一種可攻擊學者 Chang 等人之驗證機制的使用者偽裝攻擊

蔡佳倫
交通大學
crousekimo@yahoo.com.tw

李榮耀
交通大學
jlee@math.nctu.edu.tw

摘要

使用者身份驗證一直是網路安全中一個十分重要而且基本的研究領域，因為透過這樣的驗證機制，可以讓系統與使用者去驗證對方的身分是否合法。西元 2005 年，學者 Lin 和學者 Hwang 所提出的驗證機制被學者 Chang 與學者 Chang[4]發現到有驗證表被竊攻擊的安全性問題，為了改善這個安全性問題，學者 Chang 和學者 Chamg 提出了兩個改善的無驗證表驗證機制，不幸的是，本研究發現到這兩個無驗證表驗證機制中，有一個無驗證表驗證機制有著使用者假冒攻擊(Impersonation Attack)的安全性問題，所以這個無驗證表驗證機制並不是十分的安全。

關鍵詞：身分驗證、智慧卡、使用者假冒攻擊。

1. 前言

使用者身份驗證一直是網路系統中最基本的安全機制，對於一個安全無虞的驗證機制來說，不僅僅要讓伺服器要去驗證使用者身份，更重要的是必須提供使用者能夠去驗證伺服器的身分，這樣才不會讓使用者或伺服器被假冒的使用者或是偽裝的伺服器所欺騙，導致重要的資訊遭到攻擊者所偷竊。在所有的驗證機制中，以密碼為主的身分驗證機制是目前使用地最廣泛的一種身分驗證機制，因為它具備了簡單和容易實現的優點，因此有許許多多的學者專家以此為基礎，提出了各種不同的驗證機制，希望能夠提升網路的安全性。雖然這些驗證機制是用各種不同的方法去驗證遠端的使用者，但是，並不代表這些驗證機制就是十分安全，因此，當有一個驗證機制被提出時，便有許許多多的專家學者檢視其中是否隱藏有任何安全性的問題，進而提出改善的驗證機制，讓這些驗證機制能夠更加的安全。

西元 2000 年，學者 Peyavian 和學者 Zunic[1]提出一種以單向雜湊函數為基礎的使用者驗證機制，它可以在不安全的網路環境之下讓驗證資訊安全無虞地送到對方手上，並且不需要使用對稱性加密演算法或是非對稱性加密演算法去加密通訊的資料，以減少使用者或是伺服器的運算量。可惜的是，西元 2002 年學者 Hwang 和學者 Yeh[2]指出學者 Peyravian 等人所提出的驗證機制有許多安全性的問題，因為學者 Peyravian 等人所提出的驗證機制是以密碼來驗證遠端的使用者，所以學者 Peyravian 等人所提出的驗證機制容易遭受攻擊者利用密碼猜測攻擊(password guessing attack)、伺服器偽裝攻擊(server spoofing attack)以及伺服器資料竊聽攻擊(server data eavesdropping attack)等攻擊方式入侵系統。為了要改善這些安全性問題，學者 Hwang 和學者 Yeh 提出了一種改善的驗證機制來避免這些安全性問題的發生，這個改善的驗證機制除了可以有效的避免以上的安全性問題外，更在驗證結束之後讓使用者與伺服器去定義出一把階段鑰匙(session key)以保障後續資料傳輸的安全性，讓系統的安全性更加完善。不幸的是，西元 2003 年學者 Lin 和學者 Hwang[3]指出學者 Hwang 和學者 Yeh 所提出的驗證機制容易遭受阻絕服務攻擊(Denial of Service Attack)以及欠缺前推安全(forward secrecy)，所以還不是十分的安全，為了改善這些安全性問題，學者 Lin 和學者 Hwang 也提出了一種改善的驗證機制去改善學者 Hwang 等人所提出驗證機制的安全性問題。可惜的是，西元 2005 年學者 Chang 和學者 Chang[4]指出這個驗證機制有著驗證表被竊攻擊(Stolen-verifier attack)的安全性問題，因為這些驗證機制在伺服器上還是需要有驗證表存在，為了有效避免驗證表被竊攻擊(Stolen-Verifier Attack)的發生，他們提出了兩個改善的無驗證表驗證機制去改善伺服器被竊攻擊(Stolen-Verifier Attack)的這個安全性問題。

可惜的是，本研究發現到西元 2005 年學者 Chang 和學者 Chang[4]所提出的兩個驗證機制中，有一個驗證機制有著使用者假冒攻擊(Impersonation Attack)的安全性問題，靠著這個使用者偽造攻擊(Impersonation Attack)，一個合法的使用者可以很輕鬆的產生多組帳號及密碼而不需要知道伺服器所隱藏的資訊，讓系統的安全性大受影響，下面將會先簡單的介紹學者 Chang 和學者 Chang 有問題的無驗證表驗證機制，然後再提出本研究的攻擊方法。

2. 學者 Chang 與學者 Chang 之驗證機制

在這個地方，將會簡單介紹西元 2005 年學者 Chang 和學者 Chang[4]所提出的驗證機制，這個驗證機制主要包括了兩個部份：註冊期(Registration phase)以及登入期(Login phase)，在介紹這個驗證機制之前，先介紹在驗證機制中所使用到的符號，如下表所示：

表 1 符號說明表

符號	說　　明
h()	單向雜湊函數
⊕	互斥或
ID, PW	使用者帳號與密碼
‖	參數連結
N	使用者及伺服器產生的隨機亂數
X->Y:M	表示從 X 傳送一個 M 訊息到 Y
U，S	分別代表使用者及伺服器

2.1 註冊期

整個註冊期主要執行在伺服器上，令 g 是一個在 GF(p)的質數、p 是一個非常大的質數，g 和 p 這兩個系統變數都保存在伺服器之中，當一個使用者想要註冊成為一個新的使用者時，這個使用者必須將使用者帳號(ID)和使用者密碼(PW)以安全通道的方式送到伺服器，所有的註冊期執行如下所示：

Step1: 使用者自由的選擇一個使用者密碼 PW，隨後將使用者帳號(ID)和使用者密碼(PW)以安全通道的方式傳送到遠端的伺服器。

Step2: 當伺服器收到了使用者傳來的帳號(ID)和密碼(PW)時，伺服器計算 $K = h(PW) \oplus (g^{ID^{-1}} \bmod p)$，隨後，伺服器將 K 和 h()存放在智慧卡中，並且將這個智慧卡以安全通道的方式交給使用者使用。

2.2 登入期

當一個合法的使用者想要登入到遠端的系統時，這個合法的使用者必須要先插入他的或她的智慧卡於讀卡機中，並且輸入他的或她的帳號(ID)和密碼(PW)，這時讀卡機便會執行下面的登入步驟：

Step1: U->S: ID, C_2

使用者隨機產生一個亂數R_1，並且使用PW、K、R_1去計算出$C_1 = h(PW) \oplus K = (g^{ID^{-1}} \bmod p)$以及$C_2 = R_1 \oplus C_1$，隨後，使用者將ID, C_2送到伺服器進行驗證。

Step2: 當伺服器從使用者端收到訊息時，伺服器首先利用ID、g、p去計算 $C_1' = (g^{ID^{-1}} \bmod p)$ 並且使用C_1'、C_2去計算$R_1' = C_2 \oplus C_1'$。

Step3: 伺服器使用C_1'、R_1'、R_2去計算$C_4 = h(C_1'||R_1'||R_2)$並且使用C_1', R_1',R_2去計算$C_5 = h(C_1'||R_1') \oplus R_2$。

Step4: S->U: ID, C_4, C_5

伺服器將ID、C_4、C_5送往使用者。

Step5: U->S: ID, C_6

當使用者收到伺服器傳來的訊息之後，使用者使用C_1、R_1、C_5去計算出$R_2' = h(C_1||R_1) \oplus C_5$，並且使用$C_1$、$R_1$、$R_2'$去計算$C_4' = h(C_1||R_1||R_2')$，隨後使用者比對$C_4'$和$C_4$，假如他們一樣，使用者使用$C_1$、$R_2'$去計算出$C_6 = h(C_1||R_2')$並且將ID、$C_6$送往伺服器，否則，使用者中斷伺服器的連結請求。

Step6: 當伺服器收到使用者傳來的登入訊息之後，伺服器使用C_1'、R_2去計算$C_6' = h(C_1'||R_2)$，並且比對C_6和C_6'。如果他們相同的話，伺服器接受使用者登入的請求，否則，伺服器拒絕使用者的登入要求。

3. 本研究所提出之攻擊法

使用者偽裝攻擊(Impersonation Attack)是一種十分危險的網路攻擊方法，一個攻擊者可以使用這樣的攻擊方法去偽裝成其他的合法使用者入侵系統，根據西元 2000 年學者 Chan 與學者 Cheng[5]和西元 2003 年學者 Chang 與學者 Hwang[6]所發表的期刊論文中，曾提出一種使用者偽造攻擊，這種攻擊方法可以讓一個合法的使用者去產生另一組合法的帳號密碼，而不需要知道伺服器所保存的私密參數。利用這種攻擊方法，本研究發現到學者 Chang 和學者 Chang 所提出的驗證機制也可以利用這種使用者偽裝攻擊(Impersonation Attack)來產生出多組偽造的驗證資訊，進而假冒使用者登入系統之中。不過，有些許不一樣的是學者 Chang 與學者 Chang 所提出的驗證方法隱藏了變數 p，因此，如果要利用同樣的方式攻擊驗證系統的話，就必須要滿足一個先備條件，才能夠在不知這個變數 p 之下攻擊系統。在介紹本研究所提出的攻擊法之前，下面將會先介紹一下這個先備條件，這個先備條件如下所示：

$$(a \bmod p) * (b \bmod p)$$
$$\textit{if } (a \bmod p) * (b \bmod p) < p$$
$$= (a * b \bmod p)$$

證明

$$\text{Let } a = S_1 p + t_1, b = S_2 p + t_2$$
$$(S_1, S_2 \in n, 0 \le t_1 < p, 0 \le t_2 < p)$$
$$(a \bmod p) * (b \bmod p)$$
$$= [(S_1 p + t_1) \bmod p] * [(S_2 p + t_2) \bmod p]$$
$$= t_1 * t_2$$
$$if\ (a \bmod p) * (b \bmod p) = (t_1 * t_2) < p$$
$$= (t_1 * t_2) \bmod p$$
$$= (S_1 p * S_2 p + S_1 p t_2 + S_2 p t_1 + t_1 * t_2) \bmod p$$
$$= (S_1 p + t_1) * (S_2 p + t_2) \bmod p$$
$$= (a * b) \bmod p$$

介紹完這個先備條件之後，下面開始介紹本研究之攻擊方法，如下所示：

攻擊方法一：

如果要產生出其他的使用者驗證資訊的話，攻擊者在攻擊前必須要滿足兩個條件，第一、攻擊者必須先系統上註冊，其帳號必須要能被 2 所整除，如果註冊成功，攻擊者便可以獲得一個含有K = h(PW) ⊕ ($g^{ID^{-1}} \bmod p$)和h()的智慧卡，這樣攻擊者才可以使用個人的使用者密碼去獲得 $g^{ID^{-1}} \bmod p$，第二、攻擊者所擁有的 $g^{ID^{-1}} \bmod p$ 必須滿足 ($g^{ID^{-1}} \bmod p$)* ($g^{ID^{-1}} \bmod p$)< p，這樣攻擊者才可以在不需要知道p值的情況下，利用 $g^{ID^{-1}} \bmod p$ 產生一組 ($ID_A, g^{ID_A^{-1}} \bmod p$)，靠著計算：

$$(g^{ID^{-1}} \bmod p) * (g^{ID^{-1}} \bmod p)$$
$$\because (g^{ID^{-1}} \bmod p) * (g^{ID^{-1}} \bmod p) < p$$
$$= g^{(ID/2)^{-1}} \bmod p$$

如此一來，攻擊者便可以產生一組合法帳號密碼($ID_A, g^{ID_A^{-1}} \bmod p$)=(ID/2, $g^{(ID/2)^{-1}} \bmod p$)假冒成一個合法的使用者ID_A去登入遠端的系統。

攻擊方法二：

攻擊方法一僅能製造一組合法的使用者帳號密碼，如果想要產生多組合法的使用者帳號密碼，便必須擴充攻擊方法一，如同攻擊方法一，第一、假設攻擊者可以在系統上註冊成一個合法的使用者，此時，攻擊者選用可以被多個整數所整除帳號 ID，攻擊者將可以獲得一個含有 K = h(PW) ⊕ ($g^{ID^{-1}} \bmod p$)和 h()的智慧卡，第二、如果攻擊者所擁有的 $g^{ID^{-1}} \bmod p$ 滿足 $(g^{ID^{-1}} \bmod p)^n$ <p 這樣的條件時，攻擊者便可以使用下面的方法去計算出多組偽裝的使用者驗證資訊：

$$(g^{ID^{-1}} \bmod p)^n$$
$$\because (g^{ID^{-1}} \bmod p)^n < p$$
$$= (g^{n*ID^{-1}}) \bmod p$$
$$= g^{(ID/n)^{-1}} \bmod p$$

(n 為一個可以整除 ID 的正整數)

此時，攻擊者便產生出多組合法使用者($ID_A, g^{ID_A^{-1}} \bmod p$)= (ID/n, $g^{(ID/n)^{-1}} \bmod p$)去登入遠端的系統，進而入侵系統。這個攻擊方法擴充了攻擊方法一，只要攻擊者所選用n可以整除攻擊者所選用的帳號ID時，攻擊者便可以利用這個帳號ID來產生其他的合法使用者，因此，對於攻擊方法二來說，攻擊者最好選用可以被多種不同正整數整除的帳號ID進行註冊。

攻擊方法三：

假設攻擊者得到了兩個含有K_1=h(PW_1)⊕($g^{ID_1^{-1}} \bmod p$) 和 K_2=h(PW_2)⊕ ($g^{ID_2^{-1}} \bmod p$)的智慧卡以及這兩個智慧卡的密碼PW_1和PW_2，並且同時滿足($g^{ID_1^{-1}} \bmod p$) * ($g^{ID_2^{-1}} \bmod p$) < p與ID_1*ID_2可以被ID_1+ID_2所整除這兩個條件時，攻擊者便可以不需要知道p值為何，利用 $g^{ID_1^{-1}} \bmod p$和 $g^{ID_2^{-1}} \bmod p$去計算：

$$(g^{ID_1^{-1}} \bmod p) * (g^{ID_2^{-1}} \bmod p)$$
$$\because 當 (g^{ID_1^{-1}} \bmod p) * (g^{ID_2^{-1}} \bmod p) < p$$
$$= g^{ID_1^{-1}} * g^{ID_2^{-1}} \bmod p$$
$$= g^{ID_1^{-1} + ID_2^{-1}} \bmod p$$

$$= g^{(ID_1+ID_2)/ID_1*ID_2} \bmod p$$
$$= g^{((ID_1*ID_2)/(ID_1+ID_2))^{-1}} \bmod p$$

此時，攻擊者便可以假冒成一個合法的使用者 (ID_A, $g^{ID_A^{-1}} \bmod p$)= $((ID_1*ID_2)/(ID_1+ID_2)$, $g^{((ID_1*ID_2)/(ID_1+ID_2))^{-1}} \bmod p$)。

攻擊方法四：

攻擊方法三僅能製造一組合法的使用者帳號密碼，如果想要產生多組合法的使用者帳號密碼，便必須擴充攻擊方法三，計算出其他的合法使用者，如果攻擊者擁有 n 塊合法的智慧卡，而且同時滿足 $\prod_{i=1}^{n}(g^{ID_i^{-1}} \bmod p) < p$ 且 $(\sum_{i=1}^{n}\frac{1}{ID_i})^{-1}$ 為一正整數這兩個條件時，攻擊者便可以在不需要知道 p 值為何，去計算出多組偽裝的使用者驗證資訊，靠著計算：

$$\prod_{i=1}^{n}(g^{ID_i^{-1}} \bmod p)$$
$$\because \prod_{i=1}^{n}(g^{ID_i^{-1}} \bmod p) < p$$
$$= g^{\sum_{i=1}^{n}\frac{1}{ID_i}} \bmod p$$

此時，這個攻擊者便可以產生多組使用者 (ID_A, $g^{ID_A^{-1}} \bmod p$)=($(\sum_{i=1}^{n}\frac{1}{ID_i})^{-1}$, $g^{\sum_{i=1}^{n}\frac{1}{ID_i}} \bmod p$)，入侵系統。

4. 結論與後續建議

隨著網際網路的蓬勃發展，越來越多的網路系統利用網路的便利性來提供使用者更方便的使用環境，相對的，網路安全的重要性也日益增加，本研究發現西元 2005 年學者 Chang 與學者 Chang 所提出的兩個無驗證表驗證機制中，其中一個無驗證表驗證機制有著使用者偽裝攻擊(Impersonation Attack)的安全性問題存在，因此，如果使用該驗證機制來驗證遠端的使用者，就必須要特別注意這個安全性問題。

參考文獻

[1] M. Peyravian, N. Zunic, “Methods for protecting password transmission”, Computers & Security, Vol. 19, No. 5, pp. 466-469, 2000.

[2] J.J. Hwang, T.C. Yeh, “Improvement on Peyravian–Zunic’s password authentication schemes”, IEICE Transactions on Communications, Vol. E85-B, No. 4, pp. 823–825, April 2002.

[3] C.L. Lin, T.H. Hwang, “A password authentication scheme with secure password updating”, Computers and Security, Vol. 22, No. 1, pp. 68-72, 2003.

[4] Y.F. Chang, C.C. Chang, “Authentication schemes with no verification table”, Applied Mathematics and computation, Vol. 167, No. 2, pp. 820-832, 2005.

[5] C.K. Chan, L.M. Cheng, “Cryptanalysis of a remote user authentication scheme using smart cards”, IEEE Transaction on Consumer Electronic, Vol. 46, No. 4, pp. 992-993, 2000.

[6] C.C. Chang, S.J. Hwang, “Some forgery attack on a remote user authentication scheme using smart cards”, Informatics, Vol. 14, No. 3, pp. 189-294, 2004.