doi: 10.7690/bgzdh.2023.03.004

基于博通平台的家庭网关配置文件分段加密方法

程　慧
（四川九州电子科技股份有限公司企业技术中心，四川 绵阳 621000）

摘要：针对家庭网关信息泄露的问题，提出一种基于博通平台的家庭网关配置文件分段使用 Base64 加密方法。通过分段 Base64 加密和解密，设计硬件和软件方案并加以实现。结果表明：该方法可靠性高，可提高网关系统的安全性。

关键词：家庭网关；配置文件；分段加密
中图分类号：TP393.084　　**文献标志码**：A

Sectional Encryption Method of Home Gateway Configuration File Based on Broadcom Platform

Cheng Hui
(*Enterprise Technology Center*, *Sichuan Jiuzhou Electronic Technology Co*., *Ltd*., *Mianyang* 621000, *China*)

Abstract: Aiming at the problem of home gateway information leakage, this paper proposes a Base64 encryption method for home gateway configuration file segmentation based on Broadcom platform. Through segmental Base64 encryption and decryption, the hardware and software solutions are designed and implemented. The results show that the method has high reliability and can improve the security of the gateway system.

Keywords: home gateway; configuration file; sectional encryption

0　引言

随着家庭网关设备快速发展，网络设备也越来越多，家庭网关设备的信息安全也变得越来越重要。针对目前家庭网关配置文件导出时会导致的信息泄露，笔者提出一种文件分段加密，每一段再使用 Base64 加密的设计方法及实现方案。

1　博通平台家庭网关

博通平台家庭网关是我司开发的一款基于博通 BCM63167 芯片平台的 VDSL2 高速家庭网关[1]。采用双绞线接入，提供有线 LAN 和无线 WIFI 上网方式，带 USB 和语音功能。提供 IPV4 和 IPV6 上网方式。在上行和下行方向分别有防火墙或 ACL 规则控制网络的安全。在网关中有一个基础配置文件，存储和记录了产品各个功能的数据以及用户使用中保存的各种信息，包括用户名、密码等基本登陆信息[2-6]。该配置文件可以通过在 LAN 侧或 WAN 侧登陆 WEB 页面来导出。一旦数据被网络攻击者获取，将导致用户上网数据泄露，造成严重的安全问题。为阻止该行为导致的信息泄露，笔者采用一种加密方法来保证配置文件不被窃取。

2　分段 Base64 加密和解密

Base64 是一种将二进制流表示为 64 个字符的编码方式。Base64 能够将任何数据转换为易移植的字符串，避免了传输过程中失真问题。最初，Base64 是为了解决电子邮件中无法直接使用非 ASCII 字符的问题，一段数据先经过 Base64 编码为 ASCII 字符串后，可以在接收端通过 Base64 解码还原。通常都将 Base64 编码作为数据加密后的传输/存储格式，如将一段明文数据通过 MD5、SHA 等手段加密后，经过 Base64 编码为字符串，即可很方便地进行传输和存储。正因为 Base64 容易被还原，所以用 Base64 加密并不安全；因此，笔者进行了设计改进，将配置文件分成不同的大小段，将各个段采用 Base64 编码，并在各个段之间加上特殊的符号分隔，然后按顺序将各段加分隔符生成新的文件，这样即使导出文件，也无法将整个文件解密。同理，在导入文件时，网关按照对应的方法解密[7]。

3　硬件实现方案

主芯片采用博通公司的 BCM63167 处理器，该处理器是一款高性能、单芯片多媒体多业务

收稿日期：2022-11-17；**修回日期**：2022-12-24
作者简介：程　慧（1984—），女，湖北人，工程师，从事 XPON ONU 和路由器产品开发研究。E-mail: Chenghui@jiuzhoutech.com。

ADSL2+/VDSL2 gateway，能够实现一种低成本的多模式 ADSL2+VDSL2 路由器或网关，支持有线小分组路由与多端口以太网交换并发。该设备的处理器是一个 400 MHz 双核心 MIPS32、独立 64 KB4 路缓存和一个共享的 32 KB D-cache。支持有效处理路由器应用和并发数据+语音应用的 voice-over ip 处理。BCM63167 包含专门的硬件引擎，用于执行行速率分组分类，分组修改硬件路由和 fonwards。

BCM63167 集成多模式 ADSL2 VDSL2 收发器和模拟前端(analog front end，AFE)支持符合所有 TU 和 ANSI VDSL2 和 ADSL2+规范的全速率连接。额外支持 PCIe2，串口接口(serial port interface，SPI)，NANG flash。

硬件系统如图 1 所示。

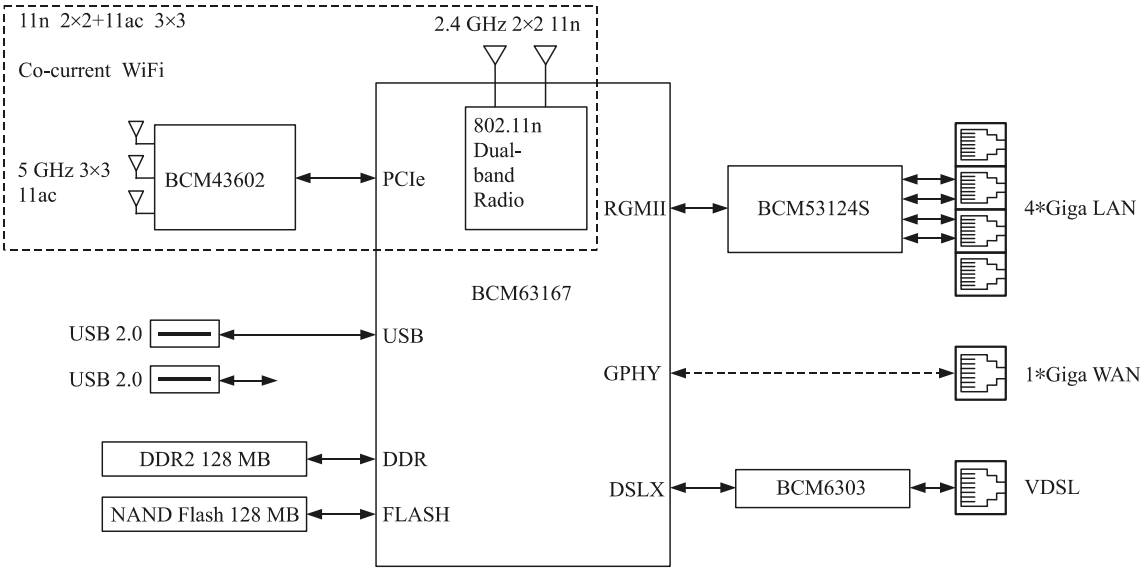

图 1　硬件系统

4　软件实现方案

4.1　软件实现流程

软件实现的流程如图 2 所示。

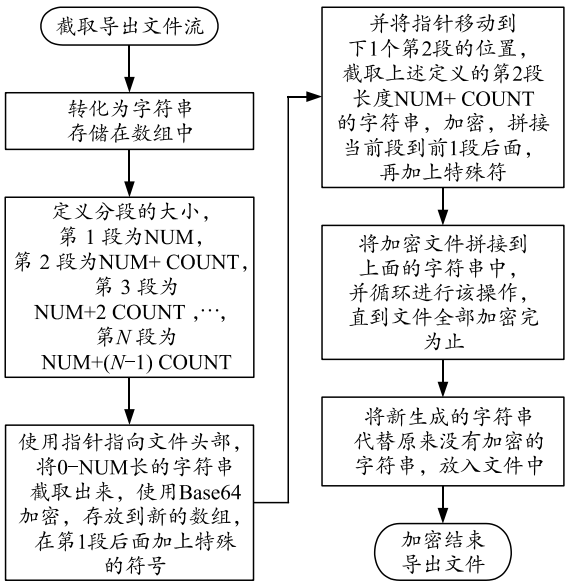

图 2　加解密流程

4.2　网关配置文件字符串流导出配置文件加密

网关配置文件字符串流导出配置文件加密流程如下：

1) 首先要截取导出的文件流，找到文件开始和结束位置；

2) 将截取的文件流内容读出到字符串，并计算文件大小；

3) 定义分段的大小，第 1 段设置为 NUM(自定义的常量)，第 2 段设置为 NUM+COUNT(常量)，……，第 N 段设置为 NUM+(N-1)COUNT；

4) 使用指针指向文件内容字符串头部，将 0-NUM 长的字符串截取出来，使用 BCM 系统 SDK 支持的 cmsB64_encode 加密，存放到新的数组。在第 1 段后面加上特殊的符号；

5) 将加密文件拼接到上面的字符串中，并循环进行该操作，直到文件全部加密完为止；

6) 将新生成的字符串代替原来没有加密的字符串，放入文件中；

7) 加密结束，导出文件。使用工具打开加密文件，文件无法查看。

4.3　网关配置文件字符串流导入配置文件解密

网关配置文件字符串流导入配置文件解密流程如下：

(下转第 43 页)