Kerberos认证协议的研究和改进

陈 云1，彭春山2，邓亚平1

1.重庆邮电大学 计算机科学与技术学院，重庆400065；2.河南质量工程技术学院 计算机中心，河南 平顶山467000

2008-04-10

摘 要： 分析比较了新Kerberos认证协议与原Kerberos认证协议，指出了对Kerberos改进的一些主要方面，并指出了其局限性。在此基础上提出了将公钥密码体制ECC与对称密码体制AES引入到Kerberos认证协议中的方案。该方案不仅解决了Kerberos认证协议中密钥的分配和管理问题，而且提高了Kerberos认证协议的安全性，使其遭受口令攻击的危险得到降低，更好地解决了工业控制网络的身份认证问题。

关键词： Kerberos协议 ECC算法 AES算法 Rijndael算法

美国麻省理工学院于2005年7月推出了新的Kerberos协议规范[1]，是针对1993年Kerberos V5版本[2]的修改。不但改正了诸多缺点，而且还给出了一些新的约定和新的操作选项，使其更符合当前应用，大大提高了其安全性及效率。但由于对称加密的固有特点使得新Kerberos协议仍有一定局限性，因此提出将公钥密码体制与对称密码体制相结合,即将ECC+AES方法引入到Kerberos认证协议中对其作进一步改进。

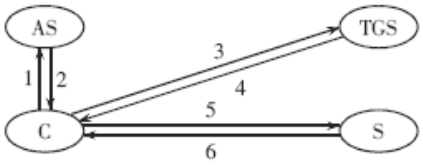

图 1 Kerberos 认证过程

1 Kerberos协议

1.1 Kerberos协议原理描述

在Kerberos协议中，AS为认证服务器，可在用户登录时确认用户身份。AS与密钥分配中心KDC类似，它与每个用户共享一个密钥。TGS为票据分配服务器，为用户之间的通信分配票据，使应用服务器相信TGS持有者的身份真实性。Kerberos协议具体实现过程如图1所示。从图1可知，用户C要访问目标服务器S，需要进行六次协议交换，即：

(1)C->AS：C，TGS，Addr，TS1。

(2)AS->C：{Kc，tgs}Kc，TGT，TGT：{TGS，C，Addr，TS2，Lifetime2，Kc，tgs}Ktgs。

(3)C->TGS：S，TGT，Authenticator1；Authenticator1：{C，Addr，TS3}Kc，tgs。

(4)TGS->C：{Kc，s}Kc，tgs，Ts；Ts：{S，C，Addr，TS4，Lifetime4，Kc，s}Ks。

(5)C->S：S，Ts Authenticator2；Authenticator2：{C，Addr，TS5}Kc，s。

(6)S->C：{TS5+1}Kc，s。

1.2 新Kerberos协议规范

Kerberos协议本身并不是无限安全的，而且也不能自动提供安全，它是建立在一些假设之上的[3]，即只有在满足如下假定的环境中它才能正常运行：①不存在拒绝服务攻击；主体必须保证他们的私钥安全；②Kerberos无法应付口令猜测攻击；③网络上每个主机的时钟必须是松散同步[4]的。ITEF改进了Kerberos协议规范（称为新规范）并且取代了原来的Kerberos协议规范（称为旧规范），新规范详细阐明了很多在旧规范上没有清楚描述的条款，增加了一些推荐性的执行选项和一些新操作。其主要改进有如下几方面：

(1)为了与当前应用相适应，新规范采用了新的加密和校验方法[5][6]，这是最主要的改进。同时删除了一些已不够强壮的方法，如DES和MD5，而采用AES。表1为DES与AES(Rijndael)加密算法的性能比较。针对密钥的生成，在新规范中，用户模式下私钥“可能”来自用户的口令，因为用户密钥可能存储在智能卡上，或者可以直接获得而与口令无关，而以前用户私钥仅通过用户输入口令生成。

表 1 DES 与 AES(Rijndael)加密算法的性能比较

ITEM	DES	AES(Rijndael)
密钥长度	密钥长度是 64bit，而有效的密钥长度为 56bit。运行速度稍慢	Rijndae 算法根据安全级别的高低可以自由选择密钥长度(128/192/256)三种[9]，明显提高了算法的灵活性和安全性，运行速度也快
是否存在弱密钥	存在弱密钥和半弱密钥，降低了 DES 算法的安全性	Rijndael 算法由于其密钥扩展函数的特点，所产生的轮密钥的随机性强，对初始密钥的选取没有特别的限制
是否具有对称性	具有。互补对称性可以使 DES 在选择明文攻击下所需的工作量减半	Rijndael 的均匀对称结构既可提高执行的灵活度，又可有效防止差分攻击和线性攻击[10]

(2)新规范依赖KDC检查传输域，并将检查标志包含在票据内，以表明该检查已经执行。目前Kerberos的执行即使忽略域标志或者不设置域标志也不存在安全隐患。新规范增强了解析主机名的能力，当Kerberos为一个命名主体提供认证时，能够确保它所认证的主体名字是完整的，并且就是它所期望通信的对象。

(3)新规范首次在参考文献中提出应用公开密钥算法对认证进行初始化。

(4)新规范增强了Kerberos的扩展性及兼容性。

1.3 新Kerberos协议的局限性

新规范虽然弥补了旧规范的许多环境缺陷和技术缺陷，但由于历史原因，它还是存在许多局限性。作为一个认证服务，Kerberos在网络上为主机身份的验证提供了一种方法，但Kerberos本身并不提供认证。如应用程序不应该接受Kerberos 服务器上所发布的服务票据作为授权票据，因为在这种情况下可能会使应用程序在其他密钥分发系统内部变得十分脆弱。

(1)密钥管理和维护问题。新Kerberos防止口令猜测攻击的能力还很弱，每一个主体必须对自身的密钥保密。如果密钥被某个入侵者获得，就会伪装成该主机或者其他关联主机的服务器。

(2)对时间同步性要求很高。在整个认证过程中都要通过时间戳的比较，才能判明合法身份。这就要求对整个网络内的时钟实现准同步。这对于一个拥有不同类型终端的分布式网络来说是很难实现的。

(3)主机标识符在一段时间内禁止重复使用。访问控制的一个典型模式使用访问控制列表（ACL）向特定主机授权许可。如果过时的入口仍然保存着已经被删除的主机，而该主机标识符是新的，则该新的主机会继承旧的记录在ACL入口的权限。即当不再重新使用主机标识符时，无意的接入威胁即可避免。

2 Kerberos协议的改进方案

2.1 基于对称密码体制的Kerberos协议的改进

参考文献[7]和[8]中提出了利用公开密钥加密进行对称加密密钥分配的方法。该方法是在通信双方通过公开密钥证书得到对方的公开密钥的基础上实现的。

2.2 基于ECC＋AES的数据传输加密的Kerberos改进方案

在Kerberos认证协议中，全都采用公开密钥密码体制传送机密信息是不够安全的。在传送机密信息的Client/Server双方，如果使用某个对称密钥密码体制并同时使用不对称密钥密码体制传送对称密钥密码体制的密钥，就可以综合发挥两种密码体制的优点，即对称密钥密码体制的高速性、简便性和不对称密钥密码体制的密钥管理的方便性、安全性。AES算法与RSA算法、ECC算法的特点比较如表2所示。

表 2 AES 算法与 RSA 算法、ECC 算法的特点比较

ITEM	AES 算法	RSA 算法	ECC 算法
密码体制	对称密码体制	公开密码体制	公开密码体制
密钥管理	密钥更换困难	密钥更新容易	密钥更新容易
数字签名和认证	不能或难于实现	易于实现	易于实现
加/解密处理速度	密钥短且灵活，加/解密速度快	基于大数分解，速度较慢	椭圆曲线取点，速度快
安全性	不可破解	不可破解	不可破解

由于AES和RSA、ECC各具所长，而ECC与RSA在相同安全强度下具有更快的速度和更低的存储要求，更符合高实时性工业控制网络的要求。综合AES和ECC的优点，得到一种新的加密方案，其基本原理为：数据在Kerberos Client/Server双方通信之前，发送方随机生成一个加密密钥，用AES算法对需传送的数据加密。然后再用ECC算法对该密钥进行加密并实现数字签名。这样接收方在接收到该密文和被加了密的密钥后，同样用ECC解密出此随机密钥，再用此随机密钥对密文解密。这样的加密方案既有AES算法的快捷特点，又有ECC算法的保密性和方便性特点。

2.3 具体改进方案

改进后的Kerberos认证过程如图2所示。

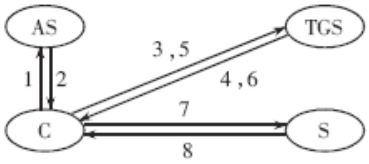

图 2 ECC+AES 改进后的 Kerberos 认证过程

改进后的Kerberos认证过程如下：

(1)C->AS：C，TGS，Pc。

(2)AS->C：Cc，Ctgs；Cc：{C，Pc，T1}P-1ca；Ctgs：{TGS，Ptgs，T2}P-1ca。

(3)C->TGS：TGS，{Kr，Cc，Authenticator，T3}Ptgs；Authenticator：{C，TGS，Ptgs，Kr，T3}P-1c。

(4)TGS->C：TGT，{C，TGS，Kc，tgs，T4}Kr；TGT：{TGS，C，Addr，T5，Lifetime5，Kc，tgs}Ptgs。

(5)C->TGS：S，TGT，Authenticator1；Authenticator1：{C，Addr，TS3}Kc，tgs。

(6)TGS->C：{Kc，s}Kc，tgs，Ts；Ts：{S，C，Addr，TS4，Lifetime4，Kc，s}Ks。

(7)C->S：S，Ts，Authenticator2；Authenticator2；{C，Addr，TS5}Kc，s。

(8)S->C：{TS5+1}Kc，s。

以上描述中，关键是对1.1节中的描述步骤（1）和（2）的改进，修改后变成现在的(1)～(4)步；而步骤(5)～(8)与1.1节中的步骤(3)～(6)一样。这里主要对前四步进行说明：

(1)用户发送自己的公钥、用户名和TGS服务器名向CA请求自己和TGS的公钥证书。

(2)CA检查用户身份合法后用自己的私钥为用户和TGS签发公钥证书，证书中包含有用户、TGS的信息以及证书的签发时间。

(3)用户收到公钥证书后，用已由安全通道得到的CA的公钥解密，得到TGS的公钥。然后用TGS的公钥加密报文向TGS发送，请求验证身份，请求报文包括用户公钥证书、随机产生的一次性会话密钥Kr、时间截和证书。时间T3是该报文的产生时间，TGS在收到该报文后，计算T3和收到报文时间的差值，如果相差太大则拒绝接受该请求报文，这样做可以防止重放攻击。Kr用于TGS对应答报文进行加密。证书用于验证用户的身份。TGS收到用户的请求报文后，首先用自己的私钥解密，得到用户公钥证书、一次性会话密钥Kr和证书。然后TGS用证书中的用户公钥对证书进行解密，用得到的信息验证用户身份。

(4)TGS通过对用户的身份验证后，产生应答报文。应答报文包括两部分，一部分是访问TGS用的票据TGT，TGT与传统Kerberos协议中的TGT完全相同；另一部分是加密数据，包含用户名、TGS服务器名、用户与TGS共享的会话密钥以及认证时间，这些数据用一次性会话密钥加密，用户收到后，就得到访问TGS的票据TGT。用Kr对加密的数据解密后，就得到与TGS会话的密钥Kc、tgs，这样用户就可以用TGT、Kc和tgs向TGS发送传统的TGS请求。

改进后的Kerberos身份验证系统的安全性得到了极大提高，如表3所示。

表 3　Kerberos 改进前后的性能对比

ITEM	Kerberos	ECC+AES 改进后的 Kerberos
密钥存储问题	需要双方事先交换解密密钥，防止口令猜测攻击的能力还很弱	在通信过程中，双方无需事先交换解密密钥就可以进行保密通信，从而 Kerberos 没有必要保存所有用户的密钥这一敏感信息，且能保证双方真实身份。可防止口令猜测攻击
对时间同步	对时间同步性要求很高	对时间戳的要求降低了，因为合法的用户才能取得自己公钥加密的消息，通过这种方式实现互相认证
主机标识符	主机标识符在一段时间内禁止反复使用	对于主机标识符没有特别的限制。节约了系统资源

本文深入研究了新的Kerberos认证协议规范，指出了其局限性。提出了在Kerberos协议中引入ECC＋AES的数据传输加密的改进方法，在一定程度上克服了传统Kerberos认证协议中密钥管理困难、容易受到口令攻击和对时间同步性要求高的缺点，提高了Kerberos认证协议的安全性，同时提高了身份认证速度，使其更符合工业控制网络的高实时性要求，可以更好地解决工业控制网络的身份认证问题。

参考文献

1 C Neuman.The kerberos network authentication service(V5).Internet RFC 4120，July 2005

2 C Neuman.The kerberos network authentication service(V5).Internet RFC 1510，September 1993

3 Frederick Butler，Iliano Cervesato，Aaron D Jaggard et al. A formal analysis of some properties of kerberos 5 using MSR.IEEE COMPUTER SOCIETY，2002；(11)

4 Ian Downnard.Public-key cryptography extensions into Kerberos.2002 IEEE POTENTIAL，2003

5 K Raeburn.Encryption and Checksum Specifications for Kerberos 5.Internet RFC 3961，February 2005

6 K Raeburn.Advanced encryption standard(AES) encryption for kerberos 5.Internet RFC 3962，February 2005

7 刘克龙，卿斯汉，蒙 杨.一种利用公钥体制改进Kerberos协议的方法.软件学报，2001；(12)：874～877

8 莫 燕，张玉清，李学干.对Kerberos协议的攻击及对策研究.计算机工程，2005；(5)：66～98

9 肖国镇，白恩健，刘晓娟.AES密码分析的若干新进展.电子学报，2003；(10)：1549～1554

10 Joan Daemen Vincent Rijmen.高级加密标准(AES)算法-Rijndael的设计.北京：清华大学出版社，2003

相关应用

地址：北京海淀区清华东路25号电子六所大厦
联系电话：82306084 / 82306085 传真：62311179 京ICP备05053646号

推荐分辨率1024*768 IE6.0版本