P.O.Box 8718, Beijing 100080, China
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn

Journal of Software, Aug. 2006,17(8):1818-1823
ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP

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

Full-Text PDF Submission Back

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)
作者简介: 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.
联系人: 朱鹏飞 Phn: +86-10-88258551, E-mail: tempzhu@163.com

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

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.

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.
DOI: 10.1360/jos171818
http://www.jos.org.cn/1000-9825/17/1818.htm

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.

基金项目：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))

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.