证书验证树CVT的扩展

李新国， 葛建华， 赵春明
（西安电子科技大学 综合业务网国家重点实验室，陕西 西安 710071）

摘 要：通过对证书验证树和证书吊销列表的比较，得出两者总体性能的一致性结论；通过一次性为签名人颁发更多的短时效证书，将证书验证树方案进一步扩展，得到的方案与前两个方案在性能上完全具有可比性，并且继承了原方案的大部分优点。说明在设计PKI系统时，可以在存储量、计算量和通信量3个复杂度指标之间做一调和，以达到不同的应用目的。

关键词：公钥基础设施；证书验证树；证书吊销列表
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-3516(2004)04-0060-03

为了建立网络世界的信任关系，以便使商家、客户乃至政府等各方面的利益和行为都有安全保障，公钥基础设施PKI的建设是必不可少的。PKI的公钥证书是支撑数字签名的载体，而数字签名可以提供消息的认证性、完整性和不可抵赖性。目前普遍应用的是X.509公钥证书及其证书吊销问题解决方案CRL[1]。证书吊销是PKI建设的关键问题，也是比较复杂的问题。随后提出的PKI大都采用X.509的由可信机构CA单个签名的公钥证书，只是在证书吊销问题上提出了新的想法，如Macali的证书吊销系统CRS[2]和Kocher的证书吊销树CRT[3,4]。解决PKI证书吊销问题的另一个思路是使用短时效证书来回避证书吊销带来的麻烦。文献[5]提出的证书验证树方案CVT不再为每个用户的公钥证书单独签名，而是签名由所有用户证书所组成的Hash树的树根，CVT进一步结合短时效证书的概念消除了证书吊销问题。文献[6]讨论了在有智能卡协作的情况下CVT方案的优化问题。

本文详细比较了CVT和CRL两种方案的各种性能，以此为动机，提出了扩展的证书验证树方案CVT-E。CVT-E方案充分结合了CVT和CRL的优点，在增加一定签名人存储量开销的前提下，将计算量和通信量降到最低。

1 证书验证树CVT

CVT的基本思想是摒弃传统的那种由CA对每个用户的公钥分别签名的做法，而将所有用户的证书构造成一棵二叉树，最后只需对树的根节点进行签名。CVT隐含地使用了短时效证书地概念，系统无须提供证书的吊销信息，证书的验证者只需验证CA当天的签名即可。这里先描述CVT树的构造方法，然后对其细节和使用方法加以说明。

CVT树的叶节点对应一个用户的证书描述(C-Statements)和该描述的Hash值。将两个叶节点的Hash值级联，再进行一次Hash运算得到这两个叶节点的父节点。将两个父节点的Hash值级联并计算其Hash值得到上一级节点。该过程一直执行到根节点。得到的根节点是一个Hash值，记为RV。CA对RV和时间用自己的私钥签名。图1给出了有4个证书的树的例子，其中H是强无碰撞Hash函数。

说明1：证书的完整内容。签名人利用证书公钥所对应的私钥进行签名后，向验证人提供的证书的完整内容包括：C-Statements及其Hash值、由C-Statements直至树根这条路径上的所有的Hash值、路径上所有

收稿日期：2004-02-20
基金项目：国家自然科学基金资助项目(60332030)
作者简介：李新国(1976-)，男，河南洛阳人，博士生，主要从事PKI、PMI和安全组播研究；
葛建华(1961-)，男，江苏常州人，教授，博士生导师，主要从事信息论、密码学、高清晰度数字电视研究.

的兄弟节点的 Hash 值和 CA 对根节点 RV 的签名。例如,图 1 中用户 c_1 的完整证书包括:c_1、h_1、h_2、h_{21}、h_{22}、RV 和 CA 对 RV 的签名。

说明2:证书的时效性以及 CA 的工作。C - Statements 的内容包括用户的公钥以及一些身份信息。这些信息和传统的证书的内容的主要区别在于:传统的证书中有关于该证书的一个较长的有效期,而 CVT 在证书描述中不提供有效期,或者说可以缺省为一天。长时效证书的有效期的存在是证书吊销问题存在的根本原因。CA 必须每天根据各个用户证书的动态来更新 CVT 树。如果某个用户声称自己的证书需要吊销或者新的用户要申请一个证书,CA 必须在 CVT 树中删除或者增加一个叶子节点,然后重新构造出一棵 CVT 树,并对根节点签名。如果用户的总数为 N,则开销为 $O(\log N)$[4]。事实上,由于 CVT 树隐含地使用了短时效证书,即使前一天没有证书需要吊销,也没有新的证书申请,CA 还是要在第二天重新为树的根节点签名。所不同的是,这时不用重新构造 CVT 树,签名中要体现当天的时间。这样,用户的一个公私钥对在使用时可以不受天数的限制,但每次向验证人提交证书时,必须在 CA 公开 CVT 树的目录中获得 CA 当天的签名和相关路径上的 Hash 值。

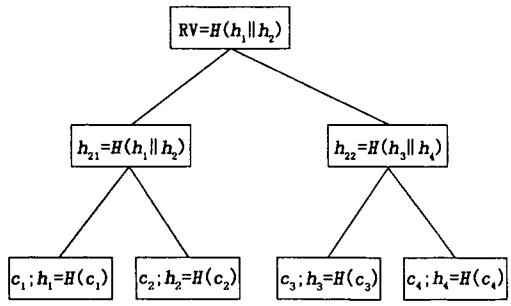

图1　证书验证树

CVT 树和 X.509 系统中的证书吊销列表 CRL 的性能相似性,尽管文献[5]说明 CVT 树无需验证相关的证书吊销即有效性信息。通过下面的比较可以发现,其实二者的计算量和通信性能总体上是一致的。CVT 只是把 CRL 中验证人的查找并验证证书吊销信息的开销转移给了签名人。

X.509 证书的签名人在签名时有 1 次签名运算,验证人有 1 次验证签名人的证书的验证运算和 1 次验证签名人对消息签名的运算,还要查找 CRL,并对 CA 对 CRL 的签名做 1 次验证运算。这样,合起来是 1 次签名运算和 3 次验证运算。CVT 树方案中,签名人对消息有 1 次签名运算,在查找自己当天的证书时,有 1 次对 CA 对树的根节点的签名的验证运算,这次验证是不可或缺的,只有这样才能保证签名人所提供的证书的有效性,验证人有 1 次消息签名验证运算和 1 次证书签名验证运算。可见,CVT 方案也是 1 次签名 3 次验证。CVT 将 CRL 中验证人查找并验证 CRL 的通信和计算开销转变成了签名人查找并验证 CVT 的开销。

2　扩展的证书验证树 CVT - E

对 CVT 方案的扩展方法比较直观,严格使用短时效证书,用户可以一次申请相当于原方案中的 30 个证书(这里假设 CRL 的更新周期是 30 d,并以此为参照),用户依次每天使用 1 个,这样所有的证书可以使用 30 d;CA 将每个用户所有的证书连续地呈现在 CVT 树的叶节点上,并将所构造的 CVT 树公布在 1 个公开目录上;用户可以查找并一次性验证属于自己的 30 个证书,然后存储下来,在以后的 30 d 内,无需再次查询目录。CA 只有在有新用户申请证书,或者某个用户的 30 个证书的最后 1 个已经作废时才必须更新 CVT 树,如果没有成员的动态,CA 什么也不用做。

方便起见,将上面的扩展方案记为 CVT - E。尽管将原来的 CVT 树的高度增加了 4 级,并且叶节点数增加了 30 倍,由于采用的是树形结构和 Hash 运算,CVT - E 给 CA 增加的负担是可以容忍的。之所以说用户要存储"相当于"原方案的 30 个证书,是因为这 30 个证书是以树的形式排列的,其实只在根节点处有 CA 的 1 个签名。CVT 和 CVT - E 都存在证书个数不是 2 的次方个的情况,这时所构造的树是不平衡的二叉树,但并不会带来任何不方便和不安全的因素,只是某些证书到根节点的路径短了一些。

CVT - E 完全继承了 CVT 方案中 CA 可以方便地更新签名私钥的优点,原因在于 CA 不是对每个用户的证书单独签名而只是签名 Hash 树的树根。CVT - E 同样也保持了对历史查询的方便性,以支持具有长期有效性签名的不可抵赖性(Non - Repudiation)。

3　性能比较

将 CVT - E 和 CVT 以及 CRL 在性能上做一比较,具体结果列在表 1 中。表 1 中,CRL 可以有两种运作方式。其一是验证人验证一次当前的 CRL 并存储起来,那么在当前 30 d 内进行签名验证时就没有 CRL 验

证,在验证人和 CA 所指定的目录之间也没有通信量;其二是验证人不存储 CRL,结果是在计算量上多了一次验证,并且验证人有一次查找目录的通信过程。可见,CRL 的两种工作方式是在验证人的存储量和计算量以及通信量之间所做的调和,牺牲一定的存储量可以换来计算量和通信量的减少。CVT 在存储量上对签名人和验证人的要求都是最低的,但在其它两个指标上和 CRL 的第二种运作方式在总体上是完全一致的,都是 1 次签名 3 次验证和 1 次与目录通信。

表 1 3 种方案的性能比较

方案	存储量		计算量		通信量		
	S	V	S	V	S 到 V	S 到目录	V 到目录
CRL	1 个 X. 509 证书	当前 CRL /Null	消息签名	消息验证 证书验证 /CRL 验证	签名及 证书	Null	Null/查 找 CRL
CVT	1 个 CVT 证书	Null	消息签名验证当天 CVT	消息验证 证书验证	签名及 证书	查找当 天 CVT	Null
CVT - E	相当于 30 个证书	Null	消息签名	消息验证 证书验证	签名及 证书	Null	Null

CVT - E 牺牲了一定签名人的存储量,所达到的效果和 CRL 的第一种运作方式是一致的,即将签名人和验证人的计算量和通信量降到最低。签名人一次性存储 30 d 的公钥并做 1 次验证,和 CRL 第一种运作方式中验证人存储并验证 CRL 的开销是相当的(这里假设存储 CRL 和存储 1 个 CVT - E 证书所需的空间相当,这对于以 30 d 为更新周期的 CRL 来说是合理的)。

表中没有列出 CA 和目录之间的通信量。CRL 中,CA 每 30 d 更新 1 次目录,CVT 则是每天更新 1 次,CVT - E 只是在有用户动态时才更新目录。

参考文献:

[1] Adams C , Llyod S . Understanding Public - Key Infrastructure : Cancepts, Standardsand Deployment Considerations [M] . Indianapolis: Macmillan Technical: Dublishing, 1999.

[2] Micali S. Efficient Certificate Revocation [A] . RSA Data Security Conference [C] . San Francisco: California, 1997.

[3] Paul Kocher. A Quick Introduction to Certificate Revocation Trees (CRTs) [R] . Technical report, ValiCert, 1999.

[4] Merkle R. A Certified Digital Signature [A] . Gilles Brassard. Advances in Cryptology: CRYPTO89 [C] . NY: Springer - Verlag, 1990. 218 - 238.

[5] Irene Gassko, Peter S. Gemmell, Efficient and Fresh Certification [A] . Imai H, Zheng Y. Public Key Cryptography 2000 [C] . Berlin: Springer - Verlag, 2000. 342 - 353.

[6] Josep Domingo - Ferrer, Mare Alba, Francesc Sebé. Asynchronous Large - scale Certification Based on Certificate Verification Trees [A] . Communications and Multimedia Security2001 [C] . Norwell MA: Kluwer Acedemic Pubishers, 2001. 185 - 196.

(编辑:门向生)

The Extended Certificate Verification Tree

LI Xin - guo, GE Jian - hua, ZHAO Chun - ming

(National Key Lab. of Integrated Service Network, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: A comparison between Certificate Verification Tree and Certificate Revocation List shows that both of them have the same performance as a whole. An extended scheme of Certificate Verification Tree, which is completely comparable to the former two schemes, is proposed by issuing more short validity certificates to a signer at a time. And this scheme also inherits most of the advantages of the original Certificate Verification Tree. It is demonstrated that the computation time, storage requirements, and communication complexity can be allocated properly according to the specific applications in the design of PKI.

Key words: PKI; CVT; CRL