# 基于 Kerberos 和 RBAC 技术的邮政信息网安全机制①

王 刚

(陕西省汉中市邮政局 信息技术局, 汉中 723000)

**摘 要**: 邮政信息网是由邮政综合计算机网和邮政金融计算机网两部分组成. 邮政信息网的安全机制设计是邮政信息化建设中的关键问题之一, 关系到邮政企业的重大利益, 直接影响到整个系统建设的成效. 本文从邮政信息网各系统的应用和安全需求着手, 对有关的网络安全技术进行了分析研究, 在此基础上提出了一种基于 Kerberos 和 RBAC 技术的邮政信息网安全机制, 为解决邮政信息网的安全问题提供了一种技术方案. 该方案特别注重与邮政信息网的紧密结合, 并具有较高参考价值.

**关键词**: 邮政信息网; 网络安全; Kerberos; RBAC; 基于角色的访问控制

## Security Mechanism Based on Kerberos and RBAC Technology of the Postal Information Network

WANG Gang

(The Postal Bureau of HanZhong, shanxi, The Bureau of Information Technology, Hanzhong 723000, China)

**Abstract**: Post information network is made up of two parts which integrated network and financial computer network of post. The design of security mechanism to postal information network is one of the key question in construction of postal information. It relates to great benefit of post enterprise, affects construction result of total system directly. This paper starts out from every systematic application and security needs, it analyses and studies about related technology of security network, raises a security mechanism of postal information network in view of technology for Kerberos and RBAC. The solving schemas pays a special attention to combine with postal information network closely, having higher reference value.

**Key words**: postal information network; network security; RBAC; Kerberos; role-based access control

邮政信息网由两大部分组成, 即邮政综合计算机网和邮政金融计算机网. 邮政综合计算机网是覆盖全国各级邮政生产部门和各级邮政管理部门的大型企业网, 其网点覆盖全国 31 个省、自治区和自辖市, 201 个邮区中心局, 330 多个地市局, 2300 多个县局和 16000 多个电子化支局. 邮政金融计算机网是利用邮政综合网通信平台和公用通信网资源, 由邮政储蓄业务专用的中心系统和终端系统组成的专业网络.

邮政信息网可以分为三个层次, 即网络物理层: 如广域网、局域网、网管、网络与外部环境接口; 网络基础层: 如网络软硬件平台, 包括操作系统、数据库、通信软件、软件开发工具服务器、网络设备、工作站、终端等; 网络应用系统层, 如各专用应用系统等. 邮政信息网中的网络基础层和网络应用系统层均普遍采用了 TCP/IP 技术. 因此, 基于 TCP/IP 协议的安全问题是本文研究的重要内容.

汉中市邮政信息网是陕西邮政专用信息网的一部分, 整个系统采用了 TCP/IP 协议、Client/Server 网络体系结构, 并利用邮政广域网通信平台进行连接.

## 1 邮政信息网的安全问题

随着网络应用在各个领域的日益普及, 黑客、入侵、攻击的报道经常会出现在各种媒体中[1], 其所造成的损失是无法估量的. 因此, 邮政信息网的安全是整

① 收稿时间:2013-03-25;收到修改稿时间:2013-05-10

个系统建设中的一个重要问题，网络安全问题解决得好与坏，直接关系到网络建设的成败. 由于邮政各应用系统中包含着企业生产和管理的重要信息，因此邮政信息网的安全性直接关系到企业的重大利益.

### 1.1 建立安全机制的必要性

邮政信息网属于邮政内部的专网，不允许与国内外的公众计算机网络(包括Internet)有任何形式的物理连接，以保障邮政计算机网络系统的安全，防止从外部网络对邮政内部网络的入侵和破坏[2,3]. 但是根据有关统计提供的数据表明，有 60%以上的网络入侵或破坏是来自网络内部，因为网络内部人员对自己的网络更加熟悉，而且有一定的授权，掌握一定级别的密码，进行入侵或破坏更加得心应手[4]. 对于内部人员，虽然可以用一定的法律和规章制度加以约束，但法律和规章制度还不足以确保邮政网络系统的安全，还必须采用网络安全技术建立一套安全保护体系，即建立一套邮政网络的安全机制.

### 1.2 采用的安全技术

整个邮政信息网中，可以从其所包含的三个层次分别来考虑安全问题，采取相应的安全防范措施和技术[5]. 本文研究的重点是如何在网络基础层和网络应用系统层中，利用各种网络安全技术，形成一套邮政网络的安全机制，以实现安全的、高效的邮政信息网. 本文针对邮政信息网中应用系统的实际特点，进行了选择分析，并对现有的协议进行了扩充和修改，然后提出了一套基于Kerberos 和 RBAC 技术的邮政网络安全机制.

## 2 邮政网络安全目标与安全框架

在邮政信息网中，重点的保护对象是系统中存储的各种信息，包括综合网各子系统的生产数据、金融(绿卡)系统中邮政储蓄的账户信息、经营管理的统计资料和档案资料等. 这些信息中，有很多关系到邮政企业机密的重要信息. 而对这些重要信息的保护不能只是采用一些单独、零散的安全措施，而应该构筑一个合理的安全框架，据此来建立整个邮政计算机信息的安全机制，以保障邮政信息网中的信息安全.

### 2.1 典型的邮政信息网

从典型的邮政信息网着手来分析邮政信息网的安全目标，根据笔者参加汉中市邮政局综合计算机网中心局域网、广域网、报刊发行系统、邮政金融系统建设的工程实践经验，并结合其它子系统的实际情况，给出了图 1 所示的典型的邮政信息网子系统的结构拓扑图.

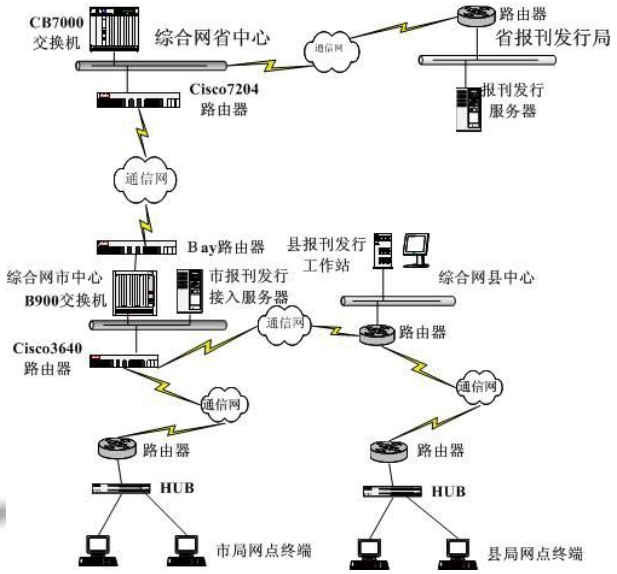


图 1 邮政报刊发行系统网络拓扑图

从图中可以看出典型的邮政信息网主要由三个部分组成：省局中心服务器、市(县)局接入点和网点终端，其中网点终端数量是不固定的，由连入网络的支局所数量来决定.

### 2.2 邮政网络安全目标

邮政信息网安全的最终目标，是采用各种网络安全技术来建立合理的安全机制以保障应用系统中信息的安全[6,7]. 信息的安全性体现在三个方面：

(1) 可用性(Availability)：可用性的含义包括两个方面，一方面是使得系统用户可以方便地获取其所需的信息，另一方面是系统不应由于攻击者的破坏而导致瘫痪，使其不能向所有或部分用户提供服务.

(2) 机密性(Confidentiality)：就是确保邮政应用系统中的信息不会被非法用户所窃取或查阅，系统中的每个用户只能访问允许其访问的信息.

(3) 完整性(Integrity)：要求邮政应用系统中的信息在网络中进行传输的时候不会被攻击者随意地添加、修改或删除，确保用户在访问系统时得到的信息是系统所提供的原始信息.

在邮政信息网的应用中，要求根据系统中每个用户的职责范围对访问权限进行严格的控制，必须与邮政企业的安全管理制度相符合.

### 2.3 网络安全框架

根据邮政信息网的安全需求与不同层次的网络安全技术的特点，在邮政信息网中，针对具体的应用采

用基于应用层的网络安全技术是比较合理、有效的.

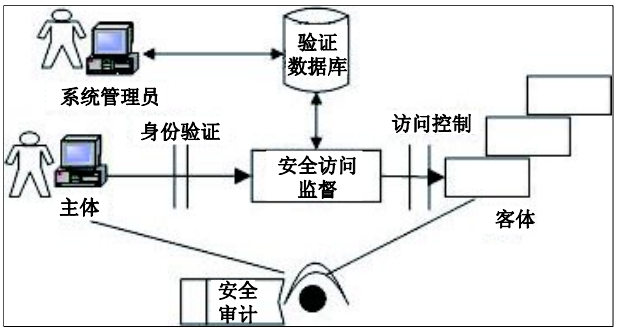


图 2 邮政信息网络安全框架

图 2 给出了一个典型的基于应用层网络安全技术的网络安全框架, 这一网络安全框架比较适用于邮政信息网. 这个框架中的几个重要概念:

(1) 客体(Object), 是指系统中包含或者接纳信息的被动的实体, 对一个客体进行访问就意味着访问客体中包含的信息.

(2) 主体(Subject), 相对客体来讲, 它是系统中处于主动地位的一个实体, 通常是指一个用户、一个正在执行的程序或者进程, 主体能够引起客体之间的信息流动, 或者引起系统状态的改变.

(3) 安全访问监督(Reference Monitor), 这一模块对主体进行身份验证、主体对客体的访问过程起到安全监督的作用, 它的重要依据是验证数据库.

在这个网络安全框架中, 主要包括了以下几项具体的网络安全技术:

(1) 身份验证技术

当系统中任一用户试图对系统进行访问的时候, 需要把自己的身份交给系统进行验证, 以此来判断用户的身份是否合法, 能否对系统中的客体进行访问.

(2) 访问控制技术

系统中主体与客体之间的关系是访问与被访问的关系, 当用户对系统中的客体进行访问时, 系统中的安全访问监督模块必须对其操作根据事先制定的策略进行严格的控制, 以防止用户非法访问系统中的客体.

(3) 加密解密技术

通过对网络中传输的报文内容加密使得系统中的攻击者在不知道密码的情况下很难读懂报文中的具体内容, 而合法用户则可以利用自己所拥有的密码使用相应的解密技术就能够对报文中的内容进行解密.

(4) 安全审计技术

安全审计技术能够以日志文件的形式把系统中所有用户的所有活动全部记录下来, 可以在事后对用户的行为进行分析处理. 通过这种分析能够获知系统中可能受到的安全侵害或非法用户的访问, 并以此来获知系统中的安全缺陷, 以便及时加以补救.

## 3 访问控制策略与RBAC

访问控制技术的作用在于对用户的各种动作根据事先制订好的策略加以限制和约束, 进而防止非法用户对网络中的资源进行访问, 同时也能阻止合法用户的越权访问[8].

访问控制策略大致上可以分为三类[9]:

(1) 自主访问控制(Discretionary Access Control, 简称: DAC)

(2) 强制访问控制(Mandatory Access Control, 简称: MAC)

(3) 基于角色的访问控制(Role-Based Access Control, 简称: RBAC)

前面两类访问控制策略是比较经典的访问控制技术, 多年来一直被众多安全专家们所认同. 这三种访问控制策略并不是完全相互排斥的, 也就是说在实际应用访问控制策略的时候, 可以把不同的访问控制策略组合起来应用, 这样可以实现更适合于实际应用系统安全需求的访问控制策略, 如图 3 所示.

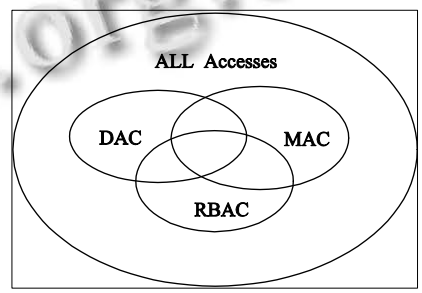


图 3 访问控制技术

### 3.1 基于角色的访问控制

基于角色的访问控制(RBAC)[10]是由美国国家标准技术研究所(NIST)于 20 世纪 90 年代初提出的一种计算机安全方面的访问控制技术. 该技术是根据计算机用户在计算机应用系统中所承担的不同任务和角色来进行以角色为基础的访问控制, 比较适用于规模较大, 用户较为繁杂的计算机应用系统.

3.1.1 RBAC 的基本模型

RBAC 是根据系统中用户的类型或者用户在系统所承担的工作建立不同的角色, 不同的角色具有对系统中不同客体的不同访问权限, 而用户对系统中的客体进行访问时则是以某个角色的身份出现在系统中, 他具有该角色所具有的访问权限. 原有的用户与客体之间的关系被变成了用户与角色、角色与权限之间的关系.

基于角色的访问控制策略与前面的自主访问控制策略、强制访问控制策略的一个最大的区别就在于: 基于角色的访问控制策略没有将访问权限直接授权给用户, 而是通过角色来建立访问权限与用户的关系, 这就使整个基于角色的访问控制策略的管理和维护工作大大简化, 特别适用于大型系统. 在采用了基于角色的访问控制策略后, 系统用户权限的管理工作就主要集中在用户与角色对应关系的管理和维护上, 管理和维护的任务就大大地减轻.

3.1.2 RBAC 的扩展模型

自 RBAC 的基本模型问世以来, 通过研究及应用, 对 RBAC 的基本模型进行了很多扩展, 使得其能够更好地适应实际应用的需要, 比较著名的有美国 George Mason 大学的 R.Sandhu 等科学家在 1996 年年初提出的 RBAC96 模型.

RBAC96 模型主要在以下两方面对 RBAC 基本模型进行了扩展:

(1) 引入层次概念

在实际应用中, 无论是现实中的职务还是系统中抽象出来的角色, 都存在着一定的上下级关系. 特别是在邮政企业中, 不但有行政职务上的上下级关系, 还有层次分明的行政级别(集团公司、省公司、市局、专业局、支局、班组等). 因此, 根据角色的这一重要特点, 在对基于角色的访问控制策略进行扩展时, 首先考虑的就是把现实生活中的职务与角色的上下级关系引入到这一理论中来, 就是在基于角色的访问控制策略中引入了角色的层次概念, 使得这一控制策略能够更好地与应用相结合.

如图 4 所示, 储汇局两位分别分管储蓄和汇兑的副局长($M_1$和$M_2$)都是支局长(C)的上级, 因此, 这两个角色都继承了支局长的访问权限, 同时, 这两个角色也都具有自己所特有的一些访问权限, 这些访问权限是不为其他角色所拥有的. 上述角色之间的层次与继承关系还存在一定缺陷, 因为在实际应用中分管储蓄的副局长($M_1$)和分管汇兑的副局长($M_2$)都可能拥有不能被局长(M)所继承的个人访问权限, 所以需要对图 4 所示的继承关系进行一定的修正. 在角色 M1 和 M2 之上分别增加一个新的角色 Ml'和 M2', 这两个角色除分别继承了角色 Ml 和 M2 的所有访问权限外, 还分别增加了那些只能由两位副局长所拥有而不能被局长(M)所继承的访问权限, 见图 5. 经过这样处理后, 能够比较好地解决私有访问权限的问题.

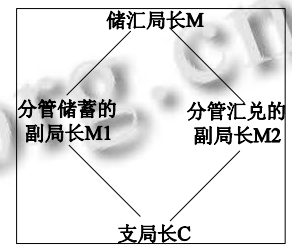


图 4　角色继承图

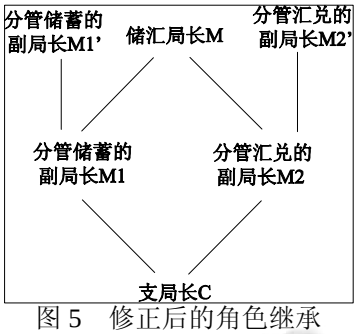


图 5　修正后的角色继承

(2) 增加约束机制

在基于角色的访问控制策略中增加约束机制是对角色及角色的访问行为加以一定的限制, 这些约束机制对增强系统的安全性是非常有必要的. 约束机制主要被应用在用户角色分配、角色权限分配、会话过程和角色层次等四个环节中.

RBAC 中最为基本的约束是角色的相互排斥约束, 经过扩展, 基于角色的访问控制策略的体系结构见图 6 所示.

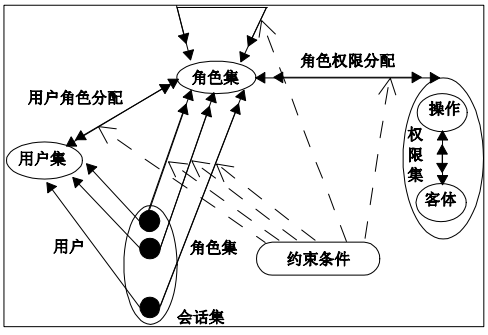


图 6　基于角色的访问控制综合模型(RBAC96)

3.1.3 最少用户约束

邮政企业的应用系统中，存在一些较为特殊的工作，必须有两个或两个以上不同的用户同时来完成，以起到相互监督的作用，例如在金融系统的前台业务处理中，每一笔交易必须由营业员和复核员共同完成. 为了满足这种安全需求，在 RBAC96 模型的基础之上，提出了一种新的约束机制——最少用户约束.

## 4 身份验证与Kerberos

身份验证一直是安全问题研究的重要课题，在不同的应用环境下，都有一套适用于自身安全需求的身份验证机制，各种身份验证体系都能够提供包含身份验证服务、数据的机密性服务、数据完整性服务等在内的一些基本服务.

### 4.1 基本的 Kerberos 模型

Kerberos 是一项著名的身份验证体系，该体系是由美国麻省理工学院(MIT)所制订的，经过多年来的实践和修订[11]，目前被众多计算机系统所采用的是 1993 年制订的 Kerberos 第 5 版协议.

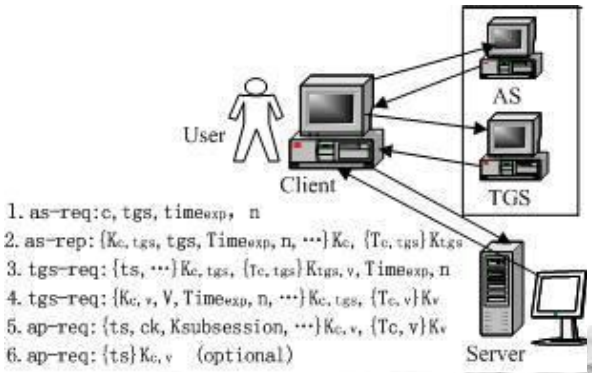


图 7 kerberos 协议模型

图 7 给出了一个基本的 Kerberos 模型，以及该模型中具体的协议会话过程. 完整的 Kerberos 协议会话过程由三个报文交换过程组成，分别是身份验证交换、票据授权交换和客户机 / 服务器交换.

当一个用户(User)通过客户机(Client)对服务器(Server)中的客体(Object)进行访问的时候，用户必须接受 Kerberos 系统的身份验证，只有在被证明是合法用户的情况下，才能够实现对服务器中客体的访问.

(1) 用户首先在客户机 Client 中输入能够向 Kerberos 系统证明自己身份的用户名 c 和口令，Client 将用户的口令通过一定的算法转换成用户的密钥 Kc，然后由客户机通过会话(1)向 Kerberos 系统中的验证服务器(Authentication Server，即 AS)提出身份验证的请求. AS 在接受到客户机提出的身份验证请求后，通过会话(2)向客户机返回一个身份验证应答报文 as-rep，这个应答报文中主要包含一个会话密钥(SessionKey)$K_{c,tgs}$、一个票据(Ticket)$T_{c,tgs}$ 以及一些辅助信息.

(2) 客户机在接收到身份验证应答报文之后，Kc 对报文进行解密得到会话密钥 $K_{c,tgs}$. 成功解密后，客户机通过会话(3)向 TGS 发出票据授权服务的请求报文 tgs-req. 最后 TGS 将生成一个新的会话密钥 $K_{c,v}$ 和票据 $T_{c,v}$，并分别用 $K_{c,tgs}$ 和 Kv 进行加密. 再通过会话(4)将含有新的会话密钥 $K_{v,c}$、票据 $T_{c,v}$ 以及其它信息的应答报文 tgs-rep 返回给客户机.

(3) Client 通过会话(5)向 Server 发送 ap-req 报文，在这个请求报文中，包含了两个部分的信息，其中一部分是用 $K_v$ 加密的 $T_{c,v}$，另外一部分是用 $K_{c,v}$ 加密的，里面含有密钥 $K_{subsession}$，该密钥将一直被用于加密 Client 与 Server 间的数据信息直到过期或者被更换. 最后一个会话过程(6)可以根据需要进行选择，该会话过程向 Client 返回一个 ap-rep 报文，应答报文中包含的是一个变量 ts，并且用 Kv 进行了加密，实际上变量 ts 本身来自于 Client，通常变量 ts 是一个时间戳. 因此，完整的(5)和(6)会话过程可以验证 Server 的合法性.

### 4.2 Kerberos 的加密措施

在 Kerberos 体系中，为了保障各次会话报文的完整性和机密性，主要采取了以下措施:

(1) 使用 DES 加密算法. 对报文进行加密能够使得攻击者在截取了报文后也不能直接识别报文中内容. 除了会话(1)的报文以明文形式进行传输外，其它报文均采用了 DES 算法进行了加密[12].

(2) 运用校验和技术. 在 Kerberos 文档中提供了多种带加密的校验和计算方法，在报文发送之前先进行校验和的计算，并把计算结果同时发送给对方，接收方在接收到报文后，重新计算校验和并与报文中的结果进行核对，以此来判断报文中的内容是否有可能被修改.

## 5 邮政信息网安全机制

根据前面对网络安全技术中比较重要的访问控制技术和身份验证技术的详细分析研究，结合邮政信息网及其应用的特点以及网络安全方面的需求，采用 RBAC 技术和 Kerberos 技术相结合的安全机制是比较

可行的, 而且也是比较安全的.

### 5.1 基于 Kerberos 和 RBAC 技术的信息网安全框架

邮政信息网安全机制采用了比较成熟的 Kerberos 体系用于身份验证, 并且把 Kerberos 协议的框架作为邮政信息网安全框架的主体. 由于 RBAC 技术能够比较好地与邮政信息网的实际应用相结合, 因此, 把 RBAC 技术运用于邮政信息网安全机制中, 并将其与 Kerberos 技术进行融合, 实现了身份验证过程与访问控制的有机结合. 图 8 给出了本文提出的基于 Kerberos 和 RBAC 技术的邮政网络安全框架.

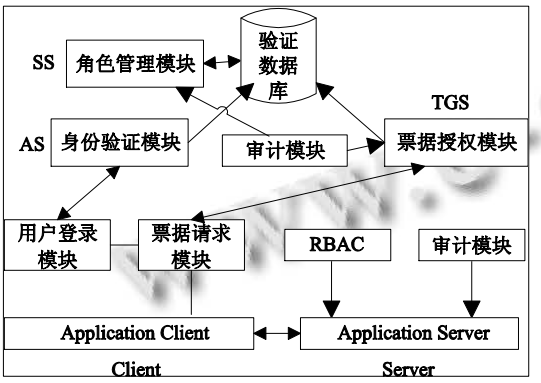


图 8 基于 Kerberos 和 RBAC 的信息网络安全框架

### 5.2 角色约束

角色约束主要表现在两个方面: 一方面为系统的用户和角色管理员在对系统中的用户、角色及访问权限进行管理所受到的一些约束; 另一方面是用户在对系统中的客体资源进行访问时, 系统中的服务器将根据该角色的约束条件对用户的访问行为进行约束. 这两种约束分别称为管理约束和访问约束.

### 5.3 Kerberos 的修改

本文提出的邮政信息网安全机制中采用了 Kerberos 和 RBAC 技术, 并且把身份验证和访问控制结合在一起, 而这两项技术本身是独立的, 因此有必要对这两项技术进行必要的修改和扩充, 才能使这两项技术能够更为紧密地融合在一起, 形成可靠的邮政网络安全机制.

#### 5.3.1 采用 RSA 加密算法

采用 RSA 算法是对 Kerberos 协议进行改进的一个方面, RSA 算法是一种公开公开密钥加密算法, 在 Kerberos 中协议采用 RSA 算法主要是为了提高 Kerberos 在防口令猜测攻击的能力, 同时在加强机密性和完整性方面也起到了重要作用.

攻击者对 Kerberos 协议进行口令猜测攻击的重点[13]是 Kerberos 协议报文交换过程中的 as-req 报文(参见图 7), 因为该报文是使用由用户口令演变而来的密钥通过 DES 加密算法进行加密的, 比较容易受到离线的口令猜测攻击. 因此, 为了提高 Kerberos 协议的安全性, 采用了 RSA 算法来替换原来的 DES 算法. 但必须对原 Kerberos 协议报文交换过程中的 as-req 和 as-rep 两个报文加以修改, 以满足 RSA 算法的需要.

对 Kerberos 协议中会话(1)的 as-req 报文的修改主要是在报文的 pre-authentication 字段中加入一些使用 RSA 加密算法所需要的信息, 其中有 RSA 算法参数, 用户公开密钥所存放的 KDC 信息以及用用户的私有密钥进行加密的数字签名等, 签名中包含一些可以防止遭受重放攻击的信息, 用户的公开密钥也可以放入 pre-authentication 字段中. 由于邮政信息网是企业内部的网络, 因此这个 KDC 实际只是 AS 中的一个模块, 即图 8 所示的验证数据库中.

#### 5.3.2 RBAC 信息的融入

在 Kerberos 协议的报文会话过程中融入 RBAC 信息, 既简化了整个邮政信息网安全机制的报文会话过程, 又避免了因增加报文会话的次数可能带来的不安全因素. 同时也可以从下面的分析中发现, 基于角色的访问控制策略在整个邮政信息网的安全机制中被分散开来, 应用于不同的环节来实现访问控制的功能[14].

(1) 首先需要融入 RBAC 信息的报文是 AS 返回给 Client 的 as-rep(as-pk-rep)报文, 加入 as-rep 报文的 RBAC 信息是提出身份验证请求的用户 c 所拥有哪些角色及其属性, 以及每个角色所能够访问的服务, 在图 9 中, 这些 RBAC 信息被表示为 $R_c$.

(2) 第二个需要加入 RBAC 信息的会话报文是 Client 向 TGS 申请访问服务器所需票据的 tgs-req 报文, 这个报文中需要加入的 RBAC 信息主要是用户选择角色的情况, 即图 10 中 tgs-req 报文中的 Rs. 这些信息将与报文中原来的 ts 等信息一样使用 DES 算法进行加密, 加密的密钥为 $K_{c,tgs}$.

(3) 在角色约束条件的许可下, TGS 将向用户返回 tgs-rep 报文, 该报文包含 C1ient 分配的访问 Server 时所使用票据中加入的 RBAC 信息, 该信息是该用户及其所代表的角色在访问用户选择的 Server 中的各项资源时所拥有的访问权限, 以及约束条件, 这些 RBAC 信息称之为 RBAC 令牌(RBACToken), 在图 9 中被表

示为 $Token_{rbac}$.

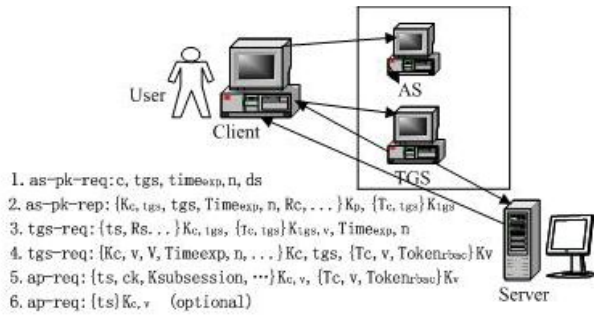


图 9 修改后的 kerberos 协议模型

5.3.3 修改后的会话过程

基于 Kerberos 和 RBAC 技术的邮政网络安全机制中, 其主要的会话过程是在 Kerberos 体系的会话过程的基础之上, 结合邮政网络的安全需求和 RBAC 技术进行了多方面的修改[15]. 下面我们通过介绍一个典型的访问过程来总结一下经过修改后的协议会话过程. 图 9 中给出了修改以后的 Kerberos 协议的会话过程及相应的报文格式.

(1) 当用户 c 需要访问邮政信息网中的应用服务器 S 时, 首先启动 Client 程序, Client 会提示用户输入其用户名和口令进行登录, 然后 Client 将向 SS 中的 AS 提出身份验证的请求, 以判断用户 c 的身份是否合法.

(2) AS 在接收到 Client 的请求后, 从验证数据库中获取该用户的公开密钥对请求的合法性进行检查, 检查通过后将向 Client 返回一个 as-pk-rep 报文, 该报文中包含 Client 向 TGS 申请访问 Server 所需的票据时使用的 TGT、Client 与 TGS 之间交换信息时使用的会话密钥、用户 c 所拥有的角色以及每个角色能访问的服务器信息等, 这些信息全部被封装在 Rc 之中.

(3) Client 在接收到 as-pk-req 报文后, 使用用户 c 的私有密钥对报文中的信息进解密, 获得角色信息, 并提示用户选择所要使用的角色, 同时选择需要访问哪个 Server. 然后 Client 将用户的选择信息 Rs 附加在 tgs-req 报文中向 TGS 提出申请票据的请求.

(4) TGS 在接收到 tgs-req 报文后, 首先对 TGT 进行解密获得加密报文中其它信息的密钥后再次进行解密. 然后根据用户所选择的角色及服务器在验证数据库中查询有关该角色和服务器的 RBAC 信息, 同时根据这些 RBAC 信息对用户 c 的访问请求进行初步验证, 如果验证获得通过, 将向 Client 返回一个 tgs-rep 报文.

(5) Client 获得了访问 Server 的票据后, 通过发送 ap-req 报文与 Server 协商在访问过程中使用的会话密钥. Client 将先产生一个随机数作为访问 Server 时使用会话密钥(被称为子会话密钥), 并使用由 TGS 生成的会话密钥进行加密后, 与票据一起发送给 Server. Server 在接收到 ap-req 报文后, 首先对 TGS 进行解密, 获得 RBAC 令牌 Tokenrba.

(6) 通常情况下, 以上 5 个步骤已经能够证明用户 c 的身份, 为了实现更高层次的安全需求, 可以使用第 6 个会话报文 ap-rep 来验证 Server 的合法性.

对协议的修改, 主要是对协议报文的内容进行了添加, 添加的是 RBAC 信息, 还替换了原来在第一次会话过程(AS 会话)中所使用的加密算法, 使其具有更强的防攻击能力, 而对协议的基本会话过程以及协议的基本内容没有任何修改, 因此这些修改不会影响协议原有的健壮性和安全性.

5.4 安全审计技术

在使用 RBAC 技术和 Kerberos 技术的同时, 还有一项重要的措施, 就是安全审计技术. 安全审计主要是把用户的的身份验证过程和用户的访问动作记录在日志文件中, 在必要的时候进行分析以确定是否存在非法操作或者尝试. 而且通过安全审计操作, 系统管理员还能够知道合法用户是否有滥用其合法权利的行为.

5.4.1 安全审计所应具备的功能

作为一个完备有效的安全审计模块, 依据 CC 准则, 应该具备三方面的功能:安全审计事件生成及存储、安全审计自动响应、安全审计分析.

5.4.2 安全审计信息

根据邮政信息网的安全需求以及 Kerberos 和 RBAC 技术的实际情况, 基于 Kerberos 和 RBAC 技术的邮政安全机制中, 主要需要记录三类安全审计信息:

(1) Kerberos 协议的会话过程中的重要信息, 如 AS、TGS 中接收到所有请求报文的有关信息.

(2) RBAC 相关信息, 如某用户以某角色的身份对系统进行的访问.

(3) 用户对 Server 的访问行为, 如用户对服务器中的某资源所进行的操作.

从总体上来讲, 每一类安全审计信息中的每一项安全审计记录均应该包含用户名、角色、动作、时间、

IP 地址、MAC 地址、访问结果等基本信息.

## 6 邮政信息网安全机制模型

计算机技术的发展是与应用实践密不可分的, 而安全问题又是一个非常实际的问题, 因此, 从理论体系的角度对邮政信息网络安全机制进行研究的同时, 针对前面所提出的安全机制开发了一个应用模型. 根据邮政信息网安全机制框架, 把安全机制模型分成了客户应用端程序、应用程序服务器端程序、身份验证模块、用户和角色管理程序、安全审计模块等五大模块[16].

### 6.1 安全机制模型的主要模块

(1) 身份验证模块是实现邮政网络安全机制中 SS 服务器的 AS 与 TGS 两大模块的功能, 实现对系统中的用户进行身份验证、票据和 RBAC 令牌的分配.

(2) 用户和角色管理程序的主要功能是根据 RBAC 理论对系统中的用户按照角色机制进行管理和维护. 该模块设有角色定义、角色权限分配、用户角色分配等主要功能, 同时也穿插约束机制的实现等辅助操作.

(3) 安全审计模块主要存在于两类服务器中, 一类是 SS 服务器, 另一类是各应用系统服务器. SS 服务器中的安全审计模块主要负责记录用户进行身份验证过程中的重要信息, 以及系统用户管理员通过系统管理模块进行用户管理时的操作行为. 而应用系统服务器中的安全审计模块负责用户对应用服务器的访问行为.

(4) 在整个系统中, 根据实际需要, 建立了两大数据库: 用户信息数据库和安全审计信息数据库, 用于存储系统中用户的各类信息和系统收集到的安全审计信息, 供系统中各大模块使用.

### 6.2 Kerberos 体系与邮政网络应用的融合

Kerberos 体系与邮政网络应用的融合问题实际上是在邮政网络的应用系统中如何运用 Kerberos 体系来进行身份验证的问题.

根据 Kerberos 体系设计的思想, Kerberos 体系所要提供的是在一个系统中进行一次性的身份验证, 也就是说当系统中的某个用户对系统中的任何客体资源进行访问时, 只需要一次性地进行登录, 输入用户名和密码请求 Kerberos 系统的服务器进行身份验证.

在设计邮政信息网的安全机制时, 如果完全按照 Kerberos 的设计思想来实现有些困难, 因为目前所使用的操作系统和邮政信息网的许多应用系统并不支持 Kerberos 协议. 为此, 专门设计了一个基于 Kerberos 和 RBAC 技术的邮政网络安全机制下的应用程序管理器, 所有符合基于 Kerberos 和 RBAC 技术的邮政网络安全机制的应用程序均需在该应用程序管理器中启动才能运行, 而不能被单独执行.

## 7 结束语

本文通过对邮政信息网安全问题的研究, 结合邮政信息网的实际应用, 提出了一套基于 Kerberos 和 RBAC 技术的邮政网络安全机制. 目前是邮政信息网建设的重要时期, 这一套邮政网络安全机制具有一定的参考价值.

当应用本文中所提出的网络安全机制来构建邮政应用系统时, 如果系统规模较大, 可以把本文中引用的 Kerberos 协议进行扩展, 引入其原有的域机制, 把整个系统功能划分成一个个小的域, 再为每个域设置域内的自己的服务器, 进行跨域的联合验证和安全控制, 这样做有利用整个系统的管理和维护.

如何把本文提出的邮政网络安全机制应用于已经开发完成的邮政金融、报刊发行等系统是需要今后进一步研究解决的问题, 只有这样才能进一步提高本文提出的邮政网络安全机制的应用价值.

## 参考文献

1 胡华平,陈海涛.入侵检测系统研究现状及发展趋势.计算机工程与科学,2001,23(2):20–25.

2 何全胜,姚国祥.网络安全需求分析及安全策略研究.计算机工程,2000,26(6):56–58.

3 刘平,曹云.入侵检测在网络安全中的地位与作用.湘南学院学报,2010,31(2):84–87.

4 李宝敏,徐卫军.计算机网络安全策略与技术的研究.陕西师范大学学报,2003,31(1):30–32.

5 黄允聪,严望佳编著.网络安全基础(第一版).北京:清华大学出版社.1999:17–39.

6 Jackson K, Dubois D, Stalllngs C. An expert system application for network intrusion detection. Proc. of the 11th National Computer Security Conference. Washington D.C. Oct., 1991. 215–225.

7 Sebring M, et a1.Expert system in intrusion detection:a case study. Proc. of the 11th National Computer Security Conference, Oct. 1988. 74–81.

(下转第 50 页)

400kbps、2.25Mbps、7.4Mbps, 这三种码率的视频流被分别传输给手机终端、PC 机终端、电视终端. 实验中, 对这 3 个码流视频分别进行传输播放, 图 7 显示了 3 个不同码流对应的播放结果, 图 7 中右边的图像是 7.4Mbps 码率对应的视频, 中间的图像是 2.25Mbps 码率对应的视频, 左边的图像是 400kbps 码率对应的视频, 这三幅图从右到左的分辨率明显减少, 但是码率也相应的减少了很多, 而且刚好满足手机用户、PC 机用户、电视用户对视频的需求, 使手机、PC、电视都能正常的观看电视节目.

图 7 三个不同码流对应的图像

实验结果表明, 整个系统能稳定正常的运行, 且在大幅度降低总码率的同时, 通过一次编码, 即可在边缘抽取出不同码率的码流, 然后传输到不同种类的终端, 并且可以正常播放视频.

## 6 总结

三网融合推动了广电系统视频业务的发展, 使 IPTV 系统开始需要面向多个不同类型的终端, 为了让手机终端、PC 机、电视能无缝的观看高清电视节目, 本文设计并实现了基于 H264/SVC 可伸缩编码技术系统. 本文首先设计了该系统的框架, 然后详细介绍了系统主要模块的实现, 其中源码解析模块为 SVC 实时编码模块准备需要编码的数据, 关键的部分就是对源码流进行 TS 解封装; SVC 封装模块主要是对 SVC 进行 TS 封装, 便于码流在 IP 网络上传输. 实验结果证明, 该系统能面向多终端进行实时高清视频的统一编码传输, 提供高质量且稳定的视频输出. 以上系统已完成原型实现, 下一步的工作是基于现有广电网络进行工程化实现.

## 参考文献


1 蒋力,施唯佳.三屏互动下的 IPTV 融合业务探讨.电信科学,2009(3):17–21.

2 郭静.三屏融合时代的手机视频内容建构.新闻实践,2010(002):59–60.

3 ITU-T and ISO/IEC JTC 1. ITU-T Recommendation H.264 and ISO/IEC 14496-10 (MPEG-4 AVC). Advanced Video Coding for Generic Audio/Visual Services: Version 9. 2009.

4 Frederick R, Jacobson V. RTP: A transport protocol for real-time applications. IETF RFC3550,2003.

5 ISO/IEC 13818-1: 2007, Information technology-generic coding of moving pictures and associated audio information (MPEG-2) -part 1: systems. 2007.

6 Wenger S, Wang YK, Schierl T. RTP payload format for SVC video. Internet Engineering Task Force (IETF), 2008.

7 ISO/IEC13818-1: 2007/Amd 3:2009.Transport of scalable video over Rec.ITU-T H.222.0 | ISO/IEC 13818-1. 2007.

8 Schierl T, Gruneberg K, Wiegand T. Scalable video coding over RTP and MPEG-2 transport stream in broadcast and IPTV channels. IEEE Wireless Communications, 2009, 16(5): 64–71.

9 MacAulay A, Felts B, Fisher Y. WHITEPAPER – IP Streaming of MPEG-4: Native RTP vs MPEG-2 Transport Stream.http://www.envivio.com/technology/white_papers.php, 2005.


(上接第 26 页)


8 王慧强,杜晔.入侵检测技术研究.计算机应用研究,2003,20(10):90–95.

9 鲁剑锋,李华文.访问控制策略的分类方法研究.武汉理工大学学报.2011,33(6):878–882.

10 Sandhu RS, Coyne EJ. Role-Based Access Control Models, IEEE Computer, Feb. 1996: 13–20.

11 齐忠厚.Kerberos 协议原理及应用.计算机工程与科学,2000,22(5):11–13.

12 胡美燕,刘然慧.DES 算法安全性的分析与研究.内蒙古大学学报(自然科学版),2005,36(6):693–697.

13 唐正军.黑客入侵防护系统源代码分析(第一版),北京:机械工业出版社,2002:41–52 .

14 李孟珂,余祥宣.基于角色的访问控制技术及其应用,计算机应用研究,2000,10(1):87–89.

15 游新娥,胡小红.Kerberos 身份认证协议分析与改进,计算机系统应用,2012,21(4):216–219.

16 乔颖,须德,戴国忠.一种基于角色访问控制(RBAC)的新模型及其实现机制.计算机研究与发展,2000,37(1):37–44.