改进抵御攻击算法的电子公文收发系统①

胡 洋，苏 琳

(广东培正学院 计算机科学与工程系，广州 510830)

摘 要：对电子公文收发系统的抵御攻击能力着手研究，分析并使用智能卡加强电子公文的安全管理。首先介绍了 Hwang-Li 方案抵御攻击的原理，分析其安全性的不足，并提出改进的方案，验证了抵御几种攻击的有效性。最后，在我校的公文收发系统中进行实践性检验。

关键词：公文收发系统；抵御攻击；Hwang-Li 方案改进；安全

Sending and Receiving Electronic Document System Based on Attack Resistance Algorithm

HU Yang, SU Lin

(Computer Science and Engineering Department, Guangdong Peizheng College, Guangzhou 510830, China)

Abstract: For sending and receiving electronic document System, the capablitity to resist attack is researched. The smart card is used to strengthen the safety management about electronic document. First, the principle about Hwang-L scheme to resist attack is introduced in this paper. The shortcomings of security system is analyzed, and improved scheme is brought out. The improved scheme is enumerated to many kinds forms about attack to be analyzed. Finally, the inspection was carried out in sending and receiving electronic document System in our college.

Keywords: sending and receiving electronic document system; resist an attack; Hwang-L improved scheme; security

1 前言

公文的方便撰写和功能完善的收发管理是电子公文收发系统的根本内容;公文收发要解决好同其他相关系统的无缝集成;电子公文的上传和下达必须建立在安全的基础上;公文公章的加盖和认证、完善的公章管理和用印管理及监督;对发送的公文进行电子签名、完整性计算和保密传输，对收到的公文进行解密、合法性验证和完整性验证;对行文过程的监控和自动错误处理;完善的人员、权限管理等。Hwang 和 Li[1]提出了一个新的使用智能卡的远程用户认证方案，它主要基于 ElGamal 密码体制.随后 Chan 和 Cheng[2,3]等人对 Hwang-Li 方案进行了密码分析，并指出其算法的漏洞所在。我们在 Hwang-Li 方案的基础上，提供了一个新的远程用户认证方案，方案在注册阶段和登录阶段加强了安全性，增加了身份的认证鉴别协议。下面先介绍一下 Hwang-Li 方案理论。

2 Hwang-Li方案理论

2000 年，Min-Shiang Hwang 和 Li-Hua Li 提出了基于 EiGarnai 公钥密码体制的远程用户鉴别方案[1]，该方案结合了智能卡技术，采用时间戳机制，可防止重放攻击，且无需在服务器端保留用户名/口令列表文件。

该方案分为三个阶段:注册阶段、登录阶段和认证阶段。访问系统前，每个新用户必须提交用户名进行注册，并由系统通过安全信道颁发智能卡和口令;当注册用户访问系统的时候、用户将智能卡插入读卡设备并输入用户名私口令进行登录。

尽管该方案仅需服务器端保留一个秘密参数，避免了恶意攻击者利用系统漏洞窃取已注册用户口令文件的危险，但经过分析，该方案仍然存在安全隐患:

① 认证服务器 AS 不保留注册用户的 ID，且在认证过程仅对登录用户的 ID 从格式上进行校验，为攻击

① 基金项目:广东省广东培正学院重点科研项目(pz2009008)
收稿时间:2010-08-11;收到修改稿时间:2010-09-09

者提供了可乘之机，也不利于系统进行访问跟踪审计。

② 注册用户的口令由认证服务器 AS 计算生成，用户不具有自主选择和修改口令的权限，即使发现口令已经泄露，也不能自行进行修改，大大降低了系统的安全性和可用性。

③ 口令猜测攻击

所有注册用户获得的智能卡中保存的数据相同，即智能卡对所有用户具有通用性;此外，登录过程中没有对智能卡持有者的合法性进行认证，方案的安全性最终弱化为用户口令，获得智能卡的攻击者可进行口令猜测攻击:其用猜测得的口令尝试登录系统，只要登录成功，此次的登录口令便是用户口令。

3 智能卡认证设计方案的改进

针对 Hwang-Li 方案的安全隐患，在此提出了一个新的远程用户认证方案，该方案也包括初始阶段、注册阶段、登录阶段和认证阶段.，主要在注册阶段和登录阶段加强了安全性，增加了身份的认证鉴别协议.协议的设计基于 Schnorr[4]利用离散对数问题的难解性而构造的身份鉴别协议以及于秀源等[5,6]提出的利用二元一次不定方程解的不定性而设计加密体制思想.这样可以有效地抵御类似 Chan-Cheng 和 Chang-Hwang 的攻击。

3.1 初始阶段

系统管理者(System Adminnistrator，以下简称 SA)选定如下参数:

(1) 一个大素数 p;

(2) 单向函数 h(.);

(3) 系统密钥 xs.

SA 做如下工作:

① 选取大素数 p，使得在 Z_p^* 中离散对数是难解的，q 是 p-1 的大素因子，取安全素数 t，满足 $q \geq 2^t$;

② 求出 $g \in Z_p^*$,满足 g 的阶为 q;

③ 选定单向函数 f(.);

④ 决定系统密钥 x_s;

⑤ 建立一个安全的签名方案，该方案的秘密签名算法为 Sig_{SA}，公开的验证算法为 Ver_{SA}.

3.2 注册阶段

① 用户 U_i 秘密选取一个随机素数 $k(0 \leq k \leq q-1)$，计算 $y=g^k \bmod p$，并将 y 发送给 SA;

② SA 产生一个针对用户 U_i 的签名 $S = Sig_{SA}(ID_i, y)$，从而得出证书 $C(A)=(ID_i, y,s)$;

③ SA 分配一个唯一只对用户 U_i 的注册号 Ri，并记录在案，然后计算用户 U_i 的远程服务口令 PW_i:$PW_i=(ID_i \oplus R_i)^{XS} \bmod p$;

④ SA 为用户 U_i 随机选取整数 c_i $(1 \leq c_i \leq 2^t)$，并将带有参数(C(A), f, p, c_i)的智能卡和相应的服务口令 PW_i 发送给 U_i。

3.3 登录阶段

假定在某时刻 T_1，用户 U_i 向 SA 提出登录要求，则先通过智能卡作如下工作:

① 产生随机数 r，满足 $0 \leq r \leq q-l$,gcd(r,k)=1，并计算 $u=g^r \pmod p$;

② 计算 $J_1=(ID_i \oplus R_i)^r \bmod p$;

③ 计算 $t=f(T_i \oplus PW_i) \bmod p-1$;

④ 计算 $m=(ID_i)^t \bmod p$;

⑤ 计算 $J_2=m(PW_i)^r \bmod p$;

⑥ 利用 Euclid 算法求出满足方程 $a_ik + b_ir=c_i$ 的整数 a_i, b_i;

⑦ 将信息 $L_i=(C(A), u, J_1, J_2, a_i, b_i, T_1)$传送给 SA.

3.4 认证阶段

假定 SA 在时刻 T2 收到了用户 Ui 的要求登录信息 $L^i = (C(A), u, J^1, J^2, a^i, b^i, T^1)$，则做如下工作:

① 验证用户 U_i 的身份有效性:

SA 通过检验 Ver (ID_i, y)来验证签名的有效性;并通过验证 $y^{ai}u^{bi} = g^{ci} \pmod p$是否成立来确定用户 U_i 身份的有效性.如果不成立,则拒绝 Ui 的登录要求;

②检验 $T_2 - T_1 \leq \Delta T$ 是否成立，ΔT 表示由于传输信息所需要的一个合理的间歇时间.如果不成立，则拒绝 U_i 的登录要求;

③验证 $J_2=(J_1)^{xs}(ID_i)^{f(T1 \oplus PWi)} \bmod p$ 是否成立.如果不成立，则拒绝 U_i 的登录要求.

4 安全性分析

本节将针对两种攻击方法来加以说明本设计的安全性。

4.1 关于 Chan-Cheng 和 Chang-Hwang 的攻击

在认证阶段，除了需要签名的验证算法 Ver_{SA} 来验证以外，还增加了一个身份的认证鉴别协议，该协议主要将 Schnorr 的身份鉴别协议与二元一次不定方程解的不定性结合起来，构造新的身份鉴别协议，从而保证了安全性，进而有效地抵御了在认证阶段 Chan-Cheng 和 Chang-Hwang 的攻击。另外在注册阶

段，按照 Chan-Cheng 和 Chang-Hwang 的攻击方法，假定合法用户 Bob 想创造出(ID_j, PW_j)，则他选择一个数 R，使得 $ID_j \oplus R=(ID_b \oplus R)^r \bmod p$，这里 r 是一个随机数，然后根据 $PW_j=(PW_b)^r \bmod p$ 即计算出 PW_j。但以上攻击法其实是不能成立的，因为注册号 R 是由 SA 惟一分配给每个用户的，并登记在案，以备核对，这样假冒者就不可能进行成功登录。

4.2 关于 Shen-Lin-Hwang 的攻击

假定 Bob 从公共网上获取了某个用户 U_k 的登录信息 $L_k = (C(A), u, J_1, J_2, a_k, b_k, T_1)$，想假冒用户 U_k 进行登录.他首先通过 $ID_b= ID_p^r \bmod p$ 计算出 ID_b，这里 r 是一个满足 gcd(r, p)=1 的随机数，然后他将 ID_b 提供给 SA, SA 收到注册要求后为其分配一个惟一的注册号 R，同时发送给他一张智能卡和相应的口令 PW_b($PW_b = (ID_i \oplus R_i)^{xs} \bmod p$。Bob 然后通过 $PW_k = (PW_b)^{\bar{r}} \bmod p$ 来计算出 PW_k，但因为此时 PW_k 只能满足式子 $PW_k=(ID_k)^{xs} \bmod p$，却不能满足式子 $PW_k = (ID_k \oplus R_k)^{xs} \bmod p$，因此该口令 PW_k 是不正确的，这样 Bob 就无法假冒用户 U_k 的身份进行登录了。

5 在公文收发系统中电子盖章的应用

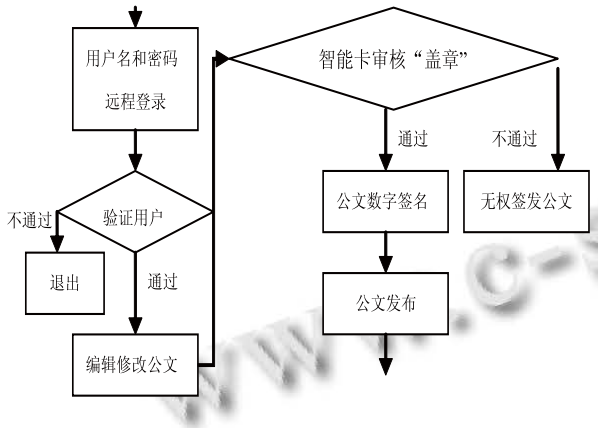

图 1 公文收发系统电子盖章工作流程

本改进方案在我校的电子公文收发系统中得到了应用及测试，智能卡在系统中的使用扮演实际公章的盖印过程。具体过程为：在系统使用之前先给具有公章管理身份的用户分配智能卡，并进行相应的初始化和注册过程，使得用户名和智能卡是唯一匹配。发公文用户首先通过用户名和密码登录本系统进行公文的编辑和修改。当公文经过校验后进行审核签发时，必需使用与用户名相对应的智能卡进行电子公文的“盖章”——也就是上述方案的利用智能卡登录和认证阶段，当智能卡和当前用户名匹配并审核认证通过（“电子盖章”），同时利用数字签名技术对公文进行加密并分发。收公文用户登录后即可得到签名后的的公文内容，具体过程如图 1 所示。通过改进可使公文的签发过程具有更高的安全性、完整性和不可抵赖性等特点。

6 结语

本文提供了一种新的抵御攻击的认证方案.在该方案中，基于 Schnorr 提出的身份鉴别协议以及二元一次不定方程解的不定性而设计了一个身份认证鉴别协议，可以抵御不同阶段的各种攻击，从而增强了安全性。并在公文收发系统中得以应用，为以后电子公文管理等方面的提升起到了一定的促进作用，而且在本方案中所用到的算法也不多，计算量并不大，从而认为该方案是安全有效的。

本文作者创新点: 1) 研究了一种新的身份认证鉴别协议，增强了抵御攻击的能力；2) 在公文收发系统的公文签发时应用本方案实现智能卡的电子盖章的效果，加强了公文管理的安全性。

参考文献

1 Hwang MS, Li LH. A new remote user authentication scheme suing smart_caxds. IEEE Trans. on Consumer Electronics, 2000,46(4):992–993.

2 Chan C K, Cheng L M. Cryptanalysis of a remote user authentication scheme using smart cards. IEEE Trans. Consumer Electron, 2000,46(3):992–993.

3 胡鸣,张小兵,等.一种新的基于智能卡的身份认证方案.微计算机信息,2010,1(3):41–42.

4 张先红.数字签名原理与技术.北京:机械工业出版社, 2004.95–97,141–144.

5 吴挺,于秀源.一个安全有效的身份鉴别协议与对应的数字签名方案.通信学报,2002,23(7):70–75.

6 谢琪,于秀源.有指定秘书的(t, n)门限群签名体制.高校应用数学学报,2005,20(2):156–160.