基于可信计算的用电信息采集终端完整性检测方案

张少敏,王志男,王保义
(华北电力大学 控制与计算机工程学院,河北 保定 071003)

摘要:针对信息物理融合下用电信息采集终端面临的信息安全风险问题,结合采集终端的特点,提出了一种基于可信计算的终端完整性检测方案以保护终端安全。从信任结构、可信平台模块扩展方式、扩展策略三方面改进了可信计算组织的检测方案,减少了信任传递损失,并提高了扩展在计算上的灵活性。在验证所提扩展方式可行性和安全性的基础上,重新设计了扩展策略。与原方案相比,所提方案对计算资源、存储空间的占用都有一定的优化,也为终端提供了支持动态信任度量的方法。

关键词:信息物理融合系统;用电信息采集;完整性检测;可信计算;信任结构;扩展方式;扩展策略
中图分类号:TM 73 **文献标识码**:A DOI:10.16081/j.issn.1006-6047.2017.12.008

0 引言

信息物理融合系统 CPS(Cyber-Physical System)是一种各物理组件具有信息处理和通信能力、信息组件与物理组件高度集成、在时间以及空间等维度上具有多重复杂性的网络化的大规模复杂系统[1]。

当前用电信息采集系统部署了大量的嵌入式采集终端,构建了从主站到各级终端的通信网络,实现了主站与终端间的命令通信和数据通信,已经部分符合信息物理融合的特征。在信息共享和融合、海量数据处理、信息双向交互等新趋势下[2],用电信息采集系统将实现深度的信息物理融合。

嵌入式终端是 CPS 中的重要组成部分,对于攻击者而言,只需要操纵小部分节点就可能导致整个耦合系统的崩溃[3]。根据以往的经验,忽略了对终端本身的保护就是安全问题频发的主要原因。终端往往是创建和存放重要数据的场所,绝大部分攻击事件是从终端发起的[4]。因此,对于用电信息采集系统而言,采集终端的安全性应该受到足够的重视。

文献[5-6]描述了传统应用环境中采集终端面临的诸如窃听、篡改、删除、系统程序升级、软硬件损毁等安全问题。信息空间、物理空间和人类世界三元空间的融合使得安全威胁变得更为复杂[7]。文献[8]从 CPS 体系结构层次的角度对攻击类型进行了总结,对于采集终端此类多层次设备,其攻击类型多样。文献[9-11]介绍了电力 CPS 中配电侧、用户侧的网络攻击场景和威胁来源。

收稿日期:2017-05-14;**修回日期**:2017-11-14
基金项目:国家自然科学基金资助项目(61502168,61300040);河北省自然科学基金资助项目(F2016502069)
Project supported by the National Natural Science Foundation of China(61502168,61300040) and the Natural Science Foundation of Hebei Province(F2016502069)

针对各种安全威胁,采集终端已经采用了物理封装、电路保护、安全硬件、OS 加固等设计手段。但是在安全设计上仍然存在着以下问题:部署环境和工作特性决定了采集终端不能被有效地监控,物理防护不能有效阻止攻击的发生;安全硬件对信息加密能力有限;操作系统和应用程序承担了采集终端的主要工作,但是缺乏对终端程序的检测手段;采集终端是一个复杂的设计,纵然系统自身的每一部分都是安全的,组件之间的整合也可能会引起一些新的问题[12]。

为了从根本上提升终端的安全性,研究者提出了可信计算 TC(Trusted Computing)。可信强调实体行为的可预期性,即实体能够按照预期安全可靠地运行。IBM、HP 等公司组成的可信计算组织(TCG)制订了主要的技术规范。规范包括了可信计算所需的硬件和软件、终端和网络架构等。其中,可信平台模块 TPM(Trusted Platform Module)是可信计算中的基础部件。

由于缺少直接计算实体可信性的方法,目前主要通过度量实体的完整性间接地反映实体可信性,令"完整性等于可信性",这一度量过程称为信任度量。本文讨论的完整性检测是可信计算中检测终端配置的重要方法,是一种由底层开始的安全防护手段。该方法在终端检测的过程中能及时发现并阻止异常对象运行,并可以将完整性信息作为远程证明的依据。

以往的嵌入式终端可信计算研究大多仍沿用了 TCG 的设计思想,侧重于终端完整性检测方案由 PC 向嵌入式的移植[13-16],使得原方案中的一些弊端仍然存在。本文在信息物理融合的背景下,结合用电信息采集终端的特点,从信任结构、平台配置寄存器 PCR(Platform Configuration Riegister)扩展方式和扩展策略 3 个方面改进了 TCG 的终端完整性

检测方案,减小了信任传递损失,提高了扩展灵活性,在一定程度上节约了过程中占用的计算资源以及存储空间,也为终端提供了一种支持动态信任度量的方法。

1　TCG 可信计算终端完整性检测方案

TPM 是集成在终端中的安全硬件,实质上是一个小型片上系统。TPM 的功能繁复,本文主要介绍其在完整性检测中存储完整性信息的功能。TPM 中有一组 160 位的 PCR,用以存储信任度量值,通过这些值反映终端完整性。PCR 值可以通过接口读取,只允许在终端重启时重置,禁止直接写入。其内容的更新过程称为扩展(extend)。TPM 硬件结构如图 1 所示。

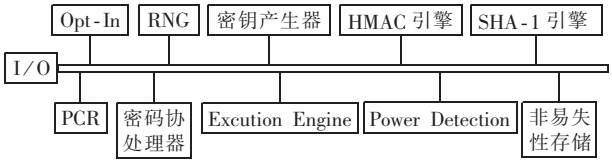

图 1 TPM 硬件结构

Fig.1 Hardware structure of TPM

TCG 的终端完整性检测方案是在部署可信计算基本硬件和软件的基础上,在终端启动时依照信任链,由上一级组件中写入的信任度量算法得到链中下一级的度量值,并将其扩展到 PCR 中,由 TPM 比较 PCR 值与预期值并做出响应。该方案将完整性检测的工作重心放在了终端启动配置的静态检验上,其中的技术细节也决定了该方案并不适用于反映终端运行时的动态状况。

1.1　信任结构与 PCR 扩展

信任链是由 TCG 提出的一种监测操作系统是否被攻击的方法。其典型的信任结构是:创建一个信任根,然后建立信任链。由信任根–硬件平台–操作系统–应用,在上一级中加入度量下一级的代码,逐级度量,传递信任。典型的链式信任结构如图 2 所示。

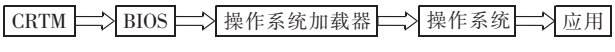

图 2 链式信任结构

Fig.2 Chain trust structure

在 TCG 的方案中,链式信任传递过程也体现在 PCR 的扩展操作中。扩展操作是将操作系统中各级的引导程序、程序的整体特征或部分特征、硬件特征、模块特征等度量值按照度量的先后顺序依次作为输入,在 TPM 中采用如下扩展:

$$PCR_{[i]}=\mathrm{hash}(PCR_{[i-1]}\|\mathrm{newMeasurement}) \quad (1)$$

这种扩展方法的实质是迭代的连接和散列运算,具有有序性和不可逆性。其中,有序性是指即使度量值相同,如果输入顺序不同也会产生不同的运算结果;不可逆性是指不能通过计算 PCR 值得到输入的变量。

TCG 方案中链式信任结构和扩展方法可以较好地描述终端启动伊始的配置,但是缺点也比较明显。由于度量位置处于组件的上一级,因此该方案在某一组件改变时会对上下级组件都造成一定的影响,进而可能影响整条信任链。链式结构和扩展都包含对度量序列的要求,使得 PCR 值是终端组件在某种度量序列下的特有值。原扩展方式能够限制 PCR 值回溯,也导致当组件改变时,若不重启终端,只能在原值上扩展,否则将不能说明平台配置。更值得注意的是,TCG 的扩展建立在启动时的静态信任度量上,难以支持运行时的动态信任度量,启动时的配置不能说明当前状态,为 TOC-TOU(Time Of Check to Time Of Use)攻击留下了安全隐患。

赵波[17]等人针对链式信任结构在可信测量根 CRTM 易受攻击,系统组件删除、添加,升级更新带来的维护和管理问题以及信任损耗等问题上的不足之处,设计了星型信任结构,如图 3 所示。

该信任结构将可信测量根部署在 TPM 中,系统部件度量改由 TPM 直接负责,减小了信任传递长度。但 TPM 负担了更多的工作,在小型终端的移植上会存在一定限制。

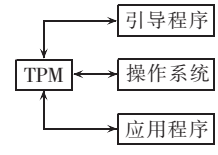

图 3 星型信任结构

Fig.3 Star trust structure

徐开勇[18]等人结合链式信任结构和星型信任结构各自的优势,提出了一种星型–链式混合信任结构,如图 4 所示。图中,E_i 表示度量对象;M_i 表示度量方法。

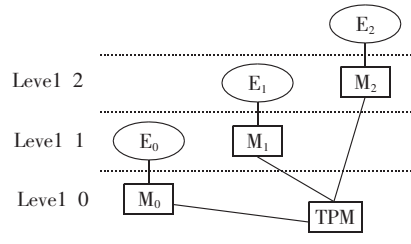

图 4 星型–链式混合信任结构

Fig.4 Star-chain mixed trust structure

这种模型在整体上采用星型信任结构,在各个分支上采用链式信任结构,将整个系统划分安全层次,由上一层的度量者对下一层的被度量者进行逐级的度量,各层的可信性由不同的度量者度量。但多个度量者细化了度量方法的同时,也给度量方法

的设计和整体性能带来较多的负担。对信任结构做出修改的文献都没有谈及 PCR 的更新问题,虽然新信任结构中 TPM 可以实现对各组件的直接度量,但是度量结果的存储仍然存在问题。

1.2 TCG 完整性检测方案扩展策略

由于链式扩展的特点,在原 TCG 方案中,组件只在启动时被度量,扩展操作也仅发生在此时,其 PCR 值说明的是终端的启动配置而不能说明终端的实时状态。如果终端配置不发生改变,每次策略执行的结果都是相同的,和终端的当前工作状态无关。对于连续工作的采集终端而言,其启动时的终端配置不能有效说明平台的安全性。

原方案中 PCR 在所有度量对象启动之后便不再扩展,终端完整性的可信度会随着时间下降,安全性也降低;如果再次度量并扩展,需在度量存储日志 SML(Stored Measurement Log)中添加新度量事件,以使日志内容与 PCR 值对应,其存储空间随度量次数不断变大,不利于预期值设定,进而影响完整性的判断。

综合而言,以上对信任结构的探讨建立在 PC、PDA 上,对于用电采集终端的可移植性并不强。相关文献中也都没有对 PCR 的扩展方式提出合适的建议,而 PCR 的扩展是反映信任结构度量结果的重要操作,PCR 值直接反映终端的检测结果,是判断完整性检测是否符合预期的重要证据。TCG 的扩展方式和链式信任结构是相同的设计思路,不支持动态信任度量,沿用过去的扩展方式会因运算特点制约新信任架构下的工作策略。新的技术规范虽然提出了支持动态信任度量的可重置 PCR,但其依赖具有新指令集的处理器,对采集终端并不适用。

2 采集终端完整性检测方案改进

2.1 采集终端完整性检测方案改进思想

针对第 1 节提到的当前终端完整性检测中仍然存在的问题和采集终端长时间连续工作、设备专用、缺乏有效监控等工作特点,本文在其他对嵌入式可信计算相关研究的基础上,对完整性检测过程提出了改进方案。

在完整性检测的改进方案中,本文主要对信任结构、扩展方式和扩展策略进行了改进。新的信任结构通过减少中间度量环节从而减小了采集终端信任度量中的信任传递损失;借鉴 Zobrist 散列思想,使用异或运算,改变了对度量结果的扩展方式,消除了扩展对顺序的要求,同时保证了新扩展方式的安全性;在改进扩展方式的基础上,利用异或运算的特点,在扩展策略中实现了 PCR 值的可回溯性,以支持动态信任度量算法,使 PCR 值能准确地表示当前终端状态,减少了 SML 占用的计算资源和存储空间。

2.2 改进的信任结构模型

本文提出的信任结构模型整体上沿用了星型信任结构的思想,由集成了信任根的 TPM 开始构建可信的采集终端。

该信任结构将度量过程分为 2 个阶段。在启动阶段由 TPM 依照启动序列,以星型结构处理组件的信任度量和组件间的控制权传递。在系统稳定运行时,主要的进程监视和度量工作交由支持动态信任度量的度量进程,TPM 对度量进程提供支持和监视功能。改进的信任结构如图 5 所示。

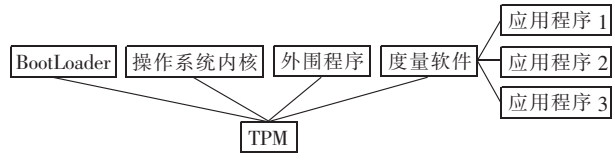

图 5 改进的信任结构

Fig.5 Improved trust structure

设计本模型的原因有以下 4 点:TPM 直接度量底层能够消除组件间的信任传递损失,提高安全性;革除链式结构组件间上下关联带来的弊端;终端中 TPM 的计算能力有限,使用终端中的处理器对应用进程进行信任计算的效率更高;度量软件本身的可信性需要监督,较短的链式结构造成的信任损失也可以接受。

2.3 改进的 PCR 扩展方式

本文对 PCR 的扩展方式做出改进,以符合改进的信任结构模型。参考 Zobrist 散列思想,引入异或操作代替之前的连接操作,新的扩展方法如下:

$$PCR_{[i]}=PCR_{[i-1]}\oplus hash(newMeasurement) \quad (2)$$

其中,$\oplus$ 表示异或运算。

Zobrist 散列[19]原本是一种用于复杂的棋类游戏程序中的哈希函数,用来避免重复分析相同的棋局局面。其计算方法的一大优点就是只需考虑当前的状态和将要进行的变化就可以描述整体所处的状态,而不必考虑形成当前状态的整个过程。并且,该方法的状态描述空间的大小由描述动作的随机数长度决定。其思想是为所有棋盘位置与棋子的组合情况,对应地生成一组互异的随机数。可以通过描述当前棋局局面的数与变动对应的数进行异或运算得到变动后局面。

改进的 PCR 扩展方式与链式 PCR 扩展方式相比,在计算效率上,2 种方式都进行了一次散列运算,不同点是本文提出的扩展方式采用了对 PCR 内所存数据的异或操作,替代了原有的连接操作,散列运算的对象也不再包含 PCR 值。与扩展操作中占

计算主体的散列运算相比,异或运算消耗很小。因而,改进 PCR 扩展方式几乎不会对单次扩展的时间造成影响。在安全性上,改进扩展方式利用异或运算特点消除了原扩展计算中的有序性,保持了度量对象对度量结果的不可逆性和 PCR 值对终端状态描述的唯一性。

2.3.1　度量对象对度量结果的不可逆性

定义 1　度量对象特征 M_{new} 等同于 newMeasurement。度量对象特征包括终端启动和运行阶段的程序整体或部分、硬件属性、启动次序等可以将该度量对象与其他对象区分的属性。

定义 2　散列值 P_i 表示终端中的度量对象 i 特征的散列值,由 TPM 内部的散列运算计算得出,即 $\text{hash}(M_{new})$。

攻击者可以在任意时刻获得此时刻的 PCR 值,也就可以得到度量对象对应的 P_i。在终端启动阶段 M_{new} 由 TPM 度量获得。攻击者不能构造一个输出与 P_i 相同的 M'_{new},更不能由此计算出度量对象的整体。

在终端的稳定运行阶段,M_{new} 则由度量进程获得。这时 M_{new} 同样不能由 P_i 反推得到。与原 TCG 扩展方式相同,不可逆性都来源于散列运算特性。

2.3.2　PCR 值对终端状态描述的唯一性

PCR 值对状态描述的唯一性是指 PCR 值与终端状态具有一一对应关系,包括 2 层含义:相同的状态对应同一个 PCR 值;一个 PCR 值只能对应一种状态。

异或运算满足交换律使得改进的扩展方式不再具有有序性,且由每个度量对象产生的散列值应是不变的。所以改进的扩展方式下,终端处于某种状态下的 PCR 值是唯一的,第一层含义得证。

由于新的扩展方式采用了异或运算,在消除一些弊端的同时,也给攻击者提供新的攻击思路。假设攻击者可在某时刻绕开度量算法,就可以从多个度量对象入手,构造一个含有攻击组件的度量对象集合,使其最终生成的扩展值与某一正常状态下的 PCR 值相同,令该攻击集合的对外表现为正常。在此,本文从宽限度和终端内现实约束两方面对第二层含义进行了分析。

a. 宽限度分析。

新扩展方式下终端满足 $PCR_{[i]}=P_1\oplus P_2\oplus\cdots\oplus P_n$。攻击者只需要满足 $P_a\oplus P_b=P_j\oplus P_k$,攻击者就可用 P_j 和 P_k 替换 P_a 和 P_b,这样就达到了 PCR 表现出正常状态而发动了攻击的目的。

假设某状态下 PCR 的正常值 α 已确定,正常对象集合得到正确的异或运算结果 β,这时只需要令异常对象的异或运算结果 γ 满足 $\alpha=\beta\oplus\gamma$,就可以达到状态欺骗的目的。但是构造这样的 γ 同样是困难的。攻击进程散列值是固定的,为了得到 γ,必然要通过构造一个散列值满足特定要求的输入,而这样的输入是难以得到的,难度也来自于散列运算特性。因此构造上述的攻击是困难的,不会破坏 PCR 值的唯一性。

同理,攻击者甚至可以插入更多无意义的度量过程以利用异或运算尝试碰撞出特定的 PCR 值。

PCR 具有的 160 位存储空间使其描述空间大小达到 2^{160}。前文从攻击者角度分析了通过 2 步异或运算得到特定 PCR 值的情况,由于构造大量进程造成 PCR 值碰撞的攻击场景与终端正常工作情况有相似之处,在此从终端工作产生状态冲突的角度分析多步异或破坏唯一性的难度。给出以下的 2 个定义。

定义 3　状态是一个由终端中度量对象构成集合的非空子集,包含当前终端中存在的活跃的度量对象。状态实质上反映了当前终端的基本配置和正在运行的进程等情况,是对终端整体情况的描述。状态冲突指不同状态对应于同一个 PCR 值。

定义 4　度量对象分类,终端中共有 n 个度量对象,度量对象可依照度量发生的阶段被划分为启动阶段对象和运行阶段对象。其中 n_1 为启动阶段的度量对象数,n_2 为运行阶段的度量对象数,共产生 n 个不同的散列值。终端状态共 m 个,其中 m_1 为启动阶段状态数,m_2 为运行阶段状态数。每种状态都有对应计算出的 PCR 值。

假设度量对象彼此独立,终端状态数 m 可以看作是以度量对象作为元素构成的非空集合数量。n 个度量对象的前提下,在宽限度内分析 m 一定满足:

$$m\leqslant C_n^1+C_n^2+\cdots+C_n^{n-1}+C_n^n=2^n-1 \tag{3}$$

当度量对象个数 $n>160$ 时,状态数一定会在 160 位的空间中溢出,某个 PCR 值至少表示 2 种终端状态的情况即是发生状态冲突。

在终端当前不存在状态冲突的前提下,加入一个新的度量对象,执行扩展但不发生状态冲突的概率 V 可表示为:

$$V=1-\frac{M}{2^{160}} \tag{4}$$

其中,M 为当前终端状态数。在使度量对象个数接近 n 的过程中,始终有 $M\leqslant m$,那么,再扩展 n 个对象散列值之后,不发生冲突的概率 P 必定满足:

$$P\leqslant\left(1-\frac{m}{2^{160}}\right)^n \tag{5}$$

在此取 m 的最大值为 2^n-1,根据式(5)每隔 5 取 n,得到度量对象数量 n 和状态不冲突概率 P 的关系如表 1 所示,表中 P 为计算精度内得到的近似值。

由表 1 可知,理论上 n 的取值在很大范围内满足 PCR 对状态描述的唯一性。但 n 越大,对度量对

表1 n 与 P 的对应关系

Table 1 Relationship between n and P

n	P
5~105	1.0
110	0.999 999 999 999 902 300 373 832 986 224 442 720 413 208 007 812 5
115	0.999 999 999 996 731 503 415 503 539 144 992 828 369 140 625
120	0.999 999 999 890 860 635 787 248 611 450 195 312 5
125	0.999 999 996 362 021 192 908 287 048 339 843 75
130	0.999 999 878 928 072 627 459 755 494 783 166 795 969 009 399 414 062 5
135	0.999 995 976 694 511 234 939 000 132 726 505 398 750 305 175 781 25
140	0.999 866 494 444 698 328 258 880 337 671 143 934 130 668 640 136 718 75
145	0.995 584 660 051 084 369 136 731 311 300 536 617 636 680 603 027 343 75
150	0.863 677 410 672 676 892 922 083 879 966 521 635 651 588 439 941 406 25
155	0.007 291 483 623 679 124 483 063 507 256 019 875 057 972 967 624 664 306 640 625

象的设计要求会越严格,所以应该对 n 做出一定的限定。

b. 终端内现实约束分析。

考虑到终端实际环境,n 个度量对象不发生状态冲突的概率比表1中数据大。原因在于,在宽限度分析中,度量对象之间没有联系,状态数 m 都取到了可能的最大值。为了进一步讨论度量对象数量限制这个问题,将终端状态按阶段划分为2种。

在终端的启动阶段,度量对象需要按照特定的启动次序由TPM度量,状态数 m_1 随着启动度量对象的增多呈线性增长,每增加一个度量对象,状态数 m_1 加1,远小于度量对象无关联情况下的指数增长。最终启动阶段状态数 m_1 与启动阶段度量对象数量 n_1 相等。启动阶段是运行阶段的基础,所以启动阶段的度量对象一定是以整体的形式与运行阶段度量对象组合体现在PCR值中。

在终端运行阶段的主要度量对象是运行的进程,m_2 的大小在很大程度上取决于度量对象间的关系。Linux程序设计中若限定父进程结束引起某一子进程随之结束,那么代表子进程的 P_i 不会在没有父进程的情况下参与扩展。假设在 n_2 个度量对象中存在 k 种此类情况,状态量 m_2 会受到影响,有:

$$m_2 \leqslant (3^k-1)(2^{n_2-2k}-1) \tag{6}$$

对比宽限度下的 m_2:

$$m_2 \leqslant 2^{n_2}-1 \tag{7}$$

可发现状态数量减少非常明显。

采集终端作为一种专用嵌入式设备,其功能特定,进程数量也较少。如果攻击者企图加入较多虚假度量过程实现PCR碰撞,其难度在于:需要在攻击开始阶段绕开信任度量和进程数量的限制,除攻击进程外,创建尽量多的辅助进程,获得对应的散列值 P_i,并遍历辅助进程可能的组合方式以提高攻击成功的概率。进程的组合方式会随着辅助进程数的增多呈指数增长。考虑信任结构、度量算法以及攻击对计算量的要求,这种攻击方式也是困难的。可知第二层含义也满足,PCR值对终端状态描述具有一致性。

2.4 改进的扩展策略

在改进的扩展策略中,依托扩展方式中异或运算的性质,增加了进程结束时对PCR的扩展,使得被扩展的度量对象可以从PCR中消除。这种回溯性使得在进行终端本地检测时,SML只记录终端内的活跃度量对象,至多包含终端中所有组件,相比于扩展事件记录,减少了SML所用的存储空间。

而对于终端完整性的远程证明,改进策略下远程方根据SML直接使用组件预期值的异或运算结果验证当前PCR值,无需散列运算。终端在某一状态的预期值也可以使用这种方法进行快速计算。

综合来看,在完整性检测过程中,2种扩展策略的具体区别如表2所示。

表2 扩展策略比较

Table 2 Comparison of extend strategies

策略	扩展时刻	状态描述的实时性	SML空间	本地/远程散列次数	完整性检测的顺序
原有策略	启动时	非实时	与度量事件数 E 有关	E/E	SML顺序
改进策略	启动时结束时	实时	与活跃对象数 A 有关	$E/0$	无要求

2.5 可信采集终端完整性检测过程

以上是对采集终端完整性检测方案本身的改进,为了实现完整性检测,采集终端还需集成可信计算的相关技术,构建可信的终端平台。可信采集终端的整体架构如图6所示。

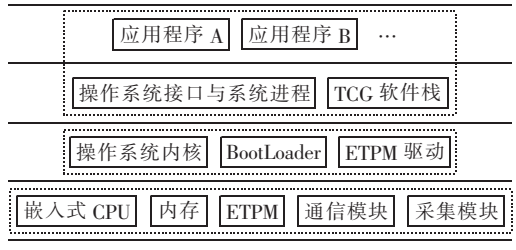

图6 可信采集终端架构

Fig.6 Architecture of trusted acquisition terminal

在可信采集终端中,嵌入式可信平台模块(ETPM)作为可信根,以总线方式集成到采集终端中,并根据终端对 TCG 软件栈 TSS(TCG Software Stack)进行适当的移植改写。上层可以通过该软件栈调用 TPM 的功能。

终端启动时,ETPM 首先进行自我验证,之后度量 BootLoader 的完整性,在 TPM 的调度下,按照组件的启动顺序在底层组件间移交控制权,按照这种方式,直到度量上层应用程序。在此期间每一个被度量组件的完整性值都要按照度量的顺序扩展到 PCR 中,TPM 根据存储的预期值与当前值做比较,判断终端当前阶段是否可信。

运行时,由于 TPM 对操作系统的主动管理性能较差,借助处理器的调度,主要的度量工作交由终端中运行的度量进程。植入动态信任度量算法的度量进程通过 TSS 对 TPM 进行扩展等操作。终端中存储度量事件的 SML 存储当前状态下平台的启动配置和所有活跃进程。已经结束的进程或者需要删改的组件,其度量值需要重新扩展到 PCR 中,以消除对值的影响,并在 SML 中删除该对象,使得当前 PCR 值能够实时体现当前终端状态。

3　结语

在智能电网推动信息物理融合的大背景下,必须重视用电信息采集终端的安全性。本文参考 PC 和嵌入式系统对可信计算完整性检测的应用和改进,提出了一种基于可信计算的用电信息采集终端完整性检测的方案。该方案从信任结构、PCR 扩展方式、扩展策略三方面入手改进了原 TCG 的方案。总体上,新的终端完整性检测方案在对计算资源、存储空间的占用上都有所优化,为动态信任度量提供了支持。

参考文献:

[1] 王中杰,谢璐璐. 信息物理融合系统研究综述[J]. 自动化学报,2011,37(10):1157-1166.
WANG Zhongjie,XIE Lulu. Cyber-physical systems:a survey[J]. Acta Automatica Sinica,2011,37(10):1157-1166.

[2] 胡江溢,祝恩国,杜新纲,等. 用电信息采集系统应用现状及发展趋势[J]. 电力系统自动化,2014,38(2):131-135.
HU Jiangyi,ZHU Enguo,DU Xingang,et al. Application status and development trend of power consumption information collection system[J]. Automation of Electric Power Systems,2014,38(2):131-135.

[3] 高昆仑. 电力信息物理系统安全研究[J]. 中国信息安全,2013,2:86-87.
GAO Kunlun. Research on electric power cyber-physical system security[J]. China Information Security,2013,2:86-87.

[4] 沈昌祥. 构建积极防御综合防范的防护体系[J]. 电力信息化,2004,2(4):18-19.
SHEN Changxiang. Construction of the protective system of active defense[J]. Electric Power Informatization,2004,2(4):18-19.

[5] 张明远,徐人恒,张秋月,等. 智能电能表数据安全性分析[J]. 电测与仪表,2014,51(23):24-27.
ZHANG Mingyuan,XU Renheng,ZHANG Qiuyue,et al. Data communication security analysis of the smart electric energy meter[J]. Electrical Measurement & Instrumentation,2014,51(23):24-27.

[6] 郜盼盼. 智能电网系统中面向用电信息安全防护的认证加密系统研究[D]. 北京:北京邮电大学,2013.
GAO Panpan. Research on authentication encryption system for the security protection of smart grid electric data[D]. Beijing:Beijing University of Posts and Telecommunications,2013.

[7] 张恒. 信息物理系统安全理论研究[D]. 杭州:浙江大学,2015.
ZHANG Heng. Research on security theory for cyber-physical systems[D]. Hangzhou:Zhejiang University,2015.

[8] 李钊,彭勇,谢丰,等. 信息物理系统安全威胁与措施[J]. 清华大学学报(自然科学版),2012,52(10):1482-1487.
LI Zhao,PENG Yong,XIE Feng,et al. Security threats and measures for the cyber-physical systems[J]. Journal of Tsinghua University(Science and Technology),2012,52(10):1482-1487.

[9] 汤奕,陈倩,李梦雅,等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化,2016,40(17):59-69.
TANG Yi,CHEN Qian,LI Mengya,et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems,2016,40(17):59-69.

[10] 苏盛,吴长江,马钧,等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术,2014,38(11):3115-3120.
SU Sheng,WU Changjiang,MA Jun,et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]. Power System Technology,2014,38(11):3115-3120.

[11] 吴长江. 电力 CPS 网络攻击模式分析与智能电表入侵检测方法研究[D]. 长沙:长沙理工大学,2015.
WU Changjiang. Analysis on cyber-attack mode to cyber-physical system and the smart meter research on intrusion detection[D]. Changsha:Changsha University of Science & Technology,2015.

[12] 李桥,胡德鹏. 嵌入式系统的安全方法研究[J]. 网络安全技术与应用,2009,7:36-38.
LI Qiao,HU Depeng. Research on security of embedded system[J]. Network Security Technology and Application,2009,7:36-38.

[13] 吴悠,李光,刘绍方,等. 嵌入式 TPM 及信任链的研究与实现[J]. 计算机工程与设计,2012,33(6):2229-2235.
WU You,LI Guang,LIU Shaofang,et al. Study and implementation of embedded TPM and chain of trust[J]. Computer Engineering and Design,2012,33(6):2229-2235.

[14] 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):2089-2091,2101.
WANG Yu,WANG Zhenyu,YAO Lining. Design and implementation of TPM extension and trusted bootstrap on embedded platform[J]. Computer Engineering and Design,2009,30(9):2089-2091,2101.

[15] 徐明迪,张帆. 可信计算技术在嵌入式操作系统中的应用[J]. 武汉大学学报(理学版),2014,60(3):237-241.

XU Mingdi,ZHANG Fan. Application of trusted computing technology in embedded real-time operating system[J]. Journal of Wuhan University(Natural Science Edition),2014,60(3):237-241.

[16] 张洵. 可信嵌入式TPM技术研究[D]. 西安:西安电子科技大学,2014.
ZHANG Xun. Research of embedded trusted platform module [D]. Xi'an:Xidian University,2014.

[17] 赵波,张焕国,李晶,等. 可信PDA计算平台系统结构与安全机制[J]. 计算机学报,2010,33(1):82-92.
ZHAO Bo,ZHAGN Huanguo,LI Jing,et al. The system architecture and security structure of trusted PDA[J]. Chinese Journal of Computers,2010,33(1):82-92.

[18] 徐开勇,尚金,杨天池,等. 基于混合信任链和特征预制的主动度量模型[J]. 计算机应用研究,2015,32(6):1791-1795.
XU Kaiyong,SHANG Jin,YANG Tianchi,et al. Active measurement model based on mixed-chain & character pre-setting[J]. Application Research of Computers,2015,32(6):1791-1795.

[19] ZOBRIST A. A new hashing method with application for game playing[D]. Madison,USA:University of Wisconsin,1970.

作者简介:

张少敏

张少敏(1965—),女,河北保定人,教授,博士,主要研究方向为电力信息化与信息安全(**E-mail**:zhangshaomin@126.com);

王志男(1992—),男,河北保定人,硕士研究生,主要研究方向为电力信息化与信息安全(**E-mail**:969070491@qq.com);

王保义(1964—),男,山东栖霞人,教授,博士,主要研究方向为电力信息化与信息安全(**E-mail**:wangbaoyi@126.com)。

Terminal integrity detection scheme of electricity information acquisition system based on trusted computing

ZHANG Shaomin,WANG Zhinan,WANG Baoyi

(School of Control and Computer Engineering,North China Electric Power University,Baoding 071003,China)

Abstract: Aiming at the information security risks faced by terminals of cyber-physical electricity information acquisition system,a terminal integrity detection scheme based on trusted computing is proposed to ensure the security of terminals considering the characteristics of acquisition terminals. The detection scheme of trusted computing group is improved from three aspects,i.e. trust structure,extended mode of trusted platform module and extended strategy,to reduce the loss of trust transmission and improve the computing flexibility of extension. Based on the verification of the proposed extension mode's feasibility and security,a new extension strategy is designed. Compared with the original scheme,the proposed scheme can optimize the computing resource and storage space to a certain level and can provide a dynamic trust measurement method for terminals.

Key words: cyber-physical system; electricity information acquisition; integrity detection; trusted computing; trust structure; extension mode; extension strategy