

网络地理信息系统中数据传输安全的探讨

郑江

(中国科学院资源与环境信息系统国家重点实验室, 北京 100101)

摘要: 在网络地理信息系统应用日益广泛的今天, 如何保证地理信息数据在网络中的传输安全, 是一个十分重要的问题。本文分析了网络地理信息系统在数据传输方面可能存在的安全隐患, 以及为了克服这些隐患所需满足的安全需求。在此基础上, 本文介绍了代理中间件技术的基本原理, 并基于代理中间件技术提出了一种网络地理信息系统数据传输安全平台的实现框架。

关键词: 网络地理信息系统; 数据传输; 代理中间件; 数据传输安全平台

中图分类号: P208; TP393

1 引言

地理信息作为一种重要的社会信息资源, 它的共享与开放是一个十分重要的问题。近年来, 随着计算机网络、通信等信息技术的飞速发展, 地理信息的处理已从传统的集中方式转向当前的网络化分布方式。如何在网络环境下更好地解决地理信息的共享与开放问题, 已成为当前地理信息系统技术研究与应用的一个热点。

目前, 在网络环境下, 各种相关的技术和产品不断地出现, 如何保证数据信息的安全是一个颇受关注的问题。在网络地理信息系统的应用中, 传送地理信息数据是一个重要的步骤, 尤其是当某些地理信息可能会关系到私人秘密、集体利益乃至国家安全。因此, 保证各种地理数据信息传输的安全, 是一个值得思考的问题。

代理(proxy)是一种在计算机系统中广泛采用的技术。将它的设计原理与网络地理信息系统和安全技术相结合, 可以为解决网络地理信息系统数据传输安全问题提供一种可行的方案。

2 网络地理信息系统构建的技术基础

建立网络地理信息系统的主要目的是实现地理信息的开放与共享。目前, OPEN GIS 等国际标准化组织正在加紧研究和制订地理信息共享方面的相关

技术标准, 但是, 一套完整的系统结构规范还没有被普遍采用。国际上不同的相关机构都根据各自的需求采用了不同的设计方案, 总体来说有以下几种。

2.1 CGI方法(通用网关接口)

CGI是通用网关接口的缩写, 它的作用是在 Internet 服务器与后端应用程序之间建立一个接口, 使用户端程序可以访问服务器端的应用程序。在基于CGI方式下, 用户按如下方式与网络地理信息系统进行通信。用户端首先向服务器发送一个请求, 服务器通过CGI程序将这个请求转发给后端的网络地理信息系统, 后端的网络地理信息系统会按照给定的要求产生结果并交还给服务器, 服务器在把这一结果通过网络返回给用户端显示。在这一过程中, CGI起着沟通用户与网络地理信息系统软件的桥梁作用。

2.2 Server API方法(服务器应用程序接口)

Server API方法与CGI方法的基本原理类似。不同点主要在于CGI是可以单独运行的程序, 处理用户请求的CGI程序每次处理一个请求, 都需要重新启动, 而Server API是必须基于特定的服务器运行的动态连接模块, 它在启动后会一直处于运行状态, 服务器可以通过IPC(Interprocess Communication)与之进行信息交换。

2.3 plug-in 方法(插件)

plug-in 方法的基本原理是服务器端在客户端安装一个专门能够和浏览器进行信息交换的地理信息系统软件, 通过这个插件, 服务器端可以将部分数据处理工作发送到客户端进行处理, 从而减轻了服务器端的处理压力。

2.4 Java 程序语言的方法

Java 是 SUN 公司提出的一种专门为网络设计的程序语言。基于 Java 开发的网络地理信息系统运行的基本原理是: 由服务器端向客户端发送一段在客户端运行的程序, 该程序可以与用户交互, 处理用户的简单请求, 所需的数据直接向服务器申请; 只有当发送的程序无法处理客户端的一些比较复杂的请求时, 才将请求提交给服务器端处理。

3 网络地理信息系统在数据传输上存在的安全问题

目前基于以上几种技术构造的网络地理信息系统, 它们在数据传输上具有如下特点:

(1) 客户端与 WEBGIS 服务器端基本都需要采用基于 HTTP 协议的 WEB Browser/WEB Server 方式来进行双方之间的数据传输。

(2) 客户端与 WEBGIS 服务器之间的数据传输基本上是以明文方式进行。虽然通用的浏览器(Netscape 的 Navigator 和 Microsoft 的 IE)和 Web 服务器, 目前都可以提供一些安全功能, 但是由于国外对安全产品出口限制以及国内对安全产品使用方面的一些规定, 这些功能还不能适应国内的应用需求。

(3) 客户端与 WEBGIS 服务器之间不能准确地确定对方的真实身份。

基于上述特点, 网络地理信息系统在数据传输方存在的安全隐患, 主要有以下几个方面:

(1) 对用户身份的仿冒

攻击者盗用合法用户的身份信息, 以仿冒的身份与服务器端通信, 从而骗取信息。

(2) 对网络上信息的窃取

攻击者在网络的传输链路上, 通过物理或逻辑的手段, 对合法用户与服务器端之间传送的数据进

行非法截获与监听, 从而得到其中的敏感信息。

(3) 对网络上信息的篡改

攻击者可能对网络上合法用户与服务器端之间传送的数据信息, 进行截获并且篡改其内容(增加、截去或改写), 使数据信息的接收方无法得到真实的数据信息。

4 代理中间件技术

在计算机系统中, 代理中间件有着广泛的应用。不同用途的中间件都有各自专门的标准程序接口和协议规范, 可以根据应用需要被装入系统的任何一个层次, 提供相应的服务。比如, 构造安全的操作系统内核、对通信系统间不同数据格式进行转换等应用。

代理中间件技术的主要好处是它可以简化系统的研制与开发。尤其是对于一些需要采用异构系统分布式处理的应用场合, 利用代理中间件技术可以大大简化系统构建的复杂度。

在 Client/Server 结构的应用中, 经常由于某些特殊的应用需求而需要在通信双方之间插入代理中间件, 以监控客户端与服务器端的通信。在这种情况下, 对于客户端, 代理中间件可以被看成是它的服务器, 它接受客户端发来的请求, 并向客户端返回数据; 对于服务器端, 代理中间件可被看成是它的客户端, 可以向其提出请求, 并接收其响应信息。Client/Server 环境下采用代理中间件方式进行通信的一般系统结构如图 1 所示:

在下文中, 将提出一种利用代理中间件技术构造网络地理信息系统数据传输安全平台的实现框架。

5 网络地理信息系统数据传输的安全平台

5.1 网络地理信息系统数据传输的安全需求

根据网络地理信息系统在数据传输方面存在的安全隐患, 采用代理中间件技术构造的网络地理信息系统数据传输安全平台应该满足如下安全需求:

(1) 数据保密 通过某种方法对需要传送的数据进行加密, 以保证在被非法截取的情况下, 未授权的用户无法得知其中包含的真实信息。

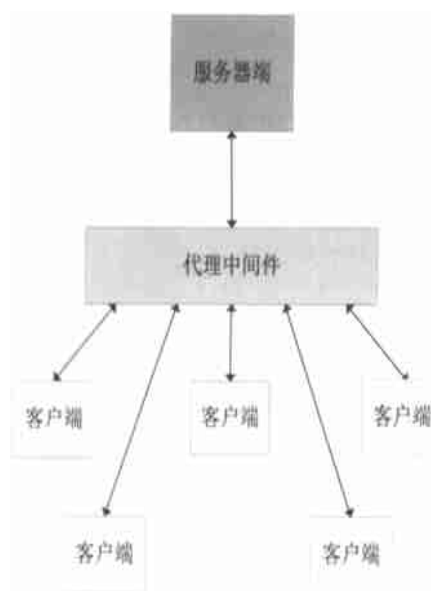


图 1 采用代理中间件的系统结构

Fig. 1 Normal frame of agent system

(2) 数据完整性 需要通过某种方法来确认接收到的数据在传输过程中没有被篡改。

(3) 身份认证 需要使客户端与服务器端能够互相进行身份验证, 以确认对方的真实身份。

5.2 网络地理信息系统数据传输安全平台的总体结构

网络地理信息系统数据传输安全平台可以被分为 4 个层次:

第一个层次: 客户端 Browser

第二个层次: 客户端安全代理

第三个层次: 服务器端安全代理

第四个层次: 服务器端 WebServer

根据上述的系统安全需求, 可以设计出系统的逻辑结构, 具体的逻辑框图如图 2 所示:

5.3 系统工作原理描述

1) 安全代理中间件的组成和作用 安全代理中间件主要由两部分组成: 客户端安全代理和服务器端安全代理。

对于客户端安全代理, 它可以分为两个部分, 即 HTTP 协议代理部分和安全通信部分。它主要的作用有:

(1) 接收来自浏览器的访问请求, 对访问普通页面的请求和有安全需求的请求分别进行处理后再

进行发送。

(2) 与服务器端安全代理进行安全通信。

(3) 使客户端与服务器端实现相互间的身份认证。

对于服务器端安全代理, 它一般只由安全通信部分构成。它主要的作用有:

(1) 同时与多个服务器端安全代理进行安全通信。

(2) 使客户端与服务器端实现相互间的身份认证。

2) 网络地理信息系统数据传输安全平台的工作过程

基于安全代理中间件建立的数据传输安全平台的工作过程可以分为如下 4 个阶段:

(1) 客户端与服务器端建立安全的连接。

(2) 客户端与服务器端协商安全通信参数, 相互认证对方身份。

(3) 如果双方认证成功, 则双方利用协商好的参数进行安全通信; 否则, 如果双方认证失败, 则断开第一步建立的安全连接。

(4) 在安全通信结束后, 双方断开连接。

在这里有两个需要具体注意的问题:

(1) 互联网采用的 HTTP 协议是一个无连接、无状态的协议。它每次连接仅处理一个请求, 而且在服务器端与客户端均不保存前一次连接的状态, 因此连接的建立和关闭很频繁。如果每一次连接通信, 双方都必须执行一次相互身份认证, 势必将明显降低客户端与服务器端的通信速度。所以, 应当采取某种机制, 比如象虚连接的处理方式, 使得在一定时期内只有当客户端第一次向服务器端发出连接请求时才需要进行身份的认证, 此次认证所产生的安全参数可以为该服务器端与客户端随后进行的连接所使用, 即一次认证可对应多个连接。

(2) 当同时有大量用户访问网络地理信息系统时, 如何保证安全代理系统可靠、高效地提供服务, 也是一个十分关键的问题。在这里, 服务器端安全代理与客户端安全代理都应该是作为一种守护进程在各自的系统上后台运行, 监听相应的连接请求。一般来说, 采用线程虽然具有速度快、系统开销小、易于同步等特点, 但是由于线程的运行是基于进程的, 如果低层的进程运行出现问题(比如进程崩溃), 以它为基础的线程势必全部都会受到影响; 而且由于同一进程的多个用户线程的数据在内存中是共享同一

存储区域的,因而有可能出现不同用户的线程之间数据发生相互干扰或者恶意的用户非法获取或破坏其它用户线程数据的情况。因此,在系统的实现中应该尽量采用多进程的设计方式。

客户端与WEBGIS服务器端进行安全数据传

输的具体过程设计如下:

(1) 客户端安全代理启动,在某一指定端口(通常为8080)监听客户端浏览器的连接请求。

服务器端安全代理启动,在某一指定端口监听客户端安全代理的连接请求。

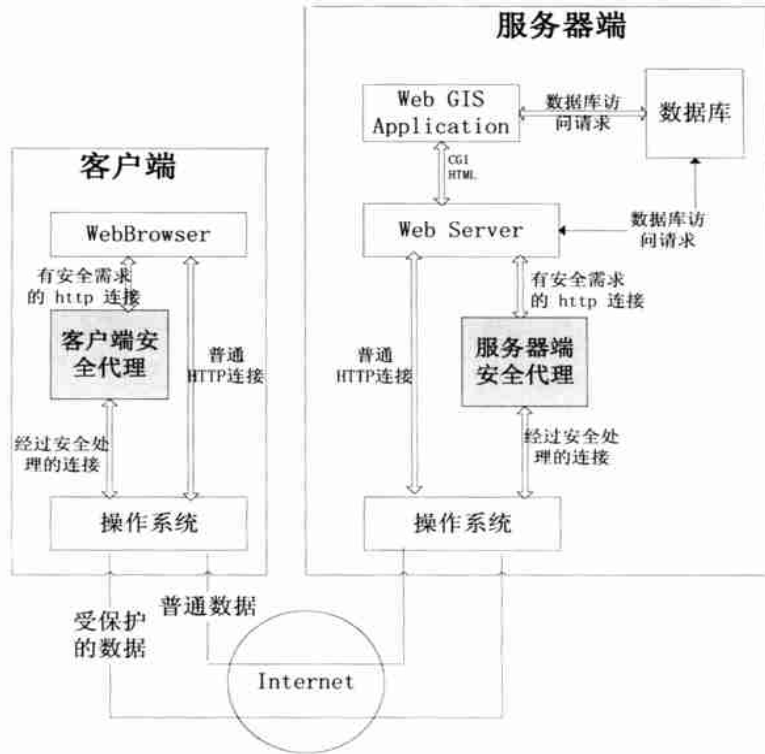


图2 系统逻辑框图

Fig 2 System main frame

(2) 客户端安全代理接收客户端浏览器的连接申请,解析申请,确定将要连接的服务器端安全代理的IP地址和端口号。

(3) 客户端安全代理向服务器端安全代理发送一个建立连接请求。

(4) 服务器端安全代理启动一个子进程(p)处理这个连接请求,它自己仍然在原端口继续监听其它连接请求。

(5) 如果此次连接申请为该客户端与服务器端的第一次连接,则双方互相需要验证对方身份,否则返回接受连接的消息。身份验证过程主要涉及到双方身份信息的交换与确认、各种安全参数的协商等操作。

(6) 客户端安全代理在收到服务器端代理的接受连接消息后,利用双方在认证阶段协商好的安全参数对准备发送的信息进行加密处理,将密文发送

给服务器端的子进程p。

(7) 子进程p通过相同的安全参数对接收到的密文进行解密,将结果转发给后台的Web Server和网络地理信息系统。

(8) 网络地理信息系统对用户的请求进行处理,将处理结果由Web Server发送给子进程p。

(9) 子进程p利用协商好的安全参数对结果消息进行加密处理,并将结果传送回客户端安全代理。

(10) 客户端安全代理利用协商好的安全参数对接收到的数据进行解密,将结果转发给客户端浏览器。

(11) 在数据传送完毕后,客户端与服务器端关闭建立的连接和子进程p。

至此,客户端与服务器端的安全数据传输完成。

6 结论与展望

采用安全代理中间件来解决网络地理信息系统中的数据传输安全问题有如下优点:

(1) 安全代理中间件集成了成熟的安全技术, 可以为网络地理信息系统中的数据传输提供可靠的安全保障。

(2) 安全中间件与原有应用系统和底层网络通信协议的耦合度较低, 它可以在对原由系统性能几乎没有影响的情况下方便地集成到原有的系统中去, 使系统具有良好的可扩展性和易维护性。

(3) 安全中间件的适用范围很广泛, 它不仅可以与目前采用 Client/Server 结构的系统相结合, 而且经过修改后它也可以为采用其它体系结构的网络地理信息系统(比如组件式的网络地理信息系统)的数据传输提供安全保护。

本文讨论了网络地理信息系统在数据传输中存在的安全隐患, 并基于已有的网络地理信息系统技术和信息安全技术, 提出了一种网络地理信息系统数据安全传输的系统框架。

随着社会的发展, 人们将会越来越多地通过网络获取、共享地理信息。但是, 地理信息的开放与共享通常会带来地理信息的安全问题。因此, 为了更好

地利用地理信息资源, 在设计各种地理信息应用系统时, 对地理信息在相应环境下的安全保护问题进行研究是十分必要的。

参考文献

- [1] 龚健雅, 李斌等. 当代 GIS 的若干理论与技术. 武汉: 武汉测绘科技大学出版社, 1999.
- [2] 周成虎. 地理信息系统概要. 北京: 中国科学技术出版社, 1993.
- [3] 齐锐, 张大力, 黄磊, 李琦. 网络化地理信息系统中数据传输技术的探讨. 计算机研究与发展, 1999, 36(3): 380 ~ 384.
- [4] 韦卫, 王德杰, 张英, 王行刚. 基于 SSL 的安全 WWW 系统的研究与实现. 计算机研究与发展, 1999, 36(5): 619 ~ 624.
- [5] 王育民, 刘建伟. 通信网的安全——理论与技术. 西安: 西安电子科技大学出版社, 1999.
- [6] ISO 7498-2-1989 "Information processing system—Open System's Interconnection—Basic Reference Model—Part2: Security architecture".
- [7] Peng Z. An Assessment of Internet GIS. Department of Urban Planning, University of Wisconsin Milwaukee, 1998.
- [8] RFC 2818, "HTTP Over TLS", 2000.

Study of Data Transfers Security in WebGIS

ZHENG Jiang

(State Key laboratory of Resources and Environment Information Systems of CAS, Beijing 100101)

Abstract: With the increasingly wide application of WebGIS, it is very important to assure the geo information data transfers security in the network. In this paper, the author analyzes some hidden security troubles and the security necessity in order to overcome those troubles. On the basis of the above description, this paper discusses the technique of proxy middleware, and proposes an implementation framework of secure data transfers platform for WebGIS.

Keywords: WebGIS; Data transfers; Proxy middleware; Secure data transfers platform