文章编号:1001 - 9081(2006)05 - 1055 - 03

Ku-Chien 远程身份认证方案的安全性分析

张利华[1,2]
(1. 华东交通大学 电气与电子工程学院,江西 南昌 330013;
2. 北京航空航天大学 电子信息工程学院,北京 100083)
(lh_zhang@ee.buaa.edu.cn)

摘 要:Ku-Chien 远程身份认证方案是一种使用智能卡、低开销、实用的口令认证方案。分析了 Ku-Chien 方案的安全性,指出了 Ku-Chien 方案的安全缺陷:不能抵御并行会话攻击和伪造主机攻击。分析了产生安全缺陷的原因:登录阶段用户计算出的秘密信息和认证阶段远程主机计算出的秘密信息具有类似的结构。最后,利用口令更改计数器,给出了一种改进的口令认证方案。该方案允许用户自主选择并更改口令,实现了双向认证;能够抵御重放攻击、内部攻击,具备强安全修复性;能够抵御并行会话攻击和伪造远程主机攻击。

关键词:身份认证;口令;智能卡;安全分析
中图分类号:TP393.08 **文献标识码**:A

Security analysis of Ku-Chien's remote authentication scheme

ZHANG Li-hua[1,2]
(1. *School of Electrical and Electronic Engineering, Eastchina Jiaotong University, Nanchang Jiangxi* 330013, *China;*
2. *School of Electronic and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing* 100083, *China*)

Abstract: Ku-Chien proposed a low cost and practical solution to password authentication using smart cards. The security of Ku-Chien's scheme was analyzed in this paper. It still has some weaknesses: it cannot resist parallel session attack; it also cannot withstand masquerading remote system attack. The reason of faults is due to the similar structure of secure information of login phase and authentication phase. Based on password changing counter, an enhanced password authentication scheme with better security strength was presented. This scheme has many merits: freely choosing and changing passwords; providing mutual authentication; resisting message replaying attack and inside attack; having strong security reparability; withstanding parallel session attack and remote system attack.

Key words: authentication; password; smart cards; security analysis

口令认证由于容易实现并且用户界面友好,是最简单也是最常用的一种远程身份认证方法。1981 年,Lamport 给出了一个使用口令表的远程身份认证方案[1]。但是,在一般计算机系统上,口令表的安全性是难以保证的。为了提高远程身份认证方案的安全性,2000 年,Hwang 等人[2]提出了基于 ELGamal 算法的使用智能卡的口令认证方案,该方案不需要口令表,能抵御重放攻击,其安全性基于计算有限域上离散对数的困难性。但是 Hwang 方案中用户不能自主选择口令,没有实现双向认证。为了改善算法的效率、降低开销,Sun[3]提出了一种基于单向 hash 函数的使用智能卡的口令认证方案,该方案计算和通信开销小,是一种效率很高的方案。Chien 等人[4]在此基础上提出了一个改进方案,用户能够自主选择密钥、实现了用户和远程主机的双向认证。Hsu[5]对 Chien 方案和 Sun 方案进行了安全分析,指出 Chien 方案不能抵御并行会话攻击,Sun 方案不能抵御口令猜测攻击。Ku 等人[6]也对 Chien 方案进行了安全分析,针对 Chien 方案不能抵御重放攻击、内部攻击和弱安全修复性提出了改进方案:Ku-Chien 方案,该方案是一个低开销、实用的、安全性较强的、使用智能卡的口令认证方案。

本文进一步分析了 Ku-Chien 方案的安全性,指出了该方案的安全缺陷。同时分析了产生安全缺陷的原因,并针对 Ku-Chien 方案不能抵御并行会话攻击和假冒远程主机攻击的安全缺陷,给出了一种改进的、使用智能卡的口令认证方案,能够实现较高的安全性。

1 Ku-Chien 方案

为叙述方便,全文作如下约定:

RS:可信的第三方即注册中心;AS:远程主机;$h(\cdot)$:安全 Hash 函数;U_i:合法用户;U_a:入侵者;T_*:当前时戳;ΔT:最大允许时延;$\Rightarrow$:安全信道;$\rightarrow$一般信道。

1.1 注册阶段

RS 生成如下参数:$h(\cdot)$;系统密钥 x_s。U_i 是请求 RS 注册的第 i 个用户,向 RS 提交其身份标识 ID_i 和 PW_i,智能卡和 RS 执行下面的步骤:

$R1$:智能卡生成随机数 b,计算 $h(PW_i \oplus b)$,$U_i \Rightarrow RS$:$(ID_i, h(PW_i \oplus b))$;

$R2$:如果是第一次注册,RS 令口令更改次数 $n = 0$ 并存入数据库,否则,令 $n = n + 1$,计算 $R = h(EID_i \oplus x_s) \oplus h(b \oplus PW_i)$,其中 $EID_i = (ID_i \| n)$;

$R3$:$RS \Rightarrow U_i$'$Smartcards$:$(h(\cdot), R, x_s, b)$。

1.2 登录阶段

$L1$:当 U_i 登录 AS 时,将智能卡插入读写器,输入 ID_i 和

收稿日期:2005 - 11 - 07;**修订日期**:2006 - 01 - 12 **基金项目**:国家自然科学基金资助项目(60271012)
作者简介:张利华(1972 -),男,湖北京山人,副教授,博士研究生,主要研究方向:网络安全、移动 Ad Hoc 网络、无线传感器网络.

PW_i,智能卡计算 $c_1 = R \oplus h(b \oplus PW_i)$;$c_2 = h(c_1 \oplus T_1)$;

$L2: U_i \rightarrow AS: C = (ID_i, T_1, c_2)$。

1.3 认证阶段

$A1: AS$ 在时间 T' 收到信息 C 后,验证 ID_i 是否合法,判断 $T' - T_1 \leqslant \Delta T$ 是否成立。如否,拒绝登录请求。如果成立,AS 计算 $c_2^* = h(h(EID_i \oplus x_s) \oplus T_1)$,判断 c_2^* 是否等于 c_2,如相等,AS 则接收 U_i 的登录请求,同时计算 $c_3 = h(h(EID_i \oplus x_s) \oplus T_2)$;反之,$AS$ 则拒绝 U_i 的登录请求;

$A2: AS \rightarrow U_i: (T_2, c_3)$;

$A3$:智能卡在时间 T'' 收到 (T_2, c_3) 后,如果 $T'' - T_2 \geqslant \Delta T$ 或 $T_2 = T_1$,智能卡中止协议。如否,计算并判断 $c_3^* = h(c_1 \oplus T_2)$ 是否等于 c_3,如果成立,则远程主机 AS 的合法性得到验证;反之,则智能卡中止登录 AS。

1.4 口令更改阶段

当 U_i 要将口令改为 PW_{new},用户将智能卡插入合法终端的读写器,输入 ID_i 和 PW_i,智能卡和终端之间完成相互认证后,用户选择进行口令更改,并根据提示输入新口令:

$C1$:智能卡计算 $R_{new} = R \oplus h(b \oplus PW_i) \oplus h(b \oplus PW_{new})$

$C2$:用 R_{new} 取代 R,并存入卡中。

2 Ku-Chien 方案的安全性分析

Ku-Chien 方案能够很好地抵御重放攻击、内部攻击,具备强安全可修复性[6],但是仍然有以下的缺陷:不能抵御并行会话攻击和伪造主机攻击。

2.1 并行会话攻击

U_a 在不知道 U_i 的口令的情况下,可以通过监听 U_i 和 AS 间的通信来假冒 U_i 登录 AS:

(1) 当 U_i 在登录阶段发送 (ID_i, T_1, c_2) 至 AS,认证 U_i 的合法性后 AS 返回 (T_2, c_3) 至 U_i,此时 U_a 截获 (T_2, c_3);

(2) U_a 假冒 U_i 重新开始一个新的登录过程,发送 (ID_i, T_2, c_2^*) 给 AS,其中 $c_2^* = c_3$;

(3) 因为 $c_2^* = c_3 = h(h(EID_i \oplus x_s) \oplus T_2)$,$AS$ 接受 U_a 的登录请求;

(4) AS 返回 (T_3, c_3^*),其中 $c_3^* = h(c_1 \oplus T_3)$,$U_a$ 截获 (T_3, c_3^*)。

至此,U_a 成功假冒 U_i 登录了 AS,并通过认证。

2.2 假冒远程主机攻击

U_a 可以通过以下方式假冒合法远程主机:

(1) 在登录阶段的第 2 步,U_a 截获 U_i 登录 AS 时的信息 (ID_i, T_1, c_2),直接令 $c_3^* = c_2$,$U_a \rightarrow U_i: (T_2^*, c_3^*)$;

(2) 因为 $h(c_1 \oplus T_2) c_3^*$,而且由于省略了登录阶段的第一步,T_2^* 的合法性能够通过 U_i 的检验,因此,U_a 被认为是远程合法主机;至此,U_a 成功仿冒合法远程主机。

3 改进的远程身份认证方案

分析上面的两种攻击方案可以发现,Ku-Chien 方案之所以不能抵御并行会话攻击和伪造主机攻击,是因为 c_2 和 c_3 具有类似的结构。只要间隔时间足够短,攻击者就能够在不知道系统密钥和用户口令的情况下假冒合法用户或假冒合法主机。因此,通过改变 c_3 的结构可以达到抵御并行会话攻击和伪造主机攻击的目的。

改进的远程身份认证方案同样包括 4 个阶段:注册阶段、登录阶段、认证阶段和口令更改阶段,其注册阶段、登录阶段、认证阶段如图 1 所示。

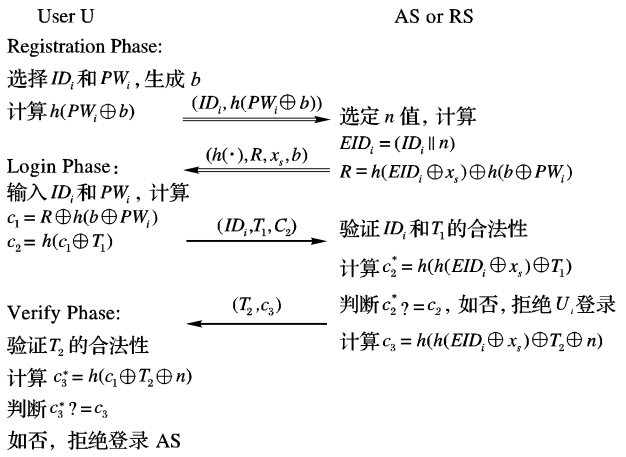

图 1 改进的远程身份认证方案

其注册阶段、登录阶段和口令更改阶段和 Ku-Chien 方案一样,认证阶段如下:

$NA1: AS$ 在时间 T' 收到信息 C 后,验证 ID_i 是否合法,判断 $T' - T_1 \leqslant \Delta T$ 是否成立。如否,拒绝登录请求。如果成立,AS 计算 $c_2^* = h(h(EID_i \oplus x_s) \oplus T_1)$,判断 c_2^* 是否等于 c_2,如相等,AS 则接收 U_i 的登录请求,同时计算 $c_3 = h(h(EID_i \oplus x_s) \oplus T_2 \oplus n)$;反之,$AS$ 则拒绝 U_i 的登录请求;

$NA2: AS \rightarrow U_i: (T_2, c_3)$;

$NA3$:智能卡在时间 T'' 收到 (T_2, c_3) 后,如果 $T'' - T_1 \geqslant \Delta T$ 或 $T_2 = T_1$,智能卡中止协议。如否,计算并判断 $c_3^* = h(c_1 \oplus T_2 \oplus n)$ 是否等于 c_3,如果成立,则远程主机 AS 的合法性得到验证;反之,则智能卡中止登录 AS。

4 改进方案的安全性分析

结论 1:改进的口令认证方案允许用户自主选择并更改口令,实现了双向认证。

结论 2:改进的口令认证方案能够抵御重放攻击、内部攻击,具备强安全修复性。

结论 3:改进的口令认证方案能够抵御并行会话攻击和假冒合法用户攻击。

结论 1 和结论 2 的证明可参考文献[6],下面证明结论 3。

4.1 抵御并行会话攻击

证明 U_a 在不知道 U_i 的口令的情况下,通过监听 U_i 和 AS 间的通信准备假冒 U_i 来登录 AS:

(1) 当 U_i 在登录阶段发送 (ID_i, T_1, c_2) 至 AS,AS 认证 U_i 的合法性后返回 (T_2, c_3) 至 U_i,此时 U_a 截获信息 (T_2, c_3);

(2) U_a 假冒 U_i 重新开始一个新的登录过程,发送 (ID_i, T_2, c_2^*) 给 AS,其中 $c_2^* = c_3$;

(3) 因为 $c_2^* = c_3 \neq h(h(EID_i \oplus x_s) \oplus T_2 \oplus n)$,$AS$ 拒绝 U_a 的登录请求。U_a 无法假冒 U_i 登录 AS,不能通过认证。

4.2 抵御假冒远程主机攻击

证明 分以下两种情况:

(1) U_a 在不知道 U_i 的口令和系统密钥的情况下,通过监听 U_i 和 AS 间的通信准备假冒合法远程主机。在登录阶段的第 2 步,U_a 截获 U_i 登录 AS 时的信息 (ID_i, T_1, c_2),直接令 $c_3^* = c_2$,$U_a \rightarrow U_i: (T_2^*, c_3^*)$;因为 $h(c_1 \oplus T_2 \oplus n) \neq c_3^*$,$U_a$ 不

能通过认证,因此无法假冒远程主机。

(2) 即使 U_a 偶然获得 U_i 的口令和系统密钥,在登录阶段的第2步,U_a 截获 U_i 登录 AS 时的信息(ID_i,T_1,c_2),由于不知道 n 的值,U_a 不能正确计算出能被 U_i 认证的 c_3,从而不能发起攻击来假冒合法远程主机。

该改进的方案和 Ku-Chien 方案相比,只是增加了一个异或操作,效率和 Ku-Chien 方案相当,但安全性更高。

参考文献:

[1] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24(11):770 - 772.

[2] HWANG MS, LI LH. A new remote authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2000, 46(1):28 - 30.

[3] SUN HM. An efficient remote use authentication scheme using smart cards[J]. IEEE Transactions on Consumer Electronics, 2000, 46(4):958 - 961.

[4] CHIEN HY, JAN JK, TSING YM. An efficient and practical solution to remote authentication: Smart Cards[J]. Computers and Security, 2002, 21(4):372 - 375.

[5] HSU CL. Security of two remote user authentication schemes using smart cards[J]. IEEE Transactions on Consumer Electronics, 2003, 49(4):1196 - 1198.

[6] KU WC, CHEN SM. Weaknesses and improvements of an efficient password base remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2004, 50(1):204 - 206.

(上接第 1052 页)

光的图片,(d)和(e)分别是采用 RGB 三通道融合和本文方法进行融合得到的融合结果。从结果中可以看到这两种方法都能够产生具有过渡效果的融合结果,而且细节保持良好,但是(d)中被融合区域色彩的色调发生了变化,绿色被明显加强。(e)在额头、下巴和脖子等人脸弧度变化比较平缓的区域和(c)非常接近,高光和非高光区域过渡很自然。进一步的 TL 平面内的分析见图 10 所示。

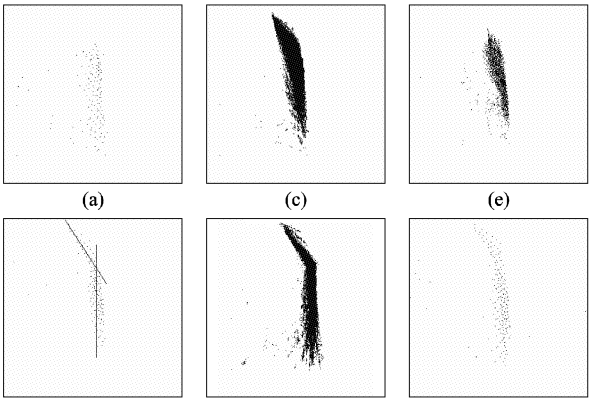

图 10　融合结果分析

图 10 中(a)和(b)分别是非高光皮肤和高光皮肤在 TL 平面内的投影,图 10(b)中两条相交的直线分别是体反射向量和面反射向量。图 10(c)是图 9(d)的融合部分在 TL 平面的投影。图 10(d)是图 9(e)中的融合部分在 TL 平面的投影。图 10(e)是对(a)和(b)直接融合得到的结果。图 10(f)是图 9(c)中融合部分像素在 TL 平面中的投影。

从图 10 中可以看出采用本文融合方法的(d)图和单侧光照图片(f)图比较接近,从 TL 平面看该方法很好地保持了人脸的肤色特征。而(c)和(e)代表的方法则呈现出像素过多地向中间聚集的情况,且像素的分布呈现椭圆形分布。反映在图片上,这两种方法处理的结果使像素亮度比较集中在平均亮度水平,而色度的变化范围增大,同时皮肤在 TL 平面中的 Γ 形分布特征也被丢失。

4　结语

本文根据双反射模型的人脸皮肤高光分析结果,对 TSL 色彩空间表示的两张人脸照片进行 T 和 L 分量的融合。融合中在考虑了样条系数的同时也充分考虑了皮肤在 TL 平面中分布特点,使 TL 中像素沿 Γ 形区域插值。实验表明两张照片中的人脸皮肤能够很好的融合,细节清晰,高光部分能够很好的过渡。没有出现 RGB 三通道融合过程中经常出现的融合结果中色彩出现错误的现象。

参考文献:

[1] 陶霖密,彭振云,徐光祐. 人体的肤色特征[J]. 软件学报,2001,12(7):1032 - 1040.

[2] 陈缎生,刘政凯. 彩色图像人脸高光区域的自动检测与校正方法[J]. 软件学报,2003,14(11):1900 - 1906.

[3] TERRILLON JC, SHIRAZI MN, FUKAMACHI H, *et al.* Comparative performance of different skin chrominance models and chrominance spaces for the automatic detection of human faces in color images[A]. Proceedings of the 4th international Conference on automatic face and gesture recognition[C]. IEEE Computer Society, 2000. 54 - 61.

[4] 何光宏,潘英俊,吴芳. 基于肤色特征和动态聚类的彩色人脸检测[J]. 光电工程,2004,(11): 47 - 50.

[5] PETER J. BURT AND EDWARD H. Adelson. A Multiresolution spline with application to image mosaics[J]. ACM Transactions on Graphics, 1983, 2(4):217 - 236.

[6] LEE WS, WU Y. Nadia Magnenat-Thalmann[A]. Cloning and Aging in a VR Family[C]. Proc. IEEE VR' 99 (Virtual Reality), 1999.

[7] ADELSON EH, ANDERSON CH, BERGEN JR, *et al.* Pyramid methods in image processing[J]. RCA Engineer, 1984, 29(6).

[8] PIGHIN F, HECKER J, LISCHINSKI D, *et al.* Synthesizing Realistic Facial Expression from Photographs[A]. Computer Graphics, Annual Conference Series, SIGGRAPH[C], 1998. 75 - 84.

[9] LEE WS. Nadia Magnenat Thalmann[A]. Head Modeling from Pictures and Morphing in 3D with Image Metamorphosis based on triangulation [C]. CAPTECH'98, Geneva, 1998. 254 - 267.

[10] KLINKER GJ, SHAFER SA, KANADE T. A physical approach to color image understanding[J]. International Journal of Computer Vision, 1990, 4(1):7 - 38.

[11] STRÖRRING M, GANUM E, ANDERSEN HJ. Estimation of the illumination colour using highlights from human skin[A]. Proceedings of the 1st International Conference on Color in Graphics and Image Processing[C]. Saint Etienne, 2000.

[12] FINLAYSON G, SCHAEFER G. Single surface colour constancy [A]. Scottsdale, Arizona, 7th Color Imaging Conference[C], 1999. 106 - 113.

[13] SHAFER SA. Using color to separate reflection components[J]. Color Research and Application, 1985, 10(4):210 - 218.

[14] KLINKER GJ, SHAFER SA, KANADE T. A physical approach to color image understanding[J]. International Journal of Computer Vision, 1990, 4(1):7 - 38.