计算机科学2002Vol.29№.11

PKI中证书库的分析与构建*)

Analysis and Construction of Repository in PKI

胡 艳 戴英侠 连一峰 卢震宇

(中科院研究生院信息安全国家重点实验室 北京100039)

Abstract In the powerful and complex PKI, the storage, management and publishing of the information are very considerable. This article describes some methods of information publishing, discusses data sharing and security considerations. In our CA system, we construct the repository considering both security and convenience. We use both directory and database to publishing information, and integrate the methods of sharing, replication and boundary to deal with data sharing and security.

Keywords PKI, Repository, Directory

1. PKI概述

信息科学技术的发展给人类社会带来了巨大的便利和经济效益,但同时也给社会的正常发展带来了前所未有的风险和威胁。随着互联网技术的飞速发展,电子商务、电子支付逐渐成为应用的热点。如何保证通信双方身份的真实性和信息的安全性成了一个迫切需要解决的问题。

数字证书(Certificate)是可以提供网络上身份证明的一种数字标识,它用来绑定特定实体姓名(以及有关该实体的其他属性)和相应的公钥,并由证书用户可信的某一成员进行数字签名。数字证书的拥有者可以将其证书提供给其他人、Web站点及网络资源,以证实他的合法身份,并且与对方建立安全的通信通道。比如用户可以使用证书通过浏览器与Web服务器建立SSL会话,使浏览器与服务器之间相互验证身份,另外用户还可以使用数字证书发送加密或签名的电子邮件。

数字证书由认证中心CA(Certificate Authority)签发,CA类似于现实生活中公证人的角色,它具有权威性,是一个普遍可信的第三方。当通信双方都信任同一个CA时,两者就可以得到对方的公钥来进行安全通信。

所谓PKI(Public Key Infrastructure)就是一个用公钥概念和技术实施并提供安全服务的具有普适性的安全基础设施。PKI的定义在不断地延伸和扩展,目前人们认为一个完整的PKI应该至少包括以下几个部分:认证中心CA、注册中心RA、证书库、证书撤消、密钥备份和恢复、自动密钥更新、密钥历史档案、交叉认证、支持非否认、时间戳、客户端软件。

2. PKI中信息的分发方式

数字证书最终要被人获得和使用,证书撤消信息也要及时地提供给证书使用者。这就涉及到PKI系统中信息的分发。最简单的方式是私下分发,用户通过"带外"的方式将自己的证书直接传送给另一个用户。但是这只能可信地支持较小的用户群,而且撤消消息的交换显然是非正式和不可靠的。证书和证书撤消信息还可以通过"带内"协议来交换,比如基于S/MIMEv3的电子邮件,还有TLS和IPSec协议。

最普遍的证书与证书撤消信息分发的方法是发布,也就是将信息放在一个广为人知,公开且容易访问的地点。作为一种惯例,企业中证书和证书撤消信息一般是被发布到证书库中,客户端可以通过多种访问协议从证书库里查询信息。

2.1 X.500目录系统代理和LDAP服务器

目录服务器是一个分布式系统,以一个大型分布式数据库为基础,它把行政组织的管理优点引入网络管理。目录服务系统是由一个或者多个DSA(目录系统代理:Directory System Agent)组成。在目录服务器系统中,用户是通过目录用户代理(DUA:Directory User Agent)与DSA打交道;DUA与DSA之间按DAP协议(目录访问协议)或者LDAP(轻量级的目录访问协议)进行通信;不同的DSA之间按照目录系统协议(DSP:Directory System Protocol)进行通信。

X.500目录服务是一个高度复杂的信息存贮机制,包括客户机-目录服务器访问协议、服务器-服务器通信协议、完全与部分的目录数据复制、服务器链对查询的响应、复杂搜寻的过滤功能等。对于PKI,X.500在目录服务器访问入口处使用标准化方法来完成证书和证书撤销列表数据结构的存储访问。

LDAP协议最早被看作是X.500目录访问协议(DAP)中的那些易描述、易执行的功能子集。后来这些用处颇大的功能"子集"被加以扩展以适应很多不同环境的需要。这些环境往往采用LDAP作为存储器的访问协议。另外,RFC2587详细说明了适用于与LDAP相兼容的信息存储,以此为PKI的证书和证书撤消列表信息存储提供基于标准化的办法。

2.2 Ocsp响应器

在线证书状态协议(OCSP)是一种相对简单的请求/响应协议,它提供了一种从名为OCSP响应者的可信第三方获取在线撤消信息的手段。OCSP请求中包含一个或者多个证书标识符,OCSP响应者做出的响应中包含了相应证书的状态(即"正常"、"撤消"或者"未知")。OCSP响应必须包含签名,可以是CA签名,也可以是由CA认可的实体签名。响应的签名者必须被用户信任,所以用户必须得到OCSP响应者的公钥证书的拷贝。但是OCSP仅仅用来说明一个给定证书是否已被撤消,不能验证一个证书是否在有效期内,也不能保证证书是否被正确使用。

*)国家973项目(G1999035801)、国家自然科学基金(90104030)资助。胡 艳 研究生,研究方向为计算机网络安全。戴英侠 教授。连一峰 博士研究生。卢震宇 研究生。

2.3 Web服务器、基于FTP的服务器和域名系统DNS

通常CA将CRL表和证书发布到目录服务器，但是在Internet的很多地方没有提供目录服务。FTP和HTTP就为证书和CRL表发布提供了可选的方式。在证书和CRL表的扩展项中，GeneralName中的URI形式是用来表明发布者证书和CRL表可以被获得的位置。证书扩展中的subjectAltName可以含有URI识别证书的主体，IA5String描述了用匿名FTP或者HTTP获取证书和CRL信息。

另外，证书和CRL表还可以存储在域名系统中。在这种方式中，定义了一种称作证书资源记录的结构，其中包含证书类型以及证书或者CRL表，证书的证书资源记录以与subject相关的域名存储，CRL的证书资源记录以与发布者相关的域名存储。

3. 域间证书库的选择和安全考虑

客户端可以通过多种访问协议从证书库中查询信息，理想的情况是客户端可以即时地查询证书和证书撤销信息，而不需要太多的访问控制，但是未授权的访问会带来一定的安全风险，所以将PKI信息发布到证书库中还是需要一些访问控制的，以防止未授权的数据修改，而且，如果策略上有必要，证书库也需要进行机密性上的保护。当域和域之间需要共享信息时，域间数据库有很多种实施选择。

3.1 直接访问

直接访问方案允许一个域里的用户直接访问另一个域里的证书库。如果两个域相互信任或者证书库自身能保持安全性，这种方案是合适的。当信息从一个域向另外一个域传递时，还需要相应的保密机制防止信息的泄漏。

3.2 共享数据库

共享数据库允许每个PKI域将有效的证书和证书撤销信息发布到同一个证书库中。共享数据库被多个域共同拥有，共同操作，发布和查询的机制可以不同，如果需要的话，也要对共享数据库进行访问控制和加密措施。

3.3 域间复制

域间复制是将有效的证书和证书撤销信息从一个域直接拷贝到另一个域。这个过程可以有一些现成的协议来实现，比如X.500目录服务中的DISP(Directory Information Shadowing Protocol)协议。

3.4 边界数据库

边界数据库是指在防火墙外独立维护一个证书库，有效的证书和撤销信息被发布到边界数据库里，外部通过边界数据库可以访问到必需的信息，而不用访问内部资料库中的敏感信息，也不会危及到内部证书库的安全。

3.5 代理

代理进行访问控制检查，接受外部的访问请求，通过内部网直接访问内部目标证书库，然后将查询结果返回给外部请求者。

4. RealCert认证系统中证书库的构建

4.1 系统结构

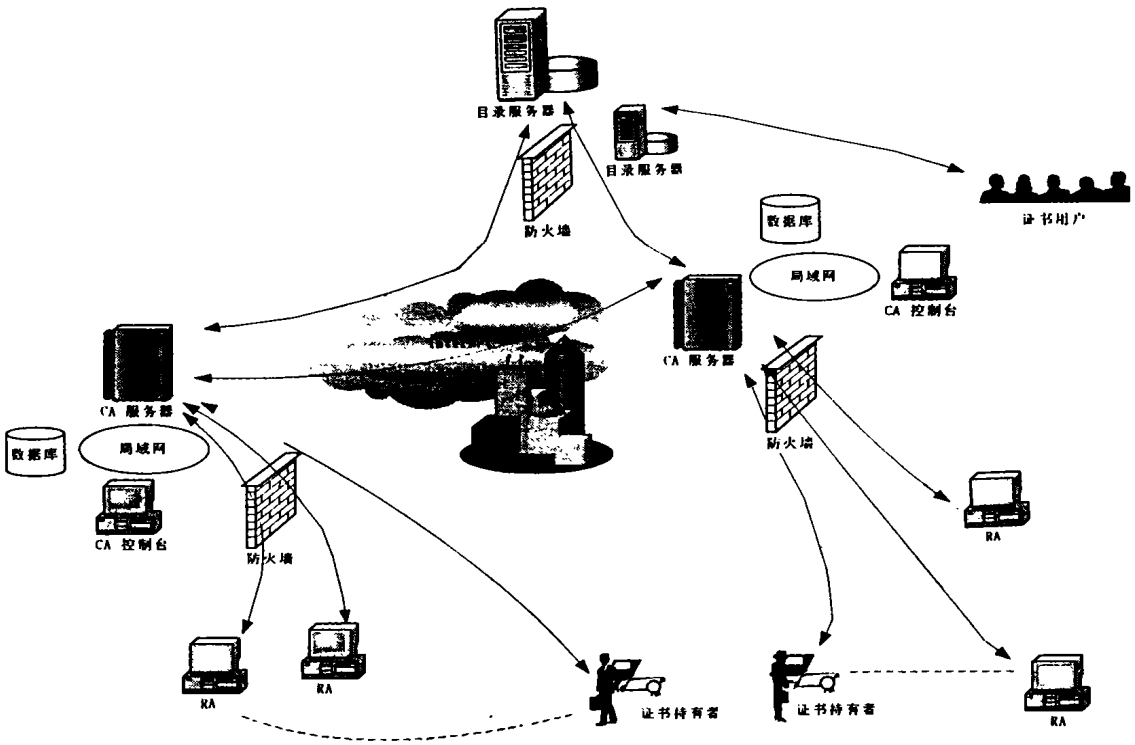

图1 RealCert多级CA认证系统结构图

RealCert认证系统是我们构建的一个多级CA认证中心系统，它的结构如图1所示。认证系统由多个CA证书中心、RA注册中心和客户端程序组成。CA(Certificate Authority)为证书签发中心机构，是系统的核心，它要执行用户证书的维护和管理、CRL表的维护和管理以及证书和CRL表的发布等功能。CA证书中心主要包括三个组成部分：运行在Sun Solaris平台下的CA服务器程序；运行在windows平台下为系统管理员操作和管理CA提供方便界面的CA控制台程序；以及存储这个CA证书中心相关数据的Sybase数据库。RA(Registration Authority)为证书注册机构，分理CA系统中的"带外"(Out of Band)功能，包括接受用户证书申请、审核数据、向CA提交请求以及作废用户证书等功能。用户则通

过客户端软件使用系统提供的各种功能。

4.2 系统数据的存储分布

系统中有很多数据需要存贮和管理，我们对于信息的发布综合采用了数据库和目录服务器的方式，对于域间数据的共享综合采用了共享数据库、复制数据库和边界数据库的方式。在证书库的构建上，我们综合考虑了使用的方便性和安全性，同时还考虑了系统自身的安全性。系统中的数据主要有当前系统中的有效证书、有效 CRL 表、过期归档证书、过期归档 CRL 表和审计事件表。系统数据的存储分布见图2所示。

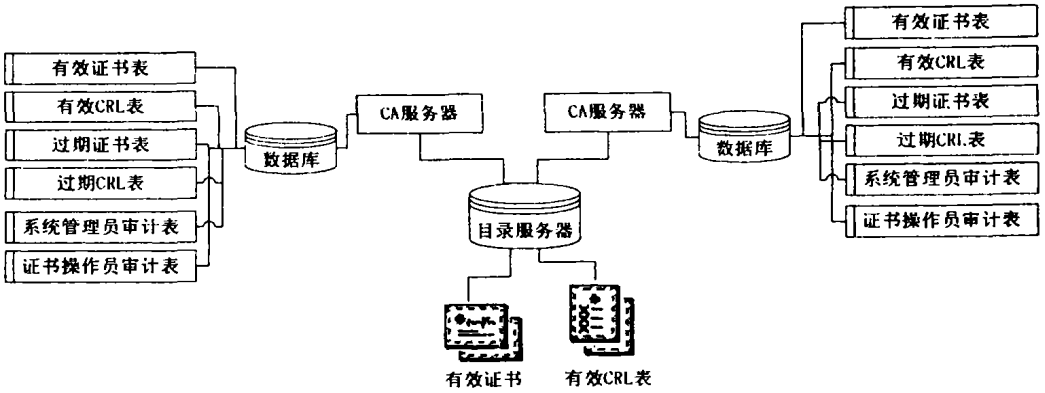

图2 系统数据的存储分布

4.3 目录服务器

当前系统中的有效证书、有效 CRL 表是系统中最重要、最经常被访问的数据，因此我们将系统中所有 CA 发布的有效证书和有效 CRL 表都发布到一个统一的共享的目录服务器中。这些数据被整个系统所共享，是系统中的公开数据。证书和 CRL 表在目录服务器中是以 DN(distinguished name)存储的，当前有效的证书和 CRL 表在整个系统中具有唯一的 DN。

从访问控制考虑，系统内任何用户都可以对目录服务器进行匿名读取，这时系统中任何用户的权限都是相同的。系统管理员工作在 CA 控制台，证书操作员工作在 RA，证书持有者或者非证书持有者的证书用户使用客户端程序，他们都可以匿名访问目录服务器，对系统当前有效证书和有效 CRL 表进行查询。目录服务器中的数据只有每个 CA 服务器可删可写，CA 服务器颁发证书时，将证书写入目录服务器；撤销或者更新证书时，将证书从目录服务器删除；更新 CRL 表时，从目录服务器删除过期 CRL 表，写入新的 CRL 表。

从机密性考虑，用户只能已知特定用户在目录服务器中的 DN，来查询该用户的证书，或者已知某个 CA 的 DN，来查询此 CA 发布的当前有效 CRL 表。用户不能进行模糊查询。这也是根据实际的需要来决定，比如有些公司觉得证书库中信息是生来敏感的，不适合完全公开，或者不希望公司的结构信息被泄漏。或者证书用户不希望自己的 DN 和证书无限制地公开，只要使用他证书的用户可以在公开访问的地点获取其证书就可以了。

另外，如果实际使用的需要，可以在防火墙外侧另设一个备份目录服务器，CA 服务器修改防火墙内部的目录服务器，内部目录服务器定期往外部目录服务器上备份，用户只能匿名访问防火墙外部的目录服务器。这样做可以保证目录服务器和 CA 服务器的安全，因为普通用户不能通过防火墙，即使篡改了防火墙外部的目录服务器也不影响系统的安全。但是这样做访问的信息就不是绝对即时，实际使用中可以综合考虑安全性和使用方便性的需求。

4.4 CA 服务器数据库

每个 CA 服务器都带有一个 Sybase 数据库，存储本 CA 相关的所有数据，包括本 CA 所颁发的当前有效证书、当前有效 CRL 表、过期归档证书、过期归档 CRL 表和审计事件表。这个数据库是本 CA 系统所私有的，只有这个 CA 对它有完全的控制权，可读可写。另外，系统管理员或数据库管理员可以通过数据库的前端管理程序来查询、管理数据库中的信息。

数据库中存储的信息首先是这个 CA 颁发的当前有效证书和当前有效 CRL 表。CA 服务器同时将有效证书和有效 CRL 表发布到公用共享的目录服务器和自身带的数据库中，首先是一个备份的考虑。系统中访问的主要是目录服务器中的有效证书和有效 CRL 表，CA 服务器带的数据库外界是不能访问的，所以安全。也就是说，对于目录服务器中的信息，每个 CA 服务器将属于自己的信息在本地做了一个备份。除了备份的考虑以外，CA 服务器的系统管理员可以通过数据库前端管理程序对本 CA 颁发的有效证书进行各种方式的查询和管理。

数据库中存储的另一类信息是这个 CA 颁发的过期归档证书和过期归档 CRL 表。对于归档证书和归档 CRL 表，证书用户不常访问，通常在交易发生纠纷时才需要查询当时的证书和 CRL 表信息，这时可以让系统管理员或者数据库管理员在局域网中代用户查询。

为了查询和管理的方便，在数据库中存储证书和 CRL 表时，除了存储证书和 CRL 表本身，还将证书和 CRL 表解码，存入一些关键字段。比如证书可以存储证书号、证书主题、发布者、证书的生效日期和失效日期等信息；而 CRL 表可以存储 CRL 编号、发布者、此次更新时间和下次更新时间等信息。这样查询的时候就不用每次都要将证书和 CRL 表解码。

为了系统自身的安全性，数据库中还存放了系统审计信息，主要包括系统管理员审计表和证书操作员审计表。审计表中保存了操作的时间、操作者的 DN、操作类型、操作结果、登录 IP 和端口等信息。系统管理员可以在控制台程序上查询这些审计表来发现异常，维护系统自身的安全性。系统管理员通过查询系统管理员审计表查看自身的操作，来发现别人是否窃取了系统管理员的权限；通过查询证书操作员审计表来查看证书操作员的操作，来发现证书操作员是否有非法的操作。如果发现某个证书操作员的行为异常，先切断该证书操作员与 CA 服务器的连接，再从审计信息中取证，查明是被人攻击

(下转第123页)

在上图中，安全基础体现为各种底层算法。如各种对称密钥算法、公开密钥算法、HASH 函数等。本层是最基本的安全技术。为安全机制层提供算法支持和其它服务。

安全机制是实现安全服务的具体软件或芯片，它为上层安全服务提供具体的实现方法。它包括了加密机制、数字签名机制、访问控制机制(访问控制表机制、基于能力和安全标签的访问控制机制)、数据完整性机制、路由控制机制、安全审记与追踪机制等。

在安全机制的基础上，形成了安全服务，体现为一系列安全协议。主要包括五种通用的安全服务。认证服务，提供对某个实体(人或系统)的身份的保证。如对等实体的的认证服务、数据起源认证服务等。认证服务是最重要的安全服务，因为其它的安全服务都在一定程度上依赖于认证服务；访问控制服务，防止对任何资源进行未授权的访问；机密性服务，保护信息不被泄露或暴露给未授权用户，如连接机密性服务、无连接机密性服务；数据完整性服务，防止对数据进行未授权的改变、删除或替换，如可恢复的连接完整性服务、不可恢复的连接完整性服务、无连接完整性服务；反否认服务，防止参与某次通信交换的一方事后否认本次交换曾经发生过。如数据起源的反否认服务、传递过程的反否认服务。一种安全服务的实现可能会需要下层的几种安全机制的支持。例如机密性服务，就包括握手协议、密钥生成、密钥交换协议，需要下层的密钥产生、密钥交换机制予以支持。

安全管理指与安全相关的基本数据的管理。如密钥和证书的生成、交换、替换等。

安全策略定义了在一个通信资源集合之上、用于所有与安全行为相关的一套规则。这套规则主要包括三方面主要内容：保护的目标，如何保护，付出的开销。安全策略的详细制定将涉及安全框架的各个层次。在应用层，我们指出针对某一特定应用进行访问控制。由于不同的安全机制及其组合提供不同级别的安全服务，因此需要综合考虑应用所带来的效益和提供安全服务的开销，共同确定采用何种安全机制甚至底层的基本算法以提供所需的安全服务。

在整个电子安全框架中，底层的安全基础提供算法支持。基本安全机制和扩展的安全机制通过使用特定的加密算法、数字签名算法、HASH 函数、随机数发生器等提供安全服务的具体实现。安全服务则表现为若干协议，电子商务具体应用通过遵循这些协议使用安全服务，从而防范电子商务交易环境中出现的各种安全威胁。安全管理则提供了对电子商务应用、安全服务、安全机制中所涉及的基本安全数据的管理和一定的人员管理。同时，为实现安全电子商务必须提供一整套安全策略明确描述对何种资源进行何种保护，这套策略覆盖到安全框架的各个部分，一般还会包括政策和制度因素在里面。上文提到的电子商务七个基本安全需求，映射到安全框架中的六种安全机制和对应的上层五种安全服务。该安全框架是实现安全电子商务的理论框架，可为设计和实现具体的电子商务安全技术提供理论指导。

目前的问题和下一步的工作 值得关注的是，我们只是提出了一个安全框架，要完全实现该框架还存在一些困难。这主要是：电子商务的复杂性，涉及交易活动的种类和需求多，相关的法规尚不健全；技术上还存在一些难点。如 Java 平台固有的安全漏洞，已知的操作系统漏洞等。另外，随着应用技术和安全技术的发展，上述安全框架也不是一成不变的，它在每一层中都留有扩展余地，应视具体情况有所调整。电子商务安全性已经引起学术界、企业界的广泛关注，并在相关的安全技术方面取得了一些成就。但是相关的安全技术还很不完善，多项研究尚处于探索阶段，我们可以在此领域有所突破。

参 考 文 献

1 Kou Weidong. Networking security and standards. Kluwer Academic Publishers

2 Schneier B. Applied Cryptography Protocols, algorithms, and source code in C(Second Edition) 应用密码学：协议、算法与 C 源程序(第二版). 机械工业出版社

3 Stallings W. Cryptography and Network Security Principles and Practice Second Edition 密码编码学与网络安全：原理与实践(第二版). 电子工业出版社

4 冯登国著. 计算机通信网络安全. 清华大学出版社

5 Li Gong 著，王运凯等译. Java2平台安全技术——结构、API 设计和实现. 机械工业出版社

6 Tang Zheng. Introduction to E-Commerce. 人民邮电出版社

7 秦志光，刘锦德. 安全系统的有限自动机. 电子科技大学学报，1996，25(1)：72～75

8 秦志光，刘锦德. 客户与服务器之间的安全交互作用. 电子科技大学学报，1996，25(1)：69～71

(上接第120页)

还是内部的证书操作员执行了非法操作。如果是内部证书操作员执行非法操作，可以删除这个证书操作员，即从系统人员表中删除这个证书操作员的身份，甚至撤销他的证书。

数据库中保存了本 CA 系统中的所有信息，其自身的安全性也需要考虑。最简单地说来，可以设置一个备份数据库。将 CA 服务器直接访问的数据库和系统管理员通过数据库前端管理程序查询管理的数据库分开，减少对数据库的有意或无意的破坏。另外，从入侵检测的角度考虑，可以对数据库中的数据计算完整性校验值。每次存入数据项时，计算并存储完整性校验值，在需要时再对数据进行完整性检查，保证数据库自身的安全性。

结论 公钥基础设施 PKI 是个功能强大、结构复杂的系统，系统中有大量的数据需要存储、发布和管理。PKI 系统中信息的发布有很多种方式，域间数据的共享和系统的安全性也有很多考虑。在证书库的构建问题上，我们综合考虑了使用的方便性和安全性，同时还考虑了系统自身的安全性。我们对于信息的发布综合采用了数据库和目录服务器的方式，对于域间数据的共享综合采用了共享数据库、复制数据库和边界数据库的方式，成功地构建了我们的 RealCert 多级 CA 认证系统。

参 考 文 献

1 Adams C, Lloyd S. Understanding Public-Key Infrastructure : Concept , Standard , and Deployment Considerations. Macmillan Technical Publishing, 1999

2 RFC2251 Lightweight Directory Access Protocol (v3) 1997

3 ITU-T Recommendation X.500 (1997)-The Directory: Overview of concepts, models and services