维普资讯 http://www.cqvip.com

基于OpenSSL的嵌入式网络安全通信设计与实现

章晓明,王则林,陆建德
(苏州大学 计算机学院 江苏省计算机信息处理技术重点实验室,江苏 苏州 215006)

摘 要:嵌入式网络安全设备的通信,如对设备的状态查询、配置等必须是安全的。文中探讨了嵌入式网络安全设备的远程安全通信设计。首先分析了OpenSSL的工作原理、数字证书在OpenSSL中的重要作用;然后给出了在嵌入式网络安全设备中进行远程安全通信的总体设计方案,并结合笔者一个实际的嵌入式网络安全设备的开发项目,详细介绍了其设计与实现过程。通过这种方法可以达到相对较高的安全通信要求。

关键词:OpenSSL;数字证书;嵌入式系统;安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-3751(2006)01-0217-04

Design and Implementation of Embedded Network Secure Communication Based on OpenSSL

ZHANG Xiao-ming, WANG Ze-lin, LU Jian-de
(Jiangsu Province Computer IT Key Lab., School of Computer Sci. & Tech., Suzhou Univ., Suzhou 215006, China)

Abstract: The communication of embedded network secure devices, such as status query and configuration of devices should be secure. Discusses the design of remote secure communication on embedded network devices. After analyzing the principles of OpenSSL and the key role of digital certification in OpenSSL, gives out a general design scheme of remote secure communication on embedded network devices. Combined with the authors' project developed on an actual embedded network secure device, has illustrated the overall design and implementation procedure in detail. The requirement of communication with high security can be met in such a way.

Key words: OpenSSL; digital certificate; embedded system; security

0 引 言

随着计算机应用的不断深入,许多嵌入式网络设备诸如网络远程监控设备、防火墙、安全网关等正被一批批开发出来。与桌面PC系统相比,嵌入式网络设备具有面向特定应用、资源有限等特性。不同的应用环境及目标决定着不同的系统平台,目前许多嵌入式设备都采用了Linux系统,针对特定的应用进行具体系统的设计;在资源使用方面,嵌入式网络设备一般体积小、设计精练、资源有限,往往要借助其它手段辅助控制。嵌入式网络设备的软、硬件必须合理选择和设计,辅助控制常常通过与嵌入式网络设备进行数据通信来实现。

一般,对嵌入式网络设备进行配置、控制等通信操作时,常常使用下述两种方法:

(1)通过串口。通过TELNET协议,使用终端登录到嵌入式网络设备。这种方法必须近距离配置,操作者必须熟悉嵌入式系统的配置、控制命令,如设置嵌入式网络设备的IP地址等初始化工作;

(2)通过网络。一般在嵌入式网络设备中集成设计一个内嵌的HTTP Server部件,给网络上近程、远程用户提供网页操作接口,用户可以使用浏览器登录嵌入式网络设备进行操作。如在防火墙、安全路由器等设备的配置时,可以将各种配置用表格的形式设计成网页让客户选择。这种方法方便灵活,不受限于距离,使用户更容易操作。

上述第二种方法具有明显的优势,使用这种方法必须解决两个问题:一是由于嵌入式网络设备的功能单一且资源有限,若采用Apache之类的通用HTTP服务器软件不但臃肿而且浪费,因此需要自行设计紧凑精练的专用HTTP服务模块;二是普通的HTTP交互是以明文的形式进行的,在网络上,尤其是远程操作时很容易被监听、截取或伪造,而有些通信,如对防火墙的配置,绝对不容许此种情况发生,除了采用用户密码,还必须提高数据通信的安全性,对整个通信过程进行加密保护,实现机密性、数据一致性与身份鉴别。

文中将结合笔者从事的一个实际的嵌入式防火墙设备开发项目,探讨嵌入式网络安全设备的远程安全通信设计,文章将讨论使用SSL与数字证书,给出在嵌入式网络

收稿日期:2005-04-14
基金项目:江苏省自然科学基金资助项目(BK2004039)
作者简介:章晓明(1981—),男,江苏常州人,硕士研究生,研究方向为计算机网络与网络安全、嵌入式Linux系统分析;陆建德,教授,研究方向为计算机网络与网络安全。

维普资讯 http://www.cqvip.com

安全设备中进行远程安全通信的总体设计方案，并详细介绍其设计与实现过程。

1 SSL 与 OpenSSL

安全套接层协议(SSL)由 Netscape 公司设计，其主要目的是提供安全可靠的网络传输，防止通信内容被偷听、篡改或伪造。SSL 在网络模型中的位置处于应用层与传输层之间，在 TCP 上运行，能提供保密性、数据一致性和身份鉴别。

SSL 通过在客户端、服务器端之间首先创建一个 TCP 连接，进行 SSL 握手，包括认证和会话密钥的协商，然后在此连接上面建立一条 SSL 通道，让所有的应用数据都通过该通道来发送接收，这些数据都使用握手阶段协商的会话密钥进行加密[1]。

X.509 数字证书在 SSL 握手交互与协商过程中起着重要作用，它在网络通信中标志服务方实体的身份。证书中含有服务方的公开密钥。SSL 连接分 SSL 握手和数据传输两个阶段。握手阶段通过用服务方数字证书中含有的公钥进行不对称加密来协商数据传输阶段的对称加密算法和会话密钥，还可以选择是否需要客户端提供客户方数字证书进行客户端的身份认证。握手完成后，所有应用层的数据就可以用会话密钥加密传输。

SSL 握手交互和加密算法的过程比较复杂，现在 SSL 已有各种开发套件，OpenSSL[2]是其中较为流行的版本。OpenSSL 采用 C 语言编写，实现了 SSL v2/v3 和 TLS v1[3]两种协议，并提供了一个通用加密库，包含有各种加密算法、摘要算法与密钥交换算法等，它封装了具体实现过程，程序员使用其提供的 API 能实现 SSL 通信。除此之外，OpenSSL 提供了 CA 等命令，用于生成各种 X.509 证书、密钥文件等，这些都为程序的编写、调试提供了方便。

2 基于 OpenSSL 的网络远程安全通信的总体设计

在嵌入式防火墙设备的设计中，由于防火墙设备属于高安全敏感设备，可以采用基于 OpenSSL 的网络远程安全配置与通信的设计方法。用 C 语言设计一个内嵌的 HTTP Server 部件[4]，并引入 OpenSSL 机构，客户端使用浏览器通过 SSL 访问该 HTTP Server 部件进行配置，与其进行安全数据通信，HTTP Server 部件使用 SSL 安全数据通道上得来的数据执行相应参数的配置。整个流程如图 1 所示。

HTTP Server 部件充当客户端与嵌入式防火墙设备之间通信的桥梁，它对客户提供 HTTP 服务，又根据客户在配置网页中的设置设定嵌入式防火墙设备的各种参数。根据嵌入式防火墙设备配置的特殊安全需要，调用 OpenSSL 的相关 API，使用 SSL 进行相关配置网页的交互。由于配置操作仅限于合法的防火墙管理人员，还需要使用 SSL 进行客户端认证。配置时首先双方建立 TCP 连接，服务器向客户返回登录页面。在用户提交登录信息时立即进行 SSL 握手，双方建立 SSL 连接，此后双方的数据，包括登录信息，都在 SSL 通道上进行传输。登录成功后用户可以进行配置。服务器端根据客户端送出的 HTTP 方法判断要进行的操作：如果是 GET 请求 + 相关配置网页，就返回请求的配置网页；如果是 POST 请求 + 提交的用户配置数据，则分析该数据，生成相应的配置脚本(防火墙配置使用 iptables 命令实现)并执行该脚本，修改防火墙配置。

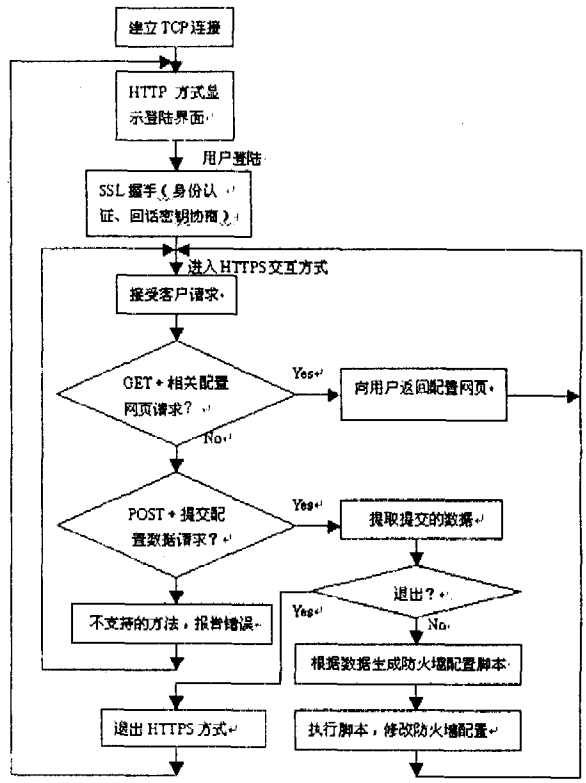

图 1 嵌入式防火墙设备安全远程配置过程流程图

考虑到在 SSL 握手过程中，不但客户端要验证服务器端的身份，同时由于只能让某些用户(如网管员)有访问的权限，还需要进行客户端的身份认证，只有通过认证的客户才能登录并配置防火墙。根据 SSL 协议，握手过程的流程设计如下[5]：

(1) 客户端发送的 ClientHello，其中包含了客户端推荐的加密参数、准备使用的加密算法和随机数。服务器返回的消息中，包含了选择的算法、服务器证书，以及要求客户端提供认证的 CertificateRequest 信息。

(2) 客户端提交证书，选择密钥。

(3) 为了防止中间人攻击，双方均向对方发送一条包含对整个连接过程的校验信息的消息，并各自检验对方发来的消息。

如果一切正确，那么握手完成，可以进行数据传输阶段，否则 SSL 交互终止并释放所有资源。数据传输完成后，客户端首先关闭连接。客户端先发送一条 close-ntify alter 消息以通知服务器端连接即将被关闭，随后立即发送 TCP FIN 消息。服务器端收到该消息后也返回 TCP FIN 消息。至此，整个 SSL 连接过程结束。

维普资讯 http://www.cqvip.com

3　SSL 握手、数据传输流程的具体实现

在系统中，设计的 SSL 消息交互如图 2 所示[5]。

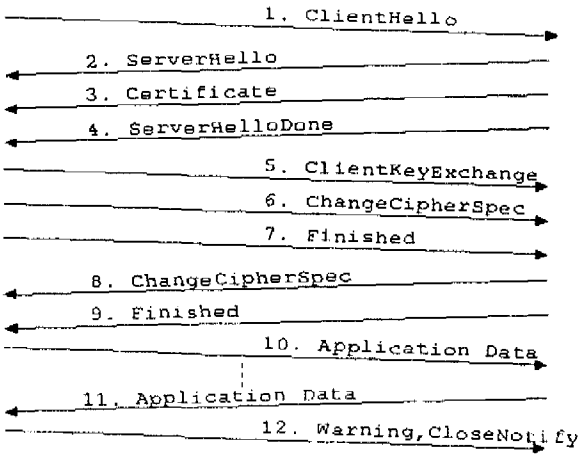

图 2　SSL 消息序列交互图

其中，步骤 1～9 是握手阶段，要完成 3 件事：协商加密算法；确定加密密钥；选择是否进行客户端认证。这 9 条消息的具体含义如下：

第 1 条消息为客户端发送的 ClientHello，其中包含了客户端推荐的加密参数、准备使用的加密算法和随机数。服务器以消息 2～4 作为响应，分别为选择的算法、服务器证书、ServerHelloDone 消息。

客户端经过验证后，发送消息 5～7。5 为 ClientKeyExchange，其中包含一个用服务器 RSA 密钥加密的密钥；6 为 ChangeCipherSpec，用于指示客户端从此以后的消息都用前面商定的密钥加密；7 和后面的 9 的 finished 是必要的，因为在此之前服务器和客户端之间的握手过程都是明文传输的，只有相互之间都进行 ChangeCiperSpec 握手过程之后进行的通信才是密文传输，为了防止中间人攻击，就必须保证整个握手过程都是来自合法的客户端和服务器端，第 7，9 步就是对整个握手过程的所有信息进行认证。

服务器收到客户端的 finish 消息就发送自己的 ChangeCiperSpec(8)和 finished(9)。至此，握手阶段成功结束，连接准备就绪。

步骤 10 和 11 就是数据的发送和接收阶段。数据传输完成后，客户端发送 close-notify(12)，通知对方连接即将关闭，并且不再发送数据。随后双方关闭连接，一次连接结束。

注意上面的 SSL 连接未使用客户端认证。如果需要的话，在第 2 步后服务器要发送 CertificateRequest 消息，而客户端随后要提交其证书，并发送 CertificateVerify 消息，在通过服务器认证后，交互才能继续。

系统中为实现 SSL 处理过程的各模块设计如图 3 所示。

在图 3 中，程序根据接收到的 HTTPS 连接请求判断是否为会话重用，如果是，则省去握手过程(这主要是为了节省开销，提高性能)，否则就进入握手模块。握手包括初始化、接受连接和身份验证 3 部分。图中的密钥组控制模块是服务器端出于效率和安全的考虑，可以让客户端修改所用的密钥组。数据传输模块用于双方的数据传输。这里任何一步出错都将导致 SSL 交互停止并释放所有资源。下面详细介绍 SSL 初始化、接受连接和数据传输 3 部分，而身份验证也在接受连接部分完成。

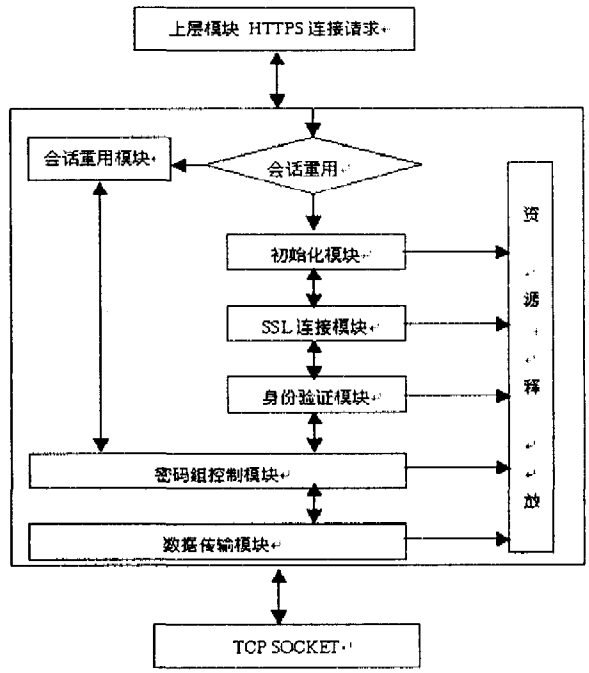

图 3　OpenSSL 设计中各模块关系图

1)SSL 上下文初始化。

在 SSL 初始化前，要进行一些附加工作：

```
SSL_library_init(); /* 在创建 SSL 上下文前，必须用该函数初始化 OpenSSL 函数库本身 */
SSL_load_error_string(); /* 出错时可以显示提示字符串而不是错误码，对调试十分有帮助 */
```

接着创建 SSL 上下文：

```
SSL_METHOD *meth = SSLv23_method(); /*需要支持的 SSL 协议*/
SSL_CTX *ctx = SSL_CTX_new(meth); /*根据上面的结构创建 SSL 上下文*/
```

SSL_METHOD 结构中包含了具体实现协议版本的方法。如果编写的服务器要能够与各种 SSL 版本的客户端兼容，那么必须用 SSLv23_method 函数创建。

在上面提到，该服务器需要提供客户端认证，所以必须加入请求客户端认证的内容：

```
SSL_CTX_set_verify(ctx, SSL_VERIFY_PEER
| SSL_VERIFY_FAIL_IF_NO_PEER_CERT, NULL);
```

其中标志位 SSL_VERIFY_PEER 表示需要进行客户端认证，SSL_VERIFY_FAIF_IF_NO_PEER_CERT 表示如果客户端不提交证书，连接立即终止。

此外，在初始化阶段还需要要完成的任务有：指定使用的根证书文件、密码文件随机数文件等等，这些信息都

维普资讯 http://www.cqvip.com

保存在 SSL 上下文 ctx 中。

2)接受连接请求。

一旦收到客户端发出的连接请求,服务器就创建 SSL 对象来对应一条 SSL 连接。这里要注意的是,SSL 对象并不直接附加在套接字上[6],在两者的中间有一个 BIO 对象,SSL 对象附加到 BIO 上,再由 BIO 与套接字即底层 I/O 设备通信。这样做的好处是:通过中间层 BIO 对象,这样各种底层设备,比如内存缓冲区、串口等都可以实现 SSL,而不局限于套接字[5]。具体实现方法如下:

```
BIO *sbio = BIO_new_socket(s, BIO_NOCLOSE); /*创建 BIO 对象*/
SSL *ssl = SSL_new(ctx); /*创建 SSL 对象*/
SSL_set_bio(ssl, sbio, sbio); /*连接两个对象*/
SSL_accept(ssl); /*接受客户端连接请求*/
```

由于上面设定了要求客户端认证,所以在这一部分会完成双方的互相认证。如果双方认证成功,SSL_accept 返回 1,SSL 连接成功建立,可以开始进行数据传输。

3)数据传输。

数据的传输交互时,发送数据用 SSL_read 函数,接收数据用 SSL_write,与系统调用 read,write 不同的只是其第一个参数为 SSL 对象。由于之后的加密解密过程被 OpenSSL 封装,调用这些发送和接收的数据以明文形式表示。不过,需要注意的是,SSL_read 以及 SSL_write 和 TCP 读和写有些不同,前者每次读或写都是记录片段长的倍数,而后者却没有此限制。

最后,数据传输完成后要终止连接,释放资源,过程在上一节已有说明。

4 总 结

文中对基于 OpenSSL 实际嵌入式设备的安全通信进行了讨论,使用文中方法,可适用于多种基于嵌入式 Linux 的嵌入式设备需要安全通信的场合。需要指出的是,使用 SSL 有两点必须注意:一是由于握手和数据加密解密都需要额外的开销,所以 SSL 的响应速度相对来说要慢一些;二是 SSL 的安全性取决于算法的性能、密钥的长度和随机数的强度,因此,如果要获得较高的安全性,那么 RSA 或 DH 密钥至少要取 768 位或更高,在 OpenSSL 通信中加强安全强度也是需重点关注的,可以用引入新的加密算法来加以解决。

参考文献:

[1] SSL 3.0 Specification[EB/OL]. http://www.netscape.com/eng/ssl3/index.html,1996-09.

[2] OpenSSL 官方网站[EB/OL]. http://www.openssl.org, 2004-2005.

[3] Dierks T, Allen C. The TLS Protocol Version 1.0[S]. IETF RFC2246, 1999.

[4] Matthew N, Stone P. Linux 程序设计(第 2 版)[M]. 杨晓云等译. 北京:机械工业出版社,2002.

[5] Rescorla E. SSL 与 TLS Designing and Building Secure Systems [M]. 崔 凯 译. 北京:中国电力出版社,2002.

[6] Gay W W. 实战 Linux Socket 编程[M]. 詹俊鹃,于 卫 译. 西安:西安电子科技大学出版社,2002.

(上接第 206 页)

者主要采用数据库动态生成用户目录树技术来实现员工的不同需求。将树形目录的节点存入数据库,为动态形成树形目录打下良好的基础。当然,也有些目录树是表现一个数据库中的数据结构(父节点是数据库名,子节点是数据表)。

```
<iframe name="nav" width=100% height=100%
src="/netsys/sysmenu/SysMenuTree? Action=Nav"
frameborder=0 NORESIZE scrolling="auto" marginheight=0 marginwidth=0></iframe>
```

其中 SysMenuTree 为采用函数递归算法实现动态目录树的 Servlet 程序。

(4)容错处理。

在实际的系统应用中,由于开发时没有考虑到或是考虑欠妥当而造成的错误是可能发生的。为降低错误所造成的影响,可以使用 JSP 的防错技术:

```
<%@ page contentType="text/html; charset=gb2312" language="java"
import="java.sql.*" errorPage="error.jsp"%>
```

其中可以在 errorPage 中设置容错页面。一旦 Web 服务器出现错误时,可以自动转向 errorPage 所指定的页面。

3 结束语

JSP 技术很好地实现了 OA 系统的功能要求,而且性能优良、运行稳定,对比其他实现技术,优势比较显著。OA 系统很好地替代和减轻了日常工作,满足了公司定制 OA 系统的初衷。该动态集成系统还具有良好的可拓展性,以此为基础,结合公司需求,可进一步完善或扩展已有的 OA 系统。OA 系统为进一步吸收国外先进管理技术提供了平台和基础。

参考文献:

[1] 齐鲲鹏. 用 JSP 技术开发基于 WEB 的房地产网络管理信息系统[D]. 大连:大连理工大学,2003.

[2] 吴其庆. JSP 网站设计经典教程[M]. 北京:冶金工业出版社,2002.

[3] 飞思科技. JSP 应用开发详解[M]. 北京:电子工业出版社,2002.

[4] 陈国华. JSP 技术及其在安全管理信息系统中的应用[J]. 中国安全科学学报,2003,13(1):45-48.

[5] Kamdaf T, Joshi A. On Creating Adaptive Web servers Using Web Log Mining[EB/OL]. Http://citeseer.nj.nec.com/Kamdarocreating.html,2002.