一种改进的公钥证书系统 [1]

王常杰 张方国 王育民
(西安电子科技大学 ISN 重点实验室 西安 710071)

摘 要 该文针对目前公钥证书系统中存在的安全漏洞，在 Bruno Crispo 等人 (1996) 和 F. Bergadano 等人 (1997) 的工作基础上，给出了一种改进的公钥证书系统．该改进的方案不仅可以抵抗外来攻击，也可以防止来自系统内部的欺诈．

关键词 证书，CA 服务器，RA 服务器，注销
中图号 TN918.1

1 引 言

在一个分布式系统中，两个用户之间为了确认对方的身份，并建立一个共享的秘密会话密钥，通常有以下两种方案：

(1) 两个远端用户在通信前，需要向一个被系统内各用户完全信任的第三方提出申请，由第三方分配该次通信的会话密钥，然后两个用户使用该密钥实现互相认证和保密通信 [1]．

(2) 每个用户各自产生一对公、私钥，然后提交公钥到可信任的第三方 CA (Certification Authority)，由 CA 对该用户的公钥进行签字，从而产生一个相应的公钥证书，然后各用户可通过某个协议 (如：X.509)，根据每个用户的证书实现相互认证和保密通信 [2-3]．

与方案 (1) 相比 [4]，方案 (2)，即 CA 系统更安全，且每对用户之间的通信不需要可信任第三方的参与，这在大型网络中是非常必要的．CA 系统通过公钥证书和数字签名可以使得从未联系过的两个远端主机可以建立可信任连接，并实现安全的通信．这个特点使得 CA 系统成为电子商务等 Internet 的相关应用中的一个十分重要的底层结构．

但我们注意到，不论是在方案 (1) 或 (2) 中，都作了这样一个假设：即第三方或 CA 是完全可以信任的，而这在实际生活中是不现实的．因而目前的 CA 系统只能有效地抵抗系统外部的攻击，而无法防御来自内部 (如：CA 本身) 的攻击，在下文中，我们将给出具体的例子．

Bruno Crispo 和 Mark Lomas 在文献 [5] 中对现有的 CA 系统作了改进，但这种改进并不完善，本文将在此基础上，对现有 CA 系统作进一步的改进，并给出具体的证书发放、撤消等的步骤，从而实现一个完善的 CA 系统框架．

2 现行 CA 系统的安全漏洞及已有的改进

我们先看一个例子：假设用户 A 和 B 都拥有 CA 发放的公钥证书，且 A 和 B 先前从未有过联系 (这在现实中很常见，如某用户在一个新的网上商店购物)，在通常的 CA 系统中，如 X.509，CA 作为唯一的可信任机构，他虽然不知道 A 的私钥，不能伪造该私钥下的签字，但 CA 可以重新产生一个表示 A 身份的公钥证书和相应的公、私钥对，然后用此证书和相应的私钥签署消息与 B 通信，用户 B 在通信过程中将无法发现这一伪装．甚至，在通信结束后，当发生纠纷时 (若 CA 企图以 A 的身份进行欺诈)，CA 可以声称是 A 丢失原来的私钥，并请求 CA

[1] 1999-11-18 收到，2000-04-17 定稿
国家自然科学基金重点项目 (批准号：19931010) 资助

注销原有证书，发放了一个新证书，作为仲裁者 (如法庭)，将不能确定到底是 CA 冒充了 A 的身份进行欺诈，还是 A 蓄意抵赖，以推卸其该负的责任 (如：网上定货，结帐等)．

为了解决以上问题， Bruno Crispo 和 Mark Lomas 提出一个改进的方案，他们的主要思想是基于权限隔离的原则，这有一点类似于门限方案，即 CA 不再是唯一完全被信任的机构，他的权限被分为了独立的两部分，在实现上即为 CA ，和 RA(Revocation Authority)，其中，CA 负责发放证书，而 RA 负责注销证书，最重要的是，二者管理必须独立，且完全隔离，下面是其方案的逻辑结构：

在图 1 中， CA 在线服务器负责接收各用户的申请请求和所提交的公钥和相关信息，然后提交至 CA 脱线服务器，经验证后产生证书并用其私钥加以签字，由 CA 在线服务器转发并备份存储在本地硬盘．若某个用户发现的私钥被泄露或丢失，则需要向 RA 在线服务器提出注销申请，应包含其私钥的数字签名，若私钥丢失，则需提交其身份证明材料 (该用户首次申请证书时提交的身份证明)， RA 通过验证后，作注销记录，并发给用户注销证明，该证明由 RA 的私钥签字．然后该用户可向 CA 提交其注销证明及新的公钥以产生新的证书．

虽然，改进后的方案使得 CA 无法再通过产生一个新证书来冒充用户 A ，因为通过对照 RA 发布的注销记录很容易确认是 CA 还是 A 的责任．但该方案存在以下几个问题：

(1) 在改进的方案中，虽然最终 CA 的伪装行为可以被发现，但在通信过程中，用户 B 无法确认收到的证书是用户 A 的或者是 CA 伪造的 (当然 B 可以查询公布的注销记录以确定该证书是否已被注销)，所以有可能 CA 进行大量的诈骗后潜逃，在大型网络环境下，由于网络时延和复杂的层次管理，这种可能性更大．

(2) 这种改进的安全性依赖于 CA 和 RA 之间的完全隔离，但在改进的方案中，这种隔离并不是由安全协议来保证，一但二者相互勾结 (在现实中存在这种可能)， CA 将能够冒充所有的用户．

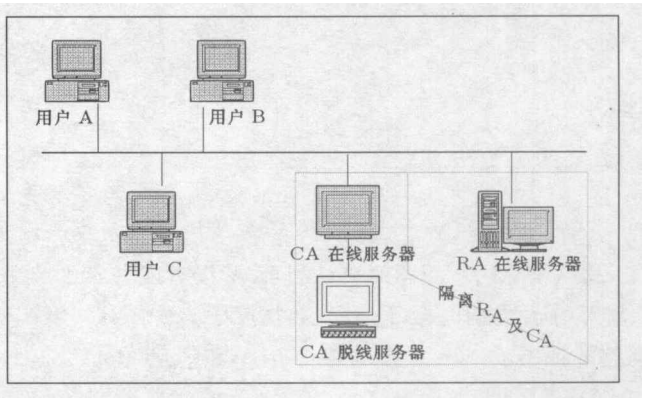

图 1　改进后的 CA 系统的逻辑结构

3 一个改进的公钥证书系统

下面，我们将针对以上存在的问题，在文献 [5,6] 的基础上，设计一个新的 CA 系统，使其不仅可以抵抗来自系统外部的攻击，也可抵抗来自 CA 本身的攻击，甚至是在 CA 与 RA 勾结的情况下．为了方便起见，我们延用 Bruno Crispo 等人方案中标识符号，并采用图 1 所示的逻辑结构．

首先，我们的方案基于如下的假设：

(1) 系统中的每个用户都有不同的用户名或网络标识符.

(2) 系统中每个用户都可以自行产生公、私钥对，且私钥对于其他用户，甚至是 CA 或 RA 服务器而言，是保密的.

(3) 我们假设方案中所用到的公钥算法及 Hash 函数都具有足够的强度，能够抵抗外来攻击.

(4) 我们认为每个用户有能力安全地存储对方 (某个用户、 CA 或 RA) 发送的每个信息，这将有助于解决日后的争端.

下面，我们给出改进部分的实现协议，包括证书的申请、注销等，并介绍改进的性能.

3.1 用户首次申请证书

(如图 2 示)

(1) 用户 A 首先将身份证明信息 (如：身份证、护照等) 、用户名 $\mathrm{ID_A}$ 提交到 CA 处.

(2) CA 验证 A 的身份后 (同时确认目前 A 没有证书)，将为 A 产生一个证书 CertA′，其中包括 X.509 中的所有内容 [2]，如： A 的用户名 $\mathrm{ID_A}$ 等及 CA 对这些信息的私钥签字. CA 备份该证书，然后将 CertA′ 发给 A .

(3) A 首先验证 CertA′ 上 CA 的签字，然后产生一个足够长的随机数 X_A，将 X_A 安全存储后， A 将 CertA′ 和消息 Msg1: $\{\mathrm{ID_A}, h(X_\mathrm{A}), T_1, \mathrm{Sig}_{s_\mathrm{A}}(\mathrm{ID_A}), T_1)\}$ 提交给 RA，其中 $h(X_\mathrm{A})$ 表示 X_A 的 Hash 函数值， T_1 为时戳 (以下含义相同) .

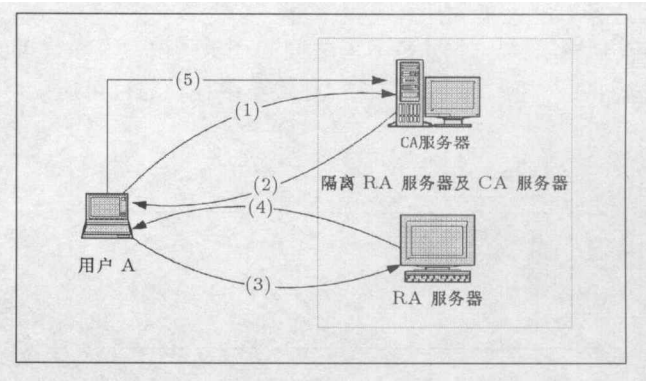

图 2 用户 A 首次申请证书

(4) RA 验证 CA 及 A 的签字后 (同时确认目前 A 没有证书或已被注销)，将 A 的用户名 $\mathrm{ID_A}$ 、相应的 $Y_\mathrm{A}' = h(X_\mathrm{A})$ 及当前时戳 T_2 存入数据库中，然后 RA 用其私钥对 CertA′ 中的内容签字，从而形成完整的证书 CertA . 接着将 CertA 和消息 Msg2: $\{\mathrm{ID_A}, h(X_\mathrm{A}), \mathrm{ID_{RA}}, T_2, \mathrm{Sig}_{s_\mathrm{RA}}(\mathrm{ID_A}, h(X_\mathrm{A}), \mathrm{ID_{RA}}, T_2)\}$ 发送给 A .

(5) A 验证 RA 签字后，保存 CertA，留待以后使用. 同时将 CertA 及消息 Msg3: $\{\mathrm{ID_A}, \mathrm{ID_{CA}}, T_3, \mathrm{Sig}_{s_\mathrm{A}}(\mathrm{ID_A}, \mathrm{ID_{CA}}, T_3)\}$ 发送给 CA 以通知 CertA 开始生效.

3.2 证书的注销与再申请

(如图 3 所示)

若用户不慎泄露或丢失了私钥，则需要用户提出注销申请，由 RA 服务器负责审核注销，并刷新所公布的注销证书列表 RCL(Revocation Certification Lists) .

(1) 首先用户 A 应向 RA 服务器提出注销申请，令 DATA 表示 (注销标识， $\mathrm{ID_A}$, CertA, X_A, T_4)，则 A 向 RA 发送消息 Msg4: $\{\mathrm{DATA}, \mathrm{Sig}_{s_\mathrm{A}}(\mathrm{DATA})\}$，若 A 丢失其私钥，则需提交 DATA 和身份证明信息 (即用户首次申请时提交的身份证明) .

(2) RA 首先验证 A 的签字或提交的身份证明信息，然后验证 A 提交的 X_A 是否满足 $Y_A = h(X_A)$(Y_A 为 RA 的数据库存储的相应的数据)，若都满足，则 RA 从其数据库中注销 A 的记录，并将 CertA 及相关信息 (如：注销时间等) 加入 RCL，通过 Internet 或其他公共网通知系统其他用户刷新其 RCL 记录.

(3) RA 将给 A 返回一个注销证明，即 Msg5: $\{\mathrm{DATA}, \mathrm{Sig}_{s_{\mathrm{RA}}}(\mathrm{DATA})\}$，其中 DATA 为：(注消标识 Msg4, T_5).

(4) A 可以向 CA 申请一个新证书，与首次申请不同的是，A 需要首先提交给 CA 的是 RA 发放的注销证明，而 CA 将分别验证 RA 及用户 A 的签字，其他步骤与首次申请相同.

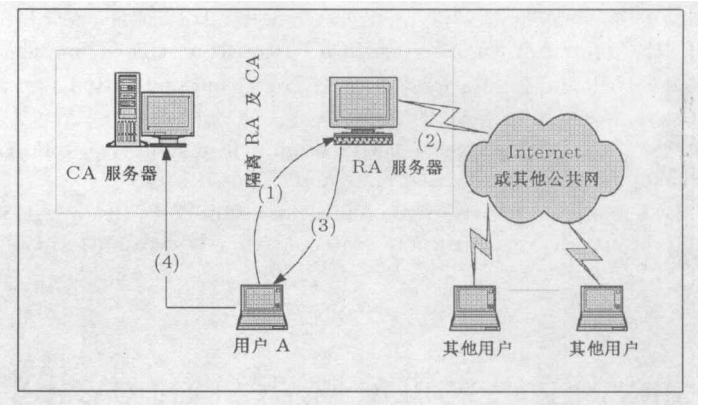

图 3　用户注销当前证书并重新申请

3.3 改进方案的性能

以上，我们介绍了对证书发放、注销及再申请部分的改进，下面我们针对原有系统存在的问题，介绍一下改进后系统的性能. 首先，改进后的方案依然具有原系统的优点，即可抵抗来自系统外的攻击，其次我们来分析它如何抵抗来自内部的攻击，我们分别讨论以下几种情况：

(1) 在改进的方案中，由于证书的产生需要 CA 及 RA 分别用私钥签字，因此，CA 将不能单独伪造用户的证书，以进行大额诈骗后潜逃，用户可以立刻发现这种攻击.

(2) 即使 CA 和 RA 勾结，即 RA 伪造用户 A 的证书注销记录，CA 和 RA 共同伪造 A 的证书，这种攻击依然能够被发现，因为 RA 无法伪造消息 Msg4，其中包含只有 A 才能提供的 X_A，同样的道理，如果 A 申请注销证书后，为了抵赖其用新证书进行的交易，而谎称其从未进行注销，RA 可向仲裁者出示 Msg4，通过验算 $h(X_A)$ 可证明 A 的谎言.

(3) 即使用户 A 不慎丢失其私钥，也可以通过 X_A 及相关的身份证明信息 (如：身份证、护照等) 唯一的确定 A 的身份和注销证书的权限. 有必要指出的是，用户的私钥，在每次通信中都要使用，因此有可能丢失或泄露 (如受到选择明文攻击等)，而与之不同，用户所产生的随机数 X_A 只在申请和注销证书时使用，且下次申请时会重新产生，因此，X_A 丢失和泄露的可能性是非常小的.

4 总　结

以上，我们指出了现有公钥证书系统的安全漏洞，并提出了一种改进的公钥证书系统，并给出了具体的实现协议，通过性能分析，我们看到改进的方案能够有效地防止 CA 伪装为某用户进行欺诈，或用户对其申请注销证书等行为的抵赖，并通过提供足够的签字信息给仲裁者 (如：

法庭)，可解决相关的争议．另外，在目前的公钥证书系统中，还存在这样一个问题，一个不怀好意的用户可能一边申请注销，一边使用其证书 (如：网上购物等)，事后再通过声称其私钥泄露，已申请注销证书，来进行抵赖，由于大型网络的网络时延以及服务器的处理耗时等，可能另一用户无法立刻发现这一欺诈，从而引起争议。相关问题的解决，有待进一步的研究。

参 考 文 献

[1] T. Ts'o, B. C. Neuman, Kerberos, An authentication service for computer networks, IEEE Communication Magazine, 1994, 32(9), 33-38.

[2] William E. Burr, Noel A. Nazario, W. Timothy Polk, A proposed federal PKI using X.509 V3 certificates, http://csrc.nist.gov/pki/papers/ conops, 1997.

[3] S. Kent, Privacy enhancement for Internet electronic mail, Part II: Certificate-based key management, IETF RFC (Internet Engineering Task Force Request For Comments) 1422, Feb, 1993.

[4] M. M. erritt, S. M. Bellovin, Limitations of the Kerberos authentication system, Computer Communication Review, 1990, 20(5), 53-68.

[5] Bruno Crispo, T. Mark, A Lomas: A certification scheme for electronic commerce, Security Protocols Workshop, Cambridge, United Kingdom, 1996, 19-32.

[6] F. Bergadano, B. Crispo, M. Lomas, Strong authentication and privacy with standard browsers, http://maga.di.unito.it/security/projects/ protected/www2/www2.html, 1997.

IMPROVEMENT UPON PUBLIC KEY CERTIFICATION SYSTEM

Wang Changjie Zhang Fangguo Wang Yumin

(*National Key Laboratory on ISN, Xidian University, Xi'an* 710071, China)

Abstract An improvement upon public key certification system, based on the work done by Bruno Crispo(1996) and F. Bergadano(1997), is proposed in this paper, which can solve the security problem of the existing public key certification system. Not only the attack from outside of system but also the fraud of system inner can be resisted by the improved scheme.

Key words Certification, CA server, RA server, Revocation

王常杰： 男，1974 年生，博士生，研究方向为网络安全、电子商务.
张方国： 男，1972 年生，博士生，研究方向为电子商务和 ECC.
王育民： 男，1936 年生，教授，博士生导师，研究方向为通信、信息论、编码、密码.