一种基于角色的校园网统一身份认证解决方案

黄朝阳

(厦门海洋学院 信息技术系,福建 厦门 361100)

摘 要：在对高校校园网统一身份认证安全需求进行分析的基础上，提出基于角色的校园网统一身份认证解决方案,即在同一个身份认证系统中兼容三种改进的、具有不同强弱认证标准的认证机制。在大学校园网具体应用环境中,分析这一解决方案的系统开销和网络开销,并与其安全性能分析相结合,找寻效率与安全性能的最佳平衡点。

关键词：统一身份认证;角色;口令认证;Kerberos;数字证书

中图分类号：TP302 **文献标识码**：A **文章编号**：1674-7720(2010)23-0044-03

An unified identity authentication scheme of campus network based on role

HUANG Chao-Yang

(Department of Information and Technology, Xiamen Ocean College, Xiamen 361100, China)

Abstract: Firstly, on the basis of analyzing the security requirement of unified identity authentication system of campus network, the unifie identity authentication scheme of university campus network based on role which had three improved authentication schemes and different security capability was proposed in this paper. Secondly, the system spending and network spending proposed by this thesis were analyzed at length under the concrete environment of the campus network. Thirdly, from the view of security and efficiency, the paper found a perfect balance to design the unified identity authentication system of university campus network.

Key words: unified identity authentication; role; password authentication; Kerberos; digital certificate

校园网统一身份认证系统是实现数字校园多应用系统集成的必要条件。如果在校园网统一身份认证系统中只使用某一种协议,会出现如下情况:或者效率较高,但安全性能却不能满足需求;或者能满足安全需求,但系统开销和网络开销又太大。因此,认证系统中身份认证方案的选取应当与具体应用环境有机结合,才能发挥其最佳效能。

1 基于角色的统一身份认证解决方案

高校应用系统的使用者可以粗分为学生、普通教职员工和管理者。这三种角色对应用系统的访问权限存在着明显的差别,他们对身份认证也有着完全不同的安全需求。

如果全面推行强身份认证机制,在获取高安全性能的同时,必然存在实现复杂、系统要求高、所需的建设和维护费用高的缺点。若全面延用简单身份认证机制,虽使用方便、实现简单,但认证的安全性偏低。而如果在身份认证机制的选择上采取折衷的方法,Kerberos 身份认证机制似乎是一种不错的选择,但认证过程相对复杂,用户量大时密钥管理困难。

本文提出一种基于角色的统一身份认证解决方案,即在同一个身份认证系统中兼容三种改进的、具有不同强弱认证标准的认证机制。

1.1 适用学生用户的身份认证协议

以学生为代表的用户人数最多,且每年有大量的学生毕业离校,又有大量的新生入学,而学生用户所使用的校园网服务除图书借阅和选课系统外,多为信息浏览功能,即使口令泄露,造成的损失也比较小,不需要使用强认证标准。本文选用一种改进的基于挑战/应答机制的动态口令认证机制来实现这一部分用户的身份认证,其中随机数技术的引进,使其安全性高于常用的动态口

令认证、且具有额外开支小等优点，在实现通信双方相互认证的同时还能够完成双方会话密钥的协商。认证过程中所使用的标记及其含义如表 1 所示。改进动态口令的双向身份认证过程如图 1 所示。

表 1 认证过程中所使用的标记及其含义

标记	名称
C	客户端
AS	认证服务器
Tgs	门票服务器
S	应用服务器
KDC	密钥分发中心
c	用户的 UserID
as	认证服务器端标识
ADc	用户 C 的网络地址
Rn	随机数
Rx	x 产生的随机挑战
||	连接操作
H(x)	对消息 x 进行 Hash 运算
K	对称密钥
Kx	x 的秘密密钥
Kx,y	x 与 y 的会话密钥
Kpub_x	x 的公钥
Kpri_x	x 的私钥
{m}Kx	以 Kx 加密的 m
LifeTime	票据有效时限
RealmU	用户 U 所属的范围
Cert_x	x 的数字证书

图 1 改进动态口令的双向身份认证过程

1.2 适用教职员工用户的身份认证协议

以普通教职员工为代表的用户群体，他们既是应用系统的信息生产者，也是应用系统的信息管理者，他们在使用各种应用系统时的权限应该比学生大，在身份认证安全性能上的要求也相对较高。本文选用一种改进的基于公钥的 Kerberos 身份认证机制供此类用户进行身份认证，其认证格式及过程如表 2 和图 2 所示。

表 2 改进 Kerberos 的认证票据 T、鉴别码 A 的格式

名称	格式
Tc,tgs	={as||{Kc,tgs||c||ADc||RealmU||LifeTime}Kpri_as}Kpub_tgs
Tc,s	={tgs||{Kc,s||RealmU||LifeTime}Kpri_tgs}Kpub_s
Ac,tgs	={s||c||ADc||Rn||RealmU}Kc,tgs
Ac,s	={c||ADc||Rn||RealmU}Kc,s
As,c	={Rn}Kc,s

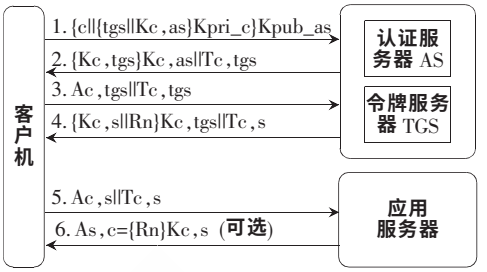

图 2 基于公钥的改进 Kerberos 认证机制工作流程图

其中随机数技术替代时间戳，避免了网络中时钟难于同步带来的问题，可以承受重放攻击；采用基于公钥的 Kerberos 认证，密钥分发中心无需再管理认证服务器与各个被认证实体之间的秘密密钥，大大降低了密钥分发中心的运行、维护费用；非对称加密体制的使用避免了口令猜测攻击，进一步加强了认证系统的安全性。上述 Kerberos 认证机制的系统信息交换量虽然较大，但它部分地解决了传统 Kerberos 认证协议的安全隐患，提供了相对较高的安全性能。而以教职员工为代表的用户数目不过区区数千人，对这类用户采用改进的基于公钥 Kerberos 认证机制来保障认证的安全，在校园网络中应用是可行的。

1.3 适用管理者用户的双因素身份认证

第三类是要求使用强认证机制的校园网用户群体，主要有各应用系统的管理人员、掌握学校电子签章的主要负责人员等，他们所接触的应用系统包含重要及敏感的数据信息，对身份认证的安全要求最高，应考虑使用基于数字证书和 USB Key 的双因素强身份认证机制。其认证格式及过程如图 3 所示。

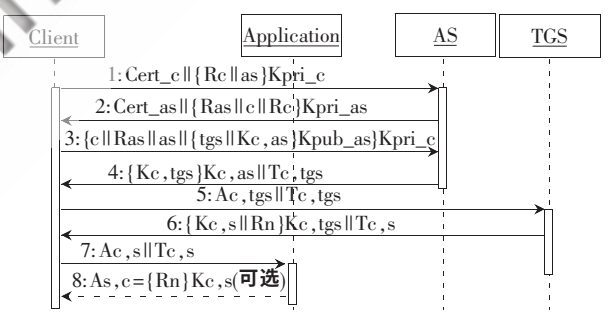

图 3 双因素身份认证的时序图(含消息交换格式)

上述机制借鉴了 Kerberos 协议的有关票据的概念，具有 Kerberos 认证的一切优点，同时通过引入 USB KEY、随机数和公钥密码技术，实现双向认证和统一认证，安全性和实用性得到较大的提高。同时，该群体的用户数量最少，采用高强度的认证方式所需要的系统开销和认证费用是必需的，也是可以承受的。

2 方案性能分析

性能分析过程中所使用的缩写：PKE，使用 1 024 bit 非对称密钥加密；PKD，使用 1 024 bit 非对称密钥解密；SKE，使用 128 bit 对称密钥加密或解密；Hash，使用安全散列算法计算信息摘要。分析过程中所使用的参数：公

钥,1 024 bit RSA 密钥;证书内容,1 536 bit;CA 对证书的数字签名,160 bit;身份 ID,512 bit;用户口令(对称密钥),128 bit;随机数,1 024 bit;随机挑战,128 bit;Adc,128 bit(IPV6);RealmU,8 bit;LifeTime,24 bit。

2.1 三种认证协议效率对比

根据本文所提出的三种认证协议的具体认证流程及其安全性分析,基于对称密码的动态口令认证协议、基于公钥的 Kerberos 认证协议和基于数字证书认证协议所能提供的认证安全性能是依次递增的。而表 3 的有关效率估算数据则表明:它们造成的网络开销依次成倍增长,系统开销的增长则不止一倍。在基于数字证书认证协议中,客户端和服务器之间的交互次数更是达到了 6 次之多。这还未把使用 USB Key 所造成的客户端系统开销及时延的因素考虑在内。

2.2 校园网统一身份认证具体案例性能分析

校园网中三类角色的用户数目呈数量级变化。在综合性高校具体环境中,假定三类角色的用户数量分别为 100 000、3 000、100,平均每人每天登录一次统一身份认证系统。

表 3 方案中三种认证机制效率对比

认证协议	交互	系统开销		网络开销
		客户端	服务器	
基于对称密码的动态口令认证	4 次	4SKE(3 609)+3Hash(1 152)	1PKE(664)+4SKE(3 609)+3Hash(1 152)	4 633
基于公钥的 Kerberos 认证	4 次	2PKE(1 792)+3SKE(3 464)	4PKE(2 944)+4PKD(3 904)+3SKE(3 464)	7 912
基于数字证书双因素认证	6 次	3PKE(5 376)+2PKD(2 720)+3SKE(3 464)	5PKE(5 504)+6PKD(7 648)+3SKE(3 464)	17 128

综合分析表 4 数据及相应安全性能,本文所提出的基于角色的统一身份认证解决方案为整个校园网所提供的认证安全性能接近于基于数字证书的认证协议,而它所需的系统开销和网络开销则接近于基于对称密码的动态口令认证协议,说明这一解决方案能在安全性能与效率这一对矛盾体中取得较好的平衡。

表 4 校园网环境下认证方案效率及对比

身份认证		服务器开销(各种加解密运算次数及数据量)				网络开销(客户端与服务器总交互次数、数据量)
		PKE	PKD	SKE	Hash	
简单动态口令认证	次数	103 100	0	412 400	309 300	412 400
	数据/bit	68 458 400	0	372 087 900	118 771 200	477 662 300
基于角色认证方案	次数	112 500	12 600	409 300	300 000	4×100 000+4×3 000+6×100=412 600
	数据/bit	73 766 400	12 188 800	371 638 400	115 200 000	100 000×4 633+3 000×7 912+100×17 128=488 748 800
双因素强认证	次数	515 500	618 600	309 300	0	618 600
	数据/bit	567 462 400	788 508 800	357 138 400	0	1 765 896 800

在实际应用中,认证方案的选择应当从系统需求和认证机制的性能两个方面来综合考虑。本文所提出的统一身份认证解决方案在明显提高认证安全性能的同时,又能有效地控制认证过程的系统开销和网络开销,具有实际应用价值。

参考文献

[1] 黄朝阳, 徐颖. 一种改进的基于挑战-应答机制的动态口令认证方案[J].中国科技信息,2009(4):103-105.

[2] 黄朝阳.一种实用的 Kerberos 双因素统一身份认证方案[J].中国科技信息,2009(19):109-110.

[3] 许学洋. 数字化校园统一身份认证平台的作用与实践[J].中原工学院学报,2009,20(6):72-75.

[4] 孙月洪. 统一身份认证在数字化校园中的作用与实践[J].廊坊师范学院学报,2009,9(2):37-39.

[5] 梁飞鸽,方刘基,潘一楠.基于校园网平台的统一身份认证系统设计[J].绍兴文理学院学报,2007,27(10):42-44.

[6] 李伟明. 基于 ECC 的无线身份认证和密钥协商协议[J].广东公安科技,2003(2):33-40.

(收稿日期:2010-07-02)

作者简介:

黄朝阳,男,1975 年生,硕士,高级工程师,主要研究方向:信息安全。