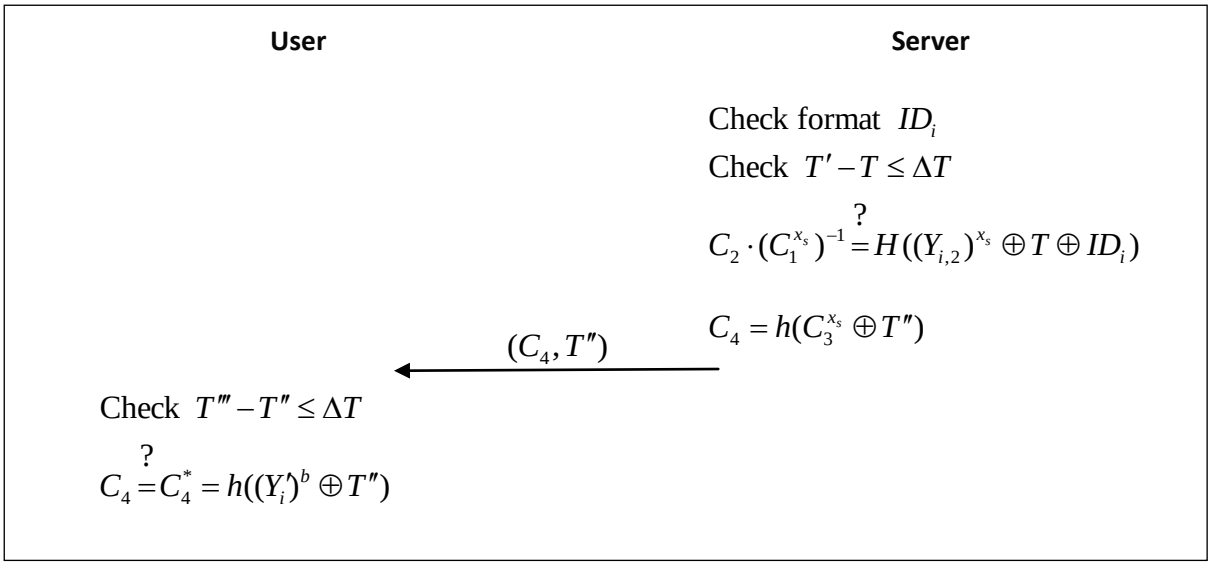
若不相等，則認定此登入訊息是不合法的並拒



圖一 註冊階段流程



圖二 登入階段流程



圖三 認證階段流程

絕使用者U_i登入，反之遠端伺服器S產生新的時戳T''，並計算$C_4 = h(C_3^{x_s} \oplus T'')$，回傳驗證訊息$(C_4, T'')$給使用者$U_i$，使用者收到遠端伺服器$S$回傳的驗證訊息後，產生當下的時戳$T'''$，並檢驗$T''' - T'' \le \Delta T$，確認驗證訊息是否在合法時間內送達，若驗證訊息送達時間超出合法時間範圍，則拒絕這個驗證訊息，反之計算$C_4^* = h((Y_i')^b \oplus T'')$，並確認$C_4 \stackrel{?}{=} C_4^*$是否相等，若相等則代表此次通訊的遠端伺服器為合法，並且完成相互認證，以上認證動作如圖三所示。

3 Rhee-Kwon-Lee 的協定安全問題

由於這個協定是使用儲存裝置來儲存註冊後的認證資訊，儲存裝置沒有智慧卡和驗證表防止資訊洩漏的機制，我們便可假設攻擊者能輕易的取得儲存裝置以及網路上的資訊，並且對使用者U_i和遠端伺服器S進行安全上的攻擊。

3.1 簡易攻擊

在登入階段，攻擊者可以自行創造登入資訊，以便假冒ID_i登入伺服器。先抓取當下時戳T，使用參數$Y_{i,2} = 1$，$C_1 = (Y_{i,2})^a = 1$，$C_2 = H(1 \oplus T \oplus ID_i)$，$C_3 = 1$，便可將登入訊息$(ID_i, 1, 1, H(1 \oplus T \oplus ID_i), 1, T)$傳送給遠端伺服器$S$，遠端伺服器$S$在收到攻擊者傳送的登入訊息後，可輕易的通過$ID_i$格式和時戳$T$的檢查，接著遠端伺器$S$會計算$C_2 \cdot (C_1^{x_s})^{-1} \in G$和$H((Y_{i,2})^{x_s} \oplus T \oplus ID_i)$，並檢查是否相等，上述參數代入公式可得$(H(1 \oplus T \oplus ID_i)/1^{x_s}) = H(1^{x_s} \oplus T \oplus ID_i)$這個結果，攻擊者則可通過驗證並成功登入到遠端伺服器S。

3.2 低序之 ID 的弱點

在註冊階段，算式$Y_{i,2} = ID_i^{r_i}$的安全性是建立在解離散對數的問題上，取得ID_i、r_i可輕易計算出$Y_{i,2}$，取得$Y_{i,2}$要計算出r_i相對困難，由於身份資訊ID_i是使用者U_i自己選擇，若ID_i之序太低，在解離散對數問題上相對簡單，攻擊者可用暴力法從$Y_{i,2}$解出r_i。

3.3 密碼猜測攻擊

假設攻擊者截取登入訊息$C = (ID_i, Y_{i,2}, C_1, C_2, C_3, T)$，便可計算$C_3' = Y_{i,2} = ID_i^{r_i}$，並將登入訊息中的$C_3$換成$C_3'$傳給遠端伺服器$S$，則登入訊息仍可以正確登入，而且遠端伺服器$S$會計算$C_4 = H(C_3'^{x_s} \oplus T'')$，並將訊息回傳給攻擊者，攻擊者在拿到儲存在 USB 儲存裝置中的元素

$Y_{i,1}$，$Y_{i,2}$，則可進行 Password guessing attack，攻擊方法步驟如下：

(1) 從 PW 字典中選擇一個 PW_i'。

(2) 計算 $Y_i' = Y_{i,1} / H(PW_i')$。

(3) 計算 $H(Y_i' \oplus T'')$ 並與 C_4 做比較，如果相等，攻擊者成功的猜測到 PW_i'，反之回到(1)繼續猜測。

3.4 不用密碼可登入伺服器

如同上述攻擊 3.3 之方法可得 PW_i，並知道 $Y_{i,1} = ID_i^{r_i \cdot x_s} \cdot H(PW_i)$ 和 $Y_{i,2} = ID_i^{r_i}$，故可得 $ID_i^{r_i}$ 和 $ID_i^{r_i \cdot x_s}$，攻擊者不需要密碼 PW_i 便可計算 $Y_{i,2} = ID_i^{r_i}$，$C_1 = (ID_i^{r_i})^a$，$M = H(ID_i^{r_i \cdot x_s} \oplus T \oplus ID_i)$，$C_2 = ID_i^{r_i \cdot x_s \cdot a} \cdot M$ 和 $C_3 = (ID_i^{r_i})^b$，並且傳送登入訊息 $(ID_i, Y_{i,2}, C_1, C_2, C_3, T)$ 給遠端伺服器 S，可通過伺服器驗證並成功登入。

3.5 使用者冒名攻擊

由上述攻擊 3.4 方法可得知 $ID_i^{r_i}$ 和 $ID_i^{r_i \cdot x_s}$，攻擊者可假冒身份 ID_j，計算 $Y_{i,2} = ID_i^{r_i}$，$C_1 = (ID_i^{r_i})^a$，$M' = H(ID_i^{r_i \cdot x_s} \oplus T \oplus ID_j)$，$C_2 = ID_i^{r_i \cdot x_s \cdot a} \cdot M'$ 以及 $C_3 = (ID_i^{r_i})^b$，並將登入訊息 $(ID_j, Y_{i,2}, C_1, C_2, C_3, T)$ 傳給遠端伺服器 S，在收到登入訊息後，遠端伺服器 S 會先確認 ID_j 的格式和訊息傳送時間是否合法，接著檢查 $C_2 \cdot (C_1^{x_s})^{-1} \stackrel{?}{=} H((Y_{i,2})^{x_s} \oplus T \oplus ID_j)$，因為 $M' = H(ID_i^{r_i \cdot x_s} \oplus T \oplus ID_j)$，所以攻擊者可以通過遠端伺服器 S 的驗證並登入成功。

3.6 伺服器冒名攻擊

由上述攻擊 3.2 之方法可得知 PW_i，攻擊者可截取登入訊息中的使用者身份 ID_i，產生新的亂數 r_i' 以及新的伺服器私鑰 x_s'，可計算 $Y_{i,1}' = ID_i^{r_i' \cdot x_s'} \cdot H(PW_i)$ 和 $Y_{i,2}' = ID_i^{r_i'}$，並將使用者儲存裝置中儲存的 $Y_{i,1}$ 和 $Y_{i,2}$ 更改成新的 $Y_{i,1}'$ 和 $Y_{i,2}'$，由於攻擊者知道 x_s'，便可假冒遠端伺服器 S 對使用者進行伺服器冒名攻擊。

4 結論

我們認為 Rhee-Kwon-Lee 的協定是不安全的。攻擊者可以輕易的成功登入遠端伺服器，並且會受到 Password guessing attack 使得使用者的密碼洩漏，而且在先前攻擊中在取得資訊，可對使用者和伺服器做偽造攻擊。本篇文章中，我們指出 Rhee-Kwon-Lee 的協定不安全部分，希望將來可以針對這個協定的問題來做改善，並加強使用儲存裝置的認證協定在現實生活上的實用性。

參考文獻

[1] Rhee, H.S. Kwon, J.O. and Lee, D.H., ”A remote user authentication scheme without using smart cards,” ***Computer Standards & Interfaces*** , Vol. 31, No. 1, pp. 6-13, 2009.