

基于椭圆曲线组算法的安全令牌与联合验证

陈海燕^{1,2}, 王合闯³, 李英豪^{1,2}, 王华军¹

(1 成都理工大学 地球物理学院, 四川 成都 610059;

2 濮阳职业技术学院 数学与信息工程系, 河南 濮阳 457000;

3 华北水利水电大学 信息工程学院, 河南 郑州 450045)

摘 要: 提出、设计完成了一种基于数字椭圆曲线加密算法的安全令牌与数据传输的通用算法. 该算法提供的非对称加密和数字签名, 能够有效解决非法数据访问, 较好解决无状态协议下的数据安全传输问题, 为解决云分布环境下无状态协议数据安全访问提供了另类的解决方法, 该方法具有较高的效率和安全防范措施, 可避免伪造、篡改等不安全因素带来恶意的攻击, 对分布式数据的安全访问设计具有一定的参考意义.

关键词: 数字椭圆曲线; 安全令牌; 联合验证; 非对称密钥; 数字签名

中图分类号: TP301

文献标识码: A

文章编号: 1000-7180(2014)11-0088-04

Security Token and Federated Authentication Based on Elliptic Curve Groups Algorithm

CHEN Hai-rui^{1,2}, WANG He-chuang³, LI Ying-hao^{1,2}, WANG Hua-jun¹

(1 College of Geophysic, Chengdu University of Technology, Chengdu 610059, China;

2 Department of Mathematics and Information Engineering, Puyang Vocational and Technical,

Puyang Henan 457000, China; 3 College of Information Engineering, North China University of

Water Resources and Electric Power, Zhengzhou 450045, China)

Abstract: This paper designed and completed a general algorithm based on elliptic curve encryption algorithm. The algorithm provides asymmetric encryption and digital signature, and it can effectively solve the illegal data access, and it can better solve data security problem under the stateless protocol. It provides an alternative solution to solve the data security access with stateless protocol in cloud distributed environment. This method has high efficiency and safety precautions, it prevents forgery and tamper with the unsafe factors, It has certain reference significance for the designing of the distributed data access.

Key words: digital elliptic curve; security token; federated authentication; asymmetric key; digital signature

1 引言

为了保护存储于树状结构数据中心节点的机密数据, 使未授权用户不得越权访问, 需要一种安全的策略, 保证网络中发送的数据或存储在服务器中数据的可用性、完整性和保密性. 存储的数据能够通过本节点安全认证和父级节点联合验证. 将数据以分散的方式, 分布存储于各个物理区域, 可解决瞬时网

络风暴问题. 过度集中的树状结构数据存储为机群带来了网络带宽吞吐的巨大压力, 同时分散存储机群节点的添加与删除、数据的安全检索和访问等都对系统提出了更高的要求, 为了提升机群的松耦合能力, 将认证分散在各个存储节点中, 且要求各个节点服务器能够进行联合验证. 本文基于椭圆曲线组算法, 采用安全令牌措施, 提出一种联合验证方法, 用于确保分布存储在数据节点中的机密数据, 在本

收稿日期: 2014-01-22; 修回日期: 2014-02-27

基金项目: 河南省教育厅科学技术重点研究项目(14B520040); 河南省科技攻关计划项目(142102210041)

身认证和父级节点授权的基础上,完成具有权限安全的数据访问策略.用户名密码认证是保证软件安全的重要机制之一,提升数据的安全性可采用双种或多种认证机制^[1].为了解决本系统的多重认证机制,设计的数字安全令牌能够提供灵活的认证机制,且提供较为复杂的认证信息和服务器联合验证,数字安全令牌采用安全性较好的椭圆曲线组^[2]进行不对称密钥方式加密,加入数字椭圆曲线加密算法^[3]的数字签名,以二进制数据格式发放给客户端,客户端携带该令牌访问系统资源,并以令牌进行系统联合验证.为了减轻服务器端的计算压力,只对令牌数据采用了非对称密钥加密,而传输数据采用对称密钥进行加密传输.

2 安全令牌访问模型

在通过参考非对称密钥算法^[4]、WIF 联合验证和数字椭圆曲线签名^[5]的基础上,系统设计的安全令牌访问算法模型如图 1 所示.

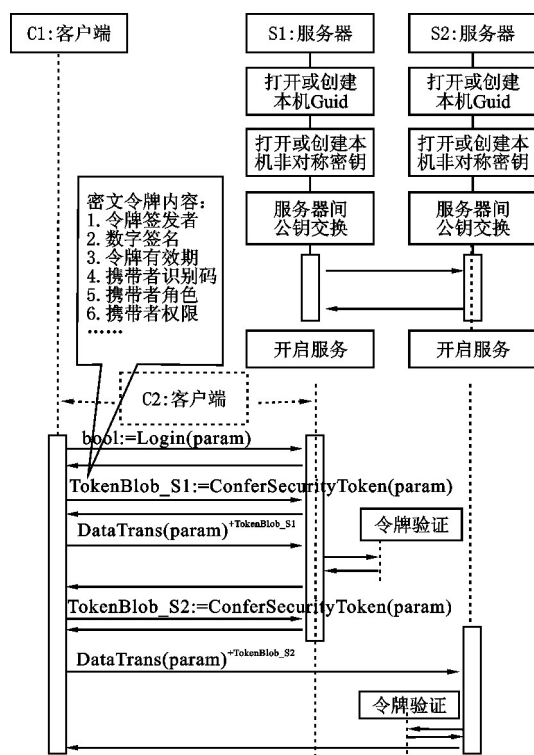


图1 安全令牌访问算法模型

服务器采用 Guid 进行标识,该标识是安全令牌识别发放的基础,为此,在服务启动之前,需要打开服务器的 Guid 标识,如果服务器不存在 Guid 表示,则创建其 Guid 标识.为了能够使得服务器获得非对称加密的能力,需要打开或创建服务器非对称密钥,并提供服务器间用于交换的公钥.服务开启后,服

器端可提供安全令牌验证客户端的身份,并提供同步或异步方式与客户端进行通信.为了满足服务器间的联合验证,需要在服务器间进行公钥交换,公钥交换方式是保证服务器安全的前提必要条件,公钥泄露导致安全令牌验证失败是漏洞攻击无法防范的关键症结所在.

具有安全令牌发放条件的服务器 S1 为客户端 C1 提供服务,C1 首先登录服务器 S1,进行身份验证.对于身份验证通过的客户端 C1,可申请访问 S1 的安全令牌.S1 通过识别 C1 申请令牌的参数,发放针对自身还是具有发放权利许可的其他服务器的令牌.当客户端 C1 试图访问服务器 S1 的资源,其登录认证是在服务器 S1 上通过,则 S1 采用本身公钥将令牌加密,以密文的形式下发给客户端,令牌的内容包括令牌签发者、数字签名、令牌有效期、携带者识别码、携带者角色、携带者权限等以及系统要求的其他信息,但令牌不易过大,以免增加服务器与客户端之间的通信流量,带来不必要的系统资源开销.客户端没有解密令牌的公钥,因此不能解密令牌,因此也无法、无权力修改令牌,客户端只能识别拥有的令牌是用于访问哪个服务器的令牌.当服务器收到携带安全令牌访问的请求时,首先采用相应公钥对令牌进行解密,之后对令牌的关键数字签名字段进行验证.数字签名是对整个令牌关键内容进行的数字椭圆曲线加密签名,当试图通过更改令牌二进制内容伪造令牌时,签名验证将会失败.通过令牌验证的 C1 客户端,服务器将响应其请求,并将数据以对称加密方式或明文回传给客户端,完成客户端一次数据通讯.

经过登录认证的客户端 C1,试图访问 S2 服务器,C1 可以再次向 S2 发起登录认证,也可以采用联合验证的方式,携带 S1 发放的访问 S2 的安全令牌进行数据请求.C1 首先向 S1 发起获取 S2 安全令牌的请求,S1 收到请求后,查询本机是否包含 S2 的公钥,如果曾经和 S2 交换过公钥,则 S1 已经得到 S2 联合验证的许可,S1 采用 S2 的公钥,采用本机非对称加密算法,将令牌进行加密后回传给客户端 C1.客户端 C1 携带 S1 发放的令牌,不经过登录认证,向 S2 发起数据访问请求.S2 收到 C1 的请求后,验证令牌为 S1 所颁发,查询本机是否与 S1 进行过密钥交换,当本机不存在 S1 的公钥,则认证失败,否则 S2 采用 S1 的公钥,用 S2 的非对称加密机对令牌进行解密,认证通过后响应 C1 的请求,完成 S1 和 S2 服务器间的联合验证.

模型中的 C2 客户端试图通过非法手段拦截 C1 和 S1 之间的通信,伪装 C1 非法向 S1 请求数据,S1 收到 C2 的请求,其携带了 C1 的完整令牌,令牌数字签名验证通过,但侦测到请求端与令牌的携带者识别码不匹配,C2 虽然获得了 C1 的安全令牌,但令牌验证依然失败;C2 试图更改 C1 安全令牌的内容,C2 没有 S1 的公钥,C2 无法对令牌进行解密,因此无法更改令牌内容,认证失败;C2 试图模仿其他服务器,颁发访问 S1 的安全令牌,由于 S1 不含有 C2 的公钥,C2 颁发令牌在 S1 端无法解密验证,认证失败;C2 试图采用直接更改获取安全令牌的二进制内容,则令牌数字签名验证无法通过,认证也会遭遇失败,达到了安全令牌数据访问的基本保障。

3 安全令牌模型及联合访问验证实现

模型非对称加密算法采用了 .net 提供的 CngKey 类,该类定义与下一代加密技术对象一起使用密钥的核心功能^[6]. 验证实现该系统模型的类图如图 2 所示。

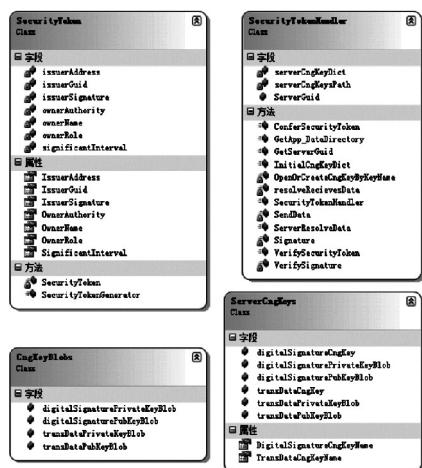


图 2 系统实现类图

类图中的 SecurityToken 是服务器向客户端颁发的安全令牌,CngKeyBlobs 是存储在服务器上非对称密钥算法的密钥对,为了能够将令牌和密钥对进行传输与存储,为两个类添加[Serializable]属性进行序列化。ServerCngKeys 是存储在服务器字典中联合验证服务器的非对称密钥。SecurityTokenHandler 是安全令牌模型实现及联合访问主操作类,该类实现了安全令牌的颁发与验证。服务器安全令牌的颁发和验证通过 WCF 提供给客户端访问,其类图如图 3 所示。

为了减少客户端访问时服务器频繁读取密钥对

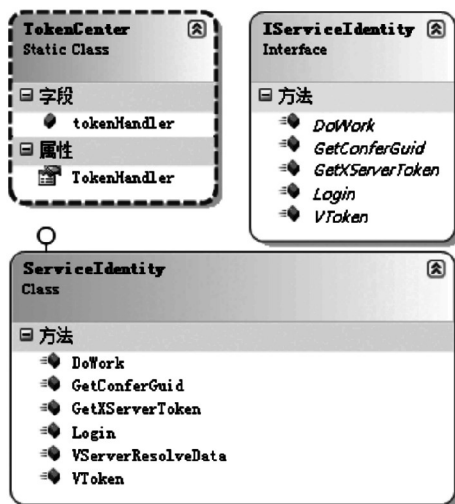


图 3 安全令牌类图

带来的压力,WCF 中对 TokenCenter 类声明时添加了[ServiceBehavior(InstanceContextMode = InstanceContextMode.Single)]属性,采用单一模式将密钥对装入到内存。WCF 服务启动后,可通过 GetServerGuid()方法访问目标服务器的 Guid,登录后通过 ConferSecurityToken(string XServerGuid)申请安全令牌,通过 VerifySecurityToken(byte[] securityTokenBlob,string serverGuid)进行令牌验证。方法 Signature(byte[] data,CngKey digitalSignatureCngKey)提供了基于 ECDSA P256 数字签名算法,方法 VerifySignature(byte[] data,byte[] signature,byte[] pubKey)用于对数字签名进行验证,方法 SendData(byte[] rawData,CngKey senderCngKey,byte[] receiverPubKeyBlob)和 resolveReceivesData(byte[] encryptedData,CngKey receiverCngKey,byte[] senderPubKeyBlob)分别用于基于 ECDiffieHellman P256 数据安全传输的数据加密与解密。方法 byte[] ConferSecurityToken(string XServerGuid)为客户端颁发令牌,令牌中采用 Signature()方法对关键内容进行数字签名,将令牌内容及其签名写入 MemoryStream,并对令牌对象采用 BinaryFormatter 进行序列化,序列化后的加密令牌以二进制 byte[] 方式进行发送。发送者为服务器,接收者只是携带,安全令牌需要回传到服务器进行解密验证,所以 receiverPubKeyBlob 仍采用发送者的 Blob。

方法 VerifySecurityToken()提供对令牌的验证,验证者收到携带者的安全令牌后,首先对令牌进行解密,解密后采用 VerifySignature()对令牌内容

进行数字签名认证,服务器对非本机的令牌和经过篡改的令牌无法解密,对伪装的令牌无法通过数字签名认证,均返回 false.

4 系统测试

为了进一步验证实现的系统,分别在服务器 S1 和 S2 上部署该系统,位于客户机的 C1 首先向服务器 S1 发起颁发安全令牌请求,获得令牌后在 S1 上进行令牌验证,令牌内容和验证结果如图 4 所示.

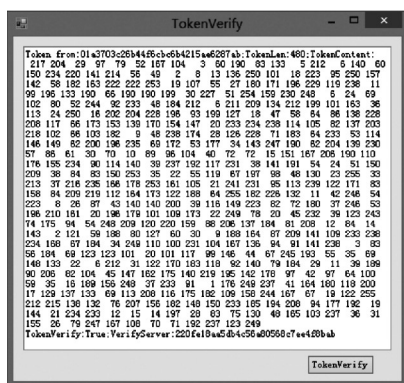


图 4 令牌验证

令牌顺利通过 S1 服务器的验证, C1 再次向 S1 发起请求向其颁发 S2 的令牌. 服务器 S1 接到请求后, 查询本机是否具有颁发 S2 令牌的能力. 由于 S1 和 S2 相互交换过公钥, S1 拥有颁发 S2 安全令牌的能力, S1 用 S2 的公钥加密安全令牌, 颁发给 C1. C1 用 S1 颁发给其 S2 的令牌, 向 S2 请求令牌验证. S2 收到 C1 的请求后, 查询令牌得知该令牌由 S1 颁发, S2 拥有 S1 的公钥, 用 S1 的公钥解密令牌, 认证通过. 令牌内容及验证结果如图 5 所示.

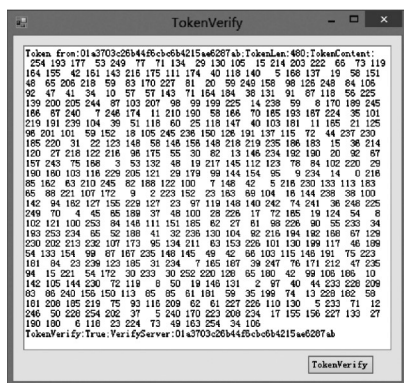


图 5 联合验证

5 结束语

为了解决无状态保持情况下的数据传输和联合验证问题, 通过参考国内外比较成熟的非对称密钥算法、WIF 联合验证和数字椭圆曲线签名等技术, 提出并设计了基于数字椭圆曲线加密的安全令牌认证体系及其模型, 实现并验证了其正确性和可用性, 为分布式存储数据的访问提供了一种联合验证方法. 在系统测试中, 将 WCF 宿主于 Winform 应用程序中, 以获得较大的系统权限. 测试中的数字椭圆曲线加密采用 CngKey 类, 过于依赖 .Net 体系, 独立数字椭圆曲线加密算法是系统进一步需要改进的重点. 测试结果表明, 该算法能够实现基于安全令牌无状态保持下数据的加密传输与服务器间的联合验证. 系统的实现验证了该模型的正确性和可用性, 为解决其他类似分布式存储数据安全传输及联合验证问题提供了一定的参考价值.

参考文献:

- [1] 柳纯录, 黄河, 陈涪萍, 等. 软件评测师教程[M]. 北京: 清华大学出版社, 2005.
- [2] 巩思亮, 刑涛, 梁庆伟, 等. 基于椭圆曲线密码系统的分簇 WSNs 节点身份认证机制[J]. 传感器与微系统, 2012, 31(12): 58-61.
- [3] 郝玉洁, 刘贵科, 秦科, 等. 信息安全概论[M]. 成都: 电子科技大学, 2007.
- [4] 黄中伟. 计算机网络管理与安全技术[M]. 北京: 人民邮电出版社, 2006.
- [5] Pablo Cibraro, Kurt Claeys, Fabio Cozzolino. Professional WCF4 [M]. Indianapolis: Wiley Publishing, 2010.
- [6] Christian Nagel, Bill Evjen, Jayglynn. Professional C# 4 and .NET4 [M]. Indianapolis: Wiley Publishing, 2010.

作者简介:

陈海燕 女, (1977-), 博士研究生, 讲师. 研究方向为地球探测与信息技术、软件应用技术.

王合闯 男, (1975-), 博士, 讲师. 研究方向为计算机仿真、软件工程.

李英豪 男, (1980-), 博士研究生, 讲师. 研究方向为地球探测与信息技术、图形图像技术.

王华军 男, (1964-), 教授, 博士生导师. 研究方向为地球探测与信息技术、电子通讯.