文章编号:1005－0523(2007)02－0110－03

基于 Linux 的嵌入式安全 Web Server 的实现

杨丰萍,邢 剑,马书研

(华东交通大学 电气与电子工程学院,江西 南昌 330013)

摘要:阐述的嵌入式 Web 服务器是基于 ARM 处理器和 Linux 操作系统.首先给出了嵌入式 Web 服务器的整体设计方案,然后详细探讨了其核心模块:双进程模块,CGI 模块以及安全认证模块等的实现.

关 键 字:嵌入式 Web 服务器;进程;CGI;安全认证

中图分类号:TP393;TM77 **文献标识码**:A

0 引言

计算机和通信技术的发展正越来越深刻地改变着人们的生活,特别是在工业控制领域.近些年,把 Internet 技术和 Web 技术应用到工业控制系统,实现终端设备智能化、网络化,一直是热点,并形成两个技术分支:嵌入式因特网(Embedded Internet－EI)技术和嵌入式 Web 服务器(Embedded Web Server－EWS)技术.本文即结合变电站自动化领域一种网关的设计,实现一嵌入式安全 Web 服务器.由于自身资源的限制和应用场合不同,嵌入式 Web 服务器和通用 Web 服务器有着很大差别,但基本原理是没什么区别.本嵌入式 Web 服务器就是根据服务器的基本实现原理,硬件核心模块采用 S3C2410A 处理器,软件采用嵌入式 Linux 操作系统构建三层 B/S 结构的瘦服务器.服务器和客户端间的通信协议采用标准的 HTTP1.1 协议,用 C 语言实现 Berkerly Sockets 编程网络接口,服务器和 CAN 总线驱动程序之间的交互接口为标准 CGI,使该服务器更具有通用性.

1 整体设计要求及方案

嵌入式 Web 服务器的体系结构如图 1 虚线框所示.应用软件部分主要包括通信协议模块、监控模块、进程处理模块和安全认证模块.通信协议模块实现上行和下行数据的格式转换;监控模块实现对现场总线数据的监听,并将参数进行统计保存在 Flash 上,随时掌控设备的运行状态;进程模块用以解析和处理请求;安全认证模块的作用是防止系统被攻击,

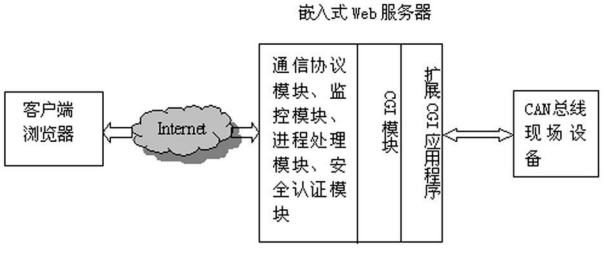

图 1 嵌入式 Web 服务器的功能结构图

确保系统的信息安全.作为 EI 接入的核心软件,嵌入式 Web 服务器应尽量发挥 Internet 在监控领域的远程数据传输及控制方面的优势.结合本网关在变电站系统中的应用需求,该服务器主要包括采集实时数据及历史数据动态发布、设备运行和状态参数设置、远程实时监控、电子邮件告警、文件下载等功能.其中实时数据包括遥测量、遥信值、电能、设备故障记录、事件顺序记录、故障录波、扰动记录等;控制功能包括遥控、遥调、同期操作和定制切换等,服务器接收到远方客户提交的控制操作命令后,通过现场总线驱动相应的终端设备动作;电子邮件告警功能用于通过 Internet 自动发送电子邮件及时给管理员,通知其进行设备维护,并发送系统运行日志;下载是将历史数据的备份文件从服务器端下载到客户

收稿日期:2007－02－15

作者简介:杨丰萍(1967－),女,副教授,主要从事交通信息工程及控制,计算机测控等方面的研究.

端.

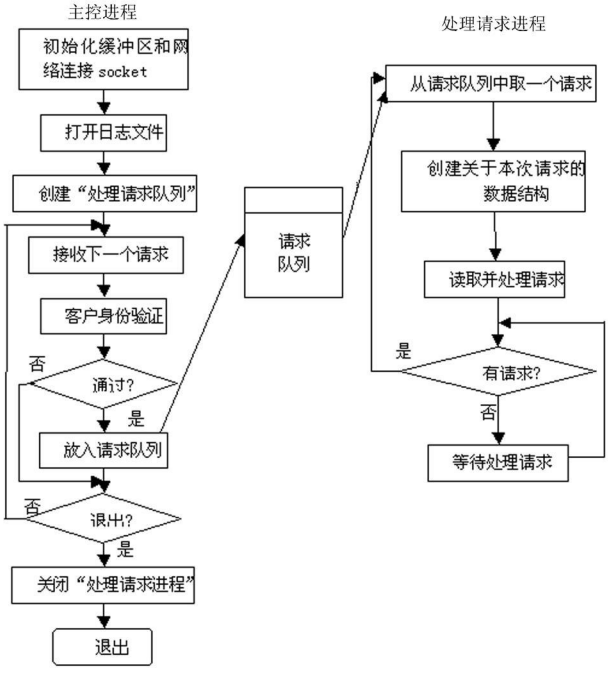

图 2　双进程模式工作流程图

2　核心进程处理模块的实现

Linux 系统网络服务器模型主要有两种，即并发服务器和循环服务器，而并发服务器可以用多线程或多进程来实现.本服务器采用“阻塞模式”和“进程池模式”相结合的双进程模式响应客户端请求，主进程为守护进程，其主要任务是初始化服务器运行环境，创建倾听套接字函数和一个用于存放客户连接请求信息的请求队列，并接受新的连接.当接收到客户连接请求时，主控进程将预先处理该进程，进行权限认证，然后将请求放到请求队列中并将请求信息填充到“请求结构体”，返回确认连接响应信息给客户.主控进程在接收第一个请求的同时创建第二个进程即处理请求进程.处理进程从请求队列中取出一个客户请求信息，加以解析处理后，把结果发回给客户端，而后循环往复.双进程工作模式如图 2 所示.

主进程用到的主要函数说明：

```
init_log();//初始化日志
init_signals();//初始化信号
int creat_daemon;//把主进程转化为守护进程
auth_check();//权限检查
void update_requestlist();//在指定端口创建新请求任务,并添加到请求队列中
request * remove_worklist();//从请求队列中取出一个任务,并返回对应的请求信息结构体指针
typedef struct requestqueue_s //请求队列定义
{
    int exit_now;
    int request_n;//请求队列中请求的个数
    semaphore * requestsemaphore;//请求队列同步量
    mutex * requestmutex;//请求队列互斥量
    requestlist * requesthead;//请求队列头指针
    requestlist * requesttail;//请求队列尾指针
}requestqueue;
```

请求处理进程循环从请求队列中取出主进程已经预处理的客户请求，解析后通过调用 CGI 程序访问终端设备，最后把结果封装成 HTTP 报文返回给客户端.在解析客户的请求信息结构体 request *req 后，进程调用 handle_request(File f*, request *req)函数处理客户请求，例如处理目录 do_dir()、处理文件 do_file()、CGI 程序调用 do_cgi、发送 HTML 内容 do_html 等等.

3　CGI 模块

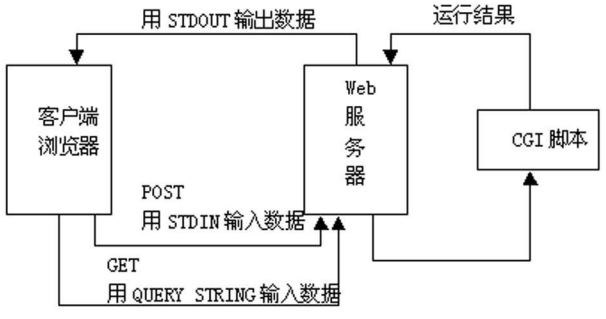

图 3　CGI 工作流程示意图

CGI(Common Gateway Interface 通用网关接口)是一种标准扩展技术，是外部扩展应用程序与 Web 服务器交互的接口标准.当客户端的用户完成输入工作向服务器发出 CGI 请求，服务器进程收到该请求后，首先设置处理 CGI 请求环境变量，然后启动 URL 指定的 CGI 程序，并与该进程保持同步.CGI 进程把处理结果传递给服务器进程，服务器再以 HTML 格式输出返回给客户端.环境变量是 Web 服务器和 CGI 脚本进行数据传递的途径.整个过程可以用图 3 表示.

嵌入式 Web 服务器可以通过三种途径接收信息：环境变量、命令行和标准输入.具体使用哪一种方法由＜FORM＞标签的 METHOD 属性来决定.在

“METHOD=GET”时，向CGI程序传递表单编码信息的正常做法是通过命令行来进行的.大多数表单编码信息是通过QUERY-STRING的环境变量来传递的.如果“METHOD=POST”，表单信息将通过标准输入来读取.还有一种不通过表单就可以向CGI传递信息的方法，那就是把信息直接追加在URL地址后面，信息和URL之间用“?”隔开.METHOD的缺省值为GET方法.由于本网关系统只需要对终端设备执行简单操作，所以使用C语言编写外部可执行程序.CGI程序处理结束输出的应答信息是HTTP应答信息，它一般由两个部分组成：应答头和应答数据.常见的应答头包括三种头域：Content—Type(数据编码类型，用MIME表示)，Location(指定文档的URL)和Status(处理结果的状态码和状态描述).应答头和应答体之间用以空行分割.应答体为CGI扩展程序的输出数据，其数据类型应该与Content—type一致.

4 安全认证模块

结合嵌入式系统的特点，本系统采用紧凑安全策略，把资源划分为不同的安全等级，不同等级的资源采用不同的访问控制.中低安全级的资源请求主要由Web服务器的主进程在80端口监听，收到请求后进行HTTP摘要认证，通过后交给请求处理进程进行处理；而高安全级的请求由Web服务器专门进程在SSL默认端口443监听，当接收到响应请求后，采用SSL协议进行安全身份验证及相应数据的传输，并且直接由进程处理请求.摘要认证的程序代码嵌于守护进程中，用到的数据结构和函数简介如下.

这样定义请求处理时的摘要信息数据结构digest-header-rec：

```
typedef struct digest-header-struct{
char* username;//用户名
char* realm;//用户所属域
char* now;//当前值
char* requested-uri;//被请求资源的uri
char* digest;//摘要值
}digest-header-rec;//记录摘要认证体制的头信息
```

调用的几个重要函数如下：

(1)get-digest-rec(request-rec* r,digest-header-rec* response)

函数从请求队列中解析出摘要认证信息，在authenticate-digest-user()中调用.

(2)find-digest(request-rec* r,digest-header-rec* h,char* a)

本函数根据用户送来的认证头域信息及从本地授权数据库中的用户口令文件查出的密码信息，按摘要认证机制算出用于验证用户摘要值的正确摘要值，返回32字符长的16基编码字符串.

(3)authenticate-digest-user(request-rec* r)

本函数对用户进行摘要认证，验证用户的身份真实性.

(4)digest-check-auth(request-rec* r)

本函数检验是否能访问该资源目录，进行文件/目录级的授权检查，用户的权限信息存放在授权数据库中.

5 结束语

嵌入式Internet的目的是使现场终端设备接入Internet，实现远程监控.而作为整个系统最核心的部分就是嵌入式Web服务器的实现，其本质就是把PC机上的Web服务应用到嵌入式系统.本服务器是为应用于变电站综合自动化领域开发的网关的核心部分，在实现的过程中，充分考虑了嵌入式系统资源有限的特点，构建最小的安全可靠系统，其很多设计方法还可以用到其他嵌入式系统中.

参考文献：

[1]天夜创作室.Linux网络编程技术[M].北京：人民邮电出版社，2001.

[2]Jeremy Bentham，陈向群等译.嵌入式系统Web服务器TCP/IP Lean[M].北京：机械工业出版社，2003.

[3]阙喜戎.信息安全原理与应用[M].北京：清华大学出版社，2003.

[4]魏洪兴，胡亮，曲楼学.嵌入式系统设计与实例开发实验教材[M].北京：清华大学出版社，2005.

[5]倪继利.Linux内核分析及编程[M].北京：电子工业出版社，2005.

[6]李磊，杨柏林.嵌入式Web服务器软件的设计与实现[J].计算机工程与设计，2003，24(10)：100—102.

[7]赵跃华，杜云海.嵌入式安全Web网关的设计与实现[J].计算机工程与设计，2006，27(4)：565—567.

(下转第117页)

参考文献：

[1]Web Services Enhancements 3.0 for Microsoft.NET[S].http://www.microsoft.com/downloads/details?aspx?familyid=018a09fd-3a74-43c5-8ec1-8d789091255d&displaylang=en,2005-12.

[2]于国良，韩文报.XML 的安全性研究[J].信息工程大学学报，2006,7(1):7-10,22.

[3]Web Services Enhancements(WSE)3.0 的新功能[EB/OL].http://msdn2.microsoft.com/en-us/library/ms977317.aspx,2005-6.

[4]Protect Your Web Services Through The Extensible Policy Framework In WSE 3.0 [EB/OL].http://msdn.microsoft.com/msdnmag/issues/06/02/WSE30/,2006-2.

[5]张维勇，程俊，王建新.基于 WS-Security 安全规范的 Web 服务设计[J].合肥工业大学学报(自然科学版)，2006,29(8):972-975.

Implementing Signature and Encryption of Web Services Security with WSE 3.0

HU Xiao-hong，DING Zhen-fan

(School of Information Engineering，East China Jiaotong University，Nanchang 330013，China)

Abstract：Signature and encryption are the technique often used in implementing Web services security.The issuance of Microsoft Web Services Enhancements(WSE)3.0 supplies a new solution to Web Services security.The paper explores the implementation ways of partial signature and partial encryption by using WSE 3.0，which has wide-spread practicability.

Key words：Web Services Security；WSE 3.0；signature；encryption

(上接第 112 页)

Realization of Embedded Secure Web Server Based on Linux

YANG Feng-ping，XING Jian，MA Shu-yan

(School of Electrical and Electronic Engineering，East China Jiaotong University，Nanchang 330013，China)

Abstract：The embedded Web Server here is based on processor ARM9 and operating system Linux.Firstly，the paper presents its whole design，then it expatiates three modules of the Web Server：double processes module，CGI module and secure mechanism module.

Key words：embedded Web Server；process；CGI；security authentication