

Kerberos 协议及其授权扩展的研究与设计

马佩勋, 李 杰

(中南大学 计算机软件系, 湖南 长沙 410075)

摘 要: 尽管 Kerberos 协议被证明是一种在分布式网络环境下最理想的身份认证系统, 却存在一些安全缺陷和协议结构自身的局限性。虽然大部分得到了有效改进, 问题依然存在。在深刻理解 Kerberos 协议思想的基础上, 提出了一种基于 Kerberos 认证协议的授权扩展系统。该系统在不改变原 Kerberos 认证流程的情况下, 充分利用票据机制加载基于角色的访问控制信息, 成功实现了 Kerberos 认证与授权功能的无缝集成。

关键词: Kerberos; 认证; 授权; 票据; 角色

中图分类号: TP311

文献标识码: A

文章编号: 1673-629X(2006)05-0109-03

Research and Design of Kerberos Protocol Extended in Authorization

MA Pei-xun, LI Jie

(Department of Computer Software and Theory, Central South University, Changsha 410075, China)

Abstract: Though it has been proved that Kerberos protocol is the best authentication system in distributed network environment, there're still some limitations in security and protocol structure. Some of these problems are improved, while others still exist. With thorough studying of the principle of Kerberos protocol, this paper proposes an improved Kerberos protocol extended in authorization. The system can fully exploit tickets mechanism to load role-based access control information and successfully realize the seamless integration of Kerberos authentication and authorization.

Key words: Kerberos; authentication; authorization; ticket; roles

0 引 言

网络环境中的身份认证协议及系统, 是保证网络安全通信的必要条件, 具有十分重要的研究和应用价值。从1978年 Needham-Schroeder 协议——最为著名的早期认证协议的诞生算起, 安全协议的发展已经历经20余年了。其间涌现的经典安全协议还有 Otway-Rees 协议、Yahalom 协议、大嘴青蛙协议等, 以及一些重要的实用协议, 如 Kerberos 协议、CCITT X.509 协议等。而其中 Kerberos 系统是目前分布式网络计算环境中应用最广泛的认证协议之一。

Kerberos 是为 TCP/IP 网 (Internet) 设计的基于 Client/Server 模式的、以可信赖的第三方为基础用户身份认证协议, 也是 Internet 访问控制技术的一个代表, KryptoKnight 和 SESAME 便是在其借鉴之上的成果。它广泛应用于 Internet 服务的安全访问, 具有“高度的安全性、可靠性、透明性和可伸缩性”等优点。目前许多远程访问认证服务系统都支持 Kerberos 认证协议, 如微软的 EAP (可扩展认证协议)、CISCO 的终端访问控制器访问控制系统

(TACACS/XTACACS) 以及远程认证拨号业务 (RADIUS) 等, 同时 Windows2000 操作系统也将其集成作为本地认证协议。然而 Kerberos 协议本身却存在着固有的安全缺陷。文献[1]枚举了 Kerberos 的诸多安全缺点, 其中一部分问题在 Kerberos v5 中得到了解决, 还有一些由于 MIT 环境的局限以及本身协议设计的缺陷导致的问题一直是学术界的研究热点。例如 Kerberos 面临的重放攻击、口令猜测攻击、系统程序的安全性和完整性问题以及密钥的存储管理问题等等, 为此学术界和研究机构提出了大量的改进方案。在文献[2]中, 作者建议在 Kerberos 中引入序列号循环机制, 即由用户自己产生的一次性使用的随机数来代替时间戳以解决时间同步问题, 虽然在一定程度上达到了抵御重放攻击的目的却引起了协议结构的变更。在文献[3]中, 作者提出将 Smart Cards 集成到 Kerberos 中, 虽然利用其优良的安全特性能有效解决口令猜测攻击问题, 系统却需要附加新的硬件设备支持 Smart Cards 技术。另外一个研究热点则是利用公钥密码技术^[4,5]改进 Kerberos 协议, 从而有效解决 Kerberos 系统中密钥存储管理耗费太大的问题。同时却出现了公钥体制加解密的时间耗费远大于对称密钥系统的新问题。文中首先着重分析了 Kerberos 协议思想、协议流, 然后提出了一种基于 Kerberos 认证协议的授权扩展系统。

收稿日期: 2005-08-04

作者简介: 马佩勋 (1978-), 男, 湖南湘潭人, 硕士研究生, 主要研究方向为信息安全、企业信息集成; 李 杰, 教授, 主要研究方向为信息安全、企业信息集成。

1 Kerberos 认证方案

Kerberos 系统最初是美国麻省理工学院(MIT)为 Athena 项目开发的,它是基于 Needham-Schroeder 协议的变形,Kerberos 建立了一个中心认证服务器(KDC)来向用户和服务器提供相互认证,执行可信仲裁的作用,从而使得只有通过了认证的用户才能访问服务器,以防止未授权的用户得到服务和数据。有关 Kerberos 协议详细的介绍可以参照经典文献[6]。目前该协议已经有 5 个版本,其中 v1 到 v3 是内部开发版,v4 是 1988 年开发的,它们均只支持 DES 加密算法。而 v5 则是对 v4 中的某些安全缺陷做了改进,例如对多密钥系统的支持、票据生命周期的可设置性、身份证明传递功能、跨域密钥管理优化、预认证功能等等,并于 1994 年作为 RFC 标准(RFC1510 [KOHL93])公布。文中在 Kerberos v5 的基础上进行讨论。

符号说明:

C,ADC:表示客户端 Client 以及客户端的 IP 地址

S:应用服务器—Application Server

AS:认证服务器—Authentication Server

TGS:票据发放服务器—Ticket Granting Server

DB:用来保存各个客户端和应用服务器的标识信息以及它们与 AS 的共享对称密钥

KDC:由 AS, TGS, DB 构成统称为密钥分发中心—Key Distribution Center

IDC, IDS, IDTGS: 分别表示参入认证过程实体—C, S, TGS 的特定标志符

RealmC, RealmTGS, RealmS: 分别表示 C, TGS, S 所属的域

TicketTGS, TicketS: 分别表示客户端 C 访问 TGS 和 S 的访问票据

KC, KTGS: 分别表示 C 与 AS 的共享对称密钥和 C 与 TGS 的共享对称密钥

KC, TGS; KC, S: 分别表示 C 与 TGS 的临时会话密钥, C 与 S 的临时会话密钥

$\{ \{ KC, \} \{ KTGS, \} \{ KC, TGS, \} \{ KC, S, \}$ 分别表示以密钥 KC; KTGS; KC, TGS; KC, S 加密的信息

Times: 表示票据的时间信息,包含起始时间、结束时间、更新时间

TS1, TS2: 表示时间戳

Seq #: 起始序列号可选字段,用来检测重放攻击

SubKey: 客户端 C 对加密密钥的选择,缺省则用 KC, S 加密

Option, Nonce: 随机值,作为预认证信息

AuthenticatorC: 用户认证符,包含 IDC, RealmC, TS 等信息

Kerberos 协议思想很简明,认证模型如图 1 所示。整个认证过程分 3 个阶段,6 个步骤。客户从认证服务器(AS)请求一张票据许可票据(Ticket Granting Ticket,

TGT)用作票据许可服务(Ticket-Granting Service, TGS),该票据用用户的秘密密钥加密后发送给用户。为了使用特定的服务器,客户需要用 AS 颁发的 TGT 从 TGS 那里请求一张对应的服务票据,TGS 经过验证后将服务票据发送给客户,客户将服务票据呈现给应用服务器,服务器经过认证之后允许客户访问服务。

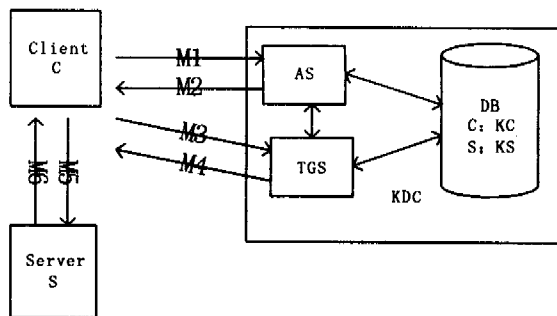


图 1 Kerberos 认证流程图

在图 1 所示的 Kerberos 认证过程中,用户 C 与 AS, TGS 和服务器 S 之间所交换的信息结构比较复杂,详细说明如下:

(1) 身份验证服务交换: 获得票据授予的票据。

M1: C → AS: Options, IDC, RealmC, IDTGS, Times, Nonce

M2: AS → C: IDC, RealmC, TicketTGS, $\{ KC, TGS, Times, Nonce, RealmTGS, IDTGS \} KC$

其中: TicketTGS = $\{ KC, TGS, RealmC, IDC, ADC, Times \} KTGS$

(2) 票据授予的服务交换: 获得服务授予的票据。

M3: C → TGS: Options, IDS, TicketTGS, Times, Nonce, AuthenticatorC

M4: TGS → C: IDC, realmC, TicketS, $\{ KC, S, Times, Nonce, RealmS, IDS \} KC, TGS$

其中: TicketTGS = $\{ KC, TGS, RealmC, IDC, ADC, Times \} KTGS$

TicketS = $\{ KC, S, RealmC, IDC, Times \} KS$

AuthenticatorC = $\{ IDC, RealmC, TS1 \} KC, TGS$

(3) 客户机/服务器身份验证交换: 获得服务。

M5: C → S: Options, TicketS, AuthenticatorC

M6: S → C: $\{ TS2, SubKey, Seq \# \} KC, S$

其中: AuthenticatorC = $\{ IDC, RealmC, TS2, SubKey, Seq \# \} KC, S$

在客户机从认证服务器申请得到的票据许可票据 TGT 的有效生命周期之内,如果客户机需要申请另外一个应用服务器上的服务只需重复 M3~M6 的消息交换步骤即可。这就表示 Kerberos 协议能够很好地用于共享认证数据,同一个客户机能够与不同的应用服务器相互认证,并且整个过程对于用户来说都是透明的,所以 Kerberos 特别适应于单点登录的场合。有关 Kerberos 跨域认证的流程请参考文献[6],这里不再赘叙。

2 Kerberos 认证方案中授权机制扩展

Kerberos 认证系统仅仅为申请服务的客户提供身份证明,它本身并不能提供任何信息来决定客户是否真正被授权使用所申请的服务。也就是说,Kerberos 仅仅是一个认证系统,它不提供授权机制。而实际上,认证只有和授权、记账服务集成在一起才会构成完整的访问控制过程。然而围绕 Kerberos 的研究大多依然集中在其身份鉴别功能和安全特性之上,或者仅在本本地环境下讨论授权和记账机制。对于应用日益广泛的分布式网络环境,相应的授权和记账机制的研究并不多。在文献[7]中,作者讨论了如何在 Kerberos v 鉴别系统中实现受限代理,并介绍了网络环境下如何利用受限代理实现分布式授权和记账机制。但是此种方案实现和应用起来比较复杂。在文献[8]中,作者介绍了一种利用 Smart Cards 技术在 Kerberos 基础上实现一次性授权的机制。其安全性固然得到了加强,却需要引入新的硬件设备支持 Smart Cards 技术,同时还存在需要添加众多功能组件、难以实现与原 Kerberos 认证系统无缝集成等缺陷。下面介绍 Kerberos 授权扩展系统(简称为 Kerberos_Ps_Extend),则是在 Kerberos 强认证功能的基础上,采用基于角色的访问控制技术,成功实现了 Kerberos 认证和授权的无缝集成。

2.1 Kerberos 授权扩展系统设计

目前比较流行的企业网(Intranet)属于典型的分布式网络环境,存在各种各样的应用服务,而这样的应用服务还在不断增加。各个应用服务均有自己的一套安全管理机制,包括身份认证、权限管理等等。所以亟待一种提供统一身份认证、分布式授权的解决方案。Kerberos 授权扩展系统旨在提供这样一套完整的解决方案。同时笔者认为,在 Kerberos 认证系统的基础上做授权机制的集成应该遵循如下几个设计原则:首先应该充分考虑其应用场景;其次应当保证在不破坏原 Kerberos 协议的基础上做相应的授权机制集成;最后在保证安全的前提下,应当尽量降低系统实现的难度。

首先考虑到一个企业里面职务种类划分相对固定,故采用的权限管理策略就是:员工对应职务,职务对应角色,角色对应权限。为此使用了授权服务器(Privilege Server)保存下表所示的权限对应关系:

客户标志符 (IDC)	角色值 (Role_Values)
----------------	----------------------

其中角色值(Role_Values)是一个二进制值(暂定为八位,根据企业具体情况而定),其值的变化范围为 0~255。每个值代表一个角色,故可表示 256 种角色。这样授权服务器便可以根据需要修改客户与角色值的对应表,随时调整用户的角色,达到灵活控制授权的目的。

其次为了保证不破坏原 Kerberos 协议而又与基于角色的授权机制无缝集成,将 Kerberos 授权扩展系统嵌套运行于原 Kerberos 认证框架之内,整个 Kerberos 授权扩展系统的体系结构如图 2 所示。

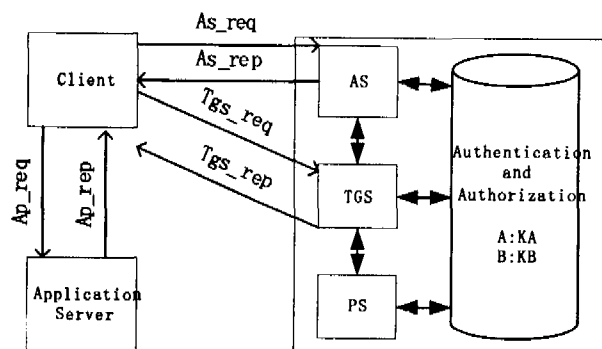


图 2 Kerberos 授权扩展系统体系结构示意图

其工作过程与原 Kerberos 系统一样,依然分为 3 个阶段,6 个步骤。所不同的是,当客户用从认证服务器(AS)申请到的票据授予票据(TicketTGS)去票据授予服务器(TGS)申请特定的服务票据(TicketS)时,TGS 根据客户标志符 IDC 与授权服务器(Privilege Server)通过安全握手取得客户对应的角色值,然后将其填充到服务票据(TicketS)中。最后当客户用服务票据到特定的应用服务器申请服务时,应用服务器提取出客户的角色值,然后到授权服务器中查询客户角色值对应的具体权限列表,从而授予用户相应的权限。

协议流更改如下:

M4: TGS → C: IDC, realmC, TicketS, {KC, S, Times, Nonce, RealmS, IDS} KC, TGS

其中:TicketTGS= {KC, TGS, RealmC, IDC, ADC, Times}KTGS

TicketS= {KC, S, RealmC, IDC, Role-Values, Times}KS

AuthenticatorC= {IDC, RealmC, TS1}KC, TGS

2.2 Kerberos 授权扩展系统性能分析

1) 该系统完全利用了 Kerberos 原有的认证机制及安全特性。在实现用户认证的同时进行了授权控制。

2) 该系统利用 Kerberos 原有的票据机制封装简单的用户授权映射信息,充分体现了方便性和灵活性。

3) 该系统采用基于角色的访问控制模式,实行访问控制信息统一集中管理和分布式认证、授权相结合的访问控制策略。

4) 该系统不足之处在于目前尚且只适用于企业网(Intranet)环境,暂只支持单一的基于角色的访问控制策略。同时应用服务器端的模块需要做部分修改以支持分布式授权。

3 总结

Kerberos 协议作为一种主要的身份认证协议,自诞生以来就得到了广泛的应用,增强了网络通讯安全。虽然存在一些局限性和缺陷,经过不断改进已经变得越来越成熟。与以往 Kerberos 改进方案不同,文中介绍了一种在 Kerberos 认证协议的基础上进行授权机制扩展的新系统,

(下转第 114 页)

DIUS-LDAPv3 两个 schema 文件,并且设置了相应的目录结构,通过 ldif 文件加入记录,每一条 user 记录中包括用户名和密码,以及认证类型 Auth-Type,内容的多少可以根据需求(如计费需求)增减。

2.3 Web 认证中的问题

- NAS 和 Portal 之间的通信协议不是标准协议,需要 NAS 设备提供商提供接口,否则不能交互;

- 用户端浏览器第一次连接时 NAS 应将其定向于 Portal 的页面上,之后用户端通过 Web 执行 Java 小程序用以计时或者流量等;

- 用户非正常下线的处理:可以通过 NAS 定时发送握手信息给用户主机,如果连续 3 次不响应,可以判断用户离线。

3 RADIUS 服务器的性能测试

RADIUS 服务器的性能关系到正式投入运行后用户的等待时间、网络稳定性,直接影响到服务质量的好坏,所以一个简单的性能测试是必需的:

测试环境为:

- 软件环境:

OS: REDHAT ENTERPRISE Linux AS 3.0

RADIUS: Freeradius-1.0.0-pre3

LDAP: OPENLDAP-2.2.13 + Berkeley DB. 4.2.

25

Database: MySQL-Standard-4.0.20-pc-Linux

WebServ: Apache-2.0

- 硬件环境:

4 台普通 PC + Dell Linux 服务器

- 网络环境:

Hub 式共享局域网内

测试结果如图 6 所示。

图中横轴表示使用的客户机的台数,纵轴表示 log 文件中平均每分钟服务器响应的个数。显然随着认证来源的增加,服务器响应速度有所减慢,但总体的负载能力基

本满足电信负荷的要求,并且这里是在普通试验环境,若移植到分布式或者集群的环境中,负载能力会进一步提高。

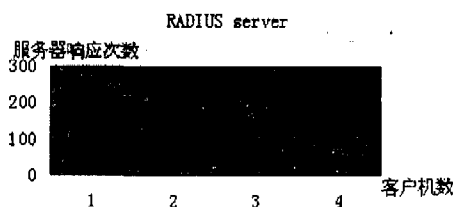


图 6 性能测试结果

4 结 论

描述了 FTTH 宽带网络中的用户 Web 认证技术,并且对其性能作了一定的测试,Web 认证有很明显的优点,当然也有一些缺点,如认证效率相对于 PPPoE 较低^[7],但现代 OSS 强调的是“以客户为中心”,对新业务的支持要非常灵活,而这正是 Web 认证的优点,也是未来发展的方向。可以预见,随着 FTTH 宽带业务的进步和发展,Web 认证技术会更有用武之地。

参考文献:

- [1] 邹洁. 宽带接入认证和计费方式分析[J]. 广东通信技术, 2002(6):15-20.
- [2] 崔晓波. RADIUS 协议的原理(上)[J]. 中国数据通信, 2001(2):49-51.
- [3] Hassell J. Radius[M]. America: O'Reilly, 2002.
- [4] RFC2865, RFC2866. Remote Authentication Dial In User Service, RADIUS Accounting[S]. 2000.
- [5] 李有斌. 宽带城域网建设主要接入认证方式及其分析[J]. 江西通信科技, 2003(3):40-41.
- [6] 邢小良. 宽带网接入认证的发展方向——WEB 认证[J]. 通信世界, 2002(4):23-26.
- [7] Hill J. An Analysis of the RADIUS Authentication Protocol [EB/OL]. <http://www.untruth.org/josh/security/radius/radius-auth.html>, 2001.

(上接第 111 页)

实现了 Kerberos 认证和授权功能的无缝集成。

参考文献:

- [1] Bellare S M, Merritt M. Limitations of the Kerberos Authentication System[J]. ACM SIGCOMM Computer Communication Review, 1990, 20(5):119-132.
- [2] Kehne A, Schonwalder J, Langendorfer H. A nonce-based protocol for multiple authentication[J]. Operating Systems Review, 1992, 26(4):84-89.
- [3] Itoi N, Honeyman P. Smartcard integration with kerberos v5 [J]. Lecture Notes in Computer Science, 2001, 2041:73-78.
- [4] 蒙杨, 刘克龙, 卿斯汉. 一种利用公钥体制改进 Kerberos 协议的方法[J]. 软件学报, 2001, 12(6):872-877.

- [5] 文铁华, 谷士文. 增强 Kerberos 协议安全性的改进方案[J]. 通信学报, 2004, 25(6):76-79.
- [6] Steiner J G, Neuman B C, Schiller J I. Kerberos: An Authentication Service for Open Network Systems[A]. In Proceedings of the {USENIX} Technical Conference[C]. [s.l.]: USENIX Association, 1988. 191-202.
- [7] Neuman B C. Proxy-Based Authorization and Accounting for Distributed Systems [A]. International Conference on Distributed Computing Systems [C]. [s.l.]: The Washington Technology Center, 1993. 283-291.
- [8] Au R, Looi M, Ashley P. Cross-domain one-shot authorization using smart cards[A]. In Proceedings of the 7th ACM conference on Computer and communications security[C]. [s.l.]: ACM Press, 2000. 220-227.