开放实验室数据安全传输系统设计与实现

陈 宛[1,2]，曹元大[3]

(1. 中国科学院 高能物理研究所，北京 100039；2. 北京理工大学 信息科学技术学院 计算机科学与工程系，北京 100081；3. 北京理工大学 软件学院，北京 100081)

摘 要：通过添加基于 SSL 协议的安全代理，解决了开放实验室远程数据传输中数据的安全问题，讨论了实现 SSL 协议的几种技术。介绍了系统在网络中的整体结构、安全代理的组成及各组成模块的作用以及远程安全通信管道建立过程。简述了系统的实现方法。实际测试表明，该系统有效地保护了传递数据的安全。

关键词：数据安全；SSL 协议；安全代理

中图法分类号：TP309.2 **文献标识码**：A **文章编号**：1001-3695(2005)07-0156-02

Design and Implementation of Secure Data Transmission System for Open Laboratory

CHEN Wan[1,2], CAO Yuan-da[3]

(1. *Institute of High Energy Physics, Chinese Academy of Sciences, Beijing* 100039, *China*; 2. *Dept. of Computer Science & Engineering, School of Information Science & Engineering, Beijing University of Technology, Beijing* 100081, *China*; 3. *School of Computer Software, Beijing University of Technology, Beijing* 100081, *China*)

Abstract: Through adding security proxy based on SSL protocol in data transmission system of open lab, the problem of data security is resolved. Discussing the implemented technologies of SSL protocol. The structure of data transmission system and the components of the SSL security proxy with their function are introduced. The process of building transmission channel is concluded. The implementation method of the system is given. Experimental results show that it protects the data effectively.

Key words: Data Security; SSL Protocol; Security Proxy

扩大专业开放实验室的用户群，是提高实验室资源利用率的有效手段。随着互联网的发展与网络应用的迅速普及，使各专业实验室对互联网用户开放成为可能。通过互联网，需要做实验的科技人员不必亲临实验现场就可以实时、高效地获得测量数据并控制测量设备的操作，根据测量结果随时调整测量策略，确认设计结果。在以往的网络开放实验室系统中，实验信息不加任何保护地在网络中传递，很容易受到监听和窜改，这大大阻碍了开放实验室对网络开放的进程。因此，有效保障实验信息在互联网上传输的安全性和可靠性，是实验室面向互联网用户开放所必须解决的关键问题。通过对各种加密技术进行分析，建立了一套基于 SSL 协议的，适用于实验室网络化的安全数据传输系统。

1 数据安全传输实现的方案

为了抵御假冒、重放、中间人等各种形式的主动和被动攻击，保证数据信息在网络中的安全，对应网络模型的每一层都提出了相应的协议，其中较为常用的信息安全协议有 IP 安全协议、SET 协议、SSL 协议。SSL 协议由 Netscape 公司最先提出，是一种基于会话的加密和认证的 Internet 协议，位于传输层和应用层之间，即位于 TCP/IP 之上，对应用层透明，主要目的是为通信双方提供一条安全的通信管道。SSL 协议完全可以满足开放实验室数据安全传输的要求，并且比其他协议实现起来简单，因此选择了以 SSL 协议作为安全系统的基础，提供网络上数据安全传输的保障。

对于 SSL 协议具体实现，一般有三种构建方式，即使用 SDK 在应用程序中集成 SSL；SSL 层实现在操作系统内核；使用代理机制实现 SSL。

综合考虑在实际应用中的要求，以及具体可能的应用方式，在所设计的数据安全传输系统中，采用了代理结构实现 SSL 的安全通信。代理技术一般在 TCP 层之上，对应用程序透明，因此对原有的实验采集/控制系统影响较小，建设成本较少，并且代理服务的实现技术成熟，方案比较容易实现。

2 系统结构

开放实验室远程数据安全传输系统由位于中心实验室的 SSL 代理服务器端(Sserver)，实验设备控制主机，实验数据采集处理机(Sclient)，以及位于远程用户实验室的 SSL 代理客户端(Cserver)，远程实验采集控制机(Cclient)组成。

中心实验室的实验设备控制主机直接用于控制实验设备的各种操作和实验数据的采集、处理，实验数据采集处理机和本地多套实验设备控制主机连接，用于集中采集各套设备的实验数据、下发操作指令，同时通过 SSL 代理与远程用户实验室的实验控制采集机通信，完成实验信息的传递。一般情况下认为中心实验室和远程用户实验室的内部局域网比较可靠，

收稿日期：2004-06-06；修返日期：2004-09-14

Sclient到 Sserver 和 Cclient 到 Cserver 的信息以明文方式传递。中心实验室和用户实验室之间一般通过广域网进行连接,不安全信息必须以密文方式传递,信息的加/解密和有效性等由 SSL 代理处理完成。Sclient 和 Cclient 必须且只有通过 SSL 代理才能实现连接。

图 1 所示,为实验室安全传输系统的标准使用环境示例。SSL 代理设置于防火墙后面。对于有 DMZ 设置的安全网络,从便于管理和加强安全的角度出发,SSL 代理应该和 Web 服务器、Mail 服务器一同放置在 DMZ 区。

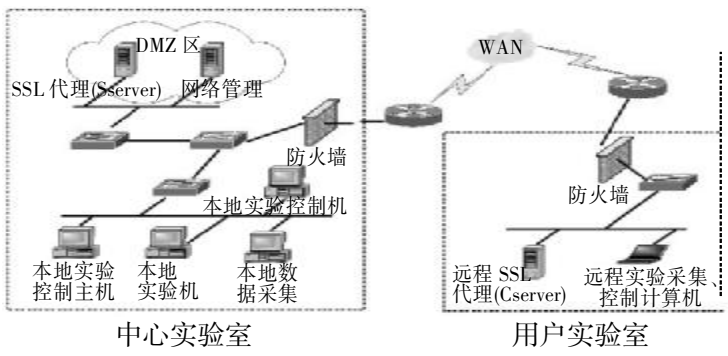

图 1　实验室远程数据安全传输系统

3　安全代理的组成

SSL 代理为典型的 C/S 结构,包括服务器和客户端两部分,是数据安全传输系统的核心,用于完成通信双方身份的鉴别、握手连接、信息的加/解密、数据源的鉴别以及信息完整性的鉴别。安全代理的服务器和客户端均由用户管理模块,证书管理模块,通信及 SSL 模块和密码算法模块四个功能模块组成。各模块之间的结构、功能关系如图 2 所示。

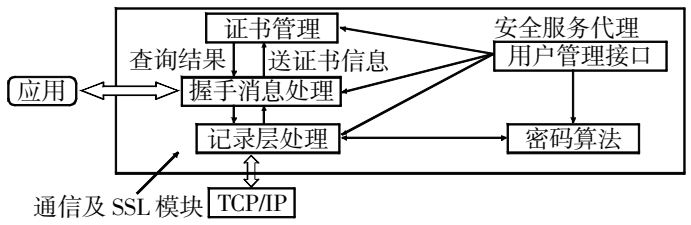

图 2　安全代理组成

(1) 用户管理模块。实现安全代理的 SSL 模块配置功能,为 SSL 模块配置必要参数:端口号、主机名、密码套件、可信任的 CA 证书和可以使用的服务器(客户端)证书等。

(2) 证书管理模块。它包括一个证书库,用于存放代理的客户端或服务器端的证书和可信任的 CA 证书。负责新证书的申请,客户端或服务器端的证书和可信任的 CA 证书的鉴别。通过用户管理进行操作。

(3) 通信及 SSL 模块。它们包括 SSL 握手协议处理和记录层协议处理两个子模块。首先使用用户管理界面中配置的参数在 SSL 握手协议处理子模块中完成握手消息的处理,服务器(客户端)证书的认证,协商共同支持的密码套件等会话所需参数,计算加密密钥等。在记录层协议处理子模块对通信数据进行分段、计算 MAC 值并用握手协商得到的加密密钥加密数据,或对收到的加密数据进行解密、重组、信息校验等。

(4) 密码算法模块。支持常用的密码算法,如 DES, RC4, RC5, MD5, SHA, SHA-1, RSA 等。在该系统中将加密算法实现与 SSL 协议实现独立分开,预留了对密码算法进行扩充的接口,便于用户添加自己的密码算法。考虑到用户不同的安全需求,在该模块中设计了主秘密输出接口,将主秘密截取一部分提供给应用程序,作为应用程序生成自主加密密钥的密钥源。是否输出密钥源由用户设定。

4　SSL 代理之间通信过程的实现

SSL 安全代理的客户端与服务器端之间建立可靠的通信连接,是数据安全传输系统的主要关键技术之一,如图 3 所示,为数据传输、握手的流程。

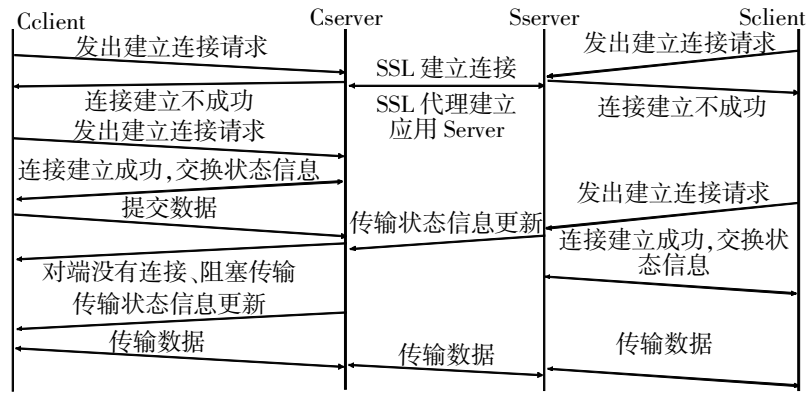

图 3　安全系统数据传输流程

Cclient 和 Sclient 传送信息时,需要启动安全代理,构造一条安全传输线路传输加密数据。

4.1　连接的建立

通信连接过程如下:

(1) Sserver 与 Cserver 首先建立连接。在 Sserver 与 Cserver 之间的 SSL 连接没有建立之前,Sserver 端处于对 Cserver 请求的监听状态,此时没有用于实际数据传输的服务,无论是处于 Sserver 端的应用 Sclient 还是处于 Cserver 端的应用 Cclient,它们所发出的 Socket 连接请求都由于没有响应而被拒绝。

(2) Cclient 和 Sclient 与各自的安全代理 Cserver、Sserver 建立连接。信道建立成功,可以开始正常通信。如果 Cclient 和 Sclient 有一方没有连接到安全代理上,则相应的安全代理会阻塞服务并返回状态信息。

(3) 断开连接。Cclient 与 Sclient 通信结束后,分别发通信结束信息到安全代理,并断开连接,Sserver 与 Cserver 也断开连接。Cclient, Sclient 任意一方或双方非正常退出与安全代理的连接都可以中断安全代理之间的 SSL 连接。Sserver 重新在固定端口侦听下一次连接请求。如果下一次连接通信双方没变则可通过使用会话重用技术,使通信双方直接使用已有的会话参数,从而简化握手连接的过程,提高通信效率。

4.2　连接状态

应用发出连接请求,当 Socket 连接建立时,SSL 安全代理将当前的连接状态发给发出请求的应用。连接状态包括:

(1) 可用于应用程序完成自定义加密的密钥源。如果用户选择了使用密钥源,连接状态中将包括此项。

(2) 对端应用连接状态。包括三种状态,即无可用 SSL 连接、对端应用未连接和对端应用已连接。只有应用双方的连接都建立之后,应用之间才可以形成有效的通信,当只有一端应用与 SSL 代理连接时,数据的传输置于阻塞状态,而该应用等待通信状态的信号灯的改变。

当 SSL 代理接收到另一个应用的连接请求时,它一方面和该应用建立一个有效的 Socket 通道;另一方面对上述的连接状态进行更新,将通信状态信号灯置为“真”。　(下转第 160 页)