第34卷 第15期 计 算 机 工 程 2008年8月
Vol.34 No.15 Computer Engineering August 2008
·安全技术· 文章编号：1000—3428(2008)15—0162—02 文献标识码：A 中图分类号：TP309

基于OCSP中间件的PKI/PMI时钟同步

赵 朋，周 宇，王晓东
(宁波大学信息科学与工程学院，宁波 315010)

摘 要：PKI/PMI体系如果缺乏规范的时钟机制可能产生时钟不同步现象，因此，在可用性和安全性方面存在隐患。该文通过对在线证书状态协议(OCSP)及PMI认证特性的分析，提出一种基于OCSP中间件的时钟同步技术。应用该技术构建的身份认证与访问控制系统可以消除上述隐患，不会明显加重系统负担，或引入额外风险，适用于多数一般性的数字证书应用。

关键词：权限管理基础设施；时钟同步；在线证书状态协议；网络时间协议

PKI/PMI Clock Synchronization Based on OCSP Middleware

ZHAO Peng, ZHOU Yu, WANG Xiao-dong
(College of Information Science and Engineering, Ningbo University, Ningbo 315010)

【Abstract】 The lack of normative clock mechanism in PKI/PMI probably causes asynchronization, thus the infrastructures has hidden defects of usability and security. By analyzing the features of OCSP and PMI, this paper brings a clock synchronization technology based on OCSP middleware to solve the problem. An identity authentication and access control system with the technology can eliminate those defects above, and it neither overtasks the system markedly nor imports extra risk. It is applicable in most common digital certificate application.

【Key words】Privilege Management Infrastructure(PMI); clock synchronization; Online Certificate Status Protocol(OSCP); Network Time Protocol (NTP)

1 概述

公钥基础设施(Public Key Infrastructure, PKI)和权限管理基础设施(Privilege Management Infrastructure, PMI)[1]作为一组支撑性的基础设施体系，以数字证书形式实现了较好的身份认证与访问控制功能，为信息交互的保密性、完整性、可控性和抗抵赖性提供了保障。但规范的时钟同步机制的缺乏导致这一体系中存在安全隐患。相对PKI而言，PMI的证书有效期较短且精度要求较高，公钥证书(Public Key Certificate, PKC)的有效期一般长达数年甚至终生有效，而属性证书(Attribute Certificate, AC)的有效期可能仅以小时甚至分钟计量。这是由于公钥证书表示的身份相对恒定，而属性证书表示的角色相对易变。因此，PKC以是否被撤销作为判断有效性的主要凭据，而对AC而言，验证是否过期更为重要。

由于有效期的验证需要依据时钟，而原本的PKI/PMI体系中没有任何时钟机制，无法保证系统内各单元时钟的绝对精度与相对同步[2]，因此在无同步情况下常出现数分钟甚至更大的误差，导致体系存在两方面的潜在风险：(1)验证者时钟超前使得可用性无法得到保障；(2)验证者时钟滞后将产生可被过期证书时差攻击的漏洞。因此，设计与部署基于PKI/PMI体系的系统必须考虑时钟同步问题。互联网分布式环境下的时钟同步通常采用网络时间协议(Network Time Protocol, NTP)为标准(RFC 868)，目前已发展到第4版。NTP通过多时间源保证时钟同步的可靠性，通过基于概率论的时间源筛选、数据过滤等算法提高精确度。在互联网环境下，采用NTP进行时钟同步可达到10 ms级的精度[3]，足以满足PKI/PMI体系的需求。但仅仅依靠NTP并不能有效解决同步问题。

目前国内外基于PKI/PMI体系的系统中，证书的有效性验证大多仍以离线方式实现。其中，验证是否被撤销通过检索证书撤销列表(Certificate Revocation List, CRL)和属性证书撤销列表(Attribute Certificate Revocation List, ACRL)，验证是否过期的时间源则来自各验证者的本地时钟。应用的多样性和认证的交互性会使需要同步的单元数目变得十分庞大，这种方式不仅需要较高的成本，而且会使管理者丧失全局掌控，无法保证所有单元确实得到了同步。在这方面目前尚无更完善的替代方案，本文提出了一种基于OCSP中间件的解决方案，能满足多数场合的一般性应用。

2 PKI/PMI体系时钟同步技术

2.1 OCSP与时钟同步

在线证书状态协议(Online Certificate Status Protocol, OCSP)[4]是一种PKI公钥证书有效性验证的方式。CRL大小的累加性决定了其存在耗费传输与存储资源等问题，而发布的周期性限制了它在对证书状态实时性要求较高场合下的应用。OCSP通过状态查询服务器解决了这2个问题，并描述了客户和服务器之间交换数据的细节。然而相对于分散的CRL，OCSP因其集中式的特性产生了潜在的性能瓶颈与单点崩溃的可能性。而且为了避免证书状态出现“未知”、提高查询的有效率，用户必须确切地知道CA与OCSP响应器之间的授权对应关系，这带来了使用上的不便[5]。这些代价都限制了OSCP在实际PKI应用中的实现，使得OCSP服务器

基金项目：浙江省自然科学基金资助项目“无线公钥基础设施关键技术及其在移动电子政务中应用”(X106869)
作者简介：赵 朋(1984－)，男，硕士研究生，主研方向：数字证书；周 宇，副教授；王晓东，讲师
收稿日期：2007-09-08 **E-mail：**levi0@163.com

常被配置为一个可选的独立组件。但在 PMI 中实现 OCSP 的代价相对较小。其用户并不持有属性证书，属性权威(Attribute Authority, AA)签发的属性证书由轻量级目录访问协议(Light Directory Access Protocol, LDAP)服务器统一存放，验证时，用户持公钥证书向 LDAP 服务器索取对应的属性证书。由于 LDAP 服务器能够承担性能瓶颈与单点崩溃的风险，此时若在其前台以中间件形式引入 OCSP 响应器，不会明显加重系统负担或带来额外风险。

通过拓展 OCSP 的适用范围来包含属性证书，并且在验证证书是否被撤销时增添验证是否过期的功能，能够方便 PKI/PMI 体系时钟同步问题的解决。由于有效期验证所处的层次在体系中有所提高，因此需要进行时钟同步的单元数量大大减少，即将同步点由客户端收缩到 OCSP 中间件，实际部署的成本将十分经济，可靠性也将大为提高。

2.2 OCSP 中间件方案

改进的 PKI/PMI 体系结构如图 1 所示。与传统结构相比，主要的区别是在验证者与 LDAP 服务器之间引入了 OSCP 中间件。考虑到对时间不敏感的需求，验证者直接进行 LDAP 检索的通道仍被保留。

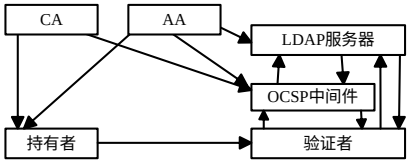

图 1 PKI/PMI 体系结构

虽然 OCSP 响应器是以中间件的形式存在，但出于性能方面的考虑，仍以独立服务器的方式实现。为了减少传输耗时、提高查询的响应速度，OCSP 响应器与 LDAP 服务器之间可通过专用的高速网络连接。OCSP 响应器的模块结构如图 2 所示，包括 4 个主要的模块。

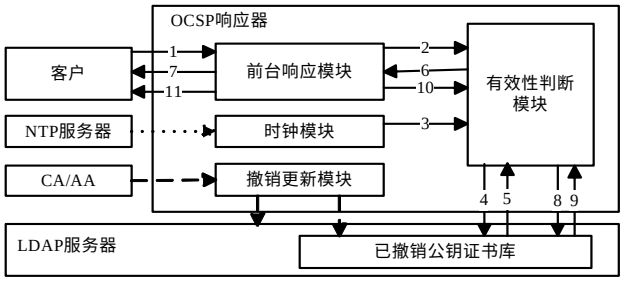

图 2 OSCP 响应器模块

(1)前台响应模块，负责处理客户请求、解封、封装、签名与发送数据。大量并发请求的处理与签名回复容易形成性能瓶颈，对该模块的优化将对系统性能起决定性作用。线程池技术的使用将有效提高响应速度并加深对系统资源的控制。由于被撤销或过期的证书其状态不会再发生变化，因此对这 2 种回复采用预签名机制可以免去实时签名的运算时间。在避免单点崩溃现象及减轻崩溃影响的处理上也可采用主从服务器集群等技术。

(2)有效性判断模块，负责 LDAP 服务器之间的通信及证书状态的判断，其中，有效期判断的“当前时间”以 OCSP 查询请求到达的时间为准，但也可根据实际应用需求进行调整。OCSP 中的证书失效状态只有“已撤销”一种。虽然单纯将过期证书标记为“已撤销”并不影响系统的安全性，但出于尽可能给予用户更明确的错误信息的原则，有必要在原协议的状态中添加“过期”。另一方面，根据 PKI/PMI 体系的特性，由于此处 OCSP 中间件实际上是与 AA 而非 CA 存在对应关系，而 AA 签发属性证书时会首先验证用户身份，即确认公钥证书的来源，因此 OCSP 响应器的查询结果通常不会出现“未知”状态，除非待查询的公钥证书在系统内不存在对应的属性证书。

(3)撤销更新模块，负责接收 CA/AA 发布的撤销证书信息并写入 LDAP 服务器。其中，公钥证书信息写入专门的撤销库，作为查询是否被撤销的信息源；属性证书则无需撤销库，只须在存储中标记是否被撤销，因为在 PMI 中不可避免地会以获取属性证书为目的对完整证书库进行检索。

(4)时钟模块，负责从 NTP 服务器获得准确的时间并维护。为保障时间源的可靠性，应当要求 NTP 服务器对其发布的时间信息签名，或选择启用签名功能的 NTP 服务器作为时间源。

在增添 OCSP 中间件后，一次完整的证书查询过程包括 11 个步骤，如图 2 所示。

步骤 1 OCSP 客户持公钥证书向 OCSP 响应器发起查询请求。

步骤 2 前台响应模块解析请求，确认格式合法性，将其传递给有效性判断模块。

步骤 3 从时钟模块得到当前时钟。

步骤 4 OCSP 响应器检索 LDAP 服务器上存储的已撤销公钥证书库。

步骤 5 依据检索结果判断此公钥证书是否被撤销：如果未被撤销，依据步骤 3 的时钟信息进一步判断其是否过期，若公钥证书失效，则完成步骤 6、步骤 7 后终止服务并关闭会话，否则在执行步骤 6、步骤 7 的同时执行步骤 8~步骤 11。

步骤 6 有效性判断模块将公钥证书状态信息传递给前台响应模块。

步骤 7 前台响应模块将状态信息打包反馈给用户。

步骤 8 OCSP 响应器以此公钥证书信息为索引检索 LDAP 服务器。

步骤 9 从 LDAP 服务器获取相应的属性证书，判断其有效性(是否被撤销、是否过期)。

步骤 10 有效性判断模块将属性证书状态信息传递给前台响应模块。

步骤 11 前台响应模块将属性证书状态信息打包反馈给客户，如属性证书有效，则还需传输完整的属性证书，供用户进行访问控制。

2.3 平台的构建与实现

基于 OCSP 中间件完善 PKI/PMI 体系可构建出安全性更高的身份认证与访问控制系统平台。对开源的 OpenPermis 的代码进行修改后，已使 PMI 验证者能够支持扩展的 OCSP。PKI 与 LDAP 服务器部分采用了 EJBCA, OpenLDAP 等开源软件实现。与 OCSP 中间件结合后，平台具备了身份/角色/权限定义、证书签发、存储、获取、身份认证、访问控制等 PKI/PMI 体系系统的基本功能，且能够满足有效期验证的要求。

在实现中发现，这种改进具有不加重 LDAP 服务器负担、减轻客户负担(无需存储证书撤销列表和属性证书撤销列表)、部分减少通信时间(在过期时无需传输完整属性证书)和不引入额外风险的优点，适用于多数一般性的数字证书应用。

（下转第 178 页）