文章编号:1001 - 9081(2008)04 - 0910 - 02

一种 CA 私钥的容侵保护机制

柴争义,白 浩,张浩军
(河南工业大学 信息科学与工程学院,郑州 450007)
(super_chai@ tom. com; chaizhengyi@ haut. edu. cn)

摘 要:保护 CA 私钥的安全性是整个 PKI 安全的核心。基于 RSA 公钥算法和(t, n)门限密码技术,采用分阶段签名方案,确保私钥在任何时候都无需重构。同时,在私钥产生、分发及使用过程中,即使部分系统部件受到攻击,也不会泄漏 CA 的私钥,CA 仍可以正常工作(即系统具有一定的容侵性)。通过 VC 和 Openssl 对系统进行了实现。

关键词:容侵;认证中心;秘密共享;CA 私钥
中图分类号: TP309;TP393. 08 **文献标志码**:A

An intrusion tolerant protection scheme of CA private key

CHAI Zheng-yi, BAI Hao, ZHANG Hao-jun
(*College of Information Science and Engineering, Henan University of Technology, Zhengzhou Henan* 450007, *China*)

Abstract: Protecting the Certificate Authority (CA) private key is the key issue of the whole Public Key infrastructure (PKI). Based on Rivest-Shamir-Alleman (RSA) and (t, n) secret shared method, the two phrase signature scheme was used to ensure that the private key never be reconstructed at any time. At the same time, in the process of CA generation, delivery and usage, even if some part of the CA was broken, the CA private key was still safe, and CA still could work. At last, the system was realized by VC and Openssl.

Key words: intrusion tolerance; Certificate Authority (CA); secret sharing; CA private key

0 引言

随着电子政务、电子商务等的快速发展,如何建立相互之间的信任关系以及如何保证传输信息的安全性已经成为一个急需解决的问题。公钥基础设施(Public Key infrastructure, PKI)是目前解决这一系列问题最有效的技术。PKI 基于公开密码算法来确保系统信息安全。在 PKI 中,认证中心(Certificate Authority, CA)是其信任中心,交易双方之间的通信和验证都依赖于 CA 所颁发的数字证书。数字证书也就是将一个公开密钥和身份信息绑在一起,用 CA 的私钥签名后得到的数据。由此可见,保证 CA 私钥安全是 CA 安全的核心。CA 的私有密钥一旦泄露,该 CA 签发的所有证书就只能全部作废。一般来说,CA 必须处于联网的状态,以便自动地提供相应的证书服务。而联网设备遭遇网络攻击是不可避免的,由于传统的防火墙和入侵检测系统不可能预知所有未知形式的攻击和安全漏洞,所以仍不可避免被一些攻击取得成功。因此,研究开发能够容忍入侵(简称容侵)的 CA 是十分必要的。

容侵是信息安全领域的一种新策略,它使系统在遭受攻击时,仍能为合法用户提供预期的有效服务。本文基于 RSA 公钥算法和 (t, n) 门限密码技术,通过把 CA 私钥分割成一些份额在 n 个共享服务器中进行分配,并结合分阶段签名方案,确保私钥在任何时候都无需重构。同时,在私钥产生、分发及使用过程中,即使部分系统部件受到攻击,根据这些份额也不能计算出整个私钥,所以不会危及 CA 私钥的安全。

1 理论基础

1.1 RSA 算法

RSA 公钥算法的安全性基于大素数分解的难度。从一个公钥和密文中恢复出明文的难度等价于分解两个大素数之积。设 d 作为 RSA 算法的私钥保存, e,n 作为公钥公开。在 CA 系统中,可以把 d 作为 CA 的私钥。假设要签名的消息为 M $(M < n)$,设 $c = (M^d) \bmod n$ 就得到了签名后的信息 c。验证签名时,设 $m = (c^e) \bmod n$,若 $m = M$,则接收签名,否则拒绝签名。基于 RSA 的安全性,在已知 n,e 的情况下无法求得 d,同样在已知 n,d 的情况下无法获得 e,所以也就很难假冒数字签名,从而保证了 CA 的安全性。

1.2 (t, n) 秘密共享

使用 Shamir 基于拉格朗日插值多项式的方案可以完成 (t, n) 的秘密共享。通过计算把 CA 私钥拆分成互不相同的 n 个份额,然后将 n 个份额放在 n 个不同的服务器上,只有当掌握 t 个分额以后才可以完全恢复出秘密。算法简单描述如下:设 P 是一个大质数,$x \in Zp$,d 是要共享的私钥信息, n 是参与秘密共享的服务器的数量, t 是重构门限。在 Zp 空间内任意选取 $t-1$ 次的多项式 $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$,其中 $f(0) = d$。并计算出 $S_1 = f(1), \cdots, S_t = f(t)$ $(S_i \in Zp)$。给定上述 S_i 值中的任意 t 个,可以通过拉格朗日插值公式计算出 $d = f(0) = \sum_{i=1}^{t} s_i \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j} \bmod p$。相反,如果仅仅知道这些 S_i 中 $t-1$ 个,则由于信息不够而无法确定 $f(x)$,所以不能够求出 d 值。

收稿日期:2007 - 10 - 13;**修回日期**:2007 - 12 - 24。
基金项目:河南省科技攻关基金资助项目(0624260017;072102210029);河南工业大学基金资助项目(07XJC029)。
作者简介:柴争义(1976 -),男,陕西渭南人,讲师,硕士,主要研究方向:网络与信息安全; 白浩(1973 -),男,河南周口人,讲师,硕士,主要研究方向:算法设计; 张浩军(1969 -),男,浙江杭州人,副教授,博士,主要研究方向:网络与信息安全。

但是,如果在签名前对私钥直接重构,就不能保证足够的安全性,所以应该考虑在不重构出私钥的前提下,用私钥份额进行分阶段签名,再将结果进行综合的方案。这样在整个签名计算的过程中,不会有私钥的出现。

1.3　分阶段签名

通过分析 RSA 算法本身的算法规则,发现其在有限域内进行的指数运算结构适用于分阶段签名算法。在保证 $d = \sum_{i=1}^{r} d_i$ 成立的前提下,对于私钥 d 可以做以下分解:$m = c^d \bmod n = c^{d1+d2+\cdots+dr} \bmod n = (c^{dl} \times c^{d2} \times \cdots \times c^{dr}) \bmod n = \left((c^{dl} \bmod n) \times (c^{d2} \bmod n) \times \cdots \times (c^{dr} \bmod n)\right) \bmod n$。可以将上式整理成 $m = \prod_{i=1}^{r} m_r \bmod n (m_r = c^{dr} \bmod n)$。同时观察 Lagrange 插值公式重构多项式 $d = f(0) = \sum_{i=1}^{t} s_i \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j} \bmod p$。这里考虑 p, x_i, x_j 为常数即可。求和是在有限域内进行的,当选取适当的 p 值,并经过预先的重构试验保证 $0 < \sum_{i=1}^{t} s_i \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j} < p$ 成立,那么就有 $d = \sum_{i=1}^{t} s_i \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j}$,这样代数上的求和运算,正可以保证指数运算得以分步进行,即满足 $d = \sum_{i=1}^{r} d_i$。这里的 $d_i = s_i \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j}$。这就结合拉格朗日重构公式和 RSA 算法在有限域内指数运算的特点得出了分阶段签名的方案。

1.4　实现步骤

1.4.1　私钥份额的初始化和分发过程

1) 选取 Hash 函数 $h(x)$ 计算信息摘要 $h(m)$, 初始化 RSA 参数 n, p, q, d, e 等。

2) 随机选取 $t-1$ 次多项式 $f(x) \in Z_p[x]$,令秘密 $d = f(0)$, 随机选择适当小的互异元素 $x_1, x_2, \cdots, x_n \in Z_p$,计算 $S_i = f(x_i) \bmod p (i = 1, \cdots, n)$。

3) 公开 RSA 参数 n, e 以及 $x_1, x_2, \cdots, x_n$,并将 S_i 私钥份额秘密传送给子签名服务器。

1.4.2　签名过程

假设参与对摘要 $h(m)$ 签名的私钥份额持有者为 p_1, p_2, $\cdots$, p_n。

1) 每个参与签名的份额持有者 p_i,使用自己的私钥份额 S_i,计算部分签名 $Sin = h(m)^{S_i} \bmod n$。

2) p_i 根据公开的 x_i 计算 $R_i = \prod_{j \neq i, j=1}^{t} \frac{-x_j}{x_i - x_j}$。

3) p_i 继续计算 $\overline{S_i} = Sin^{R_i} \bmod n$ 发送给签名代理。

4) 签名代理得到发回的子签名计算 $Sig = \prod_{j=1}^{t} \overline{S_i} \bmod n$。$Sig$ 即是最后的签名结果。

1.4.3　签名验证过程

计算 $Sig^e \bmod n$,并且与 $h(m)$ 相比较,如果相等则签名正确。如果验证结果不一致,可以调用另外一个分组继续进行签名,直到验证成功为止。

1.4.4　签名及验证过程的安全性

在整个分阶段签名的执行过程中,子签名机器只把其子签名结果 $\overline{S_i}$ 传送给签名代理者,而签名代理者本身只拥有 RSA 公开的参数 n, e 以及 $x_1, x_2, \cdots, x_n$,它可以使用公钥 e, n 来验证签名的正确性,但本身并不存储私钥。而在系统内部之间的通信过程中,只传递子签名 $\overline{S_i}$,而始终不会出现私钥份额。对于已知 $\overline{S_i}$,私钥份额 S_i 的安全性仍然可以保证,这同样是由指数求模运算的单向性来保证的。最后的签名结果可以用公钥直接验证,在整个过程中始终不出现真正的 CA 私钥,私钥 d 从来没有在单独节点上重构。

2　容侵 CA 系统结构

系统的系统结构如图 1 所示。

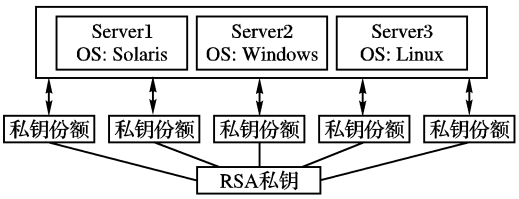

图 1　容侵 CA 的系统结构

系统的安全性分析如下:

1)对单个份额的获取无法恢复出私钥,并且只要获取的私钥份额数在安全门限 t 以下私钥本身仍然安全,改善了原来私钥完整存放于某一台机器上容易泄漏的问题。

2)内部采取使用私钥份额分阶段签名的方式。基于 RSA 公钥算法和 (t, n) 门限密码技术,在不重构私钥的情况下使用私钥份额直接进行子签名,最后由签名代理综合计算出最终签名,提高了 CA 私钥的安全性。

3)构架冗余和分布式的服务器体系结构。在选取兼顾安全和效率的合适 (t, n) 门限方案后,还可以通过多签名代理服务器的结构来提高整体证书签名服务的效率和稳定性。

4) 采用异构平台来存储秘密份额。由于操作系统各自具有自己的特点,通过操作系统差异性来提高入侵者攻击的困难,增加了系统的免疫力。

5)对于存放 RSA 私钥的核心机器,在将私钥份额发送到份额服务器存放后,就可以与系统断开,以保证 CA 私钥的安全。

3　系统实现

系统采用 VC 和 OpenSSL 实现。OpenSSL 是一个开放源代码的软件包,其库文件中包含了完整的加密算法,数字签名算法及证书算法等。使用时可以将它所提供的库文件直接链接到应用程序中,也可以下载压缩包后,自己编译库函数得到库文件。编译后,在 Windows 下得到 libeay32.lib 和 ssleay32.lib 静态库以及两个动态链接 ssleay32.dll 和 libeay32.dll,将其加载到 VC 即可。使用时,在初始化参数的时候做很少的改变,就可以使用相同的代码但采用不同的加密算法进行数据的加密和解密。开发者也可以直接调用或者修改底层的加密算法程序。

证书生成主要包括三个过程:生成密钥对文件;生成证书请求;对证书申请签发生成最终的证书。对应这三个过程的主要命令为:1)genrsa,用来生成基于 RSA 公钥算法的密钥对文件。2)req,根据指定密钥文件,并且输入相关的用户信息,来生成用户证书申请文件,确定密钥对于特定用户的所属关系。3)ca,自动加入证书颁发机构 CA 的信息,使用指定的私钥对证书进行签名,完成证书文件的生成。

(下转第 914 页)

2 数字指纹的提取

本文提出的指纹提取需要原图像,其过程由分块、混沌映射、提取水印密文以及解密得出水印明文等组成。

1)分块。将指纹隐藏图像与原图像同样地分块,使得每块为8×8子块。

2)混沌映射。根据已知的迭代初始值,按照指纹嵌入的方法,得到新的子块顺序序列,这个过程中始终保持隐藏图像与原图像的内在对应关系。

3)提取指纹码。作子块离散余弦变换,得到对应AC系数;由契比雪夫"3σ原则"提取指纹码。即:

$$w = \begin{cases} 1, & |AC' - AC| \geq \dfrac{3\sigma}{2\alpha} \\ 0, & \text{其他} \end{cases} \tag{8}$$

其中,σ为根据其他无标志子块估计得到的噪声标准差。

4)后处理。用纠检错码纠错并恢复指纹码密文序列,以映射初始值为密钥,解出水印明文。

3 实验结果与讨论

基于Matlab 7.0软件平台,可以分析来自StirMark 4.0的各种标准攻击输出图像,并得到提取数字指纹与实际数字指纹的相关程度,由此推断本文所提算法抗击StirMark标准攻击能力,也就是算法的鲁棒性。实验结果如表1所示。

实验中,取嵌入放大系数(实际上即嵌入强度)为5,混沌映射的初始值为0.1001。加密过程按照扫描次序逐段进行,最后一段序列码位数小于密钥位数,其运算以序列码位数为基准。此外,在实施StirMark攻击的过程中,采用的参数基本上是其默认值,但是结合数字指纹本身的应用场合,实验考虑了滤波、行列删除、几何变换等典型攻击,但对解释攻击以及合谋攻击随后也做了讨论。

表1显示出,针对标准StirMark攻击,提取数字指纹与原指纹的相关度均在0.10以上,并且从能够纠一位错的(7,4)汉明码来看,相关度有提升或超过0.2以上的约87.5%。这充分表明,对87.5%的攻击,至少有1~2个具有明确含义的编码单元可以精确提取出来,并且只有在具有初始密钥的条件下才能得到这组代码的实际含义。可见,本文算法具有比较强的鲁棒性。

经过比较分析,发现纠错码发生误判的情况,尤其是模拟打印后扫描过程的随机失真攻击,其误码率在25%到50%之间,其中最常见误码为2位和4位。由于不同攻击可以表示为不同带宽下的传输信道,设计一种稳健的抗干扰指纹方式是保证本文算法鲁棒的重要因素。一个简易的策略就是采用重复次数为9的重复码,则预期码字可根据最大似然估计原则精确恢复。

表1未给出剪切攻击的结果,这是考虑到指纹信息随机散列在所有块内。即使剪切到只有4×4大小的图像子块,攻击者如果没有初始密钥,则仍然无法确定该块是否为"不含指纹"的"干净"块,从而无法实施有效的拼贴攻击。类似地,合谋攻击也难以实施。这是因为混沌密钥的高度敏感性,随意拟合初始密钥不能确定相应的指纹码。

本文算法与既有方法仅仅在基于初始密钥的混沌映射以及子块特征函数选择嵌入/提取的位置方面不同,仍然满足非准可逆条件,从而可能会受到解释攻击,实际应用中尚需结合密码学签名认证机制。

4 结语

从目前大多数已有的指纹/水印算法来看,完美的鲁棒性是不存在的。本文算法在各种StirMark基准测试攻击下仍然能够精确提取指纹代码具有明确含义的组成单元,有明显的鲁棒性,从而可以在一定的协议、密码机制内有效地实现拷贝控制与版权保护功能。

参考文献:

[1] 王炳锡,陈琦,邓峰森. 数字水印技术[M]. 西安:西安电子科技大学出版社,2003.

[2] AMER S, YANG Y. A robust method for fingerprinting digital images[J]. Journal of Electronics, 2001, 18(3):193-203.

[3] PETITCOLAS F A P, STEINEBACH M., RAYNALC F, *et al*. A public automated Web-based evaluation service for watermarking schemes: StirMark Benchmark[C]// Proceedings of Security and Watermarking of Multimedia Contents III, SPIE 4314. San Jose, California, USA: SPIE, 2001:575-584.

[4] PETITCOLAS F A P. Watermarking schemes evaluation[J]. IEEE Signal Processing, 2000,17(5): 58-64.

[5] ZHU C, LIAO X, LI Z. Chaos-based multipurpose image watermarking algorithm[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6):1675-1678.

[6] 王东建,蒋铃鸽,何晨,等. Novel blind robust watermarking based on chaotic mixing[J]. Journal of Shanghai Jiaotong University(Science), 2004, E-9(2):10-15.

(上接第911页)

4 结语

本文提出了一种全新的、基于容侵技术的CA方案,并对其进行了实现。该方案主要利用了(t,n)秘密共享思想结合RSA的分阶段签名,通过理论上的探讨和系统安全性的分析,表明该方案在完成对证书签名的同时,保证了CA私钥的机密性和可用性,并能够容忍一定数量的入侵,达到了容侵的目的。

参考文献:

[1] 周玉洁,冯登国. 公开密钥密码算法及快速实现[M]. 北京:国防工业出版社, 2005:60-61.

[2] 荆继武,冯登国. 一种入侵容忍的CA方案[J]. 软件学报, 2002,13(8):1417-1422.

[3] 喻建平,伍忠东. 容忍入侵的RSA分步签名方案及其在CA中的应用[J]. 计算机科学, 2004,31(11):15-18.

[4] STINSON D R. 密码学的原理与实践[M]. 冯登国, 译. 北京:电子工业出社, 2003: 112-113.

[5] 王丽娜,张焕国,傅建明. 网络入侵研究综述[C]// 网络与信息安全重大研究计划2002年度学术交流论文集. 北京:国家自然科学基金委员会,2003.

[6] 崔竞松,王丽娜. 一种并行容侵系统研究模型RC模型[J]. 计算机学报, 2004,27(4):500-506.

[7] 张险峰,刘锦德. 一种基于门限ECC的入侵容忍CA方案[J]. 计算机应用, 2004,24(2):5-8.