

面向工控网络的区域隔离系统设计与实现

钟 能, 张志勇, 闫连山, 孙 政

(西南交通大学 信息科学与技术学院, 四川 成都 610031)

摘 要: 设计了基于微处理器的区域隔离硬件装置, 通过通信管控, 采用“白名单”技术对进出关键设备的数据包进行严格审查, 阻止非法数据包流过. 以 CTCS-3(中国列车运行控制系统)的信号系统安全数据网为例进行了扫描攻击、ARP 攻击、木马攻击和缓冲区溢出攻击等测试. 测试结果表明在不影响网络实时性、稳定性的前提下, 该区域隔离系统能够加固网内设备终端, 有效防御非法者入侵、网内设备间相互攻击和病毒在局域网内的传播.

关键词: 工控网络; 网络安全; 区域隔离; 白名单

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2014)10-0090-04

Designation and Implementation of a Regional Isolation System for Industrial Control Network

ZHONG Neng, ZHANG Zhi-yong, YAN Lian-shan, SUN Zheng

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: The hardware of a kind of regional isolation system has been designed based on the Arm Chip platforms. Using which, the illegal packets are prevented to pass through, by examine the packets flow to these critical equipments with the communication control method and "white list" technology. Several typical network attacks method were used to test the security of the CTCS-3 (Chinese Train Control System), which include the scanning attacks, the ARP attacks, the Trojan attacks and the buffer overflow attacks. Results show that security of these devices in this industrial network is reinforced without influence real-time performance of the network. The illegal incursions, the attacks within the network and the spread of the virus are efficiently prevented using this region isolation system.

Key words: industrial control network; network security; regional isolation; white list

1 引言

目前对工控网络的防护, 大都采用防火墙技术、入侵检测技术和网络隔离技术等常规网络安全技术, 但是这些设备都有很强的针对性和局限性^[1]. 且防火墙和网络隔离技术主要用于防御非安全网络对安全网络发起的攻击, 不能防御安全网络内部攻击和病毒在网内的传播. 本文设计的区域隔离系统(以下简称隔离系统)确保放行数据为正常的业务数据包, 能防御针对各层的攻击.

2 区域隔离系统原理

2.1 硬件结构

隔离系统基于 ARM(LPC3250)平台, 采用双 CPU 和高速双端口静态 RAM 结构, ucos 实时操作系统, 硬件结构和硬件实物图分别如图 1、2 所示. 双端口 RAM 作为两 CPU 信息交互缓存, 两 CPU 分别集成以太网物理层收发器, 负责从线路上捕获数据帧并通过 DMA 技术缓存到 CPU. CPU 对缓存数据包进行深度分析, 若完全符合通信协议要求, 则将数据包写入双端口 RAM 中, 并利用中断通知对

收稿日期: 2013-12-18; 修回日期: 2014-02-13

基金项目: 铁道部重大项目(2012X004-A)

端 CPU 对数据包进行转发;否则直接丢弃.隔离系统通过 RS232 与监测上位机相连,将对数据包的分析、处理结果实时传送至上位机.

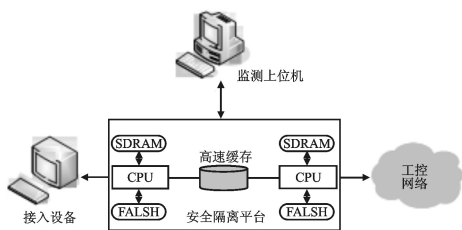


图1 隔离系统硬件结构

2.2 数据包处理流程

隔离系统对数据包处理流程如图2所示.

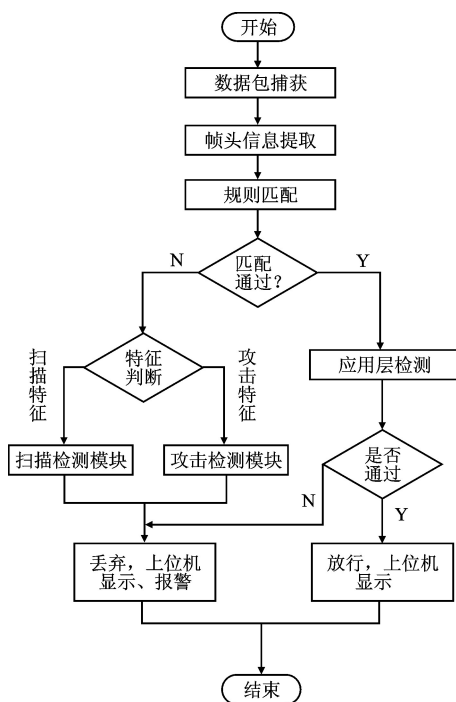


图2 数据包处理流程

(1) 物理层收发器从线路上捕获一帧数据并缓存至CPU,CPU提取出帧头信息,包括MAC、IP、端口号等.

(2) 调用预先存储的合法信息库(存有与该设备通信的所有主机地址信息及相应端口)进行规则匹配,检测源、目的地址以及通信端口是否合法.

(3) 若(2)检测通过,则进行应用层检测.调用预先存储的业务数据包信息库(存有经过该设备的所有合法业务数据包格式及内容),若应用层检测合法,则放行该数据包并通知上位机进行日志记录;若检测为非法应用层数据,则判定为针对此应用程序的攻击或木马攻击(端口复用),丢弃数据包、通知上位机记录并报警.

(4) 若(2)检测异常,根据其具体特征调用相应检测模块进行非法意图检测.特征包括信息收集(如主机扫描、端口扫描)、常用攻击(如ARP攻击、木马攻击)等.检测完成后丢弃数据包,并将检测结果传至上位机显示记录并报警.

2.3 可行性分析

隔离系统采用“白名单”技术对数据包各层进行深度匹配、分析.“白名单”贯穿于链路层到应用层,当各层协议内容完全符合规范时放行数据包,否则直接丢弃.采用白名单技术的前提是网络结构和网内主机地址相对稳定,设备间通信数据帧格式固定且较少,因为“白名单”需要存储设备间通信的所有业务数据帧格式及内容.

隔离系统有两种工作模式:监听模式和过滤模式.监听模式只负责监听数据包并通过上位机显示,不对数据进行过滤,避免因加入隔离系统对管理员正常管理网络造成不便.过滤模式用于对非法数据包进行过滤,发现异常包直接丢弃.

工控网络中控制设备间主要传输控制命令和设备参数等信息,网络及通信流量符合“白名单”要求,因此将该隔离系统应用于工控网是可行的.

3 常用攻击及防御方法

3.1 非法信息收集及防御

非法信息收集包括主机扫描、端口扫描等,做好信息收集的防御工作是防御网络攻击的第一步.

主机扫描的基本原理是向目标主机发送探测包,根据目标主机是否响应来测试主机的存活状态,包括Ping扫描、ARP扫描等.

端口扫描分为TCP和UDP扫描,基本原理是向目标主机的不同端口发送探测数据包,并根据目标主机的响应信息判断端口是否开放,进而判断开放端口运行的服务.UDP扫描原理简单,容易被检测到,且准确率低,很少使用.TCP扫描详细分类如图3所示^[2].TCP全扫描和SYN扫描原理简单,准确率高,应用广泛,但隐蔽性较差.隐蔽扫描隐蔽性强,但通用性差,扫描准确率不高.

由主机扫描原理可知,根据链路层和网络层通信协议可识别出主机扫描包.Ping扫描包将被直接丢弃,ARP扫描包则需要根据当前源、目的主机连接状态判断是否过滤:若连接正常(主机间已建立正常连接),则丢弃;若未建立连接,则可能为正常ARP协议包,予以放行.

隔离系统根据TCP端口扫描原理对数据包进

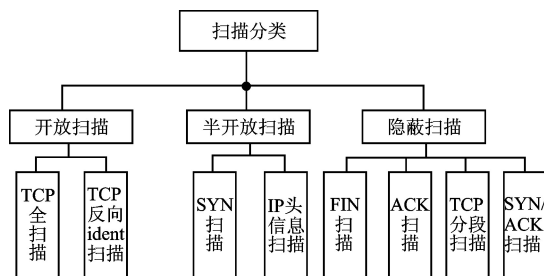


图 3 TCP 扫描分类

行识别、统计,若单位时间内某种特征数据包超过给定阈值,则判定存在端口扫描.对于慢扫描,可通过调节统计时间和阈值来进行防御.

3.2 ARP 攻击及防御

ARP 协议根据目标 IP 地址来获取相应的 MAC 地址,在设计时存在一个缺陷,没有对 ARP 报文来源的合法性进行验证,导致 ARP 攻击的出现. ARP 攻击基本原理是向目标主机发送源 MAC 地址与源 IP 地址不一致的 ARP 报文,接收端收到报文后立即对自身 ARP 缓存表进行更新,而不会验证来源合法性.

由 ARP 攻击原理可知,防范 ARP 攻击的根本方法是确保 ARP 报文中源 MAC、IP 地址的一致性.隔离系统“白名单”中存有与该主机通信的其他主机地址信息,可对流经的 ARP 报文源 MAC、源 IP 对应关系进行检测,有效防范 ARP 攻击.

3.3 木马技术

木马是一种基于 C/S 模式的计算机程序,客户端程序运行在入侵者计算机上,服务器端位于被入侵的主机上.入侵者通过客户端给服务器发送攻击指令,服务器响应指令并将攻击结果或窃取的信息返回给客户端.隐蔽性是木马的首要特征,只有实时隐藏,木马才能存活下来.

端口复用指木马程序与正常应用程序公用一个端口进行秘密通信,常规网络安全设备很难察觉^[3-4].隔离系统除了对传输层及以下进行检测外,通过对应用层重点分析进行防御.隔离系统“白名单”中存有设备间正常业务数据包的帧格式及内容,对进出正常端口的数据包应用层数据严格检查、匹配,只允许白名单中的业务数据包通过,过滤掉非法包,从而防御端口复用技术.

反弹技术针对防火墙“外紧内松”的防御特点,服务端主动连接,控制端被动等待连接^[5],而且通常使用不易被察觉的端口进行秘密通信(如 HTTP 端口).该隔离系统与防火墙“外紧内松”不同,对进出数据包采取相同的处理方式,通信端口也在“白名

单”中,内网发出的非法连接和非法数据包将被隔离系统有效拦截,从而防御反弹技术.

ICMP 潜伏技术指木马使用 ICMP 协议中特殊字段进行秘密通信.由于不采用 TCP、UDP 协议,不会有额外端口被打开,通信端口检测功能对此无能为力.该隔离系统通过对 ICMP 报文“选项”字段重点检查,防止木马通过“选项”字段建立非法通信链路.

3.4 缓冲区溢出攻击

缓冲区溢出是一种非常普遍、危险的漏洞,在各种操作系统和应用软件中广泛存在.通过往程序的缓冲区写入特殊构造的超长数据内容,造成缓冲区溢出,使程序转而执行其他攻击指令,达到攻击目的^[6-7].

隔离系统对数据包应用层内容进行严格检查,并且对各种数据帧的长度严格管控,禁止特殊构造的超长数据包通过,防御针对特定应用程序的缓冲区溢出攻击.

4 实验测试及结果分析

4.1 信号系统安全数据网

安全数据网是铁路信号系统关键网络(安全数据网、CTC 数据通信网和集中监测网)之一,其接入设备包括:列控中心(TCC)、计算机连锁(CBI)、临时限速服务器(TSRS)、无线闭塞中心(RBC)^[7].接入设备间通信主要采用两种协议:RSSP-II(TCP 方式)和 RSSP-I(UDP 方式)^[8].数据网内部封闭运行,仅网络上连接设备之间相互进行信息交换,内部未设置网络与信息安全设备.因此,将隔离系统放置于接入设备入网处,对接入设备和数据网络可双向防护,安装隔离系统后的安全数据网结构如图 4 所示.

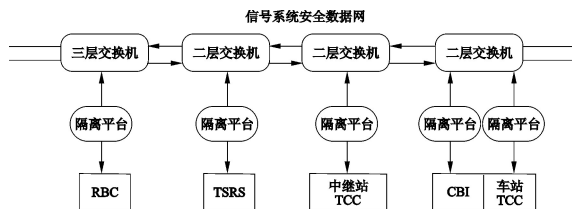


图 4 安全数据网网络结构

4.2 模拟安全数据网

本实验搭建的模拟安全数据网结构如图 5 所示,各接入设备 MAC 固定,IP 地址及设备间通信所用端口统一分配.其中 192.168.7.10-13 为网内正常设备,192.168.7.14 为入侵设备.本实验中将隔

离系统置于 RBC 入网处,TSRS、CBI 与 RBC 有信息交互,因此测试前需通过编写的上位机配置软件将 RBC、TSRS 和 CBI 的地址、通信端口以及相互间传输的业务数据包合法库写入隔离系统。

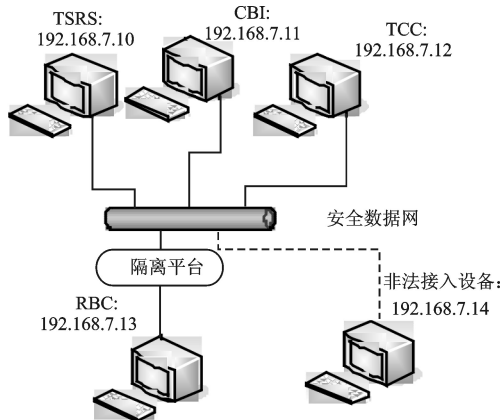


图5 模拟安全数据网

4.3 测试结果及分析

通过了隔离系统转发时延测试证明了系统有效性。

隔离系统转发数据帧时延测试结果如图6所示。

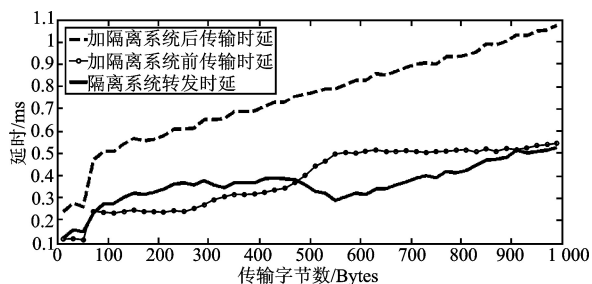


图6 隔离系统转发时延

图6中,加隔离系统后传输时延减去加隔离系统前传输时延即为隔离系统转发时延。由图可知,当数据帧长度为10~1000比特时,隔离系统转发时延为0.11~0.5 ms。安全数据网规范^[7]指定接入设备间信息传输总延时不大于50 ms,因此加入隔离系统后不影响网络传输的实时性,同时也能满足大多数工控网的实时性要求。

5 结束语

在模拟的信号系统安全数据网中使用本文设计的区域隔离系统,在RBC终端上进行实验测试,结果表明,能够过滤非法数据包,有效防止终端设备被攻击。目前各个隔离装置只能单独进行软件配置和管理,对网内所有隔离系统集中统一在线管理有待进一步的研究。该隔离系统实现了对工控机终端的有效安全加固。该隔离装置的实现对于提高整个工控网络的安全性具有重要的应用价值。

参考文献:

- [1] 宋维嘉. 基于嵌入式Linux的铁路专用安全网关关键技术的研究与实现[D]. 北京:北京交通大学,2008.
- [2] Tejasvi Anand, Yagnesh Waghela, Kuruvilla Varghese. A scalable network port scan detection system on FPGA[C]// Field-Programmable Technology (FPT), 2011 International Conference. New Delhi:IEEE,2011: 1-6.
- [3] 李健,王玲,董科军,等. 基于Linux的网络入侵检测与防火墙集成系统的设计与实现[J]. 微电子学与计算机,2006,23(4):18-22.
- [4] 罗改龙,程胜利. 基于端口复用的木马研究[J]. 计算机工程,2007,33(15):165-169.
- [5] 客运专线信号系统安全数据网技术规范[S]. 铁道部. 2010.
- [6] 罗红,慕德俊,戴冠中,等. 端口反弹型木马的通信技术研究[J]. 微电子学与计算机,2006,23(2):193-197.
- [7] Kundu A, Bertino E. A new class of buffer overflow attacks[C]// Distributed Computing Systems (IC-DCS), 2011 31st International Conference, 2011: 730-739.
- [8] RSSP-I、RSSP-II 铁路信号安全通信协议[S]. 铁道部. 2008.

作者简介:

钟能 男,硕士研究生.研究方向为嵌入式开发和网络安全.
张志勇 男,博士研究生.主要研究方向为光纤传感和光信息处理.