可信计算度量机制在信任链中的应用

韦荣 鞠磊 方勇[1,2] 杨波[1,2]
1 西安电子科技大学 陕西 710071
2 北京电子科技学院 北京 100070

摘要：本文介绍了可信计算的相关概念，以及其核心的信任链理论，具体描述了可信度量机制在信任链传递实际过程中的应用，为利用可信计算技术解决信息安全问题的研究提供了实际可行的参考实现方案。

关键词：可信计算；信任链；可信度量

0 引言

信息安全备受关注的今天，如何解决终端安全、网络安全已经成为迫在眉睫的问题。“可信计算”正在这方面研究的一个热点问题，它通过硬件结构和底层软件为基础的综合措施，来提高信息系统的安全性。本文研究可信计算中的信任链传递相关的内容，描述了一个运用度量来实现信任传递的方案。

1 可信计算概念

可信计算的推行以及规范标准的制定主要得益与TCG (trusted computing group)，该组织的前身是TCPA(trusted computing platform alliance)，集合了IBM、Intel及Microsoft等著名厂商。其理念是在PC的硬件平台上引入安全芯片架构，通过提供的安全特征来提高终端系统的安全性。可信计算平台以密码技术为支持、安全操作系统为核心，提供以下功能：

(1) 可信计算平台对用户身份的鉴别。

(2) 可信计算平台内部各元素之间存在严密的互相认证。

(3) 可信计算平台具备在网络上的惟一的身份标识。

可信计算体系中关键的部件是TPM (Trusted Platform Module)。它是一个带密码运算功能的安全微控制器，通过LPC(Low Pin Count)总线与PC芯片集结合。总体的架构组成有：负责管理通信总线的I/O部件，密码协处理器，密钥生成器，HMAC引擎，负责产生各种运算所需随机数的随机数发生器，完成一种基本的HASH运算的SHA－1引擎，感应任何电源状态变化的电源检测，选项控制，执行部件，存储器等。若干部件构成一个有机统一的安全执行环境，使TPM成为具有高集成度的嵌入式芯片部件。

另外一个重要的部件是TPM平台上的支撑软件TSS (TCG Software Stack)。其作用主要是为其他软件提供方便和统一使用标准TPM接口。把不涉及根本信任性的功能放到TPM以外的比TPM处理能力与存储能力更大的主处理器中，这样就能够很好的解决了经济方便性与功能性之间的矛盾。

2 信任链理论

信任链的理论是信息安全借鉴而来的一种机制，是可信计算概念的原理核心。它通过引入硬件上的安全芯片，从最原始的物理安全角度，建立一个信任根。再建立一条信任链。从信任根开始到硬件平台、到操作系统、再到应用系统，一级度量认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。

可度量的核心信任源CRTM(Core Root of Trust for Measurement)和可信计算模块TPM，是主板上惟一的可信组件，且CRTM到TPM之间的联结通过可信的传递建立。CRTM是可度量的信任根，即信任链的源头，平台复位后的执行必须从CRTM开始。CRTM可以有两种存在形式，一种是指BIOS的引导模块，即将BIOS分成BIOS引导模块和POST BIOS两部分，它们可单独升级而互不影响；另一种情况下CRTM就是整个BIOS，作为一个整体升级、修改和维护。

信任链的理论采用了硬件和软件技术相结合的方式来保证系统可信，PC启动应遵从如下流程来建立信任链：

(1) PC被加电；

(2) TCPA认证的BIOS启动模块(BIOS Boot Block)和TPM建立一个通话，确保BIOS是可信赖的；

(3) BIOS确认用户的使用授权；

(4) BIOS与TPM和OS loader通信，确保OS loader是可信的；

(5) 然后OS loader与OS kernel建立通话。OS kernel装入以后，它就知道在它之前有哪些软件被运行。可以看出，在TPM的控制下，BIOS将信任传递给BOOT loader，BOOT loader将信任传递给OS loader，OS loader将信任传递给OS，OS同样将信任传递给应用程序。整个信任链的创建过程如图1所示。

作者简介：韦荣(1982-)，男，西安电子科技大学通信学院2005级硕士研究生，研究方向：网络安全。鞠磊(1976-)，男，博士，北京电子科技学院讲师。方勇(1963-)，男，北京电子科技学院教授，硕士生导师。杨波(1982-)，女，西安电子科技大学通信学院2005级硕士研究生，研究方向：网络安全。

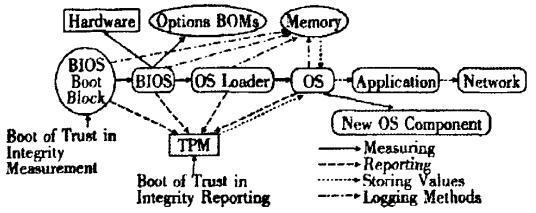

图1 信任链的建立过程

3 度量方法在信任链中的应用

在信任链的理论中，无论是最底层的BIOS启动模块还是到最上层的应用，在得到信任以运行之前，都需要经过度量，即一个测量或者认证的过程。数据完整性度量技术通过消息认证码MAC(Message Authentication Code)的一致性校验来实现度量的功能。这是现在主流的度量技术方法。对于MAC的产生，可以利用强的分组密码或者利用Hash函数来实现。TPM中提供了满足单向性、抗碰撞性的安全Hash函数SHA-1引擎，可以为度量的实现提供保证。

同时TPM还提供安全存储以及内部的平台配置寄存器PCR(Platform Configuration Register)，这样配合TPM的内部TPM_Extend命令就可以把信任链传递下去。TPM_Extend命令操作把当前的PCR值和新计算的值合并一起再调用SHA1运算，即使用SHA1(SHA1(SHA1(0+m1)+m2)+mi)的方式，计算出新的PCR值，更新PCR。这样每个更新的PCR值都是在前面已经度量过的PCR值以及新一轮度量的新计算值的基础之上产生，保证了信任链是从源头传递上来的。

具体实现过程如下：

(1) 对BIOS的度量：BIOS启动模块经过TCPA认证，确保PC被加电之后处于信任链的源头，之后对BIOS实行度量。在此之前应该对BIOS进行采样，与标准的BIOS样品库进行比较，并在BIOS漏洞库的基础上对BIOS进行安全性分析，根据最终生成的分析报告确定BIOS是否安全。对于安全的BIOS代码进行SHA1运算，得出的MAC作为此后完整性度量的依据。如果度量通过，PCR的状态更新为BIOS度量的记录。

(2) 对OS Loader的度量：BIOS运行完成硬件自检之后，在启动系统之前，首先对OS Loader进行完整性度量。真正的OSLaoder是主引导记录(MBR)中的主引导程序，所以对OSLoader的度量是通过MBR进行HASH函数校验保护来实现的，其HASH值还可以存储在主引导记录的备用存储区内。

(3) OS loader对操作系统进行度量：WINDOWS分区中的第一个扇区为引导记扇区BOOT，引导扇区由磁盘参数表和引导记录(BR)构成，系统的度量需要考虑引导记录、程序文件和存档性数据文件等方面的度量。但是WINDOWS是不开放源代码的系统，对其进行度量的难以实现。

Linux是开放源代码的操作系统，可以通过以下方案完成度量。

Linux内核文件(vmlinuz和initrd)进行完整性验证，当验证通过则将控制权交给Linux操作系统，否则中断引导过程。

Linux内核函数(start_kernel)启动进程(init)，init函数将获得该进程的控制权，该函数最后启动init程序，所以在execve函数增加了一个度量过程修改init程序中的read_inittab函数增加对/etc/inittab文件以及记录行iR (inittab Record)的完整度量。

对系统初始化/etc/rc.d/rc.sysinit和/etc/rc.d/rc脚本进行度量。

xinetd为Linux的网络服务管理程序。xinetd.conf则是xinetd的配置文件。我们将度量代码加入到xinetd程序中，只度量那些启动的服务程序的完整性。

(4) 操作系统系统对应用软件的度量。

软件数据完整性是信息安全的重要部分，但是，软件数据完整性还不能保证动态的安全性。所以上层应用软件的度量除了完整性检测度量之外，还需要借鉴其他一些度量方法。

随着现代软件的功能越来越完善，软件代码的规模也越来越庞大，需要度量的数据量也超乎寻常，需要对软件程序有所选取地进行度量过程。通过层次分析法，尽可能多地列举多种可能的度量方面，并计算出每个方面的权重值，以确定最重要的度量点。

其次对应用软件进行可信等级划分，对于基本不可信以及可信程度低的软件，则不能通过度量。另外因为软件的模糊性，需要引入专家评估系统，对应用软件的等级进行认定。只有通过完整性检验并且等级被认定为可信的软件才能得到操作系统的授权运行。

4 结束语

本文介绍了可信计算以及可信计算中重要的信任链理论，并通过一个具体实现信任链过程的应用方案，描述了度量方法在信任链实现过程中如何被使用的细节。可以看到通过信任链传递而启动的应用软件经过了层层的安全度量，其中任何一个环节出现错误，不论是因为病毒篡改了程序导致完整性检测不能通过还是软件可信度没有经过评估测试，都将导致信任链的终止，使得被破坏或者被感染的程序无法运行，从而保证了安全。这对计算机安全以及网络安全的提高有着重大的意义。

参考文献

[1]孔维广.可信计算平台的工作原理与应用研究.武汉科技学院学报. 2003.6.

[2]谭兴烈.可信计算平台中的关键部件TPM.信息安全与通信保密.2005.2.

[3]徐娜,韦卫.基于安全芯片的可信平台设计与实现.计算机应用研究.2006.8.

可信计算度量机制在信任链中的应用

作者： 韦荣， 鞠磊， 方勇， 杨波
作者单位： 韦荣(西安电子科技大学通信学院,陕西,710071)， 鞠磊(北京电子科技学院,北京,100070)
， 方勇,杨波(西安电子科技大学,陕西,710071;北京电子科技学院,北京,100070)
刊名： 网络安全技术与应用
英文刊名： NETWORK SECURITY TECHNOLOGY & APPLICATION
年，卷(期)： 2008，(5)
引用次数： 0次

参考文献(3条)

1. 孔维广 可信计算平台的工作原理与应用研究[期刊论文]-武汉科技学院学报 2003(6)

2. 谭兴烈 可信计算平台中的关键部件TPM[期刊论文]-信息安全与通信保密 2005(2)

3. 徐娜.韦卫 基于安全芯片的可信平台设计与实现[期刊论文]-计算机应用研究 2006(8)

相似文献(10条)

1. 期刊论文 徐明迪.张焕国.严飞.XU Ming-Di.ZHANG Huan-Guo.YAN Fei 基于标记变迁系统的可信计算平台信任链测试 -计算机学报2009,32(4)

可信计算是当今世界信息安全领域的重要潮流之一.根据国家有关规定,信息安全产品需要经过测评认证,但目前国内外对可信计算测试的理论与技术研究还非常不完善,也无相应测试工具或系统,这必然影响可信计算的发展.该文着眼于规范定义的信任链行为特征,以进程代数作为指称语义描述工具,以标记变迁系统作为操作语义,对规范定义的信任链行为特征进行了形式化描述,提出了一种基于标记变迁系统的信任链测试模型框架.针对信任链规范与实现之间的问题,从易测性出发对测试集进行了有效约简;并论证了信任链的规范实现与规范说明之间的关系,为测试用例构造方法提供了理论依据,从而解决了信任链测试这一难题.

2. 学位论文 王君毅 可信计算平台中信任链的可信赖性度量指标与方法研究 2007

随着人们对可信计算的需求日益迫切，互联网，金融，电信，广电等许多丰富的应用也都要求可信安全计算环境。事实上，目前很多这类计算是处于不可信的环境之中的，或者说可信计算平台的成熟程度还不足以支持这些丰富多彩的应用，这是一个日益严峻的问题。 本文通过对可信计算平台和度量理论的研究，首先提出可信计算平台的度量属性，度量子属性，度量指标；其次，搞清楚一般可信(安全)平台的软硬件架构；最后，应用形式化的方法来对可信平台进行度量。 本文主要采用了以下研究方法：第一：理论引申法；第二：抽象分析法；第三：形式化的分析方法；第四：综合的分析法；并得出了以下创新成果：第一，找出了可信计算平台的八个度量属性／子属性；第二，找出了可信计算平台的八个度量元；第三，将形式化证明的方法用于表示可信平台的度量。

3. 期刊论文 谭良.徐志伟.TAN Liang.XU Zhi-wei 基于可信计算平台的信任链传递研究进展 -计算机科学 2008,35(10)

信任链传递问题是可信计算的基本问题.阐述了信任链传递在技术与理论方面的最新研究进展.通过分析信任链传递的技术方案、可信测量技术、信任链理论和信任链的可信度度量理论,提出了值得研究的理论与技术方向,包括:以可信静态测量、可信动态测量技术等为代表的信任链传递关键技术,以信任链层次理论模型、信任链传递中的信任损失度量理论和软件的动态可信度度量理论等为代表的基础理论.

4. 期刊论文 王江少.余综.李光.WANG Jiang-shao.YU Zong.LI Guang 可信计算之信任链技术研究 -计算机工程与设计2008,29(9)

可信计算近年发展迅速,被认为是最有可能从根本上解决计算机系统安全问题的一种方案,不同于传统信息安全解决办法,它以新的思路即主动防御来解决计算机和网络系统的信息安全问题.信任根和信任链是可信计算的根本组成部分.介绍了可信计算及信任链的相关知识,介绍了信任根,可信认证机制.最后详细给出了基于PCI扩展ROM的可信计算之信任链部分链实现的可行方案.

5. 学位论文 代星科 可信计算中基于JVM构建完整信任链的研究与设计 2008

可信计算是指在计算和通信系统中使用具有安全硬件模块支持的可信计算平台，通过增强现有终端体系结构的安全性来提高整个系统的安全。可信计算组织TCG(TrustedComputingGroup)制订了可信计算硬件平台的相关技术规范，但只有硬件平台的可信整个系统还是不安全的，需要制定配套的操作系统和应用软件等的可信机制。 以电子信息产业发展基金(HO4010601W060692)为背景，本论文的研究工作致力于使用可信计算的思路增强现有终端的安全性，研究实现TCG规范中未涉及的后续软件部分的信任链构建过程，基于java虚拟机(JVM)设计一条从硬件到软件的完整信任链，最终实现java程序的可信执行环境。 文中分析了信息安全技术的现状和发展要求，阐明了终端安全研究的思路和技术发展方向，详细介绍了TCG提出的可信计算的概念，构成和目前的研究进展情况。最终通过分析改造java程序的启动执行流程中涉及到的两个关键部件(JVM加载器和JVM的类加载子系统)，提出了一种在可信PC硬件平台、linux操作系统以及java程序运行时环境JRE6下构建一条完整的信任链，实现java程序认证执行环境“可信JVM”的设计。在构建过程中通过使用可信平台模块提供的密码服务和安全存储功能，采用了在应用程序模块加载执行前插入控制点实现完整性状态信息的度量验证技术。通过实际测试，验证了该信任链系统具备的可信属性。在该环境中可以避免非信任软件或者被非法篡改的信任软件执行，从而防止恶意软件的攻击或者病毒传播，并具备了对当前的完整性信息的报告证实能力。 本文的主要贡献包括： 1.针对TCG规范中未涉及应用软件的可信机制，提出了一种基于JVM构建完整信任链的设计，对进一步研究可信计算与软件可信技术有一定的指导意义和参考价值； 2.结合TCG规范修改JVM，实现了java程序的可信执行环境“可信JVM”，为可信计算平台下实现java应用程序的可信提供了一套完整的、跨平台的设计思路。通过使用可信硬件平台的功能，“可信JVM”可以根据可信类列表在现有的iava安全模型下提供安全性更强控制更严格的安全策略。

6. 期刊论文 郜伟.何静.GAO Wei.HE Jing Vista中信任链建立机制研究 -计算机工程与设计2009,30(15)

信任链机制是Vista建立可信环境的基础,对其实现过程及安全性分析将为Vista的安全评估提供重要依据.针对Vista中信任链的建立过程,对可信计算机制在Vista中的实现进行了详细的分析,并通过逆向工程的手段对Vista信任链建立过程中的相关代码进行了剖析,给出它们的实现方式和主要的工作流程.并对Vista信任链机制的安全性进行了分析,给出其安全隐患.

7. 期刊论文 陈书义.闻英友.赵宏.CHEN Shu-yi.WEN Ying-you.ZHAO Hong 基于模糊集合的可信计算信任模型评估

-计算机科学2008,35(11)

可信计算是信息安全的重要研究领域,而信任模型的可信性评估是该领域中亟待解决的关键问题.在深入研究可信计算信任根、信任链及其可信性影响因素的基础上,提出了基于模糊集合理论的可信计算信任模型评估方法.基于模糊集合理论的评估方法定义了不同的可信度度量规则和模糊集合,基于计算得到的可信度,评价信任模型的可信性.分析结果表明,基于模糊集合的信任评估方法能够有效评估可信计算信任模型的可信性,丰富了可信计算信任评估理论.

8.期刊论文 石文昌.单智勇.梁彬.梁朝晖.董铭.SHI Wen-chang.SHAN Zhi-yong.LIANG Bin.LIANG Zhao-hui.DONG Ming 细粒度信任链研究方法 -计算机科学2008,35(9)

分析信任链相关研究的当前发展水平,提出细粒度信任链和细粒度系统软件信任链的思想,阐明只有细粒度信任链才能描述现实应用的真实情况.根据问题空间的复杂性,提出细粒度信任链建模的问题分解方法.该方法通过逐步拓展的策略,首先建立细粒度系统软件信任链模型,然后在此基础上建立完全的细粒度信任链模型.

9.期刊论文 胡小冰.冯广 基于可信计算的网络信任管理系统 -广东工业大学学报2009,26(3)

对可信计算平台的应用和实施作了初步探讨,指出可信计算平台应用的基本目标就是要把信任链延伸到网络上,并构建网络信任管理系统.基于网络信任管理系统结合信息保密网的应用给出可信计算平台的应用方案.在研究整体信任解决方案后,使用信任延伸模型计算信任值.此方案在广东工业大学研究生管理系统中得到了应用.

10.期刊论文 李晓勇.韩臻.沈昌祥.Li Xiaoyong.Han Zhen.Shen Changxiang Windows环境下信任链传递及其性能分析 -计算机研究与发展2007,44(11)

动态多路径信任链(DMPTC)是一个基于软件类型特点的系统可信验证和保证机制.DMPTC对静态的系统软件和动态的应用软件加以区分,并采用不同的方式和策略对软件的装载运行加以控制,使得计算平台只运行那些有可信来源的可执行代码,从而确保平台的可信和安全.DMPTC可以用来防范各种已知和未知的恶意代码,并可以用来加强对生产信息系统中应用软件的管理和控制.DMPTC可以克服传统的静态单路径信任传递在系统灵活性和实用性层面的缺陷,并且在系统性能方面进行了深入的考虑和深层的优化.系统性能分析和实际测试结果都表明,在Windows系统平台上实现的DMPTC对系统运行带来的性能损失小于1%.