基于可信计算平台的信任链传递研究进展*)

谭 良[1,2] 徐志伟[1]

(中国科学院计算技术研究所 北京 100080)[1] (四川师范大学计算机学院 成都 610066)[2]

摘 要 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。

关键词 可信计算,信任链,可信测量,可信传递

Development of the Transitive Trusted Chain Based on TPM

TAN Liang[1,2] XU Zhi-wei[1]

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing100080, China)[1]

(College of Computer, Sichuan Normal University, Chengdu 610066, China)[2]

Abstract The issue of the transitive trusted chain is the foundation for trusted computing. This paper surveys the technologies and the theories of the transitive trusted chain, including the technology projects of the transitive trusted chain, the technologies of the trust for measurement, the theories of the transitive trusted chain and the trust for measurement. Some fields are worthy to be explored are pointed out including some key technologies, such as the static trust for measurement and the dynamic trust for measurement, and some foundation theories, such as the level model of the trusted chain, the trust loss model and the theory of the dynamic trust for measurement for software, and so on.

Keywords Trusted computing, Trusted chain, Trust for measurement, Transitive trust

1 引言

在基于网络或 Internet 的信息系统中,终端计算机系统最常用的是微机。对于最常用的微机,只有从芯片、主板等硬件 BIOS、操作系统等底层软件综合采取措施,才能有效地提高其安全性,正是基于这一技术问题催生了可信计算的诞生[1-3],其基本思想是在计算机系统中首先建立一个信任根,再建立一条信任链,一级测量认证一级,一级信任一级,把信任关系扩大到整个计算机系统,从而确保计算机系统的可信[1-3]。因此,信任根和信任链传递是可信计算的基本问题。

在技术领域,信任链传递技术得到了广泛的研究和较大的发展。TCPA 和 TCG 已经制定了关于可信计算平台技术规范[1]。在该规范中,解决了系统可信根的问题,提出了可信传递的概念,阐述了系统从加电开始应该如何开展可信度量,并将系统运行控制权转移到操作系统直至应用的基本原则和过程。就这一过程,许多学者在不同的平台上,特别是 Linux 平台开展了的研究,取得了一些的成果[4-9]。另外,文献[10]还对可信启动过程中 CPU 和可信硬件(类似于可信计算平台模块 TPM)之间的工作方式、可信测量以及备份与恢复进行了详细的分析和讨论。2004 年 10 月武汉瑞达公司和武汉大学合作研制出的我国第一款可信计算机[17],它在系统结构和主要技术路线方面与 TCG 的规范是一致的,在有些方面有所创新,在有些方面也有差异。该可信计算机在主板上嵌入 ESM 模块(Embedded security module),并以 ESM 为信任根。目前无论是国外还是国内的可信计算机都没能完全实现 TCG 的 PC 技术规范[2,3]。

在理论领域,无论是国外还是国内,在可信计算领域都处于技术超前于理论,理论滞后于技术的状况。可信计算的理论研究落后于技术开发。对信任链传递的理论研究也不例外[2-3]。信任链传递的理论研究包括两个方面,一是信任链的可信度量理论,二是信任链理论模型。文献[8]和文献[10,11]分别对这两方面进行了讨论。

本文综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。

2 信任链传递的基本概念

在可信计算平台中,信任链的建立与传递涉及到三个基本的概念,一是信任根;二是可信传递;三是可信测量。下面分别介绍这三个概念。

2.1 信任根

所谓信任根,就是系统可信的基点。TCG 认为一个可信计算平台必须包含 3 个信任根:可信测量根 RTM(root of trust for measurement)、可信存储根 RTS(root of trust for

*)基金项目:四川省科技攻关项目 2008JY0105-2 支持。谭 良 副教授,博士,主要研究方向为信息安全、分布式计算;徐志伟 研究员,博士生导师,主要研究方向为网络计算、信息安全、分布并行计算。

storage)和可信报告根 RTR(root of trust for reporting)。而信任根的可信性由物理安全和管理安全确保。

2.2 可信传递

所谓可信传递,就是可信根确定其下一级功能的可信度,如果可以接受,则可信范围就从可信根扩大到下一级功能,同样,第二级功能如果确定第三级功能可信,可信范围就扩大到第三级功能,这个过程不断重复。通过可信传递,可以实现系统可信范围的延伸。

2.3 可信测量

所谓可信测量,就是对代码程序及其相关配置信息进行完整性验证。可信测量是可信计算的基础。TCG 在可信 PC 技术规范中,具体给出了可信 PC 中的信任链。这个信任链以 BIOS Boot Block 和 TPM 芯片为信任根,经过 BIOS→OS loader→OS。沿着这个信任链,一级测量认证一级,一级信任一级,以确保整个平台的系统资源的完整性。

3 信任链传递的实现技术

信任链传递的实现技术包括两个方面,一是对信任链传递技术方案的研究;其次是对可信测量的研究。

3.1 信任链传递的技术方案[11]

3.1.1 TCG 方案

如图 1 所示,这个信任链以 BIOS Boot Block 和 TPM 芯片为信任根。其工作原理为:通过不断可信测量递交的可信报告,实现一个实体与预期值的充分匹配来了解信息平台的可信程度。RTM 实现可靠平台测量,将测量结果输送给 RTR;RTP 防止非授权改变测量结果并可靠报告这些测量结果;RTS 提供最小数量的存储方法。可信测量根和可信报告根联合起来提供了平台的当前计算环境的测量数据,并可以访问这些测量结果而且将结果与期望的值比较,考察平台操作是否是期望的。如果测量结果与期望值充分匹配,那么这个实体可以再可信计算。由于这种测量和报告可以长期记录,因此为维护系统完整提供了必要的信息。

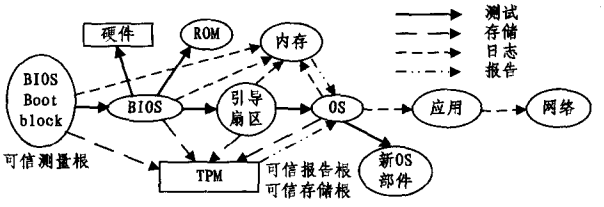

图 1 TCG 的信任链传递方案

3.1.2 第三方测试方案

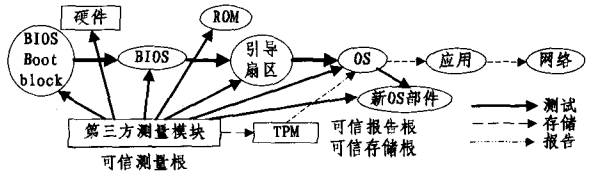

图 2 第三方的信任链传递方案

如图 2 所示,这个信任链以第三方测试模块和 TPM 芯片为信任根。其工作原理与 TCG 方案基本相同,主要不同点在于测试模块发生了变化。TCG 采用 BIOS Boot Block 作为测试模块,而该方案采用第三方的测试模块。TCG 方案实际上是跨国公司的方案。对于大多数国家来说,因为没有计算机核心系统软件技术,所以无法实现国家的信息安全。但是,大多数国家都可以采用这一种方案,即采用第三方的测试方法设计可信平台的测试模块和 TPM 模块。

3.1.3 多代理扩展方案

如图 3 所示,这个信任链仍然以第三方测试模块和 TPM 芯片为信任根。其工作原理与前两种方案基本相同。主要不同点在于增加了测试代理和 TPM 代理对本地应用和网络应用进行测试。前两种方案会遇到测试和报告的方法选择问题,这种选择的困难表现在可信测试和报告服务集中模式(TPM)上。如果这种芯片测试控制在操作系统以内,而所有的应用系统由测试根和报告根委托的代理去实现,方案就会进一步完善。多代理扩展方案就是这样的方案。

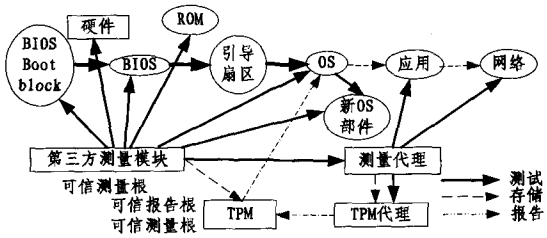

图 3 多代理扩展方案

如果在上述的可信测试链中能够掌握其中 BIOS,那么对于操作系统的测试就可以有两种方案:1)由测试芯片测试;2)由 BIOS 测试,再考虑可信根委托的应用测试的代理化,则多代理扩展方案不仅仅是跨国公司方案,而且也是国家和中小企业的安全方案。这样才能说 CPU、操作系统是跨国公司的,而 BIOS、系统的监控和监管平台是各自的。

3.1.4 三种方案的比较

表 1 是对 TCG 方案、第三方测试方案和多代理扩展方案的比较。

表 1 三种方案的比较

	可信测量根	可信报告根	可信存储根	可扩展性	适用范围
TCG 方案	TPM	TPM	TPM	一般	拥有计算机核心技术的跨国公司的安全方案
第三方测试方案	第三方测量模块	TPM	TPM	较好	大多数国家的安全方案
多代理扩展方案	第三方测量模块,测量代理	TPM,TPM 代理	TPM	好	跨国公司、国家和中小企业的安全方案

3.2 可信测量

在终端 PC 上通过可信测量(完整性)进行可信传递包括两个过程,其一是从终端加电到操作系统装载(称之为系统引导)。该过程是一个顺序固定的单一链式过程,而且 BIOS、操作系统装载器以及操作系统一般相对稳定,在此可信传递过程的完整性测量相对容易。这一过程的完整性度量称为静态可信测量。其二是从操作系统到应用程序。由于终端平台上的应用具有多样性和无序性等特点,系统可信引导的单一链式验证机制并不适用于操作系统到应用之间的可信传递。这一过程的完整性测量称为动态可信测量。

3.2.1 静态可信测量过程

目前,针对通过静态可信测量进行可信传递这一过程,国内外在不同的平台上开展了相应的研究工作。

AEGIS[4]是一个在 FreeBSD 系统上实现了从系统加电到应用程序层逐级安全验证的原型系统,它将系统启动的过

程分为五个级别，BIOS 的核心代码构成了第零级别，这部分代码被安全存放并被无条件信任。按照系统启动的流程，在将控制传递到下一个级别代码前，首先对代码进行完整性验证，验证通过才能将控制向下传递，依此类推，若某一个环节的验证失败，则强制通过预先的备份数据进行恢复。作为一个原型系统，其思想是值得借鉴的。

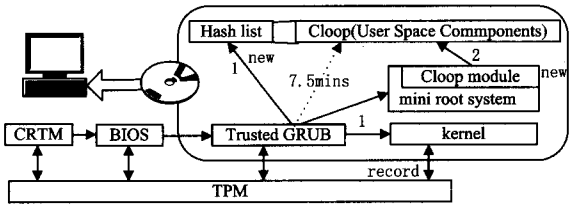

图 4　在 Linux 基于可信 CD 的可信启动过程

文献[5]也在 Linux 平台上设计与实现了可信启动过程，与其它在 Linux 平台上实现可信启动的文献不同的是，该启动过程不是基于硬盘，而是基于一个可信的 CD。

文献[6]在 Linux 平台上利用 TPM 提供的可信计算和保护存储功能，结合 TCG 规范中可信度量和可信链的思想，设计了可信启动过程 TSPL，并实现了原型。设计中充分考虑到启动过程的复杂性和度量数据的多样性，不仅度量了程序代码，还对影响执行程序行为的配置文件和环境数据进行了度量。

文献[7]比较了 Linux 平台的安全加载和可信加载的异同，如表 2，TCG patch for GRUB 是在 Linux 平台上实现可信加载的一个参考实现。

表 2　启动过程的比较

	Security Features					
	Software			Hardware		Ease of Management
	CRC ECC	Hash	Signa ture	Write Protected Bootloader	TPM	
Normal Boot	○	—	—	—	—	Easy, but no protection
Secure Boot (by diges)		○		Root of Trust (Reference Value)		Bad
Secure boot (by signature)		○	○	Root of Trust (Singer's public key)		Good +Easy to update OS image without modifying Bootloader Good(for connected device)
Trusted Boot		○		Root of Trust	Root of Trust (Secure Storage)	+Device Authentication +Integrity Protection +Integrity Report

文献[8]基于信任根和信任链的概念，利用可信服务器，结合系统的引导过程，提出了一种基于可信服务器的可信引导方案。该方案在引导过程中每次进行控制权转移时，对将要转移到的下一层，进行完整性验证。如验证通过，方进行控制权的转移。这样，系统的引导过程将按照信任链的传递进行，系统的引导处于一种可信的状态，成为一个可信的引导，从而使得整个系统的安全性得到极大的增强。同时，该可信引导方案还具有易实施及灵活的特点。

文献[9]对操作系统的完整性度量提出了可信保证策略：信任链传递关系建立在信任根、时间和空间的隔离关系和验证关系之上。

文献[10]对操作系统的可信启动过程，CPU 和可信硬件(类似于 TPM)之间的工作模型进行了深入的研究，提出了一种并行可复原可信启动过程。

总之，从世界范围内看，在静态可信测量的技术方面展开的研究是最多的，取得的成果也是最多的。但是，到目前为止，终端 PC 都没能完全实现 TCG 的 PC 技术规范，如存储、报告机制、安全 I/O 等。

3.2.2　动态可信测量过程

由于动态测量测量的不再是程序的静态结构，而是程序的动态结构，因此，软件的可信动态测量问题是一个复杂的问题。那么，怎样来测量应用程序的动态结构呢？由于软件的代码结构复杂，一个软件的构成通常包括代码和资源，而代码中往往涉及到静态函数库、动态函数库、第三方接口和一些依赖于平台的接口。也就是说，一个在操作系统中处于等待调度的应用程序的结构是离散的，应用程序的各个模块放置的位置不应用程序的性质、平台的环境、开发人员的主观意愿等决定。因此，在对应用程序进行可信测量时，没有一个已知的、完整的软件结构，就难以测量。

针对动态可信测量这一过程，国内外也逐渐展开了相应的研究工作。

文献[12]为此提出一种动态可信应用传递模型(DATTM)，在保持应用装载的灵活性基础上，着重考虑了应用之间的权限隔离问题，最大程度地实现最小特权和按需即知等安全基本原则，进一步改善了系统度量和策略执行的效率和安全问题，但该方法需要建立软件限制表，随之引出的问题包括：(1)谁建这张表？(2)这张表是存放在内核空间还是用户空间？(3)这张表是否有一个固定的长度？谁保护这张表？(4)性能和效率问题。以上这些问题在该文献中都没有进行详细彻底的讨论。

文献[13]中，对应用程序的度量和信任传递采用 DRM 的方式。应用软件的开发者开发的软件需要得到硬件厂商的签名，而可信终端必须对该签名进行测量，测量通过方可运行。应用软件的升级、维护均采用这种方式。整个过程的完成需要 PKI 基础设施的支持，信任链的传递表现为一条可信证书链。采用这种方式的好处是有成熟的基础设施支持。但这种方式涉及到内容提供商和软件制造商之间的利益折中，也涉及到终端用户的隐私保护。

Microsoft 的 NGSCB[14] 采用双重执行环境。即提供传统的运行环境，原有的 Windows 操作系统、应用等依然可以执行。但要想启用 NGSCB 所提供的可信计算功能，必须依赖可信计算平台的执行环境。但 Microsoft 并没有说明在 NG-

SCB环境中如何对应用程序进行动态测量，也没有说明NGSCB环境对应用程序有何特殊要求。

总之，从世界范围内看，到目前为止，在动态可信测量的技术方面，可信终端都没能完全实现TCG的PC技术规范，如动态可信度量等。

4 信任链传递的基础理论研究

理论来源于实践，反过来又指导实践。没有理论指导的实践最终是不能持久的。对终端信任链传递的理论研究，可以促进终端可信计算技术的健康发展。

4.1 信任链理论模型

对于终端平台，一个完整的系统可信传递过程要从可信根开始，系统控制权顺序由可信的BIOS传递到可信boot、再到可信的OS loader，从可信的OS loader传递到可信的操作系统，再从可信的操作系统传递到可信的应用。因此，我们需要建立信任链传递的“层次理论模型”，确保信任逐层传递。在此过程中，信任传递从可信根到OS具有单一性和顺序性，只要保证了信任根的物理安全、信任传递过程中的时间隔离性和空间隔离性，建立信任链的“层次理论模型”，应该是相对容易的。而在信任从OS传递到应用的过程中，信任的传递不仅涉及到对应用程序的可信动态测量，而且必须考虑主体在应用程序(客体)上的行为是否能危害系统的安全，降低系统环境的可信度。其中的任意一个方面不能保证，信任链都不能传递或传递过程中会出现损失。

在可信终端信任链的传递理论方面，文献[9,10]提出了从可信根到OS启动的可信保证策略。即在最终的运行实体L_n和初始的硬件平台L_0之间划分若干层次$L_1, L_2, \cdots, L_{n-1}$，使$L_n$通过$L_{n-1}, \cdots, L_2, L_1$层最终能在$L_0$上运行。每一层又由若干模块组成，各层之间只有单向的依赖关系，即高层依赖于低层而低层不依赖于高层。按照这种层次式结构的理想状态，如果L_0层是可信的，并且保证低层在将控制权传递给高层前，对高层的可信度进行检查和确认，则信任也是逐层传递的。如果层与层之间只要保持静态隔离、动态隔离和时间隔离关系，那么信任传递的层次模型就是可以验证的。

在信任链传递过程中的信任损失度量理论方面，几乎还找不到相关的文献。目前，关于信任的度量理论与模型，如基于概率统计的信任模型[15,16]、基于模糊数学的信任模型[17]、基于主观逻辑的信任模型[18]、基于证据理论的信任模型[19]和基于软件行为学的信任模型[11]等，还不能直接应用于终端信任链，因为这些理论仅仅是对信任的度量，没说涉及信任的传递和损失。

4.2 软件的动态可信度度量理论

可信测量是可信计算的基础。但对于软件的动态可信性的度量理论，几乎还找不到相关的文献。我们认为，要建立软件的动态可信度的度量理论，需要首先研究动态测量的软件结构模型和指标体系，以及软件多维可信属性与结构模型和指标体系的关系。其次，要研究适合于该结构模型的编译环境。第三，要研究适合于该结构模型的内存分配机制和代码加载机制。在时间和空间上保证软件的隔离性。

总之，无论是国外还是国内，在可信计算领域都处于技术超前于理论，理论滞后于技术的状况。信任链传递的研究也是如此。目前，国内外在信任链传递的相关理论方面研究较少，不够深入。

5 信任链待研究的领域

信任链是可信计算最基本的问题之一。其亟待研究的领域包括如下2方面：

(1)关键技术

- 信任链技术。如信任的传递方案、方式等；
- 静态测量技术。如存储、报告机制，安全I/O等；
- 动态测量技术。如信任的动态测量、存储和报告机制。

(2)理论基础

- 信任链理论。包括信任的传递理论，信任传递的损失度量；
- 可信性的度量理论。包括软件的动态可信性度量理论与模型。

结束语 目前可信计算已经成为世界信息安全领域的一个新潮流。信任链传递是可信计算技术的基本问题。如果信任链理论与技术能够得到较好的解决，那么，可信计算技术就会得到较大的发展。可信计算技术是一种行之有效的信息安全技术。可信计算机与普通计算机相比，安全性大大提高，但可信计算机也不是百分之百安全。我国在可信计算领域起步不晚，水平不低，应当抓住机遇发展我国的可信计算事业，建立我国的信息安全体系，确保我国的信息安全。

参 考 文 献

[1] Trusted Computing Group. TCG Specification Architecture Overview [EB/OL]. [2005-03-01]. https://www.trustedcomputinggroup.org/groups/TCG_1_0_ Architecture_Overview.pdf

[2] 张焕国,罗捷,金刚,等. 可信计算研究进展. 武汉大学学报:理学版,2006,52(5):513-518

[3] 沈昌祥,张焕国,冯登国,等. 信息安全综述,信息安全研究综述. 中国科学(E),37(2):129-150

[4] Arbaugh W, Farber D, Smith J. A Secure and Reliable Bootstrap Architecture[C]// IEEE Symposium on Security and Privacy. 1997:65-71

[5] Nakamura M, Munetoh S. Designing a Trust Chain for a Thin Client on a Live Linux CD// SAC'07. Seoul, Korea, 2007

[6] 方艳湘,黄涛. Linux可信启动的设计与实现[J]. 计算机工程,2006,32(6):51-53

[7] Johnson S, Jose S. Trusted Boot Loader, CE Linux Forum, TCG patch for GRUB. http://trousers.sourceforge.net/grub.html, 2006

[8] 黄涛,沈昌祥. 一种基于可信服务器的可信引导方案[J]. 武汉大学学报:理学版

[9] 蔡谊. 支持可信操作平台的安全操作系统研究. 博士论文. 海军工程大学,2005

[10] 谭良. 可信操作系统若干关键问题的研究. 博士论文. 电子科技大学,2007

[11] 屈延文. 软件行为学. 电子工业出版社,2004

[12] 李晓勇,沈昌祥. 一个动态可信应用传递模型的研究[J]. 华中科技大学学报:自然科学版,2005,33:310-312

[13] Garfinkel T, Pfaff B, Chow J, et al. Terra: A Virtual Machine-Based Platform for Trusted Computing // SOSP'03. Bolton Landing, New York, USA, October 2003

[14] Microsoft. Trusted Platform Module Services in Windows Longhorn[EB/OL]. [2005-4-25]. http://www.microsoft.com/resources/ngscb/

[15] Patel J, Luke T W T, Jennings N R, et al. A Probabilistic Trust Model for Handling Inaccurate Reputation Sources // Trust Management, Third International Conference, iTrust 2005. Paris, 2005, 23-26: 193-209

[16] Beth T, Borcherding M, Klein B. Valuation of thust in open network// Proceeding of the European Symposium on Re-search in Security(ESORICS). Brighton: Springer-Verlag, 1994: 3-18

[17] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究. 软件学报,2003,14(8):1401-1408

[18] Jonsang A. An Algebra for Assessing Trust in Certification Chains// The proceedings of NDSS'99, Network and Distrib-uted System Security Symposium. The Internet Society, San Diego, 1999

[19] 袁禄来,曾国荪,王伟. 基于Dempster-Shafer证据理论的信任评估模型. 武汉大学学报:理学版,2006,52(5)