容忍入侵的RSA分步签名方案及其在CA中的应用*)

吴 郁 喻建平 伍忠东

(深圳大学ATR国防科技实验室 深圳518060)

摘 要 本文应用容忍入侵以及脆弱点分析思想,结合当今PKI中关键设施CA中心的私钥保密问题及其签名服务的安全需求,提出了基于容侵思想的CA私钥分存管理以及分步签名的技术方案。该方案着重从算法理论和系统架构两个方面保证系统的容侵特性:即在即使遭受入侵的情况下,该方案可保证系统的服务能力而且CA私钥不会马上泄漏,从而提高了整个系统的安全性。

关键词 信息安全,容忍入侵,RSA,数字签名

An Intrusion Tolerant Scheme of RSA Signature Algorithm

WU Xun YU Jian-Ping WU Zhong-Dong

(ATR Lab for Station Defence Technology, Shenzhen University, Shenzhen 518060)

Abstract This paper researchs vulnerability of the CA private key and solves the security problem by intrusion tolerance method. New CA security scheme ensures that the compromise of a few system components does not compromise the private key. To do so we protect the private key by distributing it across several servers. When execute the improved RSA signature algorithm, private key is never reconstructed at a single location.

Keywords Intrusion tolerant, RSA, Digital signature, CA (Certificate Authority), Threshold cryptography

1 引言

随着信息网络的发展,信息安全的概念和实践不断深化、延拓。信息安全技术的发展经历了以下几个阶段。

第一代信息安全技术:主要集中于访问控制的技术,包括防火墙、加密、认证等技术。主要目的在于严格控制对资源的访问权限,以确保关键信息和资源的安全。

第二代安全:入侵检测。即对已知的攻击行为进行分析和归类以及模型的建立,然后在实际中根据系统的状态来判定是否遭受攻击,并及时触发相关的安全策略对系统或关键信息施行保护。

第三代安全:容忍入侵(Intrusion Tolerant)作为信息安全的最后一道防线,保证系统即使在遭受攻击时信息系统仍然可以连续正确地运行,并同时修复损坏,保障关键信息的安全。容忍入侵理论是网络安全的重要组成部分,国外这方面的研究也处于起步阶段,美国和欧洲都有资助的相关研究项目,比如美国军方的ITTC(Intrusion Tolerance via Threshold Cryptography)、SITAR(Scalable Intrusion Tolerance Architecture),欧洲的AFTIA(Malicious Accidental Fault Tolerance for Internet Application 2000-2003)等。通过对这些项目技术的分析,目前的容忍入侵技术的主要手段是从容错理论和密码技术等方面出发,研究容忍入侵技术和容忍入侵系统的体系结构。尤其是加强对现有系统脆弱点的分析,并根据容忍入侵的思想来加强对脆弱点的保护,从而作为对入侵监测等安全技术的有益补充。

2 关于CA机构的脆弱点分析

随着PKI(Public Key Infrastructure)公钥体系结构安全框架的部署,以及基于电子证书和相关协议的应用的广泛发展,证书颁发授权机构的核心CA(Certificate Authority)中心也逐渐发展起来。根据PKI的特点,数字证书以及一切上层的安全应用(包括SSL安全套阶层协议、S/MINE安全电子邮件传输协议以及SET安全协议等)的可信性最终依赖于受信CA的权威性和安全性,而CA中心中最为敏感的信息就是其自身的私钥(即签名算法时,对信息摘要(HASH值)进行私钥加密所使用的密钥)。如果私钥被攻破或者泄漏,那么任何私钥的持有者就可以随便以受信CA的名义来签发假冒的电子证书,并有得到攻破基于这一证书的任何安全应用的机会,例如最容易实施的中间人攻击。

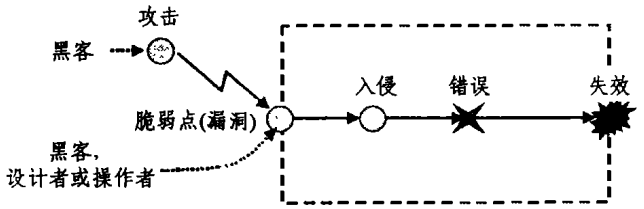


图1 AVI参考模型 (A:攻击(Attack) V:脆弱点(Vulnerability) I:入侵(Intrusion))

应用容忍入侵思想的AVI模型进行分析(如图1),一切对于CA中心的攻击和入侵行为,都是以破坏CA的证书签发服务为目的,而其中最为严重的入侵行为的目的就是窃取或者破坏根证书的私钥,那么对于私钥的存放以及签名方案的实施就是我们所要关注的脆弱点。

目前对于这一脆弱点的防护是采用物理隔离的方案,从一家国内著名CA中心的构架方案中我们看到,CA中心服务器对于审核完毕的资料进行最后的签名制作证书,不是采取在线的方式。存放私钥的服务器一般是采取与外界物理隔离的方式,它只是离线地进行证书的签发。这种保守的安全策略

*)基金项目:国家"八六三"高技术发展计划(2003AA142060)。吴 郁 硕士研究生,研究方向:信息安全。喻建平 博士后,教授,研究方向:密码学、信息安全。伍忠东 博士,副教授,研究方向:信息安全。

是采取牺牲了时间和效率的方式确保安全，而对于今后大量的和时时性要求更高的应用毕竟有很大缺点。我们考虑能否在保证在线签发证书的情况下，采取容忍入侵的思想来提高私钥的安全性，即在假设系统已经遭受攻击的情况下，仍可以保证正常的服务，而且攻击者仍然无法窃取到私钥。

3 多代理分步签名方案

针对于目前最常用的公钥算法：RSA 算法，我们分析了其算法的特点，对其进行了修改，并构造出了 RSA 分步签名算法。采取对私钥经过先发秘密共享算法的计算处理后分存在多个子服务器，在签发时采取用分步签名替代原来一次签名的方式。这样保证了在系统受到攻击时，被攻破的份额数量在安全门限以下时，系统仍能正常工作，且所窃取的份额无法恢复出私钥；此时可以结合入侵监测机制触发相应的安全策略，对系统进行恢复、子份额进行更新，使得攻击者所窃取的份额完全失效，系统重新恢复到安全状态。

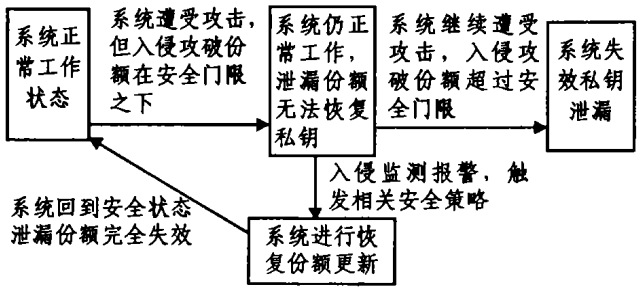


图2 系统状态转化图

图2说明了系统安全状态的转化，可以看出容忍入侵的策略只是对脆弱点（私钥安全性）的进一步防护，即保证系统在遭受攻击时，服务不至于完全崩溃，私钥也不会迅速泄漏。但是整个系统的安全性也要依赖于入侵监测等其他安全手段。

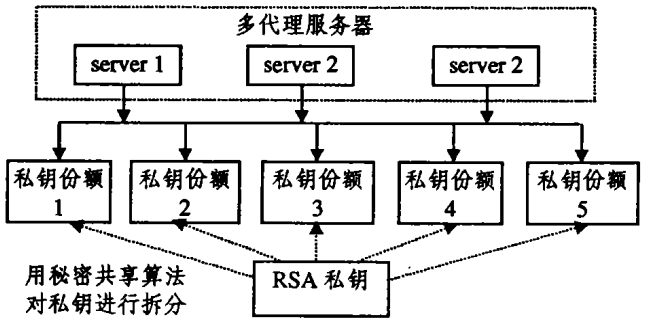


图3 多代理服务器结构

为加强系统的安全性和增加服务的效率，在整个系统的构架上采取多代理配合分步签名的方式（如图3）。对于存放核心的 RSA 私钥的机器：在进行拆分处理后发送到各个私钥份额的服务器存放。完成密钥分发后，存放私钥的服务器便可以与系统断开。

代理服务器：在进行签名算法的操作时，向存放私钥份额的机器发出请求，并根据最后得到的结果进行综合得出最后的签名。

存放份额的机器：接收到代理服务器的请求后，用自己的私钥份额计算子签名，并把结果返回给代理服务器。

多代理服务器：每个代理服务器的签名操作是独立的，多代理的机构一方面的作用是提高系统的工作效率，一方面通过代理服务器操作系统的多样性，提高攻击的难度，同时提供系统冗余，保障当系统的部分代理被攻击后，其余代理仍可继续提供服务。

4 RSA 算法的分步签名方案

下面着重从算法角度阐述分步签名方案的实施和安全性保证。

4.1 先发秘密共享算法及拉格朗日重构[5]

SHAMIR 门限体制对私钥进行拆分。(t,n)门限指：秘钥 K 被分解成 n 个份额，当得到其中的份额格的数量小于 t 时，秘密仍然无法重构恢复出来，即子份额虽然泄漏，但是私钥 K 仍然是安全的。但当得到其中任意 t 个份额后，便可以完全恢复出秘钥 K。所以这里的 t 就是安全的门限值。

直接重构私钥的安全性分析：对于私钥的直接重构，可以任意提取 t 个份额应用拉格朗日公式来计算结果。但是应用于实际是不合理的。原因是：如果在进行签名以前重构出私钥，那么即使是暂时的，也很有可能在系统遭受入侵时，私钥完全泄漏给攻击者。这与传统的直接运用私钥一次性签名拥有同样的脆弱点。所以我们考虑在不重构出私钥的前提，用私钥份额下进行分步签名，再将结果进行综合的方案。这样来说，在整个签名计算的过程中，不会有私钥的出现。

4.2 RSA 算法和分步签名算法

RSA 算法的加密和解密运算实际上都是有限域内进行的指数运算，这里所说加密和解密只是相对的过程。其公钥 n,e 公开后，私钥 d 的安全性是依赖于大素数分解这一数学难题[7]。

公钥　n：产生两个大素数 p、q，$n=p*q$

　　e：与$(p-1)(q-1)$互素

私钥　$d:e^{-1} \bmod (p-1)(q-1)$

加密　$c=m^e \bmod n$ 得密文

解密　$m=c^d \bmod n$ 得明文

数字签名这一步实际上就是对信息的摘要值作为明文，然后用服务器的私钥进行加密运算。所以实际上分步签名算法，就是对摘要值的分步加密运算。通过观察 RSA 加密运算的算法规则，我们发现了它适用于分步签名算法的一个很方便的特点，就是其在有限域内进行的指数运算结构。

根据有限域内的加法和乘法运算保证以下等式成立：N 为素数，a、b 为整数

$$(a+b) \bmod N=a \bmod N+b \bmod N$$

$$(a*b) \bmod N=(a \bmod N * b \bmod N) \bmod N$$

那么对于有限域内的指数运算来说，就有分步运算的可能，对于私钥 d 的加（解）密远算可以做以下分解：

$$m=c^d \bmod n=c^{d1+d2+\cdots+dr} \bmod n=(c^{d1}*c^{d2}*\cdots*c^{dr}) \bmod n$$
$$=(c^{d1} \bmod n * c^{d2} \bmod n * \cdots * c^{dr} \bmod n) \bmod n \quad (1)$$

这里只需保证 $d=\sum_{i=1}^{r} d_i$ 成立。

可以整理(1)式成如下形式：

$$m=\prod_{i=1}^{r} m_r \bmod n \ (m_r=c^{dr} \bmod n) \quad (2)$$

同时我们观察 LaGrange 插值公式重构多项式

$$h(x)=\sum_{r=1}^{t} s_{ir} \prod_{j\neq r,j=1}^{t} \frac{x-x_{ij}}{x_{ir}-x_{ij}} \bmod p \quad (3)$$

为了方便讨论，我们不对公式的意义做深入的解释。在这里我们只需明确各个参量的意义即可。s_{ir}就是分拆私钥 d 得到的私钥份额，重构私钥 d 即求解(4)式：

$$d=h(0)=\sum_{r=1}^{t} s_{ir} \prod_{j\neq r,j=1}^{t} \frac{-x_{ij}}{x_{ir}-x_{ij}} \bmod p$$
$$=\sum_{r=1}^{t} (s_{ir} \prod_{j\neq r,j=1}^{t} \frac{-x_{ij}}{x_{ir}-x_{ij}}) \bmod p \quad (4)$$

我们考虑 p, x_{ir}, x_{ij} 为常数即可。通过观察最右边的式子，实际上对私钥 d 的重构就是对 t 个(t 即为安全门限)带有私钥份额 s_{ir} 的子式进行求和运算，但求和是在有限域内进行的。当我们选取适当的 p 值，并经过预先的重构试验保证 (5)式成立。

$$0<\sum_{r=1}^{t}(s_{ir}\prod_{j\neq r,j=1}^{t}\frac{-x_{ij}}{x_{ir}-x_{ij}})<p \tag{5}$$

那么(4)式可以简化成：

$$d=\sum_{r=1}^{t}s_{ir}\prod_{j\neq r,j=1}^{t}\frac{-x_{ij}}{x_{ir}-x_{ij}}\bmod p=\sum_{r=1}^{t}(s_{ir}\prod_{j\neq r,j=1}^{t}\frac{-x_{ij}}{x_{ir}-x_{ij}})$$

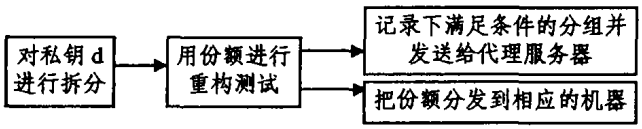
这样代数上的求和运算，正可以保证指数运算得以分步进行，即满足 $d=\sum_{r=1}^{t}dr$ 这里

$$d_r=s_{ir}\prod_{j\neq r,j=1}^{t}\frac{-x_{ij}}{x_{ir}-x_{ij}} \tag{6}$$

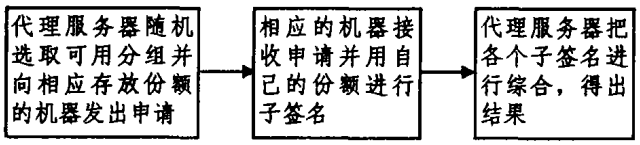
这就结合拉格朗日重构公式和 RSA 算法(有限域内的指数运算)的特点，得出了分步签名的方案。但这里对私钥进行拆分分组后，首先需要进行重构试验，选取合适的分组以满足(5)式成立。在签发的阶段采取，子签名服务器首先根据代理服务器的请求用自己的份额 s_{ir}，代入(6)式计算出 d_r，再对应求出(2)式中的 m_r，送回给代理服务器，最后代理用(2)式对收到的结果进行综合，得出最后的结果。这样，在整个签名的过程中，始终没有直接重构出私钥，确保了私钥的安全性。对于份额的窃取也不会完全暴露私钥，这一点由 SHAMIR 门限算法在数学上的安全性加以保证[5]。

实现分步签名的流程图：

步骤一：密钥拆分阶段



步骤二：证书签发阶段



步骤三：进行验证

为防止入侵者对份额的篡改，可以多次执行签名，将最后结果进行比较，若结果不同说明有份额被篡改，系统触发相关安全策略进行恢复。对密钥份额的更新即重新进行密钥的拆分。

5 实现和结果

实验在 WIN2000下的局域网环境进行，算法的编程实现采用目前广泛应用于研究领域以及小型 CA 的公开源代码的工具包 Openssl(programing in c\c++)。

私钥拆分实验

使用 Openssl 制作独立的根证书并提取私钥后，采取 SHAMIR 门限拆分方案对私钥进行拆分和重构试验，选取满足(5)式的分组策略。靠虑到增加攻击者的难度，我们的安全门限值 $T=3$，即攻击者同时获取3个以上份额才可恢复出私钥。实验数据如表1所示(分拆时的素数 P[5]由随机种子产生，其位数保证与私钥一致。"总共"表示当前(T,N)门限下总共的份额分组策略，"可用"表示经过重构测试，满足(5)式的可用分组策略)。

从实验结果看出，可用的分组策略虽然随着 N 的增加，在总共分组策略中的比例有所下降，但基本满足实际应用的需要。

表1

T / N	3	
	总共	可用
5	$c_5^3=10$	9
6	$c_6^3=20$	14
7	$c_7^3=35$	20
8	$c_8^3=56$	30

RSA 分步签名算法的实验

修改了 RSA 加解密的底层算法，并在保证加密信息严格满足 PKCS 加密信息封装标准[3]的条件下，我们成功地实验了$(T=3,N=5)$,$(T=3,N=6)$,$(T=3,N=7)$,$(T=3,N=8)$几种门限方案在分步签名和结果的正确性检验。

修改后的算法对性能的影响：通过分析 RSA 算法源代码发现 RSA 算法在私钥加密计算时默认采取直接用 p、q、e 参数使用计算的效率较高的中国剩余定理进行计算。而分步签名运算只能运用原始的有限域内指数运算，在计算效率上有一定的牺牲。但由于是多台机器同时计算子签名，总体性能的差异不大。

局域网环境的安全信道实验

利用 WIN2000内置的 IPSEC 机制[8]在局域网建立加密的安全信道，在 IP 层进行加密，增加攻击的难度。IPSEC 在代理与子签名机器首次连接握手时由于采取公钥算法进行密钥磋商，因此有一定时间损耗，但建立安全连接后采取对称加密算法加密，运算时间较快基本不对系统性能产生影响。

结论 我们成功实验了应用 SHAMIR 先发秘密算法对 CA 私钥的分存保护，并且实施分步签名代替传统的 RSA 签名方式。解决了传统密钥存放方式以及签名过程中私钥易泄漏的问题；构架的多代理服务框架进一步提供系统以容侵的特性，保证系统在部分代理服务器和存放私钥份额的服务器被攻破时(在安全门限以下)，仍可以提供证书签名服务，且 CA 私钥不会泄漏。

(T,N)门限中，N 增大的意义在于增加系统冗余，在分步签名时，通过增加执行子签名运算的单元来提高系统的运算效率；而 T 的增大，执行同样一次签名时子签名运算次数增多，系统总体运算量加大，但同时加大攻击者的难度，使其需要获得更多的份额才可恢复私钥，为入侵监测等安全技术以及系统重配置等安全策略提供更多的时间以恢复系统。

当然方案的完善还需要结合入侵监测、系统重配置的触发机制以及相关安全策略的制定。

参 考 文 献

1 Malkin M, Wu T, Boneh D. Building Intrusion Tolerant Application. http://www.stanford.edu/~dabo/ITTC
2 Chandra P, Messier M, Viega J. Network Security with OpenSSL Published By O'Reilly Pub Date. ISBN: 0-596-00270-X, 2002. 384
3 Public Key Cryptography Standards (PKCS) RSA Labs. Available at: http://www.rsa.com/rsalabs/pubs/PKCS/
4 Rescorla E. SSL and TLS Designing and Building Secure Systems Published By Addsion Wesley Longman, Inc
5 傅锦伟. SHAMIR 门限体制的推广和应用. 蒙自师范高等专科学校学报, 2001, 3(4)
6 荆继武, 冯登国. 一种入侵容忍的 CA 方案. 软件学报, 2002, 13(8)
7 [加]Stinson D R 著, 冯登国译. 密码学的原理与实践. 电子工业出版社, 2003
8 唐建雄. Windows2000中 IP 数据包安全性的实现. 信息技术, 2001(6)