# 基于优化的Kerberos协议的企业网络安全模型

# A Secure Model of Intranet Based on the Improved Kerberos Protocol

摘　要：针对目前日益突出的企业网安全问题，利用Kerberos协议具有认证和加密的特点，本文在对其进行优化的基础上，提出了一种企业网的安全模型，该模型具有身份认证、访问控制和数据加密等安全功能。

关键词：Kerberos 认证 网络安全 密钥

郑明辉　周慧华（湖北民族学院信息工程学院 445000）
马光致（华中科技大学计算机科学与技术学院 430074）

## 1 引言

在当前许多的企业网络安全解决方案中，大多集中在如何防止来自企业网外部的攻击和入侵上，即将安全控制主要放在企业网的边缘，如在与Internet连接的路由器上安装防火墙等。然而，随着网络技术的迅猛发展和用户应用水平的不断提高，内部网络用户（以前通常被认为是可信任的企业雇员）对网络的安全已造成了更大的威胁。根据有关统计资料表明，网络中60%以上的攻击来自于内部网。因此，如何设计一个内外兼顾的网络安全解决方案，是构建企业网时必须重点考虑的问题。针对这一问题，本文在防火墙的基础上引入了一种基于Kerberos协议的认证和加密机制，来有效地解决企业网的安全问题。

## 2 企业网安全管理域

企业网络是一个复杂的应用系统，根据其功能和用户对象一般将其划分成访问子网、服务子网和内部子网。根据其安全要求又可分为三个安全管理域：核心数据域、办公业务域和信息服务域。表1给出了各安全管理域在网络环境中的位置分布。

对于不同的安全管理域，应充分考虑它们不同的安全要求，使用不同的安全策略。比如文章将以服务子网作为用户访问内部子网的中间层进行基于认证的安全控制。

表1　安全管理域的位置分布

| 安全管理域 | 所在子网 | 描述 |
|---|---|---|
| 核心数据域 | 内部子网 | 进行企业敏感数据和信息的存放和处理，如科研、管理、业务、决策支持等。该域必须具有严格的安全控制策略，信息必须通过中间处理层才能获得。 |
| 办公业务域 | | 企业内部的电子办公环境，该区域内的信息（如办公文件）只能在企业管理人员之间流动。 |
| 信息服务域 | 服务子网 | 提供企业的各种信息和服务，如E-mail服务、FTP服务、WWW服务等。 |
| | 访问子网 | 客户（包括企业内、外的用户）通过浏览器访问信息服务域的各种应用服务器。 |

## 3 Kerberos安全认证体系及优化

### 3.1 Kerberos的安全认证模型

Kerberos是一种典型的用于客户机和服务器认证的协议，它通过提供中心认证服务，并应用传统的对称密钥加密算法，在客户机和服务器之间构建一个安全桥梁(即用户要求服务器所提供的每一个服务，都必需经过认证服务器的认证许可)。Kerberos认证模型如图1所示，它除了客户工作站(Client)以外，还包括三个服务器：认证服务器(AS)用于登录时验证用户身份；许可证服务器(TGS)用于发放“身份证明令牌”；应用服务器(Server)Client是请求服务的实际执行者。协议认证流程如下：

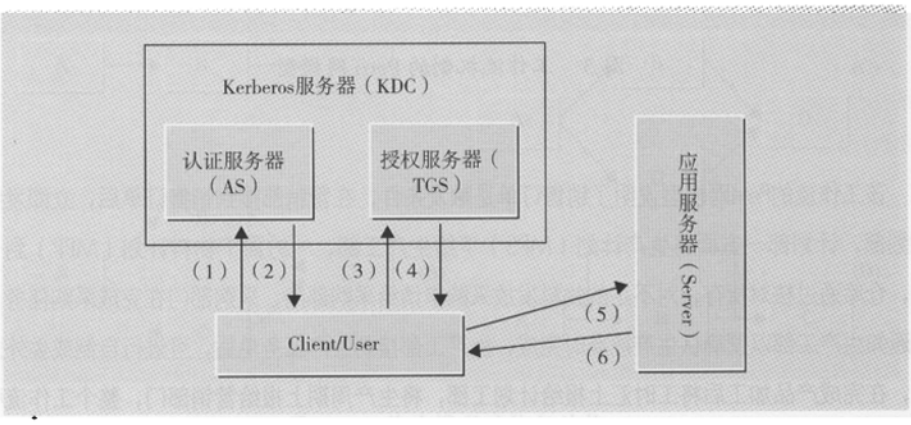


图1　Kerberos认证模型

在介绍流程之前，先给出所用到的一些符号的含义：

A为Client，B为Server，TEXP是验证的最后时间期限，N是一个随机数，KA、KB分别为A、B和AS所共享的密钥，KTGS是TGS的密钥，KAB是A和B的会话密钥，KS是A与TGS的共享密钥，TS是AS盖的时间印戳。

（1）A→AS：发送(A,TGS,TEXP,N)明文。客户向工作站注册，工作站向AS提交用户名A、对许可证服务器的请求TGS、当前时间戳TEXP及随机数N(明文)。

（2）AS→A：送回(KA[KS,TGS,TEXP,N],KTGS[A,KS])密文。AS比对域中目录数据库，生成会话密钥Ks和用于TGS的令牌KTGS[A,KS]，以用户的口令密钥KA加密传回Client端，此时系统提示用户输入口令。A通过用户口令生成KA解密密文，获得Ks和令牌KTGS[A,KS]，并验证时间戳TEXP的有效性。

（3）A→TGS：(KS[TS],KTGS[A,KS],B,TEXP,N)密文。Client端以会话密钥Ks加密令牌及请求服务地址B，送至TGS。

（4）TGS→A：(KS[KAB,B,TEXP,N],KB[A,KAB])密文。TGS回送用于与服务器B会话的密钥KAB和用于与服务器B会话的令牌KB[A,KAB]，并验证时间TEXP。

（5）A→B：KAB[TS],KB[A,KAB]。Client端以Ks解开令牌，得到与服务器的会话密钥KAB，并将令牌KB[A,KAB]送交服务器B。

（6）B→A：KAB[TS+1]。服务器以自己的私钥KB解开令牌，验证时间戳后回送TS会话有效时限，建立会话。

以上给出的是一个单AS的域内（Realm）认证模型，还有基于远程网络的多AS域间(Inter-Realm)Kerberos认证模型，文[1]对其有描述，不再累述。在为一个拥有远程子公司的大企业搭建安全认证模型时，一般选用多AS的域间Kerberos认证模型。

### 3.2 Kerberos 安全认证体系的优化

上述Kerberos协议具有一定的局限性,比如存在重放攻击问题、口令猜测攻击问题、时钟同步问题以及密钥存储问题等，因此必须针对以上问题对协议进行优化。Kerberos一般采用DES加密算法，但也支持用户自定义，例如Windows2000操作系统即使用RC4算法，文章将以Yaksha公钥密码算法优化Kerberos协议。

Yaksha算法是RSA公钥密码算法的一种变形。Yaksha与RSA一样以(ea,na)作为公钥，但Yaksha要求使用两个不同的私钥：用户的私钥daa和Yaksha服务器的私钥day。这两个新的私钥与原来的RSA私钥da有关，即daa*day=da mod na。Yaksha算法中，每个用户i有自己的dii，同时Yaksha服务器保留相应的diy，并且两者不能互相推知。优化后的认证流程分为两个阶段：

第一阶段：系统进行协议初始化，完成用户在AS的注册，并获得进行实时认证用的Yaksha密钥（注：EPM为M的公钥，ESM为M的私钥）。

（1）A→KDC：AS,A,EPA

（2）KDC→A：ESKDC[A,(ea,na),TEXP,EPA[daa]]

（3）KDC→AS：EPAS[A,(ea,na),TEXP,day]

（4）A→AS：A,KDC,ESKDC[A,(ea,na),TEXP,EPA[daa]]

用户首先向KDC发出联网申请，提交认证服务中心的名字和自己的公钥，KDC验证其合法性后，向用户发送Yaksha公钥、私钥、有效期、用户身份代号等信息，同时将相应的Yaksha公钥、服务器私钥等信息发给AS，用户得到证书解密后的信息，向AS递交证书、身份代号及KDC证明身份。

第二阶段：系统进行实时认证。TA、TB分别是A、B根据自己的时钟加盖的纪元时间戳。

（5）A→B：A,(TA,B)daa mod na

（6）B→AS：(TA,B) daa mod na,(TB,A)dbb mod nb,B

（7）AS→A：(B,TB,TA,KAB)day*ea mod na

（8）AS→B：(A,TA,TB,KAB)dby*eb mod nb

（9）A→B：KAB[TB]

（10）B→A：KAB[TA]

首先，A把B的名字等信息加盖时间戳TA并用daa加密送至B。B收到后由明文A知道是A发的信息，但是B并不知道day，无法了解信息内容，更不能伪造或篡改。B把A传来的信息传送给AS，并将A的名字加盖时间戳TB用dbb加密送至AS。AS解密B发过来的信息后，将A、B的会话密钥KAB用Yaksha私钥加密分别送至A、B。然后，A解密AS发过来的信息得到时间戳TA，并验证TA是否在当前允许的时间范围内，是否与自己发送的信息时间相符。验证通过后，A将TB用KAB加密后发给B，对B进行验证。B 对AS发过来的信息解密，得到时间戳TB，再验证TB时间的正确性。验证通过后，B将TA用KAB加密后发给A，对A进行验证。

优化后的Kerberos协议克服了原有协议的某些缺陷，如联网时不再使用口令，提高了系统安全性；在认证过程中，由用户对自己加盖的时间戳进行验证，解决了Kerberos的时间同步问题，并有效地防止了重放攻击。优化后的加密算法要比原算法加密速度慢一些，因此，系统要付出加大开销的代价。

## 4 企业网络安全模型设计

### 4.1 安全模型设计

在前面已经讨论了一个企业网的安全管理域，以及这些管理域在网络环境中所处的位置，根据这些管理域的不同安全要求，下面将在改良的Kerberos认证协议的基础上，结合防火墙技术，构建一个企业网的安全模型。随着企业规模的不同，其安全模型具有以下两种典型结构：单AS（认证服务器）安全模型，多AS安全模型。

#### 4.1.1 单AS安全模型

该网络安全模型一般适应没有远程子公

司的小型企业，企业的各种服务和信息需进行集中式管理，所以在安全系统中，只需配置单个的Kerberos协议认证系统就可。相应的企业网安全模型如图2所示：

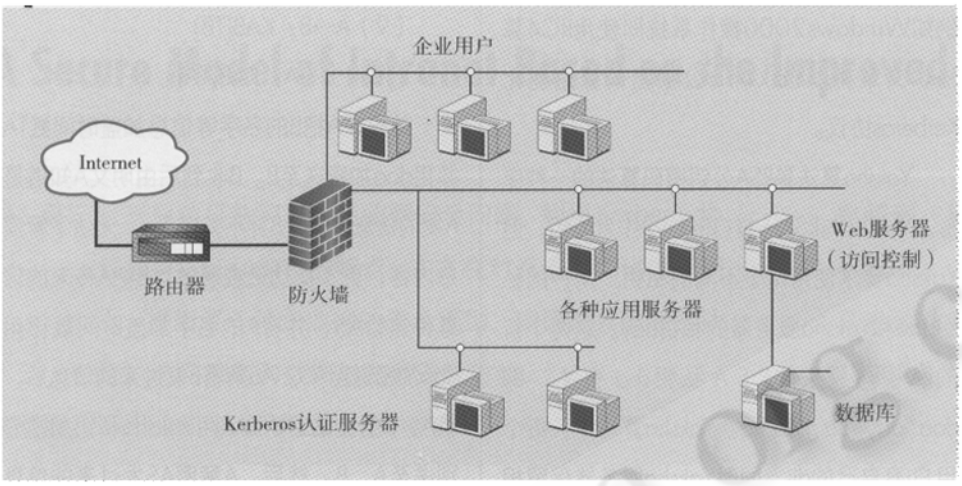


图 2　单 AS 企业网安全模型

4.1.2 多AS安全模型

该模型通常用于拥有跨地域子公司的大型企业，或具有密切合作关系的企业环境中。在这种情况下，母公司的网络与子公司的网络之间，具有密切合作关系的企业网之间存在着一种分布式的关系，它们相互信任，互通信息，物理结构上又相对独立。因此，可以先在每一个局域网中配置一个Kerberos协议认证系统，构建一个安全的企业局域网（即上面所述的单AS安全模型），然后各局域网再通过Internet互联。这样，每个局域网中都有一个独立的Kerberos协议认证系统，负责本域(Local-Realm)的认证工作，而各个域间再通过“信任链”的机制以实现分布式的安全认证。此模型实质是单AS安全模型的延伸和扩展。

### 4.2 安全模型特点

4.2.1 基于客户/Web服务器/数据库的多层结构

根据企业网的不同安全管理域具有不同的安全要求，采用目前流行的客户/Web服务器/数据库三层结构，如图3所示。前面是客户浏览器，中间层为Web服务器，后端是数据库服务器。这样，一般的普通客户不能直接操作处于最内层的数据库，增加了系统的安全性。在中间层加上适当的访问控制机制，比如访问控制列表，再与Kerberos协议认证有机结合起来，就能达到很好的安全效果。

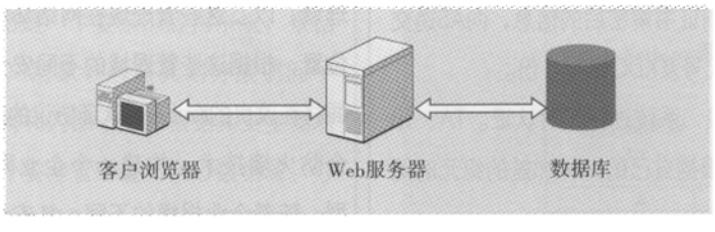


图 3　客户 /Web 服务器 / 数据库三层结构

4.2.2 实现访问认证和会话加密

基于优化的Kerberos协议认证系统，企业网在应用中可以实现认证、加密功能。无论是对内部网还是外部网的访问，都必须经过认证系统的严格认证，既可以解决客户的非授权访问控制问题，又可以解决内部数据传输和端到端数据传输的保密性问题，还能对数据的完整性进行验证，确保合法访问和安全会话。这是该系统的最大特点。

4.2.3 实现域内的集中控制

将局域网内的防火墙和Kerberos认证系统集中在一个集成的控制台上统一管理是企业安全策略得以正确实施的关键，这有助于企业对整个局域网定义一套统一的、一致的安全策略，方便系统的管理与维护，同时也大大降低了网管人员的工作量。

4.2.4 实现域间分布式管理

一个跨地域的大型企业，其母公司与子公司之间，子公司与子公司之间，其各自的局域网通过Internet互连。由于Kerberos协议具有分布式的特点，它除了负责本地域的认证和加密外，各个域之间的Kerberos认证系统还可以通过“信任链”的机制来确立跨域会话密钥，在本域中被认证的客户可以直接使用另一个与本域建立了信任关系的域中的服务，从而实现了分布式的认证。同时，由于Kerberos协议的加密功能，也保证了域间的数据的安全传输。

事实上，Kerberos协议除了可实现直接的信任关系外，还可以建立等级式的域组织方式，这对于多个具有松藕合合作关系的企业相互开展业务，更是大有裨益。

## 5 结束语

随着计算机技术和网络技术的快速发展，企业从中受益匪浅，但安全性如果得不到保障，损失也将是惨重的，因而在构建一个企业网时，首先应该考虑如何保证网络的安全性，分析网络的安全需求，制定相应的安全策略。在上面，只是从技术的角度给出了一个企业网的安全保证，实质上，好的安全策略，还应包括行政法规、维护管理等重要因素，是一个综合工程。