基于动态 ID的远程认证方案的改进

段晓毅 张其善 刘建伟

(北京航空航天大学 电子信息工程学院, 北京 100083)

摘 要: 智能卡由于具有低功耗、安全计算和便携性的特点,常常被用做身份认证终端.基于静态口令的认证方案不能由用户选择密钥并且需要在服务器保存一个密钥表,而基于动态 ID的方案能解决这些问题.提出了新的方案,指出 Liao-Lee-Hwang方案中不能抗偷窃攻击的缺点,并在其基础上做了改进.新的改进方案不仅继承了原方案中抗猜测攻击、实现共同认证、服务器不会泄露用户密钥的的优点,同时也避免了窃取攻击;并且新的改进方案在计算量上也小于 Liao-Lee-Hwang的方案.

关 键 词: 认证; 智能卡; 密钥; 偷窃攻击

中图分类号: TN 918

文献标识码: A **文 章 编 号**: 1001-5965(2007)05-0565-03

Improved security enhancement for a dynamic ID-based remote user authentication scheme

Duan Xiaoyi Zhang Qishan Liu Jianwei

(School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Smart cards are secure, compact and intelligent data carriers, which can offers strong authentication and guaranteed non-repudiation. With the traditional authentication solution, the static password is rarely altered and maintained in the verifier table on the server. This is bringing forth the important attacks of replay attacks, guessing attacks, modication attacks, and stolen-verier attacks. However, the dynamic ID-based authentication solution can solve the problem. I-En Liao et al proposed a dynamic ID-based user authentication scheme using smart cards. The scheme has a lot of advantages, such as avoiding a variety of attacks, mutual authentication and no verifier table, but it can't resist to stolen attack. A improved scheme was presented to remedy their weaknesses. Compare with Liao-Lee-Hwang's scheme, the improved scheme not only avoid stolen attacks but also reduce the computational costs.

Key words: authentication; smart cards; password; stolen attack

基于密钥的远程认证方案是用来检查一个用户登录请求合法性的. 1981年 Lamport在文献[1]中介绍了一种基于智能卡的远程密钥认证方案,随后 Hwang等在文献[2]中、Ku等在文献[3]中、Yoon等在文献[4]中不断地提高远程认证方案的有效性和安全性.然而,这些方案是基于静态 ID的,而静态 ID容易在登录信息中向攻击者泄露部分的用户信息.解决此问题的办法是在每次登录时使用动态 ID.

2004年,Das等人在文献[5]中提出了一种使用智能卡的动态 ID远程认证方案,称此方案能抗重放、猜测、伪造、内部、偷窃等攻击. 2005年,Liao-Lee_Hwang在文献[6]中指出文献[5]中的方案存在不能抗猜测攻击、不能实现共同认证和服务器会泄露用户密钥的缺陷,并在文献[5]的基础上做了改进.作者发现在 Liao-Lee-Hwang的方案中任何一个人偷走了智能卡,可以不需要用户密钥就能成功地登录远程系统.本文简介 Liao-

收稿日期: 2006-07-10

基金项目: 国家自然科学基金资助项目(60672102)

作者简介: 段晓毅(1979-),男,贵州六盘水人,博士生, duanxiaoyi@ee.buaa.edu.cn.

Lee-Hwang的改进方案[6],指出 Liao-Lee-Hwang 方案的缺陷,改进方案并进行安全性分析,以抗智能卡遭窃后的攻击.

1 Liao-Lee-Hwang的方案

Liao-Lee-Hwnag的方案同样也由注册、登录和密钥修改三个阶段组成.最后的密钥修改阶段和文献[5]中的一样,仅对文献[5]中的注册和登录阶段进行了修改. Liao-Lee-Hwang的修改方案具体如下.

本文中所使用的符号定义:

U为用户; P_W 为用户的密钥; S为远程系统; $h()$为一个单向函数; $\oplus$为比特异或运算; $A \Rightarrow B$: M为 A通过安全通道把 M 传送给 B; $A \rightarrow B$:M 为 A通过公开通道把 M 传送给 B; x为 S的密钥; y为在每个用户的智能卡中存储的 S的一个安全认证码; $\|$为连接操 .

1.1 注册阶段

1) 当用户 U_i需要注册到远程系统时执行此过程,用户 U_i选择个人密钥并计算 $h(P_{W_i})$,并把个人 ID_i和 $h(P_{W_i})$ 通过安全通道提交给远程系统.

2) 当接收到注册请求,系统计算 $N_i = h(P_{W_i}) \oplus h(x \| ID_i)$,x表示系统的密钥.

3) S使用单向函数 $h()$,N_i和 y(y是存储在每个用户智能卡中系统的密钥)对智能卡进行个人化操作.

4) $S \Rightarrow U_i$:智能卡.

1.2 登录阶段

在此阶段中, S可以认证 U_i, U_i也可以认证 S.当一个用户 U_i希望登录到 S时,他执行如下操作:

U_i把智能卡插入到终端的读卡器中,并输入密钥 P_{W_i}.

智能卡通过下式计算动态 $\mathbf{D}$, $C_{\mathbf{D}_i} = h(P_{W_i}) \oplus h(N_i \oplus y \oplus T)$, $B_i = h(C_{\mathbf{D}_i} \oplus h(P_{W_i}))$, $C_i = h(T \oplus N_i \oplus B_i \oplus y)$, T是当前的时间戳.

$U_i \rightarrow S: C_{\mathbf{D}_i}, N_i, C_i, T$.

当 S在 T^1 时接收到 U_i的登录请求后,通过以下步骤认证用户 U_i:

1) 如果 $(T^1 - T) \geq \triangle T$, $\triangle T$表示允许的最大网络延时, T^1 是当前的时间戳,则拒绝登录请求.

2) 计算 $h(P_{W_i}) = C_{\mathbf{D}_i} \oplus h(N_i \oplus y \oplus T)$.

3) 计算 $B_i^1 = h(C_{\mathbf{D}_i} \oplus h(P_{W_i}))$, $C_i^1 = h(T \oplus N_i \oplus B_i^1 \oplus y)$.检查 C_i^1是否等于 C_i,如果相等,则接受用户 U_i的登录请求,否则终止操作.

4) S计算 $D = h(T^1 \oplus N_i \oplus B_i^1 \oplus y)$.

5) $S \rightarrow U_i$: (D, T^1).

当在 T^{11}时刻到 S返回的 (D, T^1)后, U_i通过以下步骤来验证 S:

1) 如果 $(T^{11} - T^1) \geq \triangle T$, T^{11}是当前的时间戳,则智能卡报错并退出此登录.

2) 把接收到的 D与 $h(T^{11} \oplus N_i \oplus B_i \oplus y)$进行比较,如果相同,则 U_i认证 S,否则智能卡报错并退出此次登录请求.

1.3 Liao-Lee-Hwang的方案的缺陷

Liao-Lee-Hwang的方案并不能防止所有的攻击,至少其不能防止窃取攻击,对 Liao-Lee-Hwang 方案的攻击如下.

当一个攻击者 A得到用户 U_i的智能卡后,他可以在不知道用户密钥 P_W 的情况下通过以下步骤成功地登录到 S.

A把智能卡插入到终端的读卡器中,并任意输入一个密钥 P_{WC}.智能卡进行如下的计算:

$C_{\mathbf{D}_i} = h(P_{WC}) \oplus h(N_i \oplus y \oplus T)$.

$B_i = h(C_{\mathbf{D}_i} \oplus h(P_{WC})) = h(h(N_i \oplus y \oplus T))$.

$C_i = h(T \oplus N_i \oplus B_i \oplus y) = h(t \oplus N_i \oplus h(N_i \oplus y \oplus T) \oplus y)$, T是当前的时间戳.

$U_i \rightarrow S: C_{\mathbf{D}_i}, N_i, C_i, T$.

认证阶段

当在 T^1 时 S接收到 U_i的登录请求后,通过以下步骤认证用户 U_i:

1) 如果 $(T^1 - T) \geq \triangle T$, T^1 是当前的时间戳,则拒绝登录请求.

2) 计算 $h(P_{W_i}) = C_{\mathbf{D}_i} \oplus h(N_i \oplus y \oplus T) = h(P_{WC})$.

3) $B_i^1 = h(C_{\mathbf{D}_i} \oplus h(P_{W_i})) = h(C_{\mathbf{D}_i} \oplus h(P_{WC})) = h(h(N_i \oplus y \oplus T))$.

4) $C_i^1 = h(T \oplus N_i \oplus B_i^1 \oplus y) = h(T \oplus N_i \oplus h(N_i \oplus y \oplus T) \oplus y) = C_i$.

所以攻击者 A成功地登录到 S.

如上所示,不需知道用户个人密钥的情况下,攻击者 A可以成功地登录到远程系统.这与 Liao-Lee-Hwang在文献[2]中所说的能抗智能卡遭窃后的攻击不相符合,在不降低 Liao-Lee-Hwang方案安全性的基础上,作者对其做了进一步的改进,以防止窃取攻击.

2 改进方案

本节介绍一种基于 Liao-Lee-Hwang的改进方

案,本方案即保留了 Liao-Lee-Hwang方案中的安全性,又能防止针对于上面所说的攻击.改进的方案分为三个阶段,注册阶段,认证阶段,密钥修改阶段,其中密钥修改阶段和 Liao-Lee-Hwang等在文献[6]中的一样,具体过程如下.

2.1 注册阶段

注册阶段和 Liao-Lee-Hwang在文献[6]中的一样,其过程是:

1) 当一个用户 U_i需要注册到一个远程系统时执行此过程,用户 U_i选择一个个人密钥并计算 $h(P_{W_i})$,并把个人 ID_i和 $h(P_{W_i})$通过安全通道送到远程系统.

2) 当接收到注册请求,远程系统计算 $N_i = h(P_{W_i}) \oplus h(x \| ID_i)$.

x表示远程系统的一个密钥.

3) 使用单向函数 $h()$,N_i和 y(y是存储在每个用户智能卡中的远程系统的密钥)对智能卡进行个人化操作.

4) $S \Rightarrow U_i$:智能卡.

2.2 认证阶段

改进后的认证阶段分为三个部分,登录部分,S认证 U部分,U认证 S部分.

2.2.1 登录部分

当一个用户 U_i希望登录到 S时,执行如下操作:

U_i把智能卡插入到终端的读卡器中,并输入密钥 P_{W_i},智能卡进行如下操作:

$C_{D_i} = h(h(P_{W_i}) \oplus N_i \oplus y \oplus T) = h(h(x \| ID_i) \oplus y \oplus T)$.

$C_i = h(T \oplus C_{D_i} \oplus y)$,$T$是当前的时间戳.

$U_i \rightarrow S: C_{D_i}, N_i, C_i, T$.

2.2.2 S认证 U部分

当 S在 T^1接收到登录信息 (C_{D_i}, N_i, C_i, T)后,S通过如下步骤认证用户 U_i的合法性:

1) 验证 T和 T^1的时间间隔是否合法,如果 $(T^1 - T) \geq \triangle T$,则远程系统拒绝登录请求.

2) 计算 $C^1_{D_i} = h(h(x \| ID_i) \oplus y \oplus T)$.

3) $C^1_i = h(T \oplus C^1_{D_i} \oplus y)$.

4) 验证是否 C^1_i等于 C_i,如果相同,则 S接收 U_i登录请求,否则拒绝并中止操作.

5) 计算 $D = h(T^1 \oplus T \oplus C^1_{D_i} \oplus y)$.

6) $S \rightarrow U_i$: (D, T^1).

2.2.3 U认证 S部分

当 U_i在接收到 S返回的 (D, T^1)后,智能卡进行如下操作来认证 S.

1) 验证 T^{11}和 T^1的时间间隔是否合法,如果 $(T^{11} - T^1) \geq \triangle T$,则智能卡报错并退出此次登录请示.

2) 智能卡计算 $D^1 = h(T^1 \oplus T \oplus C_{D_i} \oplus y)$.

3) 检查 D是否等于 D^1,如果不相等,则智能卡报错并退出,否则 U_i成功认证 S.

2.3 修改密钥阶段

当用户 U_i想修改个人密钥时进行此阶段的操作.

1) 用户 U_i把智能卡插入到终端中输入个人密钥 P_{W_i}并请求修改个人密钥.

2) 用户 U_i输入一个新的个人密钥 $P_{W_{NEW}}$.

3) 智能卡计算

$N^1_i = N_i \oplus h(P_{W_i}) \oplus h(P_{W_{NEW}}) = h(x \| ID_i) \oplus h(P_{W_{NEW}})$.

然后 N_i将会被 N^1_i所替代,用户的密钥也由原来的 P_{W_i}替换为 $P_{W_{NEW}}$.

3 安全性分析

如果攻击者 A得到了用户的智能卡,把智能卡插入到终端中,并输入任意的个人密钥 P_{WC},智能卡进行如下操作:

1) $C_{D_i} = h(h(P_{WC}) \oplus N_i \oplus T) = h(h(P_{WC}) \oplus h(P_{W_i}) \oplus h(x \| ID_i) \oplus y \oplus T)$.

2) $C_i = h(T \oplus C_{D_i} \oplus y)$,$T$是当前的时间戳.

3) $U_i \rightarrow S: C_{D_i}, N_i, C_i, T$.

在 S接收到 A的登录请求后执行如下操作.

1) 验证 T和 T^1的时间间隔是否合法,如果 $(T^1 - T) \geq \triangle T$,则远程系统拒绝登录请求.

2) 计算 $C^1_{D_i} = h(h(x \| ID_i) \oplus y \oplus T)$.

3) $C^1_i = h(T \oplus C^1_{D_i} \oplus y) = h(T \oplus h(h(x \| ID_i) \oplus y \oplus T) \oplus y)$.

所以 C^1_i不等于 C_i,则 S拒绝 U_i的登录请求.

4结 束 语

在本文中,作者指出了 Liao-Lee-Hwang方案不能抗窃取攻击的缺陷,并在其基础上做了进一步的改进.与 Liao-Lee-Hwang的方案相比,改进方案具有如下的优点:①解决了 Liao-Lee-Hwang方案中的窃取攻击的问题;②比 Liao-Lee-Hwang方案具有更低的计算复杂性.

(下转第 621页)

时性可以保证.

3.2 目标识别率

在一定时间内,视觉正确识别目标点的次数与总实验次数的比值称为识别率,用以衡量算法效果的优劣.选择了人手常用的抓持动作作为实验动作,此动作包括手指的张开和抓合 2个过程.

实验结果如表 1所示,人手每分钟张合 45次,运动速度正常;每分钟张合 61次,即人手在 1 s的时间完成一次张合运动,此时人手运动速度较快;在这 2种运动速度下,识别率均为 100%;当人手每分钟张合次数大于 72次时,人手速度已非常快,人手操作时几乎不会使用这样的速度.所以本算法可以保证在人手的正常速度下对人手运动进行跟踪识别.

表 1　视觉识别率

实验次数 /min^{-1}	成功次数 /min^{-1}	识别率 /%
45	45	100
61	61	100
72	69	96
81	75	92

4 结 束 语

本文提出了一种利用计算机双目立体视觉实时跟踪、识别人手指尖点的方法.实验结果表明,在人手手指较快的运动速度下,此方法可以保证识别率 100%;并且算法所用时间也远远小于图像采集周期的 40 ms,充分满足实时性要求.该算法不但可以用来识别人手运动,也可以应用于对其它匀速运动目标进行实时跟踪.

参考文献 (References)

[1] Turner M L, Findley R P, Griffin W B, et al. Development and testing of a telemanipulation system with arm and hand motion [C]//Dynamic Systems and Controls. Okamura: ASME, 2000: 1 - 8

[2] Kawasaki, Nakayama H, Mouri K, et al. Virtual teaching based on hand manipulability for multi-fingered robots [C]//Proc IEEE Int Conf Rob Autom. Piscataway, NJ: IEEE, 2001, 2: 1388 - 1393

[3] Kang S B, Ikeuchi K. Toward automatic robot instruction from perception-mapping human grasps to manipulator grasps [J]. Robotics and Automation, 1997, 13(1): 81 - 95

[4] Li Jiting, Zhang Yuru, Su Wenkui, et al. Grasp planning and implementation for dexterous hands by human demonstration [C]//Huang Tian. The 11th World Congress in Mechanism and Machine Science. Tianjin: China Machine Press, 2004, 4: 1 - 4

[5] 贾云得. 机器视觉 [M]. 北京:科学出版社, 2000
Jia Yunde. Computer vision [M]. Beijing: Science Press, 2000 (in Chinese)

(责任编辑:文丽芳)

(上接第 567页)

参考文献 (References)

[1] Lamport L. Password authentication with insecure communication [J]. Communication of ACM, 1981, 24: 770 - 772

[2] Hwang M S, Li L H. A new remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2000, 46(1): 28 - 30

[3] Ku W C, Chen S M. Weakness and improvements of an efficient password based user authentication scheme using smart cards [J]. IEEE Trans Consumer Electronic, 2004, 50(1): 204 - 207

[4] Yoon E J, Ryu E K, Yoo K Y. Further improvement of an efficient password based remote user authentication scheme using smart cards [J]. IEEE Trans Consumer Electronic, 2004, 50(2): 612 - 614

[5] Manik Lal Das, Ashutosh Saxena, Ved P Gulati. A dynamic ID-based remote user authentication scheme [J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 629 - 631

[6] Liao I-En, Lee Cheng-Chi, Hwang Min-Shiang. Security enhancement for a dynamic ID-based remote user authentication scheme [C]// Next Generation Web Services Pracitces. Seoul, KOREA: IEEE, 2005

(责任编辑:娄　嘉)