输电线路在线监测可信接入系统设计

陈亚东,张 涛,曾 荣,费稼轩
(中国电力科学研究院,江苏 南京 210003)

摘 要:输电线路状态在线监测系统是智能电网环境中对重要输电线路的状态进行实时监测、预警、分析形成标准化状态监测数据的业务系统。系统通过传感器收集输电线路及杆塔周围的温度、湿度等环境特征数据,由线路上部署的嵌入式输电线路状态监测代理(CMA)经移动专网将数据传送到业务系统,因此在数据传输过程中确保 CMA 自身安全,以及 CMA 在公用数据网络中安全接入业务系统,防止数据被窃取或篡改十分重要。文中以输电线路状态在线监测系统业务场景为基础,设计了基于国产可信芯片的输电监测可信接入系统,保证了输电线路状态监测代理安全可信地接入业务系统,经过实验验证,可信接入系统达到了电力系统安全技术要求,可以确保输电线路状态监测系统安全稳定运行。

关键词:可信计算;可信接入;可信终端
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)05-0113-03
doi:10.3969/j.issn.1673-629X.2013.05.029

Design of Trusted Access System for Transmission Line Monitoring

CHEN Ya-dong, ZHANG Tao, ZENG Rong, FEI Jia-xuan
(China Electric Power Research Institute, Nanjing 210003, China)

Abstract: Transmission Line Monitoring (TLM) is a system for transmission line state conducting real-time monitoring, early warning, analysis to form standardization of condition monitoring data service in the environment of smart grid. The system collects temperature, humidity and other environmental characteristic data of power transmission lines and towers surrounding with sensors fixed on transmission lines, the data is transmitted by line deployed embedded transmission line condition monitoring agent (CMA) via mobile network to power system. So in this data transfer process, it is of great importance to ensure CMA security, to make sure CMA to securely access service system with public data network, and to prevent data tampering. Based on the transmission line on-line condition monitoring system environment, design trusted access system with domestic trusted chip, trusted access system ensures the transmission line condition monitoring agent security credible access service system, after experimental verification, trusted access system can ensure the safety of data transmission in line state monitoring system stable operation.

Key words: trusted computing; trusted access; trusted terminal

0 引 言

基于可信芯片的可信计算机是可信计算领域的研发热点,在国内,联想瑞达、同方等厂商已经研制了基于国产可信计算模块的商业化可信计算机,利用可信引导技术提供了解决各类终端安全性增强问题的方案,并且在国内一些产品中得到了应用。

可信计算机终端一般将可信芯片通过各种总线接口连接计算机主板,移植可信芯片的配套驱动程序,改造计算机系统的 BIOS,在 BIOS 中添加调用芯片配套软件栈,在操作系统引导程序和操作系统核心模块中添加调用芯片算法的可信模块,完成从 BIOS 到操作系统核心启动的度量功能,并实现度量的信任链传递,还可以基于可信芯片的软件栈服务接口库进行可信计算机上次可信应用的开发,为计算机开发面向各行业的应用层软件。

文献[1]描述了构建用户与终端、终端与终端、应用与终端的多层次认证机制,实现了基于 ARM 芯片的可信系统。文献[2]提出了带有移动可信模块的可信移动平台设计方案,与文献[1]都只是提出了单个终端实体的可信改造与设计,没有设计包括可信网络连接、可信服务端在内的完整可信接入系统。

文献[3]中所定义的结构同 TCG 所定义的可信引导过程类似。但没有涉及如何计算验证实体的预期完整性值问题,因此该可信引导过程并不完整,文献[4]设计了 TCG 规范下的可信引导方案,这两篇文献也只是描述终端可信引导机制,没有提出可信终端操作系

收稿日期:2012-08-27;**修回日期**:2012-11-30
基金项目:国家电网公司科技攻关团队项目(SG11034)
作者简介:陈亚东(1982-),男,硕士,工程师,通信作者,主要研究方向为电力系统网络安全技术。

统层和应用层的软件动态完整性度量机制。

文中以电力业务需求为基础,在输电线路状态监测业务接入场景中,设计了嵌入式终端可信引导改造机制,并在嵌入式终端上开发了静态和动态完整性度量机制,设计了服务器端完整性验证机制,开发了双向可信网络认证连接软件,形成包含终端、网络接入、服务器端的完整可信接入系统,保证了业务系统信息传输各个环节的可信,实现了业务数据的安全收集与传输。

1 电力业务场景

输电线路状态在线监测系统业务拓扑图如图 1 所示:

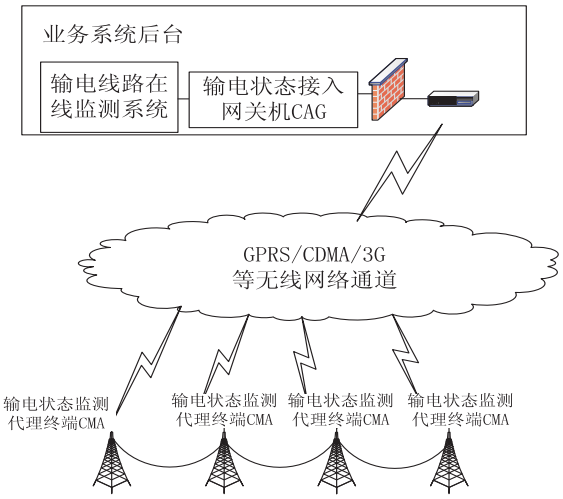

图 1 输电线路状态监测场景拓扑

输电线路状态监测代理终端(CMA)是一个运行嵌入式 Linux 系统的嵌入式终端,嵌入式终端 CMA 运行输电线路状态监测代理软件,获取状态监测传感器终端收集的输电线路状态信息,将信息通过 GPRS 模块经无线 APN 专网通道与输电状态接入网关机(CAG)进行通信。在数据传输过程中存在非法终端接入、终端被攻击等风险,因此,采用基于可信计算技术的终端加固防护、高强度身份认证、进行加密数据传输,保证业务数据传输的机密性和完整性十分必要。

2 可信接入系统整体设计

在 CMA 终端接入输电线路的业务场景中,从终端,经网络连接,到网关机 CAG,经过可信改造,文中设计了一套完整的可信接入系统,在终端和服务端可信启动、客户端和服务端之间建立可信网络连接、客户端业务软件的可信运行等三个业务信息传输的环节过程中保证可信,可信接入系统的整体设计如图 2 所示。

可信网络连接以 openssl0.9.7 为基础进行改造,首先,将 openssl 在 CMA 运行的嵌入式 Linux 上安装,其中密码算法库通过 openssl engine 机制[5],挂载 TPM 软件栈,替换原有软密码算法,实现通过 openssl 直接调用可信芯片密码算法,ssl 协议库保留,应用程序经过改造,与完整性度量模块集成在 CMA 终端上,服务器端的软件层次与改造方法与 CMA 一样。可信网络连接的软件层次如图 2。运行可信网络连接服务端的可信网关机 CAG 与 CMA 终端的可信体系相同,是一台运行 Linux 的服务器,也包括可信链、TPM 芯片、可信驱动库和可信软件栈,运行可信网络连接软件服务端和完整性验证模块。

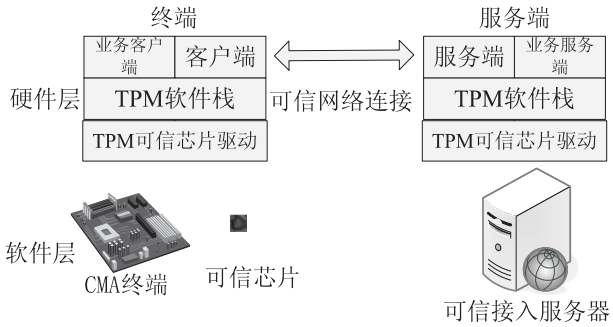

图 2 可信接入系统整体设计

可信 CMA 终端集成可信计算芯片,利用可信平台模块(TPM)和信任链技术对系统安全性进行了增强,提高了终端的安全性。

CMA 由 AT91RM9200 ARM CPU,板载 RAM,RS232、RS485 接口,GPRS 模块等构成,采用嵌入式 Linux 2.6.30 版本作为操作系统。

图 3 是集成可信芯片的 J3210 开发板,开发板集成的 J3210 安全芯片是一款通过国家认证的可信计算平台模块芯片,是 32 位微控制器芯片,芯片具有 128KB ROM、128KB FLASH、21KB SRAM,密码算法引擎有非对称 SM2 算法、杂凑 SM3 算法、对称 SMS4,支持 LPC 接口、I2C 接口和串口[6],引入 RS485 串口转 LPC 接口,CMA 终端可以将开发板可信芯片扩展到主板上,实现 CMA 终端与可信芯片的集成。

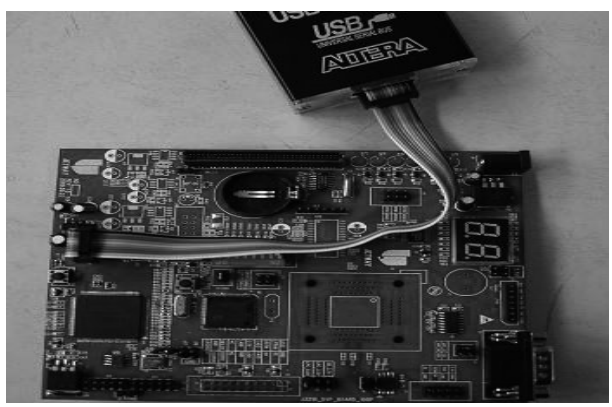

图 3 J3210 可信开发板图

将 J3210 芯片的可信驱动库和可信软件栈移植到 CMA 终端 Linux 系统上,由于嵌入式板卡没有 BIOS,

所以启动从 bootloader 开始,按照 bootloader、内核文件、启动脚本的顺序进行逐级度量,最终整个系统启动完成。

3　终端完整性度量模块设计

Linux 系统运行的应用程序包括的重要文件包括用户态可执行文件、动态库,针对这些文件设计了运行时度量完整性的机制。

用户态可执行文件:用户态可执行文件通过用户态加载器加载[7],当一个二进制可执行文件通过 execve 系统调用被调用时,内核调用一个二进制管理程序,解释二进制代码同时为可执行文件指定合适的加载器,然后内核把加载器映射到内存,设置好可执行文件需要的环境。在这种静态链接的情况下,加载的文件只有可执行文件本身,在 execve 系统调用中加入一个度量过程,调用可信芯片的密码算法计算度量值[8],与安全状态下预先计算的健康度量值比对,如果相同则文件完整性没有问题。

动态可装载库:动态链接的二进制文件通常需要加载一些需要的库,这个过程是由用户空间的装载器进行装载,并传递给内核[9],动态可装载库的装载和完整性度量过程如下:

1)用户空间的装载器将动态可装载库装载到内存中;

2)由链接器动态连接到相应的可执行代码中;

3)链接器在进行链接的过程中,调用系统调用 mm 实施动态可装载库的内存映射;

4)系统调用 mmap 执行 file_mmap 钩子函数,在该钩子函数中插入调用可信计算度量函数的度量点,对动态可装载库进行完整性度量[10]。

在一般的静态度量方法中,对应用程序的度量选择在程序启动之前,可以保证程序在度量启动的瞬间没有受到攻击,如果业务软件在运行时的安全状态被破坏,静态度量机制就不能发现。针对实时对运行软件进行完整性度量问题,文中描述的可信接入系统设计了一种针对计算机终端运行软件的动态完整性度量机制,其主要特点是利用芯片度量相关函数对计算机中的进程进行周期性动态度量,保证程序运行过程中的安全性。

程序在运行时需要建立自己的堆栈,并占用一定的空间存放程序私有数据,数据一般分类以堆栈方式存放,程序数据一般分为指针数据,包括程序中定义的指针类型的数据,如程序中的字符串指针、函数,以及非指针数据。

设立隔离标志从逻辑上将指针数据和非指针数据分开,隔离标志可以在启动时由可信芯片算法计算健康值,将若干个健康度值插入到堆栈空间[11];将非指针数据存放在隔离标志的低地址方向,将指针数据存放在隔离标志的高地址方向,形成一个存放区域,程序的内存空间中可以有多个存放区域。

存放区域中的非指针数据有可能受到攻击产生溢出或者数据越过边界,覆盖了指针数据类型,可以将非指针数据存储在低地址空间,和指针数据之间插入隔离标志,通过检查隔离标志的完整性判断双方是否发生数据越界。本方法通过在一个栈帧内将指针数据放在非指针数据之前,消除了该栈帧内非指针数据对指针数据的影响,实现了细粒度隔离[12]。

在程序运行过程中,针对指针的操作一般说来非常频繁,如果在每次涉及指针操作前对隔离标志进行检查,则效率较低,可以设定对隔离标志的检查频率,并找到一个合适的点,如果检查频度低了可能程序的健康检查起到的作用有限,如果检查频度高了检查过程占用的资源太高影响系统效率[13]。

一个完整的动态度量过程如下:

1)判断栈帧内的操作是否调用指针数据,如果涉及指针,则进入 4,检查隔离标志。

2)判断栈帧内的操作是否是压入新栈帧,如果是压入新栈帧,则跳转到 4 检查隔离标志。

3)判断栈帧内的操作是否是弹出栈帧,如果是弹出当前栈帧,则进入 4,检查隔离标志。

4)检测栈帧中所有存放区域中的隔离标志,判断是否发生如溢出等破坏事件。

5)如果 4 中针对隔离标志的检查没有发现破坏事件,执行步骤 1、2 和 3 所述的相关操作。

本逻辑隔离方法通过在缓冲区中设置细粒度数据隔离标志,在关键步骤前对隔离标志执行完整性检查,对数据区域边界进行防范和检查,从而实现对程序运行的动态完整性度量。

4　结束语

文中提出了一种实现嵌入式终端可信接入的方法,文中设计方案利用了国产可信芯片,同时提出了终端度量的方法,这些技术是对国产可信计算技术的有效利用和发展,也为其他行业的可信技术应用提供了一个思路。

参考文献:

[1]　王　禹,王震宇,姚立宁. 嵌入式平台 TPM 扩展及可信引导设计与实现[J]. 计算机工程与设计,2009,30(9):2089-2091.

[2]　Shen Changxiang,Zhang Huangguo,Feng Dengguo,et al. Sur-

(下转第 119 页)

Cryptography Standards,公开密钥密码标准)#11 接口对加密卡进行访问,建立手机信息安全体系。

本系统正是利用了冀科 TF Key 所提供的高效的身份认证、高强度的加解密服务,实现了基于 WPKI 与 DRM 等技术的智能手机信息安全存储系统。由于采用的是由国家密码管理局指定的 SM1、SSF33 等对称加密算法与 RSA、ECC(Elliptic Curve Cryptography,椭圆曲线加密算法)[9,10]非对称加密算法,并且所有算法都是由冀科 TF Key 硬件实现,因此,本系统可为智能手机用户提供安全、高效、快捷的加解密服务。

2　结束语

随着移动通信技术的迅猛发展,集通讯、电子商务、网上银行、掌上办公、随身娱乐等于一身的智能手机也迅速普及。在人们享受智能手机给生产生活带来的极大便利的同时,也逐渐认识到智能手机安全问题也越来越成为制约智能手机广泛应用的重要因素。

鉴于隐私数据外泄对个人用户及企业用户都会造成不可估量的损失,同时,考虑到现在智能手机有限的计算能力,文中研制了基于 WPKI、DRM 及冀科 TF Key 的智能手机信息安全存储系统。该系统充分利用 WPKI 与 DRM 中成熟的技术,借助独立的冀科 TF Key 作为运算单元,实现身份认证及加解密运算功能。该安全存储系统可为用户提供由国家密码管理局指定的 SM1、SSF33 等对称加密算法与 RSA、ECC 等非对称加密算法,提供保护的高效的身份认证及高强度的加解密服务,使智能手机用户在享受本系统带来的高强度的安全保护的同时,又不必饱受漫长的等待之苦。本系统特别适用于对安全性要求较高的电子商务、网上银行、网上购物等 3G 应用场合。

参考文献:

[1] 桂佳平,周雍恺,沈　俊,等. 基于智能手机恶意代码防范模型的研究[J]. 计算机技术与发展,2010,20(1):163-166.

[2] 宋　杰,党李成,郭振朝,等. Android OS 手机平台的安全机制分析和应用研究[J]. 计算机技术与发展,2010,20(6):152-155.

[3] 张　玮. 移动电子商务安全中 WPKI 证书查询机制研究[D]. 北京:北京邮电大学,2007.

[4] Chen Lunyong, Li Chunqing. Discussion and Application of WPKI Technology[J]. Modern Applied Science,2007,4(1):50-54.

[5] 张跃进,谢　昕,黄德昌. 基于 WPKI 的 3G 认证方案的研究与实现[J]. 华东交通大学学报,2008,25(3):88-91.

[6] 范科峰,莫　玮,曹　山,等. 数字版权管理技术及应用研究进展[J]. 电子学报,2007(6):133-141.

[7] Pucella R,Weissman V. A Logic for Reasoning about Digital Rights[C]//Proceedings of 15th IEEE Computer Security Foundations Workshop (CSFW'02). [s. l.]:[s. n.],2002:282-294.

[8] 黄　成,汪海航. 智能卡在 WPKI 中的应用研究[J]. 计算机技术与发展,2007,17(12):154-156.

[9] 李　姜. 基于 ECC 的组合公钥技术的研究与实现[D]. 太原:太原理工大学,2007.

[10] Afreen R,Mehrotra S C. A Review on Elliptic Curve Cryptography for Embedded Systems[J]. International Journal of Computer Science & Information Technology,2011,3(3):84-103.

(上接第 115 页)

vey of information security[J]. Science in China Series:E (Information Security),2007,37(2):129-150.

[3] 刘　皖,谭　明,郑　军. 基于平台可信链的可信边界扩展模型[J]. 计算机工程,2008,34(6):32-34.

[4] 胡中庭,韩　臻. 操作系统安全可信链的研究与实现[J]. 信息安全与通信保密,2007(2):47-49.

[5] Shen Changxiang,Zhang Huanguo,Feng Dengguo,et al. Survey of Information Security[J]. Science in Chian Series F,2007,50(3):273-298.

[6] 张京楣,金　妍. 基于对等网络的信任模型[J]. 济南大学学报(自然科学版),2002,16(4):46-47.

[7] 杨　涛,陈福接,沈昌祥. 一个安全操作系统 S-UNIX 的研究与设计[J]. 计算机学报,1993,16(6):409-415.

[8] Bell D E,LaPadula L J. Secure computer systems:mathematical foundations[R]. Bedford, MA:Electronic Systems Division,Air Force System Command,Hanscom AFB,1973.

[9] 陈志平,雷　航,杨　霞,等. 嵌入式安全操作系统的研究和实现[J]. 计算机工程,2007,33(1):83-85.

[10] 陈幼雷. 可信计算模型及体系结构研究[D]. 武汉:武汉大学,2006.

[11] 吴兴勇. 嵌入式操作系统安全保障技术研究[D]. 成都:电子科技大学,2003.

[12] 刘威鹏,张　兴. 基于非传递无干扰理论的二元多级安全模型研究[J]. 通信学报,2009,30(2):52-58.

[13] 王　飞,刘　毅,李　勇. 基于无干扰原理的终端安全模型研究[J]. 武汉大学学报:信息科学版,2008,33(10):1092-1094.

输电线路在线监测可信接入系统设计

作者： 陈亚东， 张涛， 曾荣， 费稼轩
作者单位： 中国电力科学研究院,江苏 南京210003
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(5)