doi 10.3969/j.issn.1671-1122.2015.01.001

一种可信虚拟平台构建方法的研究和改进

李海威[1]，范博[1]，李文锋[2]

（1. 公安部第一研究所，北京 100048 ；2. 北京搜狐新动力信息技术有限公司，北京 100190）

摘 要 为了减小虚拟环境下虚拟可信平台模块（vTPM）实例及系统软件可信计算基（TCB）的大小，同时进一步保护 vTPM 组件的机密性、完整性和安全性，解决传统虚拟可信计算平台下可信边界难以界定的问题，文章提出了一种新的构建可信虚拟平台的方法和模型。首先，将 Xen 特权域 Domain 0 用户空间中弱安全性的域管理工具、vTPM 相关组件等放置于可信域 Domain T 中，以防止来自 Domain 0 中恶意软件的攻击及内存嗅探，同时作为 Xen 虚拟层上面的安全服务实施框架，Domain T 可以给 vTPM 的相关组件提供更高级别的安全保护。其次，通过重构 Domain 0 中拥有特权的管理和控制应用软件，将特权域的用户空间从可信计算基中分离出来，进而减小虚拟可信平台可信计算基的大小。最后，设计并实现了新的基于可信虚拟平台的可信链构建模型。通过与传统可信虚拟平台比较，该系统可以有效实现将虚拟化技术和可信计算技术相融合，并实现在一个物理平台上同时运行多个不同可信级别的操作系统，且保证每个操作系统仍然拥有可信认证等功能。

关键词 ：可信平台模块 ；可信虚拟执行环境 ；可信计算基 ；可信链 ；可信域

中图分类号 ：TP309 文献标识码 ：A 文章编号 ：1671-1122（2015）01-0001-05

中文引用格式 ：李海威，范博，李文锋 . 一种可信虚拟平台构建方法的研究和改进 [J]. 信息网络安全，2015，(1) ：1-5.

英文引用格式 ：LI H W, FAN B, LI W F. Research and Improvement on Constructing Method of A Trusted Virtualization Platform[J]. Netinfo Security,2015,(1):1-5.

Research and Improvement on Constructing Method of A Trusted Virtualization Platform

LI Hai-wei[1],FAN Bo[1],LI Wen-feng[2]

(1. *The First Research Institute of the Ministry of Public Security of P.R.C,Beijing* 100048, *China*; 2. *Beijing Sohu New Power Information Technology Co.,Beijing* 100190, *China*)

Abstract: In order to reduce the size of the virtual trusted platform module (vTPM) instances and trusted computing base(TCB) of system software in virtual environment, and further to protect the confidentiality, integrity and security of the vTPM components, and solve the problem that the credibility boundariesare difficult to define under the traditional virtual trusted computing platform , this paper presents a new method and model to build credible virtual platform. Firstly, in order to prevent the attacks from malicious software and memory sniffer in Domain 0, the domain management tool of weak security in the user space of Xen privilege domain Domain 0 and the related components of vTPM are placed in a trusted domain Domain T. As the security services implementation framework above the Xen virtualization layer, Domain T can provide a higher level of security protection for the related components of vTPM. Secondly, by refactoring the management and the control application software with the privileges in Domain 0, the user space of Domain 0 is separated from the trusted computing base, and then the size of the trusted computing base of

收稿日期 ：2014-12-01

基金项目 ：国家自然科学基金青年基金 [61302087，61401038]

作者简介 ：李海威（1984-），男，河北，工程师，硕士，主要研究方向 ：信息网络安全 ；范博（1978-），女，吉林，工程师，硕士，主要研究方向 ：信息网络安全 ；李文峰（1988-），男，山东，工程师，硕士，主要研究方向 ：P2P 安全、Web 安全及防护。

通讯作者 ：李海威 304055019@qq.com

trusted virtual platform is reduced. Finally, a new trusted chain construction model based on the trusted virtual platform is designed and implemented. By comparing with the traditional trusted virtual platform, the system can effectively implement the integration of virtualization technology and trusted computing technology, and implement to run simultaneously multiple operating systems of different credible level on a physical platform, while guaranteeing each operating system having functions such as credible certification.

Key words: trusted platform module; trusted virtual execution environment; trusted computing base; trusted chain; trusted domain

0 引言

可信计算是一种信息系统安全新技术，包括可信硬件、可信软件、可信网络和可信计算应用等诸多方面，它能够有效保证虚拟机监视器、客户操作系统及上层应用程序的可信性和完整性。因此，将虚拟化技术和可信计算技术相结合，是可信计算技术与虚拟化技术发展的必然结果。可信平台模块[1]（trusted platform module，TPM）作为可信计算平台的信任根，它的虚拟化将成为该领域的关键技术之一。

可信平台模块从狭义上来说就是指 TPM 安全芯片。通过在计算机中嵌入该芯片，可以以该芯片作为可信度量根，并在芯片中记录系统引导和启动的过程，对系统可信程度进行链式的度量，以图构建一条完整的信任链。

为了实现可信平台模块的虚拟化，一系列 vTPM 设计方案和 vTPM 安全架构模型相继被提出。目前可信平台模块的虚拟化实现方式主要有 3 种：TPM 准虚拟化共享模型[2]、TPM 硬件环境扩展模型[3] 和基于仿真软件的 TPM 虚拟化模型。

TPM 准虚拟化共享模型采用在多个虚拟机之间“安全地”共享一个硬件 TPM 的方式实现 TPM 芯片的虚拟化。为了实现共享，部分组件如 EK、SRK、随机数生成器等利用软件中间件在多个 VM 之间实现多路复用。而其他组件如平台配置寄存器（platform configuration register，PCR）、计数器等需为每一个 vTPM 创建一个单独组件实例，并且要保证实例与实例之间能进行有效的隔离。该方案需要更改部分的设备接口。

TPM 硬件环境扩展模型通过扩展 TPM 上下文为每个客户虚拟机提供专用的 TPM 环境，客户虚拟机可以自行保存和读取上下文，虚拟机监视器能够透明地为每个客户虚拟机提供隔离的 TPM 会话。然而该方式需要 TPM 硬件支持，目前并不存在硬件虚拟化的 TPM。

目前大多数应用都是采用基于仿真软件的 vTPM 虚拟化方式[4-7]，该方式以 Xen 虚拟设备的分离驱动机制为基础，在特权域 Domain 0 中利用 TPM 仿真软件为每个 VM 创建一个 vTPM 实例，由 vTPM 实例完成各个虚拟域的可信计算操作，并提供针对这些实例的后台管理模块以及相应的 TPM 管理工具。与前两种模型相比，该模型的优势在于实现了不同 vTPM 实例之间的完全隔离，并给虚拟机提供了一个接近于真实 TPM 硬件的接口。但是不足之处也比较明显，基于 vTPM 虚拟化方式的可信虚拟执行环境架构中，vTPM 实例的可信计算基（trusted computing base，TCB）不仅包括内核态的 Xen Hypervisor、特权域 Domain 0 内核，也包括 Domain 0 用户空间下的域管理程序，vTPM 的相关组件等，这会造成可信虚拟平台的可信计算边界无法明确。同时以这种方式构建的 TCB 完整性度量结果并不能有效保证虚拟机的完整性[8]，因为系统管理员可以在任意时刻运行任意程序，包括一些恶意软件（如内存嗅探工具等），这将会严重影响虚拟执行环境的可信性和安全性[9]。

针对目前可信虚拟平台存在的问题，本文提出了一种新的可信虚拟执行环境构建方案。通过重构 Xen 中拥有特权的管理和控制应用软件，将弱安全性的域管理工具、vTPM 相关组件等放置于可信域 Domain T 中，并在此基础上重新定义该虚拟平台的可信计算边界，最终实现了减小可信计算基，有效阻止来自系统管理员的内存嗅探、TOCTOU（time-of-check-to-time-of-use）攻击等目标。

1 相关知识

1.1 可信计算平台

TCG 对“可信”的定义是：一个实体在实现给定目标时，若其行为总是可预期的，则该实体就被认为是可信的。按照 TCG 的可信 PC 技术规范，可信计算平台（TCP）是指以 TPM 为核心，将 CPU、操作系统、应用软件、网络基础设备融为一体的完整体系结构，它能够有效保证系统的

可靠性、可用性和平台配置信息的完整性。可信计算平台的主要特征是在主板上嵌有可信构建模块（trusted building block，TBB），TBB 是可信 PC 平台的可信根。软件部分的可信根是可信度量核心根（core root of trust for measurement，CRTM），硬件部分的可信根是可信平台模块（TPM）。

可信计算平台的一个重要目标就是能够使该平台具有远程证明（remote attestation ）的能力。在远程证明中，证明方必须真实地报告系统的当前状态，同时又不能将密钥和自己的身份暴露给验证方。可信计算平台有 3 个基本特征 ：保护能力（protected capabilities），证明（attestation），完整性度量存储和报告（integrity measurement, storage and reporting）。完整性度量存储和报告指的是对影响平台可信度的平台部件（硬件平台、操作系统和应用）进行完整性度量，获得完整性度量结果，将度量结果的信息摘要扩展到平台配置寄存器 PCR，将完整性度量过程记录到日志文件，并在内存中记录完整性报告等。

1.2 可信链和可信边界

在可信计算体系中，建立可信计算平台分两步 [10] ：首先需要建立可信根，包括可信度量根（root of trust for measurement，RTM），可信存储根（root of trust for storage，RTS）和可信报告根（root of trust for reporting，RTR），可信根的可信性将由物里安全、技术安全与管理安全共同确保。其次利用可信根建立一条完整的可信链（trusted chain）。按照 TCG 的可信 PC 技术规范，可信 PC 的可信链以 TPM 芯片为可信根，建立 BIOS Boot Block → BIOS → OS Loader → OS → APP 的信任链，将信任传递给操作系统，再到应用，一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统平台的可信性。

可信构建模块（TBB）主要包括 RTM、TPM 初始化信息和功能等，它本身是信任源的一部分，它和可信根的组合形成了可信计算平台基本的可信边界，可用来对平台的最小配置进行完整性测量、存储和报告。在建立可信链之前，必须建立对这些模块及代码的信任，这种信任是控制权在进行转移之前通过对代码进行完整性度量来确认的。在确认可信后，将建立一个新的可信边界，以实现所有可信和不可信模块之间的隔离。

2 可信虚拟执行环境的概念模型

2.1 可信虚拟执行环境架构

本文设计的可信虚拟执行环境架构图如图 1 所示。

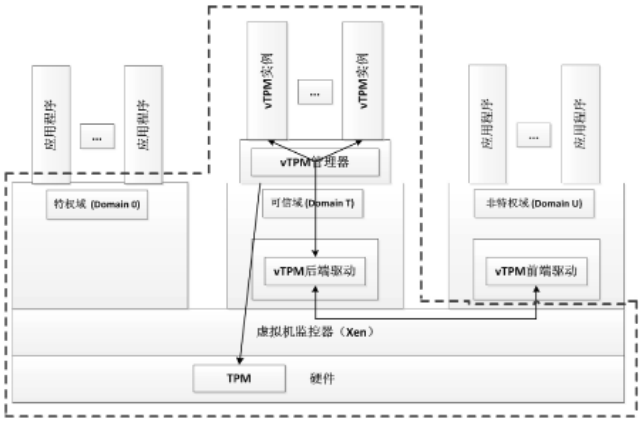

图1 可信虚拟执行环境架构图

其中，vTPM 的基本功能由运行在可信域 Domain T 中的 vTPM 管理器、vTPM 实例、vTPM 后端驱动以及运行在非特权域 Domain U 中的 vTPM 前端驱动等构成。

这里，可信域 Domain T 是一个类虚拟化的准操作系统——Xen Library OS[5]。它是 HP 实验室在 2007 年发布的一款基于 Mini-OS 的应用，由 4 部分组成 ：一个基于 GNU 工具链的 cross-development 环境、Red Hat 的 newlib C 库、Mini-OS 内核和基于 Xen 共享内存和事件通道的域间通信机制 IDC。它支持将小的应用程序直接运行在 Xen 虚拟机监视器上，这给我们提供了一种方便、实用的减小应用程序可信计算基的途径。

vTPM 实例是在 TPM Emluator 软件的基础上开发的应用程序，每一个实例都支持 TCG 的 TPM1.2 标准规范。vTPM 实例与客户虚拟机一一对应，负责为用户提供绑定、密封、密钥存储等一系列与物理 TPM 相同的功能。

vTPM 管理器负责 vTPM 实例的创建和管理。当创建虚拟机时，vTPM 管理器在可信域 Domain T 中创建一个 vTPM 实例，并将其与新创建的客户虚拟机相关联。当客户虚拟机启动后，vTPM 管理器通过监听 vTPM 的后端驱动，将来自不同客户虚拟机的 TPM 命令重定向到相关联的 vTPM 实例中。

在半虚拟化模式下，Xen 采用分离设备驱动模型来实现 I/O 的虚拟化 [11]。该模型将 TPM 设备驱动划分为前端驱动、后端驱动和原生驱动 3 个部分，前端驱动在非特权域 Domain U 中运行，后端驱动和原生驱动在可信域 Domain T 中

运行。vTPM 前端驱动负责将客户虚拟机的 TPM 请求发送到后端驱动，并从后端驱动接收 TPM 响应消息。vTPM 后端驱动负责将从前端驱动传来的 TPM 请求提交给 vTPM 管理器，TPM 处理完毕后，vTPM 后端驱动从 vTPM 管理器得到 TPM 的响应消息，并通过共享内存页将响应消息返回给前端驱动。

2.2 可信虚拟执行环境的可信计算边界

目前，基于 Xen 平台的可信虚拟执行环境架构中，vTPM 实例的可信计算基（TCB）不仅包括内核态的 Xen Hypervisor、特权域 Domain 0 内核等，也包括 Domain 0 用户空间下的域管理程序，vTPM 的相关组件等。一方面，这种将用户空间应用程序包含在可信计算基中的方式会造成可信计算基的可信边界无法明确 [12]，因为物理平台管理员在域中安装的任意软件都可能被包含在可信计算基中；另一方面，以这种方式构建的 TCB 的完整性度量结果并不能有效保证虚拟机的完整性，因为系统管理员可以在任意时刻运行任意特权的程序，包括一些恶意软件（如内存嗅探工具等）[9]，这将会严重影响虚拟执行环境的可信性和安全性。

为了解决上述问题，本文尝试将特权域 Domain 0 用户空间中这些安全性要求高的可信组件移植到一个轻量级的可信域 Domain T 中，包括域构建工具、vTPM 实例、vTPM 管理器、vTPM 守护进程、TPM 硬件驱动和虚拟平台配置寄存器等。这样做会带来两方面的好处：一方面，通过重构 Xen 特权域中拥有特权的管理和控制应用软件来减少来自系统管理员的威胁，并且将特权域的用户空间从可信计算基中分离出来，以减小 Xen 平台本身可信计算基的大小；另一方面，作为 Xen 虚拟层上面的安全服务实施框架，Domain T 可以给 vTPM 的相关组件提供更高级别的安全保护。此外将可信计算基的这些相关组件放入隔离的虚拟域中，可以充分利用域的隔离机制防止管理员的恶意嗅探和攻击。

如图 1 所示，虚线框中是本文设计的理想情况下 vTPM 实例的可信计算基（TCB），包括建立 vTPM 的软件组件（vTPM 实例、vTPM 管理器与 vTPM 后端驱动），相应的运行环境（Xen Hypervisor、Domain0 内核与域构建工具），可信域 Domain T 以及底层硬件固件等。Xen Hypervisor 作为虚拟机监视器处于处理器的最高特权级，它可以为上层的客户虚拟机提供虚拟域之间的隔离、调度及内存管理，所以 Xen Hypervisor 需要和底层固件一起成为系统可信计算基的一部分。Domain 0 内核同样被置于可信计算基中，Xen 虚拟化平台采用的是一种混杂模式的虚拟化方案，作为 Xen 启动中第一个被加载的内核，Domain 0 内核拥有一些特殊的权限。例如，它是 Xen 虚拟化平台上唯一可以获取物理 I/O 资源的虚拟机内核，同时它可以为 Domain 0 用户空间中的应用程序提供与 Xen Hypervisor 进行交互的超级调用。如果 Domain 0 内核遭到篡改，会直接导致系统的可信性遭到破坏。此外，在客户虚拟机（VM）的创建过程中，域构建工具可以向客户虚拟机的地址空间写入数据、配置客户虚拟机的虚拟 CPU 状态等，这些都会影响系统的可信性，所以也需要加入可信计算基中。

3 可信虚拟执行环境的可信链构建

在虚拟执行环境下，一条完整的可信链建立分为 3 个阶段：物理平台可信链的建立、vTPM 与底层 TCB 的绑定、客户虚拟域的可信引导和可信启动。

如图 2 所示，建立物理平台可信链时，在平台系统启动及引导过程中，可信链的每一个部件在将控制权传递给下一个部件之前需对该部件进行完整性度量。例如，一个包含 CRTM 的 BIOS 需要对随后启动的 MBR（master boot record，主引导记录）和引导加载器（OSLO bootloader）进行度量。而后面阶段在启动过程中会对一系列的其他组件进行度量，包括 Xen hypervisor、Domain 0 内核、可信域 Domain T 等。可信域 Domain T 启动完成后，硬件 TPM 会对该域中的 vTPM 的相关组件及域管理工具进行度量，并将结果扩展到物理 PCR 中。

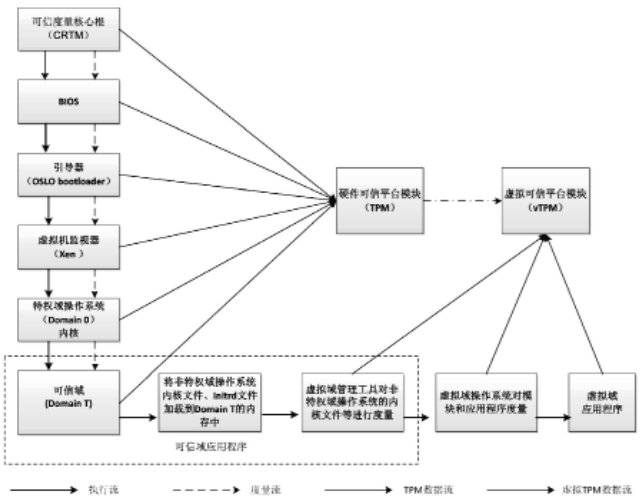

图2 可信链构建过程

在可信虚拟执行环境下，vTPM 实例的可信计算基（TCB）所包括组件的完整性度量由物理 TPM 完成，度量值保存在物理 TPM 的 PCR 中。vTPM 实例主要确保非特权域的完整性，度量的组件包括非特权域操作系统及上层应用程序，度量值保存在 vTPM 实例的 vPCR 中。为了在虚拟环境下使用可信度量功能，必须建立 vTPM 与底层 TCB 的绑定关系，以确保 vTPM 运行环境的完整性以及客户虚拟机平台环境的完整性。文献 [11] 提出了一种使用硬件 TPM 的平台信息作为虚拟域的平台信息方式，将物理 PCR 的低 9 位映射到 vTPM 的 vPCR 中，硬件 TPM 的 0~8 号这九组寄存器地址中一般存储着计算机 CRTM、BIOS、引导加载器、Hypervisor、特权域内核、可信域及可信域中的 vTPM 等部分的度量结果，这些环境信息可以作为虚拟域的初始环境信息，与虚拟域有关的一切操作都是以此平台为基础。

在该模型中，我们采用 Trusted GRUB 作为引导加载程序，同时为了支持在 TPM v1.2 中提及的 DRTM（dynamic root of trust for measurement，动态度量根），将 OSLO 引导加载模块作为 Trusted GRUB 的标准模块 [13]。在平台启动阶段，该模块会加载并度量虚拟机监视器、Domain 0 内核和域构建工具，并将完整性度量结果存储到硬件 TPM 的 PCR 中。在平台运行阶段，该模块会调用 AMD CPU 的 SKIINIT 指令集将平台初始化到可信状态，这样可以保证虚拟机监视器在平台运行的任意时刻启动的可信性。

目前 Xen 平台下非特权域的内核、Initrd 等文件存放在特权域中。为了实现对这些文件的度量，可以通过修改可信 GRUB 程序、添加 Measure 命令，在特权域的引导过程实现对非特权域的内核及其配置文件的完整性度量。但是，从度量完成到非特权域真正启动可能会有很长的时间间隔，这期间已经被度量过的非特权域的内核、Initrd 等文件可以被任意修改，从而使得度量操作没有任何实际意义。为了避免这种 TOCTOU 攻击，文献 [13] 中采用 Trusted PYGRUB，在内核文件 Initrd 等文件被加载前进行度量。我们在该设计中做了进一步的改进 ：首先非特权域在启动前，会将该域的内核文件、初始化磁盘文件和其他配置文件加载到可信域 Domain T 的内存中，此时 Domain T 作为可信链的一部分已经完成自身的可信度量操作。接着，Domain T 创建并初始化一个新的 vTPM 实例，然后对已加载到内存中的非特权域各部件进行度量，这就保证了其所度量的内核就是将要启动的内核，从而有效抵挡了 TOCTOU 攻击。

4 结束语

本文以可信域为基础，通过重构 Xen 特权域中拥有特权的管理和控制应用软件，将构建工具、vTPM 实例、vTPM 管理器等可信相关组件放置于可信域 Domain T 中，以实现将特权域的用户空间从可信计算基中分离出来，进而减小可信虚拟平台可信计算基的大小，并在此基础上，明确了虚拟域的可信边界，建立了一条完整的可信虚拟执行环境下的信任链，以实现在一个物理平台上同时运行多个不同可信级别的操作系统，且保证每个操作系统仍然拥有可信认证等功能。（责编 吴晶）

参考文献：
[1]Trusted Computing Group.TPM Main Specification version1.2 [EB/OL]. http://www.trustedcomputinggroup.org/resources/tpm_main_specification, 2006.
[2] Paul England , Jork Loeser. Para - Virtualized TPM Sharing[C]// Proceedings of the First international conference on Trusted Computing and Trust in Information Technologies: Trusted Computing Challenges and Applications.Villach, Austria, 2008:119 - 132.
[3] Ken Goldman kgold, Stefan Berger stefan. TPM Main Part 3 IBM Commands[EB/OL]. http://www.research.ibm.com/secure_systems_department/projects/vtpm/mainP3IBMCommandsrev10.pdf , 2005.
[4] Berger S, Caceres R, Goldman K A. vTPM:virtualiz - ing the trusted platform module[C]//Proceedings of the 15th USENIX Security Symposium (USENIX Security 2006) ,2006.
[5] Anderson M J, Moffie M, Dalton C I. Towards Trustworthy Virtualisation Environments: Xen Library OS Security Service Infrastructure[R]. HPL - 2007 - 69, Hewlett - Packard Development Company, L.P., 2007.
[6] Ahmad - Reza Sadeghi, Christian St ü ble, Marcel Winandy. Property - based TPM virtualization[C]//Proceedings of 11th International Conference (ISC 2008), 2008:1 - 16.
[7] Frederic Stumpf,Claudia Eckert,Shane Balfe. Towards Secure E - Commerce Based on Virtualization and Attestation Techniques [C]// Proceedings of the Third International Conference on Availability, Reliability and Se - curity (ARES 2008), 2008: 376 - 382.
[8] 王丽娜，高汉军，余荣威 . 基于信任扩展的可信虚拟执行环境构建方法研究 [J]. 通信学报，2011，(9) ：1 - 8.
[9] Bryan D Payne，Martim D.P.de A.Carbone，Wenke Lee. Secure and Flexible Monitoring of Virtual Machines[C]//Proc. of ACSAC ’ 07, 2007.
[10] 沈昌祥，张焕国，王怀民，等 . 可信计算的研究与发展 [J]. 中国科学 ：信息科学，2010，(40) ：139 - 166.
[11] David Chisnall. The Definitive Guide to the Xen Hypervisor[EB/OL]. http://books.sharedaa.com/2009/10/the - definitive - guide - to - the - xen - hypervisor.html,2007.
[12] Derek G Murray, Grzegorz Milos, Steven Hand. Improving Xen Security through Disaggregation[C]//Proc. of VEE ’ 08,2008,(08):151 - 160.
[13] Kauer B. OSLO: Improving the Security of Trusted Computing[C]// Proceedings of the 16th USENIX Security Symposium. USENIX Association, 2007.