ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.8, August 2006, pp.1818−1823
DOI: 10.1360/jos171818

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于桥 CA 的高兼容性分布式信任模型*

朱鹏飞+, 戴英侠, 鲍旭华

(信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

A Distributed Trust Model with High-Compatibility Based on Bridge CA

ZHU Peng-Fei+, DAI Ying-Xia, BAO Xu-Hua

(State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88258551, E-mail: tempzhu@163.com

Zhu PF, Dai YX, Bao XH. A distributed trust model with high-compatibility based on bridge CA. *Journal of Software*, 2006,17(8):1818−1823. http://www.jos.org.cn/1000-9825/17/1818.htm

Abstract: Distributed systems could be more secure with distributed trust model based on PKI (public-key infrastructure). The format of certificate may be different among different PKI systems. Those differences may disturb some applications performing verification of the certificate chain. In this paper, how those differences work during mutual verifications is analyzed with the new concept “certificate-format-compatibility”. Moreover, a new distributed trust model based on bridge CA (certificate authority) with high compatibility is designed out. Using this trust model, the mutual connections between entities in different trust domains would not be affected by the different certificate formats.

Key words: certificate format; compatibility; bridge CA (certificate authority)

摘 要: 基于 PKI(public-key infrastructure)的分布式信任模型能够更好地保证分布式系统的安全性.作为信任路径的载体,数字证书格式的差异性可能对不同信任域实体之间的信任路径的可用性产生影响.提出了证书格式兼容性的概念,并以此为基础分析了证书格式差异对证书有效性验证的作用方式.在桥 CA(certificate authority)的基础上,提出一种兼容性较高的分布式结构的信任模型,能够消除证书格式兼容性问题对不同信任域实体之间实现互连的干扰.

关键词: 证书格式;兼容性;桥 CA(certificate authority)
中图法分类号: TP393 文献标识码: A

随着分布式计算模型的发展,分布式系统的安全性需求越来越迫切.目前国内外已有多种分布式信任模型提出来,例如 Weimerskirch 和 Thonet 提出的适用于 Ad-Hoc 网络的轻量化分布式认证模型[1].这些分布式信任模型多是基于口令等安全性较弱的验证机制,不能很好地保证分布式系统的安全性.基于 PKI(public-key infrastructure)的分布式信任模型[2,3]能够更好地保证分布式系统的安全性.桥 CA(certificate authority)[4,5]是一种高效的基于 PKI 的分布式信任模型,它提供了多个分布式环境之间的灵活的信任策略,并且在实际中得到了初

* Supported by the National Natural Science Foundation of China under Grant No.60403006 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035801 (国家重点基础研究发展规划(973))

Received 2005-02-16; Accepted 2005-09-05

步应用,例如美国联邦桥 CA 等.然而,桥 CA 模型只考虑了分布式实体之间的信任路径(证书链)的建立和验证策略,而没有考虑信任路径的可用性.实践证明,数字证书作为信任路径的载体,其格式的差异性可能对不同信任域实体之间信任路径的可用性产生影响.

1 证书格式的兼容性问题

在我国,PKI 普遍遵循的 X.509[6−11]标准中定义了一些标准证书扩展,这些扩展是可选的,而且可以被设置为关键的或者非关键的.X.509 标准规定:如果证书中存在不能识别的关键扩展,那么应用系统必须拒绝接受此证书;如果不能识别的扩展项是非关键的,则可以被忽略.但是,如果关键扩展的格式是合法的(可以被识别)但内容是非法的,这种情况应该如何处理,X.509 没有明确规定,这就导致了应用系统的处理存在分歧.例如,CRL(certificate revocation list)扩展域 CRL Distribution Point 在 X.509 标准中规定:应当(SHOULD)设为非关键,而不是必须(MUST). 如果将证书中的 CRL Distribution Point 扩展标记为关键,其中的 fullname 字段的格式符合 X.509 标准中的 Directory Name 定义,可以被识别,但却无法访问.这样的证书在 openssl0.9.6h 中可以通过验证,但在 openssl0.9.7d 中则无法通过验证.如果将这一扩展设为非关键,在这两个版本的 openssl 中都可以通过验证.这就意味着,即使同样是符合 X.509 标准的证书,它们的格式也可能存在差异,而且有的差异能够影响到应用系统对证书有效性的验证.个别 PKI 系统的证书格式不完全符合 X.509 标准,更容易出现这样的情况.

不同信任域的实体之间实现互连、互通、互操作,首先必须建立有效而可信的信任路径(证书链).证书链有效与否,则由应用系统进行验证.由于证书可能存在格式上的差异,因此有可能出现这样的情况:证书链中来自不同信任域的证书,在所属的信任域内都是有效的,但是格式上的差异影响了应用系统对证书有效性的验证,有的被认定为有效,有的则被认定为无效,从而导致全部由有效证书组成的证书链被应用系统认定为无效.因此,有必要讨论证书格式的差异性对应用系统验证证书有效性的影响.

在实际应用中,同一信任域中的所有证书,其格式即使在细部有所差异,也不会影响基于此信任域的应用系统对证书有效性的验证.因此,同一信任域中所有证书的格式对应用系统验证证书有效性的影响是一致的.

定义 **1**. 证书格式兼容:一种格式的有效证书,能够被基于另外一种格式证书的应用系统认定为有效.

定义 **2**. 证书格式兼容系数 $C(x,y)$:表征两种证书格式兼容程度的系数.

对信任域 A 和 B,若对 B 中的任意证书 b,有:

b 能够被基于 B 的应用系统认定为有效$\Rightarrow b$ 能够被基于 A 的应用系统认定为有效

成立,则称 B 的证书格式兼容于 A,记作 $C(B,A)=1$;反之,则称 B 的证书格式不兼容于 A,记作 $C(B,A)=0$.若 $C(B,A)=C(A,B)=1$,则称 A 和 B 的证书格式互相兼容.

对信任域 A 来说,如果信任域 B 中的实体 a 要和 A 中的实体进行互连、互通、互操作,必须首先构建从 a 开始、以 A 的信任锚为根的证书链.但是,如果 A 和 B 之间存在证书格式兼容性问题,即使这样的证书链存在,而且其中的所有证书都是有效的,也不一定能够通过基于信任域 A 的应用系统的验证.只有当 $C(B,A)=1$ 时,证书链才能够通过应用系统的验证,从而实现不同信任域内实体的互连、互通、互操作.

2 桥 CA 结构的局限性

桥 CA 结构是分布式结构信任模型的一种.桥 CA 通过分别与多个信任域的信任锚进行交叉认证的方式,建立不同信任域的信任锚之间的信任路径,从而实现不同信任域实体之间的互连、互通、互操作.在桥 CA 结构中,在 N 个信任域之间建立完全的信任路径,只需进行 N 次交叉认证,而另外一种分布式信任模型——网状结构,则需要进行 C_N^2 次交叉认证.在 N 比较大的情况下,桥 CA 结构的开销比网状结构小很多.因此,桥 CA 结构十分适合解决多个信任域之前的互连、互通、互操作问题,而且在实践中已经得到初步的应用.

在桥 CA 结构中,原有的信任域结构并没有改变.因此,桥 CA 结构中有多个信任域存在.同时,桥 CA 与各信任域的信任锚进行交叉认证时相互签发了证书.因此,桥 CA 结构中一旦存在证书格式兼容性问题,其程度更加严重,各个信任域之间以及桥 CA 与各个信任域之间,都有可能存在证书格式兼容性的问题,从而导致不同信任

域实体之间的互连、互通、互操作无法实现.

3 证书的格式转换

在桥 CA 结构中,存在多个信任域.在大规模网络的环境下,对于发起互连、互通、互操作的实体来说,不一定能事先确定对方所属的信任域,因此也不能确定对方所支持的证书格式.以 SSL(secure socket layer)为例,客户端只有连接到服务器端,交换了特定的消息之后,才能获取服务器端的证书链,从而得知服务器端所属的信任域以及证书的格式.如果客户端与服务器端所属的信任域不同,记客户端所属的信任域为 A,服务器端所属的信任域为 B,考虑 A 与 B 的证书格式兼容性,则有可能出现如下 4 种情况:

1) $C(A,B)=0,C(B,A)=1$.在此情况下,服务器端持有的证书能够通过客户端的验证,客户端持有的证书无法通过服务器端的验证.客户端可以与服务器端建立单向 SSL 连接,但是无法建立双向 SSL 连接.
2) $C(A,B)=1,C(B,A)=0$.在此情况下,服务器端持有的证书无法通过客户端的验证,客户端持有的证书能够通过服务器端的验证.客户端既不能与服务器端建立单向 SSL 连接,也不能建立双向 SSL 连接.
3) $C(A,B)=0,C(B,A)=0$.在此情况下,服务器端和客户端持有的证书都无法通过对方的验证.客户端既不能与服务器端建立单向 SSL 连接,也不能建立双向 SSL 连接.
4) $C(A,B)=1,C(B,A)=1$.在此情况下,服务器端和客户端持有的证书都可以通过对方的验证.客户端可以与服务器端建立单向 SSL 连接,也可以与服务器端建立双向 SSL 连接.

由上可知,引入证书格式兼容性概念之后,如果客户端和服务器端所属的信任域存在证书格式兼容性问题,无论信任域之间是否存在可信的信任路径,客户端都有可能无法通过服务器端的验证,从而不能与服务器端建立 SSL 连接.

为了确保客户端能够与服务器端建立 SSL 连接,除了通过查找信任路径,使客户端和服务器端使用信任锚相同的证书链之外,还要保证客户端和服务器端持有的证书不存在格式兼容性问题.因此,需要对其中一方的证书进行格式转换.由于服务器端可能要处理来自多个客户端的 SSL 连接,为了避免服务器端的负担过重,优先考虑对客户端持有的证书进行格式转换.

在大规模网络应用的环境下,客户端可能要与不同的服务器端建立 SSL 连接,这些实体所属的信任域可能不同,所兼容的证书格式也可能不同.如果客户端所属信任域的 CA 以离线的方式按照服务器端兼容的证书格式为客户端重新签发证书,客户端可能同时持有多张不同格式的证书,这些证书如何管理是一个难题;如果客户端以在线的方式参与到客户端和服务器端的 SSL 握手过程中去,等到客户端获得了服务器端的证书链之后,再根据兼容的证书格式为客户端重新签发证书,一旦信任域内实体的数量较多,或者与信任域外实体的通信量较大,CA 的负担则会相当沉重.另外,如果客户端所属的信任域是多级层次结构,信任路径的所有节点都需要重新签发证书,这就使得信任锚的负担更加沉重.

为了避免信任锚的负担过于沉重,可以在信任域中设立专门的可信机构来处理证书格式兼容性问题.信任域外实体证书链的有效性,由专门机构来进行验证.如果证书链被验证为有效,则可以为该实体签发临时证书.双方使用基于同一个信任锚的证书链,就可以避免证书格式兼容性问题的干扰.由此,在桥 CA 结构的基础上提出了一种新的分布式结构的信任模型:双桥结构(double-bridge).

4 双桥结构

4.1 双桥结构的框架

双桥结构的体系框架如图 1 所示.定义两种专门机构:证书链验证机构 VA(verification authority)以及验证消息管理机构 BVA(bridge VA).每个信任域对应一个 VA.BVA 在框架中处于中心位置,呈辐射状与各个 VA 连接.

在双桥结构中,每个信任域都设有一个 VA.VA 是信任域中的实体,持有信任锚签发的证书.VA 接收所属信任域内实体提交的证书链验证消息,提交给 BVA,再从 BVA 接收验证结果,发回给相应的实体.另外,VA 也响应

BVA 发来的证书链验证消息,对所属信任域内的证书链进行验证,将验证结果提交给 BVA.VA 还负责为信任域外的可信实体签发临时证书.

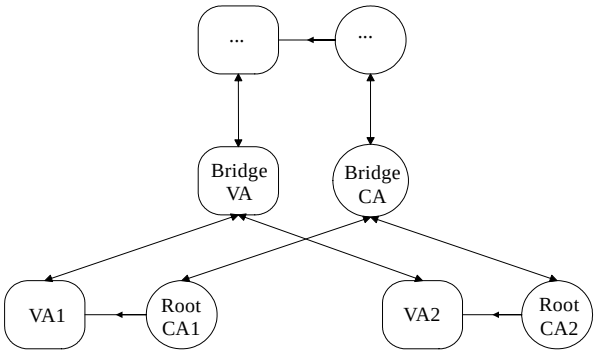

Fig.1 The framework of double-bridge

图 1 双桥结构的体系框架

VA 在 BVA 注册,注明所属的信任域之后,可以通过 BVA 与其他 VA 进行消息交互.BVA 记录了所有注册的 VA 所属的信任域以及信任域之间的信任路径的拓扑结构,包括信任域之间是否存在信任路径、信任路径的组成节点、信任路径是否被双方信任等.BVA 接收 VA 提交的证书链验证消息,从中提取信任锚的信息.如果信任域之间存在可信的信任路径,BVA 就将证书链验证消息转发给相应信任域的 VA,接收验证结果,将其返回给提交消息的 VA;否则,向提交消息的 VA 返回验证未通过的消息.信任域外实体的签发证书请求消息,也以同样方式通过 BVA 进行交互.

4.2 双桥结构中的证书链验证

在双桥结构中,不同信任域之间的实体之间进行互连、互通、互操作时,验证信任路径由相应的 VA 通过 BVA 完成.以 SSL 为例,客户端得到服务器端发来的证书链之后,不直接对证书链进行验证,而是将其提交到所属信任域的 VA1,如图 2 所示.VA1 从证书链中解析出证书链的信任锚:如果不是本信任域的信任锚,则将证书链验证消息提交给 BVA;否则,直接对证书链进行有效性验证,并向实体返回验证结果.BVA 对 VA1 提交的消息进行解析,获取客户端和服务器端所属信任域的信息.如果两个信任域之间存在可信的信任路径,BVA 就将消息转发给相应的 VA2;否则,向 VA1 返回验证结果无效的消息.VA2 收到 BVA 转发的消息后,以查询 CRL 或者其他方式验证证书链的有效性,然后将结果通过 BVA 发给 VA1.如果证书链是有效的,VA1 再通过 BVA 向 VA2 提交客户端的临时证书签发请求.如果 VA2 认为 VA1 可信,则为客户端签发证书,生成新的证书链.最后,新的证书链通过 VA2,BVA 和 VA1 传给客户端.客户端使用新的临时证书链代替原有的证书链,与服务器端继续进行 SSL 会话.此时,客户端和服务器端使用的证书链的信任锚是相同的,格式也一样,相当于两者属于相同的信任域,SSL 会话就不会受到证书格式的干扰.

为了提高消息交互的安全性,VA 和 BVA 之间的消息交互以加密的方式进行.因此,VA 和 BVA 之间需要进行密钥协商.如果通过 SSL 等在线方式进行密钥协商,则将面临两个问题:首先,VA 和 BVA 之间的消息交互数量很大.如果每次交互都重新建立 SSL 会话,则会对 VA 和 BVA 造成沉重的负担.如果在 BVA 和 VA 之间维护固定的 SSL 会话,异常处理(例如,某一端崩溃之后 SSL 会话资源的释放)又是一个难题;其次,不同的 VA 属于不同的信任域,而 BVA 不属于某一个信任域.即使 BVA 可以通过某种方式持有证书,VA 和 BVA 之间也可能存在证书格式兼容性问题.因此,VA 和 BVA 之间的密钥协商在注册的同时以离线的方式进行:当 VA 注册到 BVA 时,提交所持有的公钥,注明所属的信任域,并且与 BVA 协商加密消息所使用的对称加密算法以及密钥.VA 和 BVA 之间交互的消息分为两部分:以明文方式交互的、带有签名的消息头以及加密的、带有校验码的消息体.消息头注明消息的来源,同时通过签名机制确保消息头的完整性和不可否认性;消息体通过校验码机制确保消息的完整性,同时使用加密体制防止可能的监听.这样,可以在一定程度上防止攻击者对 VA 和 BVA 的仿冒,同时不会

给 VA 和 BVA 带来过大的负担.

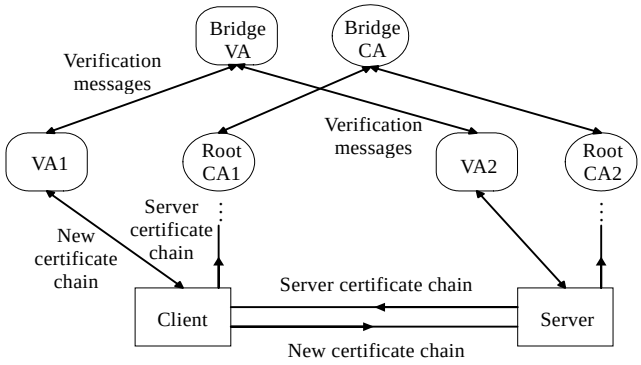

Fig.2 SSL sessions with double-bridge

图 2 双桥结构下的 SSL 流程

5 双桥结构的特点

在双桥结构中,证书链的有效性由属于同一信任域的 VA 验证,避免了证书格式兼容性的干扰,不需要调整证书格式就能够实现不同信任域实体之间的互连、互通、互操作.在实际应用中,有的已经建成的信任域由于历史原因,证书格式不完全符合 X.509 标准,而且安全基础设施与应用系统之间的关联过于紧密,调整证书格式可能会对应用系统造成重大影响,甚至导致应用系统失效.这样的信任域与其他证书格式符合 X.509 标准的信任域之间容易存在兼容性问题.双桥结构具有良好的兼容性,可以实现不同格式信任域之间的互连、互通、互操作.

在双桥结构中,BVA 记录了所有注册的 VA 所属的信任域之间信任路径的拓扑结构,证书链验证消息的转发与否由 BVA 决定.如果 BVA 不转发证书链验证消息,证书链就会被认定为无效,相应的信任路径也就失去了作用.因此,只要在 BVA 制定策略,明确在何种情况下转发证书链验证消息、在何种情况下不转发,就可以对不同信任域之间的信任路径进行集中化管理.信任域外实体的临时证书统一由 VA 签发,临时证书的有效期限便于控制. 另外,可以在 VA 集中定制策略,在证书的 SubjectName 或 Extension 等数据域中加入相应的特征字符串,便于应用系统对持有临时证书的实体的访问权限进行控制.

双桥结构的主要风险来自于 VA 和 BVA.在双桥结构中,证书链的有效性完全由信任域外的 VA 来验证.而其他信任域的 VA 是否可信并没有严格的验证,只是由 BVA 通过注册等手段以离线的方式来确认 VA 的可信程度.如果 BVA 对 VA 可信程度的确认流程存在漏洞,VA 就有可能被攻击者仿冒,从而达到骗取临时证书的目的.另外,在双桥结构中并没有严格地验证 BVA 是否可信,所以 BVA 也有可能被攻击者仿冒.因此,需要对持有临时证书的实体进行更加严格的访问控制,可能需要在应用系统中对实体的可信程度作另外的验证.为了降低风险,需要在应用系统中针对临时证书制定更加严格的访问控制策略,必要时可以通过其他途径来验证持有临时证书的实体的可信程度.

6 结束语

本文提出了证书格式兼容性的概念,给出了衡量证书格式兼容性的兼容系数的定义,在桥 CA 的基础上提出了一种兼容性较强的分布式信任模型,这有助于实现使用不同格式的证书的 PKI 之间的互连、互通、互操作.

致谢 在此,我们向对本文的工作给予支持和建议的老师,尤其是中国科学院信息安全国家重点实验室的连一峰老师表示感谢.

References:

[1] Weimerskirch A, Thonet G. A distributed light-weight authentication model for Ad-Hoc networks. LNCS, 2001,2288:341−354.

[2] Ma MC, Meinel C. A proposal for trust model: Independent trust intermediary service (ITIS). In: Proc. of the ICWI 2002. 2002. 785−790.

[3] Thompson MR, Olson D, Cowles R, Mullen S, Helm M. CA-Based trust model for grid authentication and identity delegation. In: Proc. of the GGF7. 2003.

[4] Xie DQ, Leng J. PKI Principle and Technology. Beijing: Tsinghua University Press, 2004 (in Chinese).

[5] Feng DG. Computer and Communication Network Security. Beijing: Tsinghua University Press, 2001 (in Chinese).

[6] Adams C, Farrell S. Internet X.509 public key infrastructure certificate management protocols. RFC2510, 1999.

[7] Myers M, Adams C, Solo D, Kemp D. Internet X.509 certificate request message format. RFC2511, 1999.

[8] Chokhani S, Ford W. Internet X.509 public key infrastructure certificate policy and certification practices framework. RFC2527, 1999.

[9] Ford W, Polk W, Solo D. Internet X.509 public key infrastructure certificate and CRL profile. RFC2459, 1999.

[10] Hoffman P. Internet X.509 public key infrastructure operational protocols: FTP and HTTP. RFC2585, 1999.

[11] Burton S, Kaliski Jr. A Layman's Guide to A Subset of ASN.1, BER and DER. Redwood: RSA Data Security Inc., 1991.

附中文参考文献:

[4] 谢冬青,冷健.PKI 原理与技术.北京:清华大学出版社,2004.

[5] 冯登国.计算机通信网络安全.北京:清华大学出版社,2001.

朱鹏飞(1977－),男,江苏镇江人,博士,主要研究领域为信息系统安全,公开密钥基础设施.

戴英侠(1942－),女,教授,主要研究领域为信息系统安全.

鲍旭华(1977－),男,博士生,主要研究领域为入侵检测,报警关联,人工智能.