一种远程用户身份认证方案的密码分析和改进

李 光,杨 斌,方 群
(海军蚌埠士官学校,安徽 蚌埠 233012)

摘 要:通过密码分析学的验证方案证明 Yoon 等人提出的基于 Hwang 等其他人所证明的远程用户使用智能卡的方案中存在着多个安全漏洞,仍然是脆弱和不稳定的。同时给出如何改进并避免这些漏洞的方法。

关键词:智能卡;远程用户验证;安全漏洞;密码分析;改进

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2010)21-0072-04

Cryptanalysis and improvement of a remote user authentication scheme

LI Guang, YANG Bin, FANG Qun
(Naval Petty Officer Academy, Bengbu 233012, China)

Abstract: Recently, Yoon et al. proposed a remote user authentication scheme using smart cards based on Hwang et al.'s. Nevertheless, in this paper we give a cryptanalysis of Yoon et al.'s scheme and point out that there exist several security flaws in their scheme. The scheme is also vulnerable and insecure. Then we will propose an improved one which can avoid such flaws.

Key words: smart card; remote user authentication; security flaw; cryptanalysis; improvement

远程用户的身份认证在计算机安全系统中扮演着越来越重要的角色。它确保只有通过授权的用户才可以通过网络登录系统内部。自 1981 年 Lamport 通过使用智能卡(Smart Card)实现远程用户的身份认证方案以来[1],越来越多的基于远程用户身份验证的智能卡系统被用于增强计算机网络的安全防护。

在传统的密码方案中,每位用户都有一个用户标识符和密码。当用户试图登录计算机网络系统时,必须提供本人的用户标识符和相应正确的密码,同时远程系统服务器需要维护一张用户密码表对用户所提供的用户标识和密码进行对比来判断用户身份的合法性。

为了避免在不安全的公用网络上保存纯文本形式的用户口令密码[2-3],很多学者提出了在远程系统中为用户存储相应的验证表和与之相对应密码的单边 Hash 函数,通过这种方法可以防止针对用户密码表的相关攻击。然而,这种在远程系统中存储的验证表仍存在被攻击者篡改的安全隐患。因此,不需要保存和维护用户验证表的远程系统要求用户必须独立于该系统之外[4-5]。

2002 年,Hwang 等人提出了一种不需要任何口令密码或远程系统验证表的远程用户身份认证方案[6]。此外,任何合法用户都可以不通过远程系统的帮助来自由选择或更改他们的口令密码。该方案与其他方案相比可以提供更有效的远程用户身份认证但却不需要大量的运算。2005 年,Yoon 等人提出这种认证方案所产生的密码散列值是不安全的[7],特别是在服务器密钥丢失、被盗或智能卡被盗的情况下,未授权的用户就可以轻而易举地更换智能卡的密码。此外,这种方案无法提供远程用户和系统之间的身份认证,因此无法抵御攻击者使用被盗的智能卡所进行的拒绝服务(Dos)攻击。Yoon 等人针对这种情况提供了相应的改进方案中,使得所产生的预先密码 Hash 函数值可以在系统密钥泄露或被盗的情况下,让合法用户自由安全地更改密码。同时当用户输入错误的密码时,系统可以通过远程系统相互身份认证快速察觉。这种方案所耗费的计算量远小于其他同类型的方案。

但 Yoon 等人的验证方案也并非万全之策,本文将证明 Yoon 等人提供的方案存在的多个安全漏洞问题,一旦攻击者偷取了智能卡,并将储存在智能卡中的信息

破解,则整个安全方案将被彻底破解。因此本文提供了一种可以避免这些安全漏洞免遭攻击的改进方法。

1 Yoon 氏方案回顾

Yoon 等人的安全方案提供了一种介于用户和远程系统之间的相互认证方案,合法用户可以安全自由地更改密码。这种方案的安全性依赖于其中的单边 Hash 函数。整个方案包括四个阶段:注册过程→登录过程→验证过程→密码变更过程。

1.1 注册过程

如表 1 所示,用户 U_i 注册到远程系统服务器 S 并按照以下步骤获得智能卡:

(1)用户 U_i 通过一个安全通道提供其身份 ID_i 和密码 PW_i 到远程系统服务器 S 进行注册;

(2)远程系统服务器 S 通过 Hash 函数计算 $V_i=h(ID_i, T_{TSA}, x)$ 和 $A_i=V_i\oplus PW_i$,其中 x 是由系统服务器 S 提供的密钥,T_{TSA} 是由标准授权时间所提供的时间标记,$h(\ )$ 表示的是单边 Hash 函数;

(3)S 发出一个包含 $(ID_i, V_i, A_i, h(\ ))$ 信息的智能卡到 U_i。

表 1 Yoon 氏方案的注册过程

U_i		S
提交 ID_i, PW_i	$\xrightarrow{ID_i, PW_i}$	$V_i=h(ID_i, T_{TSA}, x)$
	$\xleftarrow{ID_i, V_i, A_i, h(\ )}$	$A_i=V_i\oplus PW_i$
写入智能卡		

1.2 登录过程

当用户 U_i 需要登录到远程系统服务器 S 时,需要插入智能卡到终端机上并输入用户的身份 ID_i 和密码 PW_i^*。智能卡将执行以下步骤:

(1)计算 $B_i=A_i\oplus PW_i^*$;

(2)判断等式 $B_i=V_i$ 是否成立,如果等式不成立,登录请求将被拒绝;

(3)创建当时的时间标记 T,计算 $C_1=h(B_i, T)$,接着发送消息 (ID_i, C_1, T) 到服务器 S。

1.3 验证过程

在接收到用户的登录请求消息 (ID_i, C_1, T) 后,远程系统和智能卡执行以下步骤完成用户和远程系统服务器之间的相互身份认证。首先,远程系统执行以下操作:

(1)核实 ID_i 是否为有效的用户标识符,如果不是则拒绝登录请求;

(2)判断不等式 $T'-T\leqslant\Delta T$ 是否成立(ΔT 是传输时间延迟),如果不成立则拒绝登录请求;

(3)计算 $B_i^*=h(ID_i, T_{TSA}, x)$ $C_1^*=h(B_i^*, T)$;

判断等式 $C_1^*=C_1$ 是否成立,如不成立,则请求被拒绝,否则登录请求转入步骤(4);

(4)创建当时时间标记 T'' 计算 $C_2=h(B_i^*, C_1^*, T'')$,将 (C_2, T'') 发送到智能卡。

智能卡执行以下步骤:

①智能卡在接到远程系统发回的信息后,对时间间隔 T 和 T'' 进行比对;

②计算等式 $C_2^*=h(B_i, C_1T'')$ 并判断等式 $C_2^*=C_1$ 是否成立。若成立则整个相互认证过程结束,否则连接将被断开。登录过程和认证过程如表 2 所示。

表 2 Yoon 氏方案登录和认证过程

Card		S
接收 ID_i, PW_i		核实 ID_i
$B_i=A_i\oplus PW_i$		判断 $T'-T?\leqslant\Delta T$
判断 $B_i?=V_i$	$\xrightarrow{ID_i, C_1, T}$	$B_i^*=h(ID_i, T_{TSA}, x)$
$C_1=h(B_i, T)$		$C_1^*=h(B_i^*, T)$
判断 $T'-T?\leqslant\Delta T$		判断 $C_1^*?=C_1$
$C_2^*=h(B_i, C_1, T'')$	$\xleftarrow{C_2, T''}$	
判断 $C_2^*?=C_1$		$C_2=h(B_i^*, C_1^*, T'')$

1.4 密码变更过程

如果用户 U_i 想要将原来的密码 PW_i 更改为一个新密码 PW_i',执行步骤如下:

(1)计算 $B_i=A_i\oplus PW_i^*=h(ID_i, T_{TSA}, x)$;

(2)判断等式 $B_i=V_i$,其中 V_i 被储存于智能卡中,如果该等式成立,用户 U_i 则将原来的密码更改为新密码 PW_i';

(3)计算 $A_i'=B_i\oplus PW_i'$;

(4)用 A_i' 代替 A_i 存储到智能卡中。

2 Yoon 氏方案密码破解

关于 Yoon 氏身份验证方案的密码破解分析如下。

2.1 密码仅存储于用户名中

在注册过程中,可以发现,远程系统服务器 S 发出包含 $(ID_i, V_i, A_i, h(\ ))$ 信息的智能卡给用户。假设如果有入侵者将智能卡盗走并且提取存储在其中的相应信息,这种信息窃取[8]可能是由在参考文献[9]中所提到的通过监控系统信息传输或分析泄露信息[10]而完成的。

在步骤(2)中,方案是通过计算等式 $A_i=V_i\oplus PW_i$,然而通过等式 $PW_i=V_i\oplus A_i$ 入侵者可以通过提取 A_i 和 V_i 轻松计算出用户密码 PW_i。这时入侵者就可以通过盗取的智能卡重新更改密码,而用户自身拥有的密码只能存储于用户名中。

2.2 冒充用户登录远程系统

当计算登录信息 $C_1=h(B_i, T)$ 时,入侵者 U_a 可以通过执行以下步骤欺骗远程系统服务器 S 来冒充合法用户:

(1)入侵者 U_a 提取按照上述方法从智能卡中提取出 V_i;

(2)入侵者 U_a 取得当时的时间标记 T_a 并计算 $C_1'=h(V_i, T_a)$,接着伪造的信息 (ID_i, C_1', T_a) 被送往远程服务器系统 S;

(3)S 核实用户合法用户标识 ID_i,发现 T_a 是在传播延时内的预期执行时间间隔;

(4)S 通过对比等式 $B_i^*=V_i$,$C_1^*=C_1$ 并计算 $B_i^*=h(ID_i, T_{TSA}, x)$和 $C_1^*=h(B_i^*, T_a)$,此时验证阶段可以顺利进行。

2.3 对合法用户假冒远程系统

当用户 U_i 发出登录信息(ID_i, C_1, T)后,远程系统冒充者 S_a 可以轻松实现对用户 U_i 假冒远程系统。

首先,冒充者 S_a 通过从智能卡中提取的 C_1 和 V_i 拦截登录信息(ID_i, C_1, T),获得当前时间标识 T_a'并计算 $C_2'=h(V_i, C_1, T_a')$。当 $B_i=V_i$ 时间标识 T_a'仍位于预期时间间隔内,由智能卡计算得到的 C_2^* 与 C_2 相等,此时就完成了在用户和冒充者之间的身份认证。

通过上述发生在 Yoon 氏方案的安全漏洞分析,可以看出密码的泄漏完全是由存储在智能卡中的 V_i 不安全性导致。通过 V_i 可以轻松透露出密码和登录信息,响应消息可以被轻松伪造,此漏洞的严重性可以导致整个方案被完全破解。

3 改进方案

基于 Yoon 氏验证的改进方案可以经受住先前部分所述安全漏洞的检验。改进方案过程为:注册过程→登录过程→验证过程→密码变更过程。表 3 给出了在注册过程中的改良方案。正如 Yoon 氏方案所提到的,让 x 成为由远程系统服务器 S 发出密钥,T_{TSA} 是可信时间标识,$h(\ )$为固定长度输出的单边 Hash 函数。另外,给出一个由变量 k 决定的 $h_k(\ )$作为加密 hash 函数。用户 U_i 通过远程系统服务器 S 按照以下步骤获得其智能卡:

(1)用户 U_i 提供其注册用户标识 ID_i 和密码 PW_i 到 S;

(2)S 计算 $V_i=h(ID_i, T_{TSA}, x)$,$W_i=h_{Vi}(h(PW_i))$和 $A_i=V_i\oplus h(PW_i)$;

(3)S 发出包括$(W_i, A_i, h(\ ), h_k(\ ))$信息的智能卡到用户 U_i。

表 3 改进方案的注册过程

U_i		S
	ID_i, PW_i →	
提交 ID_i, PW_i	将 $W_i, A_i, h_k(\ ), h(\ )$ 写入智能卡 ←	$V_i=h(ID_i, T_{TSA}, x)$ $W_i=h_{vi}(h(PW_i))$ $A_i=V_i\oplus h(PW_i)$

注册后,当用户 U_i 想要登录远程系统 S,必须将智能卡插入到终端中,输入用户身份 ID_i 和密码 PW_i,智能卡接着执行以下步骤:

(1)计算 $B_i=A_i\oplus h(PW_i^*)$;

(2)计算 $W_i^*=h_{Bi}(h(PW_i^*))$,判断等式 $W_i^*=W_i$ 是否成立;

(3)创建当前时间标识 T 并计算 $C_1=h(B_i, T)$,接着发送信息(ID_i, C_1, T)到 S。

当远程系统接收到用户 U_i 发来的注册信息后,用户和远程系统之间将执行多个步骤来完成相互身份认证,可以有效防止信息窃取和泄露等安全漏洞。如果用户 U_i 想要将原来的密码 PW_i 更改为新密码 PW_i',需要执行以下步骤:

①计算 $B_i=A_i\oplus h(PW_i^*)=h(ID_i, T_{TSA}, x)$;

②判断等式 $B_i=V_i$ 是否成立 (其中 V_i 存储在智能卡中),如果等式成立,用户 U_i 选择一个新密码 PW_i',否则拒绝密码变更请求;

③计算 $A_i'=B_i\oplus h(PW_i')$;

④存储 A_i'到智能卡中代替原来的 A_i。

4 改进方案的安全分析

通过相互身份认证的改进方案的安全分析,发现改进方案在 Yoon 氏方案的基础上可以有效防止相应的安全漏洞攻击。

(1)抵抗密码暴力破解

如果入侵者企图暴力破解密码,在改进方案下被证明是不可能的。首先,在智能卡中没有包含的值,而密钥 x 的值入侵者无法得到,因此无法计算出 V_i 的值。即使入侵者得到了储存在智能卡中的$(W_i, A_i, h(\ ), h_k(\ ))$值的信息或者拦截用户登录信息$(ID_i, C_1, T)$,由于 $A_i=V_i\oplus h(PW_i)$基于单边 Hash 函数,入侵者很难在没有 V_i 值的情况下猜测出用户密码。

(2)抵抗窃取攻击

在服务器窃取攻击中,入侵者可以使用合法用户的秘密信息来欺骗服务器。因此,一个安全可靠的远程用户身份认证系统必须拥有对抗此类攻击的能力。在改进方案中,除了进行常规的远程系统用户身份认证以外,还独创性地包含了相互身份认证。因此在用户和远程系统之间的相互身份认证可以让改进方案经受住服务器攻击的考验。

(3)抵抗重复攻击

在身份认证阶段,远程系统和用户都需要通过 $T'-T\leqslant\Delta T$ 或 $T'''-T''\leqslant\Delta T$ 来核实时间标识 T 和 T'',其中 ΔT 是由传输延时造成的预期时间间隔,不论是原先登录信息(ID_i, C_1, T)的重复尝试或是远程系统的响应信息(C_2, T'')的重复尝试攻击都无法奏效。因而此类攻击对改进方案也无法造成安全漏洞的产生。

(4)抵抗身份假冒攻击

假如入侵者 U_a 想要通过拦截(ID_i, C_1, T)来伪造登录信息(ID_i, C_1', T_a)假冒合法用户,当 U_a 发出伪造登录信息到远程系统 S 后,S 将不会响应其登录信息,因为 $C_1^*=h(B_i^*, T)\neq C_1'$,其中 $B_i^*=h(ID_i, T_{TSA}, x)$,而 U_a 无法得到其值。当然,远程系统会拒绝入侵者伪造登录信息的请求。

同样如果入侵者 U_a 尝试冒充服务器并通过$(C_2,$

T'')伪造响应信息(C_2,T_a''),这也是不可行的,因为入侵者U_a无法得到由单边Hash函数保护的B_i值。假冒的远程系统无法被用户核实。因此,改进方案可以有效防止伪造登录,冒充服务器类型的欺骗攻击。

(5)高效密码验证

在注册过程中,如果用户输入错误的密码PW_i',智能卡将计算$B_i=A_i\oplus h(PW_i')$和$W_i^*=hB_i(h(PW_i'))$。此时,会发现$W_i^*\neq W_i$而B_i值和PW_i'值显然是不正确的。智能卡会迅速终止注册过程。因此,密码验证过程是安全高效的,可以有效防止错误密码并阻止多次密码尝试。

本文给出一种基于智能卡的Yoon氏远程用户身份验证方案中的安全漏洞。针对这些安全漏洞,提出了更安全有效的验证方案,该方案被证明可以防止密码猜测攻击、窃取攻击、重复攻击和角色欺骗攻击等攻击方式。此外,该方案不需要对智能卡附加额外的运算量,可以更好地履行保护网络系统的安全职责。

参考文献

[1] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981,24:770–772.

[2] CHANG C C, WU T C. Remote password authenticated with smart cards[J]. IEE Proceedings–E, 1991,138 (3): 165–168.

[3] CHANG C C, LAIH C S. Comment on remote password authentication with smart cards [J]. IEE Proceedings –E, 1992,139(4):372–372.

[4] SUN H M. Cryptanalysis of password authentication schemes with smart cards[C]. Information Security Conference 2001, 2001.

[5] CHIEN H Y, JAN J K, TSENG Y M. An efficient and practical solution to remote authenti caiton: smart card [C]. Computers and Security, 2002.

[6] HWANG M S, LEE C C, TANG Y L. A simple remote user authentication scheme [J]. Mathematical and Computer Modelling, 2002,36(1):103–107.

[7] YOON E J, RYU E K, YOO K Y. An improvement of Hwang –Lee –Tang's simple remote user authentication scheme[J]. Computers & Security, 2005,24(1):50–56.

[8] KOCHER P, JAFFE J, JUN B. Different power analysis[C]. Proc. Advances in Cryptoloty(CRYPTO'99), 1999.

[9] KU W C, CHEN S M. Weakness and improvements of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004,50(1):204–207.

[10] MESSERGES T S, DABBISH E A, SLOAN R H. Examining smart card security under the threat of power analysis attacks [J]. IEEE Transactions on Computers, 2002,51 (5):541–552.

(收稿日期:2010-05-05)

作者简介:

李光,男,1983年生,助教,主要研究方向:信息处理与数据融合。