一种基于分布式环境的 D-OCSP 服务模式*)

苏锐丹[1] 容晓峰[1] 汪 宁[2] 周利华[1]

(西安电子科技大学多媒体技术研究所 西安 710071)[1]

(国家信息安全工程技术研究中心 北京 100093)[2]

摘 要 本文简要地阐述了 OCSP 的工作原理,并对当前普遍应用的"Trusted OCSP"模式进行了分析,从可扩展性、可用性、安全性三个方面指出该模式所存在的问题,然后提出了一种新的基于分布式环境的 D-OCSP 服务模式,该模式通过将秘密信息从处于在线状态的 RTC 应答器中抽取出来,置于处于离线状态的 RTCA 服务器中,由 RTCA 针对 CA 所签发的所有证书的状态列表产生 OCSP 应答证据集合,并发布给 RTC 应答器,供其在处理依赖方 OCSP 请求时使用。通过这种方式,D-OCSP 服务模式从根本上解决了"Trusted OCSP"在可扩展性、可用性、安全性方面存在的问题,从整体上优化了 OCSP 服务。

关键词 D-OCSP,Trusted OCSP,RTCA,RTC responder

A New D-OCSP Mode Based on Distributed Environment

SU Rui-Dan[1] RONG Xiao-Feng[1] WANG Ning[2] ZHOU Li-Hua[1]

(MTI, Xidian University, Xi'an 710071)[1]

(National Information Security Engineering Technology Research Center, Beijing 100093)[2]

Abstract In this paper a brief explanation about the principle of OCSP is given at first and an analysis of "Trusted OCSP" mode is done which is widely used currently, on the basis of which the problems lying in this mode are pointed out in three aspects: scalability, availability and security. Then a new OCSP mode based on distributed environment is presented. This mode removes secret information from online RTC responder and places them in RTCA server which stays offline. RTCA generates OCSP response proof set according to the status set of all the certificates issued by CA and publishes the proof set to all the RTC responders which use them to process OCSP requests sent from relying parties. By this way, distributed OCSP solves the issues in scalability, availability and security brought by "Trusted OCSP" radically and OCSP service is optimized as a whole.

Keywords Distributed-OCSP,Trusted OCSP, RTCA, RTC responder

1 前言

OCSP(Online Certificate Status Protocol)定义了一个可被依赖方用于查验 X.509 证书当前状态的网络协议。依赖方可以通过 OCSP 基于证书的唯一识别信息来请求验证证书的有效性,OCSP 应答器将返回一个经过签名的应答,指示该证书的状态。

IETF RFC2560 已经对 OCSP 进行了标准化,规定了由依赖方发向 OCSP 应答器的 OCSP 请求的语法,但是并没有对应答器如何产生一个有效的应答做具体规定。传统的 OCSP 应答器基于可信任服务器来实现该协议,在产生 OCSP 应答时,服务器使用自己拥有的私钥对应答进行签名[6]。我们称这种方式为"Trusted OCSP"模式,下面简称"Trusted OCSP"。

"Trusted OCSP"对于低、中等安全级别和可扩展性要求低的配置环境是适用的,但是对于大型的、高安全级别的证书查验服务系统就无法达到使用要求。

本文深入分析了传统的"Trusted OCSP"在安全性、可扩展性和可用性方面所存在的问题。在此基础上,提出了一种新的基于分布式环境的 OCSP 服务模式,该服务模式解决了"Trusted OCSP"在可扩展性、可用性和安全性方面的存在的问题,同时提高了系统的高效率和灵活性。我们称之为 D-OCSP(Distributed-OCSP)。

2 Trusted OCSP

2.1 Trusted OCSP 工作原理

理想的,OCSP 服务是通过 OCSP 应答器实现:应答器从 CA 那里接收 CRL(Certificate Revoked List,证书撤销列表),并基于 CRL 信息来对来自依赖方的 OCSP 请求进行应答。每一个 OCSP 应答器都拥有自己的证书和签名私钥,用来在产生 OCSP 应答时对其进行签名。

图 1 给出了一个可信任 OCSP 应答器是如何产生具备权威性的关于证书状态的 OCSP 应答。

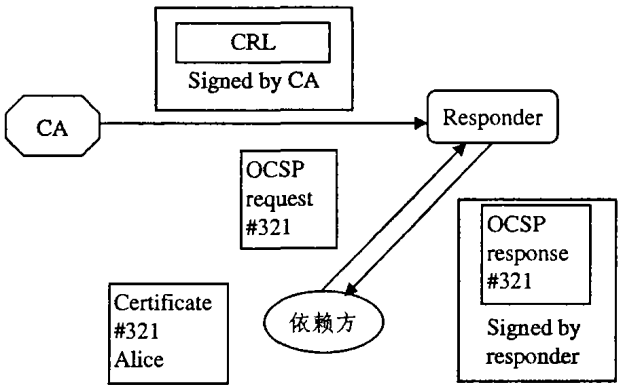

图 1 Trusted OCSP 工作原理图

*)基金项目:本文受国家"十·五"科技攻关重点项目"中国电子政务应用示范工程"资助。**苏锐丹** 博士研究生,主要从事计算机网络和信息安全方面的研究;**容晓峰** 博士研究生,主要从事计算机网络和信息安全方面的研究;**汪 宁** 高级工程师;**周利华** 教授,博士生导师。

图中，依赖方需要验证 Alice 的数字证书的有效性，该证书是由 CA 签发的，证书序列号是＃321。CA 发布具备权威性的 CRL(CA 用自己的私钥对 CRL 进行签名)，用来确定证书的有效性，当依赖方不使用 OCSP 协议进行查验证书时，就需要定期从 CRL 发布点更新本地的 CRL，当 CA 撤销的证书数量很大时，更新 CRL 需要传输的数据量很大，常导致依赖方不能实时获取并查验证书，并且这种定时更新 CRL 的方式不能保证证书状态更新的实时性。

改进方法是：依赖方向可信任的 OCSP 应答器发送 OCSP 请求，并接收 OCSP 应答器所返回的应答。根据 OCSP 应答信息，依赖方就可以确定所查验证书的有效性。在此查验过程中，OCSP 应答不是被 CA 签名，而是由 OCSP 应答器进行签名，OCSP 应答器经 CA 授权提供 OCSP 服务，在线的 OCSP 应答器拥有自己的证书和私钥，如图 1 所示。

OCSP 应答器按照预先设定的策略及时更新 CA 签发的所有证书的状态信息。当依赖方发送 OCSP 请求时，应答器检查证书状态列表，对目标证书的有效性作出判断，产生一个 OCSP 应答并对应答签名后返回给依赖方。保证了证书状态信息的完整性、不可抵赖性和及时性。

2.2 分析

在实际部署“Trusted OCSP”时，不仅需要考虑 OCSP 功能是否能实现，而且需要保证整个部署方案具备高的可扩展性、可用性和安全性，同时还要受到成本的限制。当 CA 所签发的证书数量巨大时，对 OCSP 服务器性能的要求也是很高的。OCSP 应答器是在线工作方式，可能受到来自外部的各种方式的攻击，保障 OCSP 应答的签名私钥的安全性就显得尤为重要。

总体而言，“Trusted OCSP”在提供可信 OCSP 服务方面存在以下一些缺点，按照其安全性的顺序从低到高给出如下：

- 低速网络环境或 OCSP 应答器超负荷的工作都会导致依赖方与应答器之间通信的超长延时；
- OCSP 应答器极易遭受拒绝服务(DOS)攻击；
- OCSP 应答器的错误配置或针对其进行的攻击使得应答器产生虚假的关于证书有效性的信息；
- OCSP 应答器的错误配置或针对其进行的攻击使得应答器的私钥泄露，将导致虚假 OCSP 应答，从而使中间人攻击得逞。

本质上讲，这些缺点并非 OCSP 协议自身的问题，而是由“Trusted OCSP”的具体实现带来的。“Trusted OCSP”需要保护每一个应答器的私钥。作为一个完全在线的实体，网络会带来很多安全漏洞。综和考虑上述因素，“Trusted OCSP”存在的缺点归结为三个方面：

- 可扩展性：OCSP 服务难以及时地向所有依赖方做出 OCSP 应答；
- 可用性：由于运行负载巨大，OCSP 服务很难保证 7x24x365 的不间断运行要求，甚至能容忍一定程度的攻击；
- 安全性：一旦对 OCSP 服务攻击成功，将危及整个 OCSP 系统的安全性。

已有许多方法和途径用来解决“Trusted OCSP”这些缺点带来的问题。例如，使用硬件密码模块保存和使用私钥，可以减少 OCSP 应答器私钥泄露的风险。设置防火墙、以及对运行的关键代码进行签名保护可以减少来自外部网络的攻击。另外，缩短更新应答器证书的时间周期可以降低私钥泄露带来的破坏性影响。

要使 OCSP 服务正常安全工作，必须保证应答器免受各种攻击，但是，实际环境中的任何微小的安全漏洞都可能危及整个 OCSP 服务系统的安全。例如，著名的 Kerberos 安全服务器就因为一个小的配置漏洞，使得攻击者可以获取远程服务器上的所有密钥。

可用性和可扩展性方面的问题更加难以解决。为了保证所有的依赖方能及时接收到 OCSP 应答，有两种解决途径：

第一种，负载均衡。使用 OCSP 应答器集群来提高 OCSP 系统的整体服务能力，如图 2 所示。

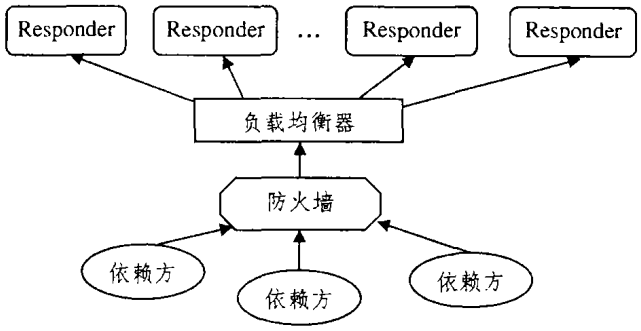

图 2 “Trusted OCSP”的负载均衡

这种负载均衡架构缩短了因单个 OCSP 应答器超负荷运行所产生的应答等待时间，但是却带来在网络和负载均衡架构上的瓶颈。这些部件中的任何一个发生了错误，将导致整个 OCSP 服务瘫痪。另外，这种方式并没有解决由网络距离所带来的延迟过长问题，例如，一个在日本的依赖方，访问一个在纽约的采用了负载均衡的 OCSP 服务，二者之间的延迟仍然很大。

第二种解决“Trusted OCSP”可扩展性和可用性问题的方法是在不同的物理地点部署 OCSP 应答器。这就使得依赖方可以向就近的 OCSP 应答器请求服务，服务的速度和可靠性都会大大提高。但是，这种方式会削弱整个系统的安全性。此外，由于异地部署的 OCSP 应答器也必须设置同等物理和网络的保护措施，以抵抗来自多方面可能的攻击。因为，攻击者可以选择安全防范最弱的 OCSP 应答器实施攻击，获取其私钥，从而对整个 OCSP 服务构成威胁，而保护这样一个地理上分布的 OCSP 服务是相当困难的，这将极大增加 OCSP 异地部署的难度。

3 分布式环境下的 D-OCSP 服务模式

3.1 D-OCSP 原理

通过上述分析，我们提出一种新的基于分布式环境的 D-OCSP 服务模式，不但可以消除“Trusted OCSP”在可扩展性、可用性和安全性方面的问题，同时也可以提供数倍于“Trusted OCSP”的服务效率。D-OCSP 将在线的 OCSP 应答器上的所有秘密信息保存在离线的 RTCA(实时信任权威机构)服务器中，RTCA 服务器根据 CA 上的证书状态列表预先产生所有证书的 OCSP 应答证据，并且按照预定的策略发布给各 RTC 应答器，由 RTC 响应依赖方的查验请求。系统体系结构如图 3 所示。

在这种模式中，RTCA 是在离线状态下维护的，CA 签发的每个证书的 OCSP 应答预先在 RTCA 中产生，称为 OCSP 应答证据，RTCA 对应答的签名操作也是离线进行的，产生好的 OCSP 应答证据集合发布给所有的 RTC 应答器。这样可以保证 RTCA 具有很高的安全性：依赖方的 OCSP 请求不需 RTCA 直接处理，由 RTC Responder 处理，而 RTC Responder 本身不包含任何秘密信息，这样就杜绝了私钥泄露所带来的种种问题，更便于部署高安全、可扩展、可用的 OCSP 服务。分布式环境下 D-OCSP 的工作原理如图 4 所示。

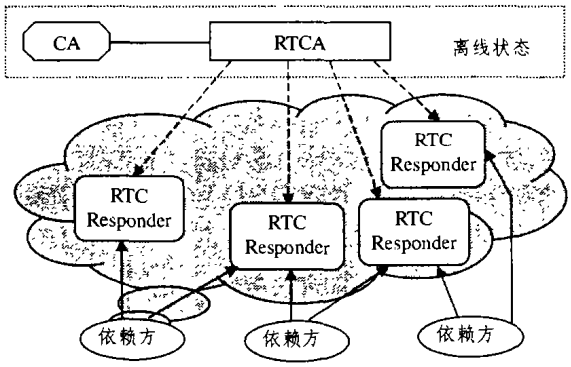

图 3 RTCA 结构图

这里，RTCA 从 CA 获取签发证书的信息，包括证书的有效性，证书的属性等等。这些信息可以在 CA 和 RTCA 之间共享，RTCA 也可以按既定的策略实时地导入证书状态列表，保证 RTC 应答器所拥有的 OCSP 应答证据集合的及时准确性。

RTCA 负责定期为每个当前证书产生 OCSP 应答证据。每个证书的 OCSP 应答定期更新，更新时间周期可以是每小时、每天或每星期等，并可以定义和修改更新策略。每一个 OCSP 应答证据都由 RTCA 进行签名，保证应答信息的安全可信性和完整性。整个 OCSP 应答证据的集合随后要被发布到所有的 RTC 应答器。每一个应答器都保存着 RTCA 上预先产生的 OCSP 应答证据集合数据的镜像。那么，RTC 应答器无需任何保密措施，因为它自身都是公开的信息。

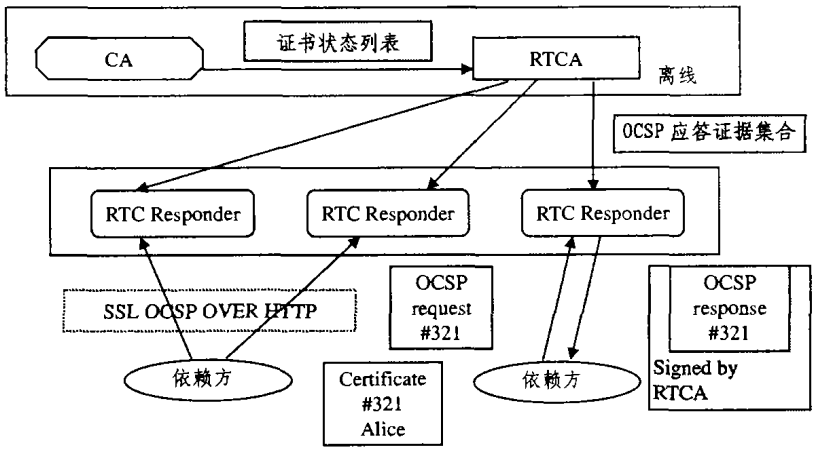

图 4 分布式环境下 D-OCSP 的工作原理图

分布式 OCSP 通过使用 OCSP 协议中的预产生响应特性提高了 OCSP 的效率，保障了 OCSP 应答器私钥的安全性，但却因为不能利用 Nonce 扩展而可能导致重放攻击。现在 OCSP OVER HTTP 方式是唯一可普遍实施的一种方式，这样就可以通过 SSL 协议来对 RTC 应答器与依赖方之间的通信进行安全保护，杜绝了重放攻击。

3.2 优越性分析

RTC 应答器根据依赖方的 OCSP 请求，从预先存储的 OCSP 应答证据集合中找到相应的信息作以应答。这仅需要在应答器上进行一个简单的查询，可以在极短的时间内响应查询。与“Trusted OCSP”方式相比较，由于没有进行复杂而耗时的签名操作，将极大地提高 OCSP 服务的响应效率。

除了效率上的改进，分布式 OCSP 在可扩展性、可用性和安全性三个方面也都优于“Trusted OCSP”。

· 可扩展性 既然 RTC 应答器没有保存任何秘密信息，也不执行密码运算，它可以根据需要被快速便捷、广泛的部署。相对于“Trusted OCSP”，每一个 RTC 应答器将能够以更高的效率、更低的成本来为更多的依赖方提供 OCSP 服务。

这种方案的可扩展性不会影响到整个系统的安全性，并且，RTC 应答器能够被异地部署。部署 OCSP 服务就象部署普通网络基础设施一样方便简单、方便，比如 DNS，从而使依赖方能就近获得及时的 OCSP 服务，实现真正的分布式 OCSP。

RTC 应答器还可以为不同的 RTCA 服务器提供应答服务，所以，该方案可以在多 CA 的应用环境下实施。

· 可用性 通过广泛地在不同的地理位置上部署 RTC 应答器，每一个依赖方应当能够发现一个就近的应答器，并从该应答器处获得 OCSP 服务，这一过程和 RTCA 没有任何关系。这种部署方式充分体现了分布式的特点，有力地防止了拒绝服务攻击。

· 安全性 分布式 D-OCSP 服务模式将其签名私钥保存在处于离线状态的 RTCA 中，RTC 应答器上只维护可公开的应答信息，有力地保障了整个 OCSP 服务体系的安全和应用。由于 RTCA 处于离线状态下运作，所以，它具有与 CA 一样的高度安全性。

通过使用 SSL 协议来对 RTC 应答器与依赖方之间的 OCSP OVER HTTP 通信进行保密，杜绝了重放(Re-play)攻击。

总结 分布式 D-OCSP 服务模式提供了一种将 CRL 的离线安全性和 OCSP 在线便捷性组合起来的有效服务模式。它通过将秘密信息从处于在线状态的 RTC 应答器中隔离出来，置于离线状态的 RTCA 服务器中，由 RTCA 对 CA 签发的证书产生 OCSP 应答证据集合，发布给所有的 RTC 应答器，供 RTC 应答器处理依赖方 OCSP 请求时使用。通过这种方式，分布式 D-OCSP 服务模式从根本上解决了“Trusted OCSP”在可扩展性、可用性、安全性方面存在的问题，从整体上优化了 OCSP 服务。

参 考 文 献

1 Myers M, Ankney R, Malpani S. HMAC: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP, RFC2560, June 1999. Available at: http://www.ietf.org/rfc/rfc2560.txt

2 冯登国，周永彬，张振峰，李德全，等译. 密码工程实践指南，162～163

3 张玉清，陈建奇，杨波，薛伟，等译. 公钥基础设施(PKI)实现和管理电子安全，174～177

4 Sytrust e-security products technical concept certcontrol. Available at: http://www.openvalidation.org/files/c_TechnicalConcept.pdf

5 Introduction to the on-line Certificate Status Protocol. Available at: http://security.polito.it/ocsp/

6 Housley R, Ford W, Polk W, Solo D. Internet X.509 Public Key Infrastructure-Certificate and CRL Profile. Available at: http://www.ietf.org/rfc/rfc2459.txt