

基于域名系统的证书验证系统研究与实现

沈士根

(嘉兴学院 信息工程学院, 浙江 嘉兴 314001)

(kxsg@21cn.com)

摘 要:为解决当前不同 CA(Certificate Authority)间证书验证过程的互操作问题,本文在分析当前证书撤销机制问题的基础上,结合域名系统(Domain Name System, DNS)的 referral 模式提出了一种新的证书验证系统 DNS-OCSP,使用该系统可构建不同 CA 间统一的证书验证,给出了 DNS-OCSP 的系统结构,说明了 DNS-OCSP 的工作流程。该系统具有较好的可存取性和可扩展性。

关键词:证书验证;域名系统;DNS-OCSP

中图分类号: TP309 **文献标识码:** A

Research and implementation of certificate validation system based on DNS

SHEN Shi-gen

(College of Information Engineering, Jiaxing University, Jiaxing Zhejiang 314001, China)

Abstract: For solving the interoperability during current certificate validation process of different CAs, the new system DNS-OCSP was proposed by incorporating DNS-style referral, which can construct a unified certificate validation mechanism between different CAs. The architecture of DNS-OCSP was presented, and the workflow of DNS-OCSP was illuminated. It has been shown that the DNS-OCSP is more accessible and scalable.

Key words: certificate validation; DNS(Domain Name System); DNS-OCSP

目前,数字证书被广泛用于多个领域,如加密和身份认证等,而在真正使用时,证书撤销和验证服务成为 PKI 系统中消耗最大的部分。当前的模式是 CA(Certificate Authority)使用它的私钥数字签名每个证书,从而保证证书持有者的身份。如果证书的私钥泄露或证书持有者不想再使用该证书,证书持有者就通知 CA 撤销证书。CA 再发布该证书的序列号作为撤销信息到指定位置,当第三方想使用一个证书时,它首先要决定证书是否合法。此时,通常需要验证发布 CA 的数字签名,检查证书的过期时间,最后还需要验证证书的状态以确信它未被撤销。

但在实际应用时存在以下问题:权威性的验证服务器位置不清;协议内容的不确定性,造成不同 CA 对同一种证书撤销机制的实现方式不同,于是,证书撤销和验证常带有专利性质,使得证书验证过程的互操作变得异常困难。这些问题的存在,使得证书的应用价值降低。本文首先简述当前的证书撤销标准及存在的问题,然后结合域名系统(Domain Name System, DNS)的 referral 模式和在线证书状态协议(Online Certificate Status Protocol, OCSP),提出一种统一的证书验证系统。

1 当前的证书撤销机制

当前,最广泛使用的证书撤销机制是 RFC3280^[1]和 RFC2459^[2]定义的证书撤销列表(Certificate Revocation List, CRL)机制。CRL 内含经 CA 撤销的证书序列号等,并以周期性列表形式给出。对一个想验证证书有效性的第三方来说,它首先要获得当前的 CRL,再确定问题证书的序列号不在 CRL 中以断定证书是有效的。CRL 的最大问题是随着证书撤销数量的增加,它可以变得很大。为减小 CRL 的大小,有

一些改进的方案被提出来,如增量 CRL 方式,但均未从根本上解决问题。

CRL 的发布周期是由发布 CA 决定的,因此不同的 CA 可能有不同的 CRL 发布周期。使用 CRL 的另一个问题是想验证证书的客户端需要知道 CRL 发布点的位置。在 X.509 证书中,已提供了相应字段来存放 CRL 分布点的位置信息。然而,CRL 分布点存放位置可能改变,但我们没有办法再去修改已发布证书中的位置信息。另外,这些存放 CRL 位置信息的证书扩展项是可选的,这样就可能造成证书撤销信息是不可用的。还有,每个 CA 采用不同的处理过程使用 CRL,这样就会出现前后矛盾的证书验证结果。

轻型目录存取协议(Lightweight Directory Access Protocol, LDAP)能被用来改善以 CRL 为证书撤销机制的易用性。通过 LDAP,客户端可存取 LDAP 服务器以获得正确的 CRL 分布点。但使用 LDAP 存在的不足是需要相关软件配合,这不适合内存容量较小的 PDA 和嵌入式系统。另一个问题是在验证证书之前增加了相关的协议,从而降低了系统的处理进度。

为了弥补 CRL 结构的内在问题,OCSP^[3]协议被提出来,它是目前应用最广泛的在线证书验证协议。OCSP 通过建立多个响应器,当响应器收到证书验证请求后,以“good”、“revoked”或“unknown”三种状态响应。对“good”和“revoked”响应需数字签名,数字签名可以由发布 CA、CA 授权指派的响应器或请求方信任的响应器完成。OCSP 虽能以快速、在线操作模式验证证书,但它仍没解决上述的所有问题,请求者必须要知道权威的 OCSP 响应器地址;响应器需要知道问题证书和签名权威的情况,而一个公司的 OCSP 响应器只知道自己公司的权威响应器,这样就不可能做到证书验

证的互操作。

2 策略问题

在所有当前使用的证书撤销机制中,CRL是最普遍的。市场份额排在前三位的 Verisign、GeoTrust 和 Thawte 公司都以 HTTP 方式使用 CRL,但在不同的公司有不同的证书处理策略,表1给出了几个主要的 CA 运营商采取的证书处理策略,以及它们的生命期,也给出了要获得 CRL 分布点 CDP(CRL Distribution Point)位置中 CRL 的协议^[4-8]。除了在 CDP 信息上缺乏标准外,不同 CA 的 CRL 更新时间也是相差很大的。RFC 规定了证书中 nextUpdate 字段包含的时间表示在此时间之前 CRL 均是有效的。但实际上,不同 CA 的 nextUpdate 时间变化很大。

表1 不同公司访问 CDP 的不同协议方式

公司名	访问 CDP 的协议方式	CRL 生命期/d
Verisign	HTTP/LDAP	14
GeoTrust	HTTP	10
Thawte	HTTP	29
Entrust	HTTP	1

许多公司提供的证书验证服务可以缓存 CRL,而 RFC 没有具体指定缓存的时间、方式等。如果验证客户端要到 nextUpdate 日期之后检查新的 CRL,那样就存在被撤销证书继续被正常使用的风险。如采用 Thawte 签名的 CRL,假如验证客户端要 nextUpdate 日期后再检查新的 CRL,那么其间隔时间将达到 29d,在这么长的时间里一张本该撤销的证书可能仍旧在被使用,因此,需要一种能及时地验证证书的方法。但引入 OCSLP 后,直接使用仍面临一个与采用 LDAP 的 CRL 方式同样的问题,那就是客户端为了得到正确的响应必须首先要知道权威响应器的位置。

3 referral 模式

referral 模式是 DNS 正常工作的基础。当客户端需要解析某个域名的 IP 地址时,它首先向任何一个已知的 DNS 服务器发送一个请求。如果要求解析的域名与客户端属于同一个域,则 DNS 服务器能立刻返回解析后的 IP 地址;否则,DNS 服务器将发送请求至上一层级的 DNS 服务器直至根 DNS 服务器,从根 DNS 服务器响应权威 DNS 服务器地址;然后,客户端发送请求到权威 DNS 服务器并从权威 DNS 服务器获得需解析域名的 IP 地址。整个处理过程是相当快的,对用户来说,基本感觉不到本地解析和在别处解析的时间差别,这也说明了 DNS 这种结构的有效性。

本文将 DNS 的 referral 模式应用于 OCSLP 中得到一种新的证书验证系统,我们称为 DNS-OCSP。相比较 OCSLP 而言,DNS-OCSP 将能显著地改进证书验证处理的易用性和可存取性,它只需要知道单个的 OCSLP 响应器地址,而且,这个 OCSLP 响应器可以象声明 DNS 服务器一样在 DHCP 配置中声明;另外,用户不需再关心 CRL 的位置改变,因为这种改变将由 DNS 机制来保证。

4 DNS-OCSP

本文给出简化的 DNS-OCSP 系统结构,如图1所示。与 DNS 系统类似,实际的情况常可能在根 DNS-OCSP 服务器和本地 OCSLP 响应器之间进行扩展,以形成域层次关系。

根 DNS-OCSP 服务器类似于 DNS 系统中的根服务器,其中包含所有发布证书的 CA 和权威 OCSLP 响应器的地址映射。根 DNS-OCSP 服务器的主要功能是解析权威 OCSLP 响应器的 IP 地址。

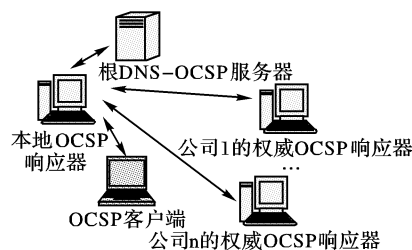


图1 DNS-OCSP 系统结构

本地 OCSLP 响应器与 OCSLP 客户端属于同一个域,且放在一个局域网内,其主要功能包括:接收和响应客户端要求的证书验证的请求;向根 DNS-OCSP 服务器发送要求解析权威 OCSLP 响应器的 IP 地址的请求;接收根 DNS-OCSP 服务器的返回信息;新生成 OCSLP 请求发送到权威 OCSLP 响应器,接收权威 OCSLP 响应器的响应等。

权威 OCSLP 响应器,由不同公司提供的 OCSLP 响应器组成,包含了问题证书的状态信息。当权威 OCSLP 响应器收到本地 OCSLP 响应器提交的 OCSLP 请求后,给出不同的三种响应方式,分别是“good”、“revoked”或“unknown”,其中“good”和“unknown”需要数字签名,数字签名可由发布证书的 CA、被客户端信任的响应器或经 CA 授权指派的响应器完成。

具体实现时,可以考虑利用 OCSLP 请求中的“Service Locator”扩展项将 DNS 的 referral 模式与 OCSLP 结合,其中“Service Locator”扩展项用于存放问题证书的权威 OCSLP 响应器的域名。具体的 DNS-OCSP 工作流程如图2所示。

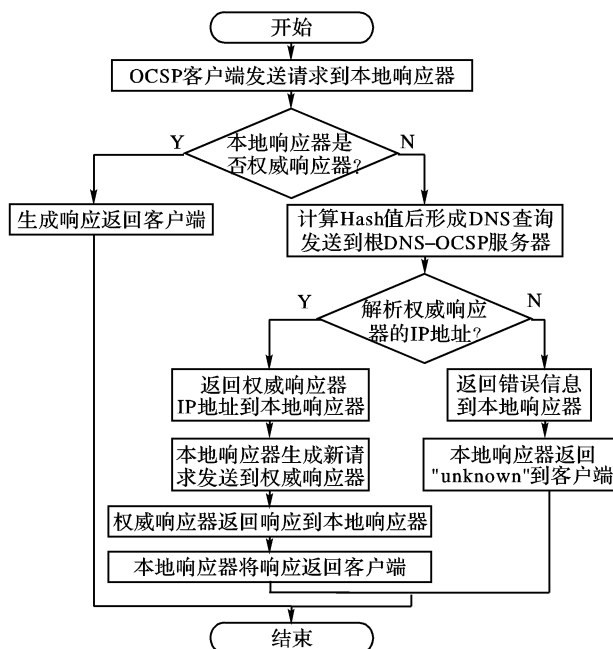


图2 DNS-OCSP 工作流程

1) OCSLP 客户端首先把问题证书的权威 OCSLP 响应器的域名信息存入“id-pkix-service-locator”扩展项,连同其他的 OCSLP 查询信息,包括协议版本、服务请求、目标证书标识和其他的扩展项等,再将所有这些发送到本地 OCSLP 响应器。

2) 如果本地的 OCSLP 响应器是问题证书的权威响应器,则生成可能数字签名也可能未数字签名的响应返回客户端,流程结束;否则转3)。

3) 本地 OSCP 响应器取出客户端请求中的“id-pkix-service-locator”扩展项内容,利用 MD5 算法计算相应的 Hash 值 H,再将包含 H 的 DNS 查询以记录类型为“A”的形式发送到根 DNS-OCSP 服务器,其中,记录类型“A”表示一个主机的 IP 地址记录。

4) 根 DNS-OCSP 服务器从收到的 DNS 查询取出问题证书的权威 OSCP 响应器信息,再解析该权威 OSCP 响应器的 IP 地址。如果能成功解析则将权威 OSCP 响应器的 IP 地址返回给本地 OSCP 响应器,否则返回错误信息给本地 OSCP 响应器。

5) 如果本地 OSCP 响应器收到的是正确的权威 OSCP 响应器的 IP 地址,则新生成一个 OSCP 请求再发送到权威 OSCP 响应器。然后权威 OSCP 响应器生成数字签名或未数字签名的响应返回到本地 OSCP 响应器,本地 OSCP 响应器再将响应返回到客户端,流程结束。

6) 如果本地 OSCP 响应器收到的是错误信息,则生成“unknown”响应返回到客户端,流程结束。

5 结语

本文提出的 DNS-OCSP 结合 DNS 的 referral 工作原理,使客户端只要求知道一个本地 OSCP 响应器的地址,而不需知道所有权威 OSCP 响应器的地址,也能查询任何一个权威 OSCP 响应器,这样,就可构建一种统一的证书验证模式,使不同 CA 的证书验证成为可能。并且,本系统建立在 DNS 基础上,所以具有较强的扩展性。

但本系统还存在两个主要问题有待进一步研究:

1) 因为从本地 OSCP 响应器到根 DNS-OCSP 服务器的 DNS 查询未加密,也未数字签名。这样就存在 DOS 攻击的可能。攻击者可能在返回给本地响应器的响应中包含错误权威

响应器的 IP 地址,造成证书状态查询时返回“unknown”信息,从而阻止正常的证书验证。

2) 与 CRL 相比,CRL 仅需在发布时进行一次数字签名,而 DNS-OCSP 对每一个返回“good”或“revoked”状态的响应均需要数字签名,这样 DNS-OCSP 响应器负载将随 OSCP 请求的增加而成比例上升,所以系统的负载平衡也是需要考虑的问题。

参考文献:

- [1] HOUSLEY R, POLK W, FORD W, *et al.* Internet x.509 public key infrastructure: Certificate and certificate revocation list (crl) profile [S]. RFC3280, IETF, <http://www.ietf.org/rfc/rfc3280.txt?number=3280>, April 2002.
- [2] HOUSLEY R, FORD W, POLK W, *et al.* Internet x.509 public key infrastructure certificate and crl profile [S]. RFC2459, IETF, <http://www.ietf.org/rfc/rfc2459.txt>, January 1999.
- [3] MYERS M, ANKNEY R, MALPANI A, *et al.* Online Certificate Status Protocol, version 2. [EB/OL] <http://tools.ietf.org/wg/pkix/draft-ietf-pkix-ocspv2/draft-ietf-pkix-ocspv2-02.txt>, March 2001.
- [4] E-Soft Inc. Secure server survey [EB/OL]. http://www.securityspace.com/s_survey/sdata/200508/certca.html, August 2005.
- [5] VeriSign Inc. Verisign international server ca-class 3 crl [EB/OL]. <http://crl.verisign.com/Class3InternationalServer.crl>, July 2005.
- [6] GeoTrust Inc. Equifax secure certificate authority crl [EB/OL]. <http://crl.geotrust.com/crls/secureca.crl>, July 2005.
- [7] Thawte Consulting Ltd. Thawte server ca crl [EB/OL]. <https://www.thawte.com/cgi/lifecycle/ThawteServerCA.crl>, July 2005.
- [8] Entrust Inc. Entrust SSL Web Server Certificate Practice Statement [EB/OL]. <http://www.entrust.com/ssl-certificates/CPS/pdf/webcps112803.pdf>, November 2003.

(上接第 1347 页)

4) 代理签名的验证过程

指定的验证人 C 收到代理签名 $((m, r, s), Q_1, Q_2, \dots, Q_n, m_w)$ 后计算:

$x_C(sP - e_2(e_1 \sum_{i=1}^n P_i + \sum_{i=1}^n r_i Q_i + P_B))$, 设 $x_C(sP - e_2(e_1 \sum_{i=1}^n P_i + \sum_{i=1}^n r_i Q_i + P_B)) = (x, y)$; 如果 $x \bmod n \equiv r$, 则代理签名 $(m, r, s), Q_1, Q_2, \dots, Q_n, m_w$ 得到验证。验证过程的正确性可证明如下:

$$\begin{aligned} & x_C(sP - e_2(e_1 \sum_{i=1}^n P_i + \sum_{i=1}^n r_i Q_i + P_B)) \\ &= x_C(s - e_2(e_1 \sum_{i=1}^n x_i + \sum_{i=1}^n r_i k_i + k_B))P \\ &= x_C(s - e_2(\sum_{i=1}^n (e_1 x_i + r_i k_i) + k_B))P \\ &= x_C(s - e_2(\sum_{i=1}^n \sigma + k_B))P \\ &= x_C(s - e\sigma')P = x_C kP = (x, y) \end{aligned}$$

可见,对验证人来说只要证实 $x \bmod n \equiv r$ 就可说明代理签名的正确性。

这个指定接收人的代理多重签名方案除了满足同上的性质外,还满足用户机密性,即只有指定的接受人 C 才可以验证签名的正确性,因此也只有 C 才可以向第三方证明签名的有

效性。除 C 外任何第三方不能从签名中得到原始签名人 A_i 或代理签名人 B 的身份。

4 结语

在我们所提出的方案中,没有求逆运算和指数运算,所以复杂度比较低,从而提高了签名生成和验证过程的速度。根据 ECDLP 的难解性和哈希函数的单向性可知该方案安全性比较高。由于 x_i, x_B, x_C 是保密的,所以对攻击者而言 σ 和 σ' 是不可求的,而且在这两个签名方案中 s 的运算法则同 Schnorr 签名方案中 s 的运算法则,所以综合上述安全因素,攻击是不可能的。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation [A]. Proceedings of 3rd ACM Conference on Computer and Communication Security [C]. New Delhi: ACM, 1996. 48 - 57.
- [2] YI LJ, BAI GQ, XIAO GZ. Proxy Multi-Signature: A New Type of Proxy Signature Schemes [J]. Acta Electronica Sinica, 2001, 29(4): 1 - 2.
- [3] 曹珍富, 李建中, 李继国. 一个新的具有指定接受者 (t, n) 门限签名加密方案 [J]. 通信学报, 2003, 24(5): 8 - 13.
- [4] 张彰, 蔡勉, 肖国镇. 一个高效的门限共享验证签名方案及其应用 [J]. 通信学报, 2003, 24(5): 134 - 139.
- [5] ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature (ECDSA) [S].