计算机应用 2012, 32(03) 686-689 DOI: 10.3724/SP.J.1087.2012.00686 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

自动信任协商中环策略依赖检测技术

王凯[1,2],张红旗[1,2],任志宇[1,2]

1.信息工程大学 电子技术学院, 郑州 450004;
2.河南省信息安全重点实验室, 郑州 450004

摘要: 针对自动信任协商(ATN)可能出现协商过程无限循环的问题,对循环产生的原因进行了分析并设计相应的检测算法以及时发现并终止协商循环。协商双方策略间的依赖关系存在环是无限循环协商产生的原因,将策略间的依赖关系建模成简单图并证明了模型的正确性;分析简单图的可达矩阵计算过程并给出简单图环检测定理,基于该定理设计检测算法对环策略依赖进行检测。最后,通过实例验证了算法的可行性。

关键词: 自动信任协商 属性证书 访问控制 环策略依赖 简单图 可达矩阵

Cyclic policy interdependency detection in automated trust negotiation

WANG Kai[1,2], ZHANG Hong-qi[1,2], REN Zhi-yu[1,2]

1.Electronic Technology Institute, Information Engineering University, Zhengzhou Henan 450004, China;
2.Henan Province Key Laboratory of Information Security, Zhengzhou Henan 450004, China

Abstract: For Automated Trust Negotiation (ATN) consultative process may encounter the infinite cycling problem, the causes of the cycle were analyzed and the corresponding detection algorithm was designed to find and terminate the negotiation cycle. Interdependency relationships among policies in ATN were modeled as simple graph and the model's correctness was proved. The process of calculating simple grahp's reachability matrix was analyzed and cycle detection theorem was given. The algorithm of detecting cyclic policy interdependency was designed according to the theorem. Finally, a case study verifies the feasibility of the algorithm.

Keywords: Automated Trust Negotiation (ATN) attribute certificate access control cyclic policy interdependency simple graph reachability matrix

收稿日期 2011-09-01 **修回日期** 2011-11-18 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00686

基金项目:

国家863计划项目(2006AA01Z457, 2009AA01Z438);国家973计划项目(2011CB311801);河南省科技创新人才计划项目(114200510001)。

通讯作者: 王凯

作者简介: 王凯(1987-),男,四川射洪人,硕士研究生,主要研究方向:信任协商、访问控制;张红旗(1962-),男,河北遵化人,教授,博士生导师,博士,主要研究方向:等级保护、信任管理、网络安全;任志宇(1974-),女,河南汤阴人,讲师,博士研究生,主要研究方向:授权管理、访问控制。
作者Email: wklwzy057@163.com

参考文献:

[1]朱贤,邢光林,洪帆.分布式环境下的访问控制综述[J]. 微型机与应用,2005,24(1): 4-7.

[2]马晓宁,冯志勇,徐超. Web服务中跨安全域的基于信任的访问控制模型[J]. 计算机应用研究,2009,26

(12):4571-4573.

[3]汪应龙,胡金柱.自动信任协商中一种策略一致性管理方法[J].计算机应用, 2008,28(7):1795-1797.

[4]WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation [C]// Proceedings of DARPA Information Survivability Conference and Exposition. Piscataway, NJ: IEEE Press, 2000: 88-102.

[5]FERRALL S. RFC3281, An Internet attribute certificate profile for authorization[S], 2000.

[6]戴常英,张会娟.基于信任度的Web服务跨域访问控制[J]. 计算机工程与科学,2009,31(8): 42-45.

[7]LI N H, DU W, BONEH D. Oblivious signature-based envelope[C]// Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2003: 182-189.

[8]卢超,卢炎生,谢晓东,等.一种基于依赖分析的并发程序潜在死锁检测算法[J]. 小型微型计算机系统,2007,28(5): 841-844.

[9]RFC2459, Internet X.509 public key infrastructure certificate and CRL profile[S], 2000.

[10]夏冬梅,曾国荪,陈波,等.基于标签树的自动信任协商策略分析[J]. 计算机科学,2009,36(12): 154-158.

[11]YU T, WINSLETT M. A unified scheme for resource protection in automated trust negotiation[C]// Proceedings of the 2003 Symposium on Security and Privacy. Piscataway, NJ: IEEE Press,2003: 245-257.

[12]李建欣,怀进鹏. COTN:基于契约的信任协商系统[J]. 计算机学报,2006,29(8): 1290-1330.

[13]WINSBOROUGH W H, LI N H. Protecting sensitive attributes in automated trust negotiation[C]// Proceedings of the ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2002:41-51.

[14]YU T, WINSLETT M, SEAMONS K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Transactions on Information and System Security, 2003,6(1):1-42.

[15]杨秀文,严尚安,曾顺鹏,等.关于可达矩阵的求法探讨[J].数学的实践与认识,2003,33(11):128-130.

[16]方世昌.离散数学[M]. 2版. 西安: 西安电子科技大学出版社, 2006: 87-100,266-267.

本刊中的类似文章

1．武海鹰.基于上下文的普适计算使用控制模型[J]. 计算机应用, 2012,32(02): 489-492

2．熊鹏.水声传感器网络中基于改进时分多址技术的MAC协议[J]. 计算机应用, 2011,31(11): 2902-2904

3．李春泉 尚玉玲 胡春杨 朱攀峰.基于K-最短路算法的云制造多粒度访问控制技术[J]. 计算机应用, 2011,31(09): 2356-2358

4．刘立群.集中式无线局域网分离介质访问控制的CCMP设计[J]. 计算机应用, 2011,31(08): 2159-2161

5．王婷 陈性元 张斌 任志宇 王鲁.基于互斥角色约束的SSOD策略实现研究[J]. 计算机应用, 2011,31(07): 1884-1886

6．易磊 仲红 袁先平 赵玉.支持容错检索的数据共享方案[J]. 计算机应用, 2011,31(06): 1525-1527

7．曹成龙 傅德胜 曹凤艳.基于文件过滤驱动的移动存储控制方法[J]. 计算机应用, 2011,31(06): 1498-1501

8．周超 周城 郭亮.IEEE 802.1X的安全性分析及改进[J]. 计算机应用, 2011,31(05): 1265-1270

9．高大利 孙凌 辛艳.基于角色-权限的普适计算受限委托方法[J]. 计算机应用, 2011,31(05): 1298-1301

10．王婷 陈性元 任志宇.授权管理中的权限衍生计算方法[J]. 计算机应用, 2011,31(05): 1291-1294

11．李健利 霍光磊 刘博 高勇.基于魔方算法的自动信任协商敏感信息传输方案[J]. 计算机应用, 2011,31(04): 984-988

12．严骏 苏正炼 凌海风 朱亮 张蕉蕉.MIS中基于部门和角色的细粒度访问控制模型[J]. 计算机应用, 2011,31(02): 523-526

13．李健利 高勇 霍光磊 刘博.基于声誉的P2P信任系统[J]. 计算机应用, 2011,31(01): 147-150

14．余永红 柏文阳.基于加密技术的外包数据库服务集成安全[J]. 计算机应用, 2011,31(01): 110-114

15．张润莲 武小年.基于信任约束的用户安全管理[J]. 计算机应用, 2010,30(9): 2383-2385

16．孙凌 辛艳 罗长远.基于扩展角色访问控制的普适计算访问控制模型[J]. 计算机应用, 2010,30(4): 1045-1047
17．孙莹莹 郑扣根.基于微过滤驱动的文件监控系统[J]. 计算机应用, 2010,30(11): 3115-3117
18．钟将 侯素娟.开放网络环境中基于属性的通用访问控制框架[J]. 计算机应用, 2010,30(10): 2632-2635
19．孙伟 王淑礼 邬长安.基于RBAC的灵活代理委托模型[J]. 计算机应用, 2010,30(07): 1797-1801
20．林一多 高德云 梁露露 张思东.基于ARM的无线传感器网络MAC协议设计与实现[J]. 计算机应用, 2010,30(05): 1145-1148
21．唐晓东 付松龄 何连跃.基于eCryptfs的多用户加密文件系统设计和实现[J]. 计算机应用, 2010,30(05): 1236-1238
22．高川 朱群雄.RBAC角色继承关系中私有权限问题的研究[J]. 计算机应用, 2010,30(05): 1230-1232
23．郭晋凯 柏文阳 刘铭.基于安全更新视图的XML更新控制方法[J]. 计算机应用, 2009,29(12): 3409-3412
24．梅小虎 李代平 郭广义 周允强 尹伟 郭琨 郭鸿志.CDMA2000芯片操作系统安全部分的研究与设计[J]. 计算机应用, 2009,29(11): 2917-2919
25．魏立峰 孟凯凯 何连跃.面向用户角色的细粒度自主访问控制机制[J]. 计算机应用, 2009,29(10): 2809-2811
26．王宇新 王政 郭禾 刘天阳 田佳.基于XML图的RBAC模型研究[J]. 计算机应用, 2009,29(1): 185-188
27．高迎 战疆.P2P环境下基于信任度的可控委托信任管理模型[J]. 计算机应用, 2009,29(09): 2332-2335
28．李时文 卢建朱.快速有效的XML访问控制新方案[J]. 计算机应用, 2009,29(09): 2336-2338
29．马博 袁丁.基于Linux驱动级内核访问监控技术研究与实现[J]. 计算机应用, 2009,29(09): 2369-2374
30．刘玉梅 郭黎利 申丽然.联合空时需求预留和功率控制的MAC协议[J]. 计算机应用, 2009,29(08): 2170-2174
31．王睿 刘占军 李云 陈前斌 赵为粮.针对非对称链路的MAC协议改进策略[J]. 计算机应用, 2009,29(07): 1868-1870
32．陈钦 原焕 冯建华.企业检索中访问权限控制方法的实现与比较[J]. 计算机应用, 2009,29(07): 2000-2002
33．沈海波.面向语义Web的基于语义和上下文的访问控制模型[J]. 计算机应用, 2009,29(05): 1289-1292
34．张立臣 王小明.普适计算环境下的动态访问控制模型[J]. 计算机应用, 2008,28(8): 1931-1935
35．林丛 向勇.支持功率和速率控制的自组网MAC协议研究[J]. 计算机应用, 2008,28(8): 1946-1950
36．张润莲 武小年 董小社.基于委托的分布式动态授权策略[J]. 计算机应用, 2008,28(6): 1365-1368
37．陈娟娟 程西军.支持动态角色切换的RBAC模型[J]. 计算机应用, 2008,28(4): 924-926
38．姚慧 高承实 戴青 张徐.一种基于动态规划的自动信任协商策略[J]. 计算机应用, 2008,28(4): 892-895
39．张德银 刘连忠.多安全域下访问控制模型研究[J]. 计算机应用, 2008,28(3): 633-636
40．欧晓鸥 王志立 魏建香.基于RBAC与GFAC架构的访问控制模型[J]. 计算机应用, 2008,28(3): 612-614
41．刘志远 杨秋伟 崔国华 洪帆.一种基于标识的隐私资源保护方案[J]. 计算机应用, 2008,28(2): 418-421
42．李焕洲 刘益和 李华.基于信任和安全等级的P2P信息流模型[J]. 计算机应用, 2008,28(12): 3168-3170
43．晏樱 李仁发.P2P网络中一种可信访问控制模型[J]. 计算机应用, 2008,28(12): 3194-3196
44．丁怡 方勇 周安民 曾蕉 樊宇.网格环境下的G-R_TRBAC访问控制模型[J]. 计算机应用, 2008,28(12): 3214-3216
45．彭智勇 杨鏖丞 任毅.可信数据库—概念、发展和挑战[J]. 计算机应用, 2008,28(11): 2741-2744
46．吴俊军 朱建新 白喆.一种改进的轻量级嵌入式安全文件系统模型[J]. 计算机应用, 2008,28(1): 242-244
47．陈岳阳 马学森 韩江洪 魏振春.RBAC模型中用户代理机制的研究[J]. 计算机应用, 2007,27(9): 2200-2201
48．王志强 黄皓 夏磊.进程内细粒度保护域模型及其实现[J]. 计算机应用, 2007,27(6): 1356-1359
49．王婷 陈性元 张斌 包义保 夏春涛.基于GAA-API的Web网页细粒度访问控制方法研究[J]. 计算机应用, 2007,27(5): 1274-1276
50．夏鹏万 陈荣国 孙剑.增强的基于角色的数据库访问控制模型[J]. 计算机应用, 2007,27(3): 597-600
51．瞿进 李清宝 白燕 魏珉.文件过滤驱动在网络安全终端中的应用[J]. 计算机应用, 2007,27(3): 624-626
52．张艳霞 王劲林.一种P2P网络鲁棒访问控制协议[J]. 计算机应用, 2007,27(3): 538-540
53．陈志祥 陆音 陆桑璐 陈道蓄.基于协议转换的安全网关原型系统设计与实现[J]. 计算机应用, 2007,27(2): 299-302
54．晏立 朱宏伟.访问权限实时更新的模型与实现[J]. 计算机应用, 2007,27(11): 2712-2714
55．陈敏 刘晓强 .扩展RBAC的CRM动态用户访问控制模型与实现[J]. 计算机应用, 2007,27(10): 2508-2511

56. 沈海波 洪帆 .基于属性的授权和访问控制研究[J]. 计算机应用, 2007,27(1): 114-117

57. 杨涛;刘锦德;谭浩.Web服务安全基础设施的研究[J]. 计算机应用, 2006,26(6): 1248-1250

58. 刘孝保; 杜平安.J2EE模式下基于角色访问控制的应用[J]. 计算机应用, 2006,26(6): 1331-1333

59. 孟健; 曹立明; 王小平; 姚亮.XML文档的加密访问控制与传输[J]. 计算机应用, 2006,26(5): 1061-1063

60. 王娜; 陈越; 汪斌强.适用于多源IP组播的安全访问控制协议[J]. 计算机应用, 2006,26(4): 818-819

61. 谭良 周明天 .带时间特性的自主访问控制政策及其在Linux上的设计与实现[J]. 计算机应用, 2006,26(12): 2906-2909

62. 王雷 庄毅 潘龙平 .基于强制访问控制的文件安全监控系统的设计与实现[J]. 计算机应用, 2006,26(12): 2941-2944

63. 李志英 黄强 楼新远 冉鸣 .RBAC模型研究、改进与实现[J]. 计算机应用, 2006,26(12): 2945-2947

64. 张智广 郭忠文 .无线传感器网络中基于分簇的自适应MAC协议[J]. 计算机应用, 2006,26(11): 2528-2530

65. 王维林 张来顺 张远洋 .基于角色的Web Services动态访问控制模型[J]. 计算机应用, 2006,26(11): 2607-2609

66. 林宏刚;戴宗坤;李焕洲.BLP模型的时域安全研究[J]. 计算机应用, 2005,25(12): 2723-2724

67. 陈岳;周明天.基于SNMPv3安全机制的密钥分配系统的设计与实现[J]. 计算机应用, 2005,25(12): 2755-2758

68. 沈海波; 洪帆.Web服务中结合XACML的基于属性的访问控制模型[J]. 计算机应用, 2005,25(12): 2765-2767

69. 陈晓林;吴永英;李专.细粒度的XML推理控制及实现[J]. 计算机应用, 2005,25(11): 2544-2546

70. 徐洪学 ;刘永贤.基于RBAC的CSCD系统工作流授权模型[J]. 计算机应用, 2005,25(10): 2424-2427

71. 王建军;宁 洪;朱政坚.基于多级安全和属性证书实施网络基于角色访问控制策略[J]. 计算机应用, 2005,25(10): 2296-2298

72. 杨宁，徐志伟，周浩杰.基于RBAC的信息网格角色表示及矛盾冗余处理[J]. 计算机应用, 2005,25(07): 1568-1569

73. 刘英，张曙光.基于空间索引的二维空间区域访问控制模型[J]. 计算机应用, 2005,25(06): 1277-1278

74. 芮国荣，邢桂芬.基于角色和规则的访问控制[J]. 计算机应用, 2005,25(04): 864-866
