面向嵌入式系统的威胁建模与风险评估 *

徐 超[1,2a], 何炎祥[2a,2b], 陈 勇[2a], 吴 伟[2a], 刘健博[2a], 苏 雯[2a]
(1. 徐州工业职业技术学院, 江苏 徐州 221000; 2. 武汉大学 a. 计算机学院 b. 软件工程国家重点实验室, 武汉 430072)

摘 要: 为提高嵌入式系统可靠性,开发安全可信的系统,需要在软件开发设计阶段尽早考虑安全问题。提出一种面向嵌入式系统的威胁建模方法,该方法分析了嵌入式系统可能存在的威胁漏洞,以威胁树的形式建立了嵌入式系统威胁模型;根据该模型,以量化的方式从下到上迭代地计算各个节点的威胁值,然后根据各个节点的威胁值对嵌入式系统进行风险评估。为更好地说明威胁模型及其各节点威胁值的计算方法,以智能电表中用户电表账单信息受到的威胁为例,说明了整个建模和量化过程。通过具体实例验证了该方法的实用性和有效性。

关键词: 嵌入式系统; 威胁建模; 风险评估; 威胁树; 智能电表
中图分类号: TP309.1 **文献标志码**: A **文章编号**: 1001-3695(2012)03-0826-03
doi:10.3969/j.issn.1001-3695.2012.03.006

Embedded system oriented threat modeling and risk evaluation

XU Chao[1,2a], HE Yan-xiang[2a,2b], CHEN Yong[2a], WU Wei[2a], LU Jian-bo[2a], SU Wen[2a]
(1. *Xuzhou College of Industrial Technology*, *Xuzhou Jiangsu* 221000, *China*; 2. *a. School of Computer*, *b. State Key Laboratory of Software Engineering*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: In order to improve the safe and reliable embedded system, software development design phase needs to consider security as soon as possible. Therefore, this paper presented a threat model for embedded system that analyzed the possible threats in embedded system. For evaluating the scale of thread, the method established the threat model in the form of trees and calculated the thread value of tree's nodes from bottom to top. It used the thread of meter billing information in smart meters as an example to illustrate the process of building the threat model and calculating the thread value of each node that verifying the practicability and effectiveness of this method.

Key words: embedded system; threat modeling; risk assessment; threat tree; smart meters

0 引言

随着嵌入式系统的广泛应用,嵌入式系统遭到越来越多的威胁,如硬件系统被物理攻击或破坏、软件系统中程序代码、数据被窜改、用户隐私被泄露等问题,已给各个国家以及众多企业造成巨大的经济损失,甚至危害到国家和地区的安全。因此,对嵌入式系统进行主动的分析、评估风险等级,就能帮助设计师尽早识别嵌入式系统面临的威胁,提前评估其安全态势,设计相应的缓和方案,增强软件系统的安全性。所以,在嵌入式系统设计阶段,针对嵌入式系统的威胁进行威胁建模,是保证嵌入式系统具有可信性的重要研究方向。

针对软件系统的威胁建模,国内外已经做了大量的研究工作。Howard 等人[1]提出了一种面向过程的威胁建模方法,采用扩展活动图和统一威胁模型作为基础,利用威胁树进行威胁模型的建立, 用 DREAD 方法评估威胁风险等级;Li 等人[2]提出了一种统一威胁模型,在设计阶段对软件可能存在的威胁进行分析与评估;CORAS 设计一个面向对象建模的风险评估框架,采用 UML 建模技术,提出了一种基于模型的软件安全风险评估方法[3]。WASC (Web Application Security Consortium) 针对 Web 应用进行了风险评估,同时对威胁类型进行了专业分类[4]; Stijn[5]同样针对 Web 应用进行了威胁建模,通过威胁树描述了可能面临的威胁;Sheynar 等人[6]提出一种自动化生成和分析攻击图的技术,使用模式检查来计算网络中多阶段、多主机的攻击路径。Wang 等人[7]提出了一种威胁模型驱动的安全测试方法,用于发现运行时的威胁行为。但这些研究仅针对面向过程、Web 应用等方面进行了威胁模型的构建,为威胁建模奠定了较好的理论基础,但它们较少从嵌入式系统的角度来建立威胁模型,嵌入式系统以其独有的特性,与之相关的攻击成本、技术复杂度、风险评估等因素进行威胁建模,是一个复杂的过程。

本文将在以上研究成果的基础上,针对嵌入式系统的威胁,提出一种基于嵌入式系统威胁的建模方法,以量化的方法对嵌入式系统威胁进行风险评估。

1 威胁建模方法

威胁建模是一项软件工程技术,能够定位系统的威胁、攻击、漏洞和对策。对可能影响系统的安全风险进行系统的识别和评估。以适当的对策对威胁进行处理,从而降低威胁的影

收稿日期: 2011-08-22; **修回日期**: 2011-10-10 **基金项目**: 国家自然科学基金可信软件重大研究计划资助项目(90818018,91018009)
作者简介:徐超(1980-),男,湖北红安人,讲师,博士研究生,主要研究方向为可信软件、嵌入式系统等(xuch@whu.edu.cn);何炎祥(1952-),男,湖北应城人,教授, 博导,主要研究方向为可信软件、可信编译等.

响[8]。威胁建模的核心目标为:确定系统可能存在的威胁(查找);如何评估系统威胁风险等级(定量);如何缓和系统威胁方案(对策)。

1.1　威胁建模过程

威胁建模方法包括六个步骤:识别资产;创建体系结构概图;分解应用程序;识别威胁;将威胁文档化;评估威胁,并给出风险评估等级,最后根据威胁评估结果制定缓和方案并确定其优先级,应用缓和方案改进应用程序设计,缓和威胁,增强安全性[9,10]。在面向嵌入式系统威胁建模的过程中,首先确定机密信息(资产),然后创建体系结构概图,定义嵌入式系统的目的与实现方法,绘制体系架构图;分解应用程序,使用数据流图(DFD)将嵌入式系统分解为子系统[11],而子系统可以分解为更低级的子系统;同时,用威胁树进行识别威胁,最后进行威胁风险评估以及缓和方案的设计。具体建模过程可参见文献[1]。

威胁树是将嵌入式系统所面临的所有威胁以树状的形式描述出来,是一种图形化的模型。构建威胁树主要包含以下几个方面:构建威胁树;标示威胁代理;利用威胁指标函数评估;消除威胁(修建树)。

1.2　嵌入式系统威胁

嵌入式系统的威胁主要由硬件威胁和软件威胁组成。在硬件威胁中可分为主动物理攻击和被动攻击,主动物理攻击包括逆向工程和探针探测[12]。被动攻击包括:a)能量分析攻击,硬件电路的能量消耗是由于电路中的转换活动引起的,转换与数据密切相关,可以根据能量消耗情况推测密钥;b)电磁分析,通过测量一个嵌入式设备的电磁辐射来获得机密信息;c)时序分析,通过观察密码计算的执行时间推断密钥;d)错误注入攻击,利用系统外部参数和环境条件,使嵌入式系统的部件产生错误[13,14]。

软件威胁可分为 OS 攻击和通信网络攻击。OS 攻击包括系统接口安全和病毒漏洞两大类;通信网络攻击是嵌入式系统中最常见的威胁之一,主要包括用户隐私问题、网络监听窃取、克隆伪造数据、干扰阻塞通信、拒绝服务等[15,16]。其中用户隐私已经成为嵌入式系统安全主要防御的重点。根据以上分析,可以建立如图 1 所示的嵌入式系统威胁模型。

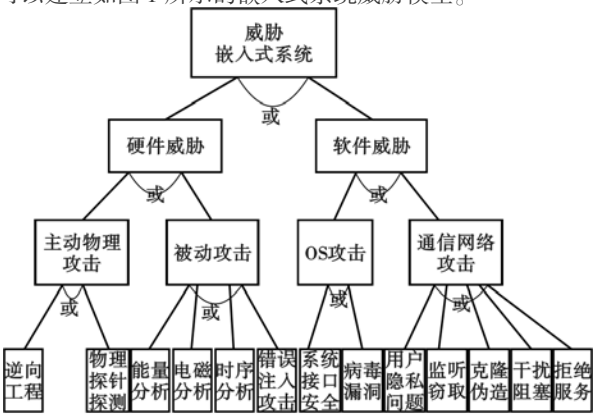

图1　嵌入式系统威胁模型

为了量化地评估以上威胁模型,将该模型表示为有向树 $T=\{V,E,T,c,l,f,h,g\}$,其中:

a) $V=V_e\cup V_m$ 表示树中节点的集合,V_e 表示树的叶子节点,V_m 表示树中的非叶子节点。

b) $E=E_u\cup E_n$ 表示树中有向边的集合,E_u 表示或边,E_n 表示与边。

$T=\{s,m,n\}$ 表示威胁类型,s 表示威胁类型为软件类型,m 表示威胁类型为硬件类型,n 表示威胁类型为综合威胁。

$c:V\to 2^V$ 用于表示节点 $v\in V$ 的所有孩子节点构成的集合。

c) $l:V\to 2^v\to R$ 用于表示边。

$e(i,j)\in E$ 的权值,当 $e\in E_u$ 时,j 表示为单点集;当 $e\in E_n$ 时,j 表示为多点集。

d) $f:V\to T$ 用于计算节点 $v\in V$ 的威胁类型,即表示该节点是硬件威胁、软件威胁还是综合威胁。当该节点是威胁树的叶子节点时,则根据具体的节点类型确定其值;如果该节点是树的内部节点,则其节点类型为综合节点。其公式表示如下:

$$f(v)=\begin{cases} n & v\in V_m \\ x & x\in\{s,m\},v\in V_e \end{cases} \tag{1}$$

e) $h:T\to R$ 用于评估该类威胁的威胁因子,当该节点是硬件类型或软件类型的威胁时,其值为一个常量,表示该类型威胁的大小;当该节点是综合节点类型时,其值即为其所有孩子节点值中的最大值。当其计算公式为

$$h(f(v))=\begin{cases} \alpha & f(v)=s \\ \beta & f(v)=m \\ \max(h(f(k)),k\in c(v) & f(v)=n \end{cases} \tag{2}$$

f) $g:V\to R$ 用于评估节点 $v\in V$ 所受的威胁,其值越大,说明该种威胁也越大,具体可采用如下公式进行计算:

$$g(v)=\begin{cases} h(f(v)) & v\text{ 是叶子节点} \\ \sum\limits_{(v,j)\in E_u} l(v,j)\times(h(f(j))+g(j))+ & \\ \sum\limits_{(v,j)\in E_n\,x\in j}\prod l(v,x)\times(h(f(x))+g(x)) & v\text{ 不是叶子节点} \end{cases} \tag{3}$$

2　实例

本文所采用的威胁建模和风险评估可采用如图 2 所示的框架进行。本章将以智能电表为例,说明具体的建模和风险评估过程。

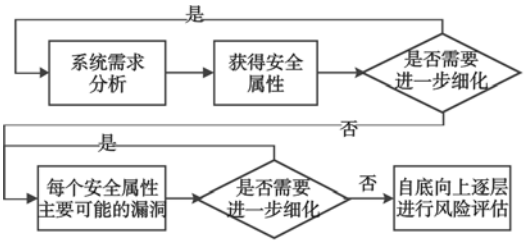

图2　威胁建模与风险评估方法架构

2.1　智能电表系统

智能电表系统是一种高精度、长寿命、低功耗的新型智能电表,可以实现数据的采集、存储和传输功能,并根据所接收的命令控制继电器操作实现供电或恢复供电;同时,含有功能强大的微控制器(MCU),在自动化和智能化方面的功能十分强大。

智能电表系统属于由智能电表管理系统和电能表构成的主从式结构。管理系统对采集的数据进行统计、分类、计费、远程控制,电能表利用 MCU 对脉冲计数来计算所消耗的电量。对用电量数据进行采集和用户负载进行监控,RFID 无线射频卡是两者之间进行信息交换的载体。智能电表的架构如图 3

所示。

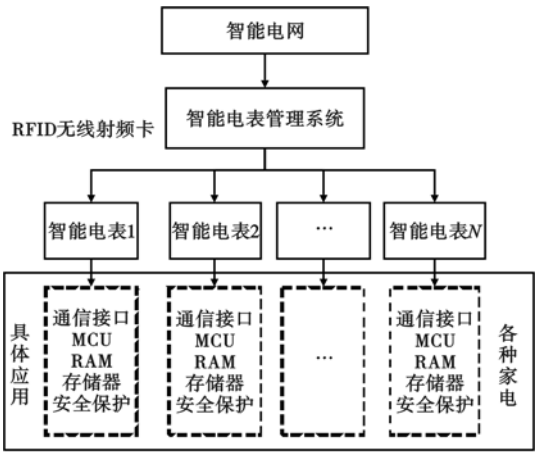

图3　智能电表的架构

2.2　智能电表威胁模型

为说明嵌入式威胁模型具体使用方法以及具体评估方法，本文将针对智能电表中用户隐私问题进行深入分析，建立相应的细化模型以及具体的评估值。

智能电表是作为一种典型的嵌入式设备，其威胁模型离不开图 1 所示的嵌入式威胁模型，其模型的上层结构同图 1 所示（在图 3 中未给出），只是对于具体的用户隐私问题，由于其又受到多个部分因素的影响，故如要评估该威胁，需要进一步分析该威胁的构成因素，细化该威胁模型（图 4）。用户隐私包含用户信息泄露、用户电表账单窜改、数据库攻击等。在智能电表系统中，用户电表账单信息是机密数据（资产），在企业和用户之间是绝对保密的，但智能电表系统整个信息交互是基于无线通信网络，无线传输的信号本身是开放的，缺乏足够的安全控制措施保护用户隐私信息，这就给攻击者的侦听带来方便。这一威胁是由应用程序中控制流设计的安全漏洞所导致。攻击者获取用户账单这一威胁目标分解为通过获取 RFID 芯片或通过网络通信获取两个子目标。通过获取 RFID 芯片进一步分解为逆向工程或物理探针探测；通过网络通信获取又可以分解为无线通信不受保护与攻击者获取通信数据。获取通信数据进一步分解为网络协议分析工具或监听无线路由器数据或破坏交换机。监听无线路由器还可分解为路由器不受保护与破坏路由器或猜测路由器，破坏交换机还可分解为各种交换机攻击。猜测路由器进一步分解为暴力破解攻击或字典攻击。暴力破解攻击分解为暴力破解用户名与暴力破解用户密码，字典攻击分解为字典攻击获取用户名与字典攻击获取用户密码。直至整个攻击结束，以获取用户电表账单为止。根据上述分析构建攻击者获取用户电报账单信息的统一威胁模型。

为简化计算，对图 4 所示的用户电表账单威胁模型，假设每条边的权值为 1，$\alpha=0.4$，$\beta=0.6$（假设的权值是为了计算威胁值的简单化，真实的权值是根据系统实际受攻击的情况，以及威胁漏洞造成的实际损失大小综合确定），根据式（1）~（3），计算出该威胁中模型各节点的威胁值，如图 5 所示（图中采用节点编号表示各个节点）。从图 5 可以看出，该用户电表账单信息获得的威胁值为 8.64。因此，通过该威胁建立威胁模型，可以很快计算出各种威胁的威胁值，从而评估出各种威胁的威胁程度，即威胁值越高，该种威胁也就越大。

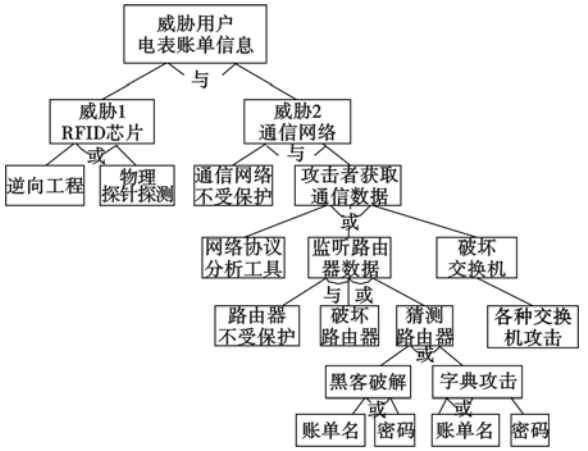

图4　用户电表账单威胁模型

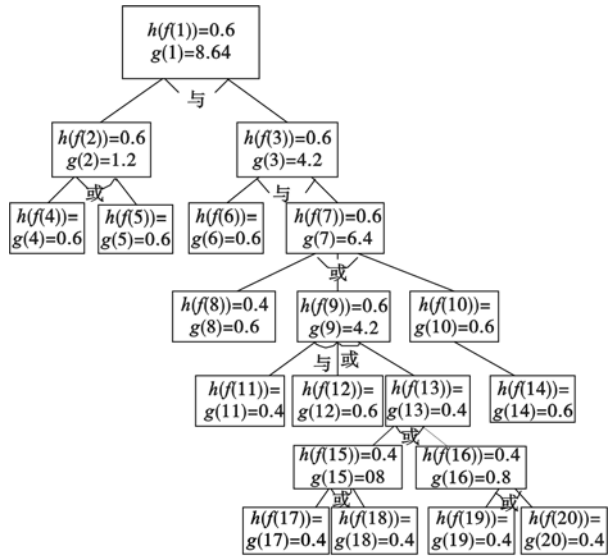

图5　用户电表账单威胁值

3　结束语

本文提出了一种面向嵌入式系统的威胁建模方法以增强软件的可信性，设计并实现了一个实例验证了该方法的实用性和有效性。相对于文献[1,14]中的威胁模型，该模型是针对于嵌入式系统的一个总体威胁的上层框架，里面主要体现了嵌入式系统中存在的共性问题，而对于具体的某类问题进行危险建模，需要根据具体的应用环境和使用过程进一步细化，以求获得更精确的威胁评估值。本文主要贡献在于：a）针对嵌入式系统的特点，以威胁树的形式建立了嵌入式系统威胁模型的上层结构，较好地揭示了嵌入式系统面临的威胁隐患；b）根据该模型，通过迭代的方式从下到上逐层求解各个节点的威胁值，从而获得整个系统的威胁评估值，达到了定量评估嵌入式系统威胁的目的，为系统开发者分析和解决系统漏洞提供了依据。

参考文献：

[1] HOWARD M, LeBLANC D. Writing secure code [M]. Redmond, Washington: Microsoft Press, 2005.

[2] LI Xiao-hong, HE Ke. A unified threat model for assessing threat in Web applications[C]//Proc of the 2nd International Conference on Information Security and Assurance. Washington DC: IEEE Computer Society, 2008: 142-145.

（下转第 846 页）

将本文算法应用到 Dolphins Social Network 中,同样设定阈值 β=0.5,θ=0.8,得到的社区结构如图 6 所示。其中形状为三角形的节点 PL、TSN83 和 Beak 为重叠社区的公共节点。

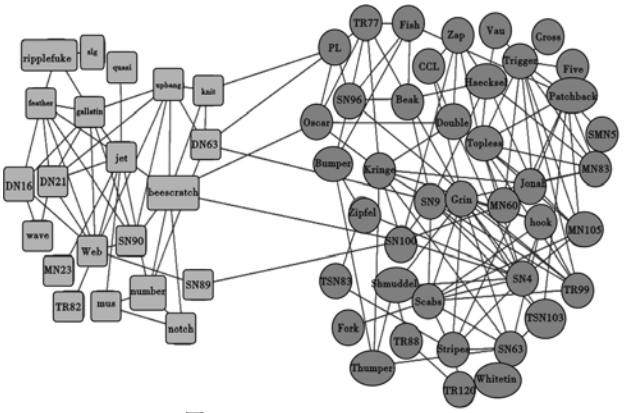

图5　Dolphins Social Network

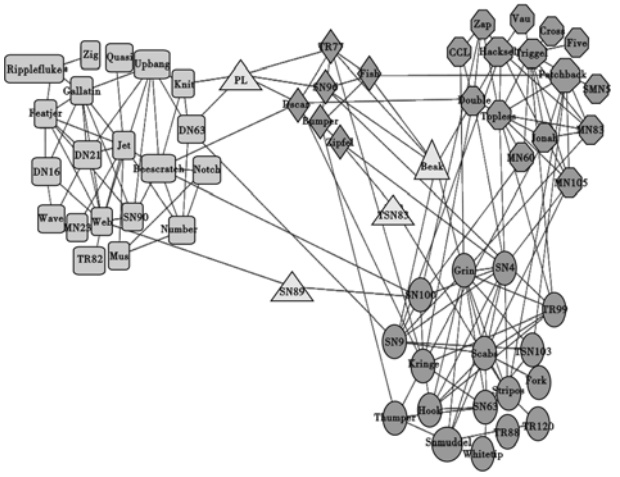

图6　本文算法所划分的四个社区

3　结束语

本文定义了节点的中心度和节点对社区的适应度,提出了一种新的重叠社区发现算法,并将该算法应用到数据集 Zachary's Karate Club Network 和 Dolphins Social Network 中。实验表明,该算法可以有效地发现网络中的重叠社区。未来的工作将致力于提高算法的效率和精确度。

参考文献:

[1] 汪小帆, 李翔, 陈关荣. 复杂网络理论及应用[M]. 北京:清华大学出版社,2006:162-188.

[2] GIRVAN M, NEWMAN M E J. Community structure in social and biological networks[J]. Proceedings of the National Academy of Sciences,2002,99(12): 7821-7826.

[3] NEWMAN M E J, GIRVAN M. Finding and evaluating community structure in networks [J]. Physical Review E, 2004, 69 (2): 026113.

[4] CLAUSET A. Finding local community structure in networks[J]. Physical Review E, 2005,72(2):026132.

[5] CLAUSET A, NEWMAN M E J, MOORE C. Finding community structure in very large networks[J]. Physical Review E,2004,70(6):066111.

[6] NEWMAN M E J. Fast algorithm for detecting community structure in networks[J]. Physical Review E,2004,69(6):066133.

[7] LANCICHINETTI A, FORTUNATO S, KERTESZ J. Detecting the overlapping andhierarchical community structure in complex networks [J]. New Journal of Physics,2009,11:033015.

[8] CHEN Duan-bing, SHANG Ming-sheng, LV Ze-hua, *et al*. Detecting overlapping communities of weighted networks via a local algorithm [J]. Physica A,2010,389(19):4177-4187.

[9] PALLA G, DERENYI I, FARKAS I, *et al*. Uncovering the overlapping community structure of complex networks in nature and society [J]. Nature, 2005,435(7043):814-818.

[10] SHANG Ming-sheng, CHEN Duan-bing, ZHOU Tao. Detecting overlapping communities based on community cores in complex networks [J]. Chinese Physics Letters, 2010,27(5):058901.

(上接第 828 页)

[3] GRAN B A, FREDRIKSEN R, THUNEM A P J. Addressing dependability by applying an approach for model-based risk assessment[J]. Reliability Engineering & System Safety, 2007, 92 (11): 1492-1502.

[4] LAKHINA A, CROVELLA M, DIOT C. Characterization of network wide anomalies in traffic flows, BUCS220042020 [R]. Boston: Boston University, 2004.

[5] STIJN V C. Threat modeling for Web application using the STRIDE model [D]. London: University of London, 2004.

[6] SHEYNAR O, HAINES J, JHA S, *et al*. Automated generation and analysis of attack graphs [C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2002: 273-284.

[7] WANG Lin-zhang, WONG W, XU Dian-xiang. A threat model driven approach for security testing[C]//Proc of the 3rd International Workshop on Software Engineering for Secure Systems. Washington DC: IEEE Computer Society, 2007: 204-213.

[8] DEWRI R, POOLSAPPASIT N, RAY I, *et al*. Optimal security hardening using multi-objective optimization on attack tree models of networks[C]//Proc of the 14th ACM Conference on Computer and Communications Security. 2007: 204-213.

[9] WYSOPAL C, NELSON L, ZOVI D D, *et al*. The art of software security testing: identifying software security flaws[M]. Boston: Addison-Wesley Professional, 2006.

[10] 王红兵. Web 应用威胁建模与定量评估[J]. 清华大学学报, 2009, 49(2): 2108-2112.

[11] 张红斌, 裴庆祺, 马建峰. 内部威胁云模型感知算法[J]. 计算机学报, 2009, 32(4): 784-793.

[12] 陈小峰. 可信平台模块的形式化分析与测试[J]. 计算机学报, 2009, 32(4): 646-653.

[13] 李梁, 黄新劳, 赵霖. 威胁树模型在风险评估中的应用[J]. 计算机应用, 2003, 23(z2): 188-191.

[14] 何可, 李晓红, 冯志勇. 面向对象的威胁建模方法[J]. 计算机工程, 2011, 37(4): 21-26.

[15] 王伟, 李春平, 李建彬. 信息系统风险评估方法的研究[J]. 计算机工程与设计, 2007, 28(14): 3473-3475.

[16] 郭春霞, 裘雪红. 嵌入式系统安全的研究与设计[J]. 电子科技, 2005, 191(8): 49-53.

[17] 陈火旺, 王戟, 董威. 高可信软件工程技术[J]. 电子学报, 2003, 31(12A): 1933-1938.