

基于硬件虚拟化的主动防御模型研究

徐 鲲, 廖小飞

(华中科技大学 计算机学院, 湖北 武汉 430074)

摘 要: 基于 HOOK 内核代码的传统主动防御软件在放行恶意驱动后对于高危险的恶意代码无法做到有效防御, 因此在已有的病毒行为分析和模式识别技术的基础上, 提出了一种基于硬件虚拟化的主动防御模型. 详细阐述了硬件虚拟化的主动防御系统的主体构架和实现, 系统功能模块的划分及实现原理, 行为视窗监控、黑白名单等关键技术的实现方法, 从更底层的角度进行行为检测防御, 并通过影子页表可以实现高强度的自我保护.

关键词: 硬件虚拟化; 虚拟机管理器; 主动防御; 黑白名单; 行为特征; 敏感指令

中图分类号: TP319

文献标识码: A

文章编号: 1000-7180(2012)12-0189-04

Research on Proactive Defense Model Based on Virtualization Technology

XU Kun, LIAO Xiao-fei

(School of Computer, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: The traditional proactive defense software based on HOOK Kernel code can't defend effectively to the high risk of malicious code after releasing malicious drivers. So based on existing virus behavior analysis and pattern recognition technology, we put forward a new proactive defense model based on Hardware virtualization. It describes in detail the main structure and realization of active defense system of hardware virtualization, the division of the module and the principle of realization of the system function, the behavior of Windows monitoring, the black and white lists and so on, all the Implementation of key technologies. It can undertake the behavior detection defense from the perspective of lower-level, and it can also achieve high strength of the self-protection through the shadow page table.

Key words: HVM; VMM; proactive defense; blacklist and whitelist; behavior pattern; sensitive instruction

1 引言

伴随信息技术的高速发展, 各种恶意程序的入侵手段日益复杂^[1]. 基于内核 HOOK 及行为特征库的主动防御系统通过拦截可疑行为并提醒用户做出响应^[2], 达到预防和保护的目.

但传统主动防御软件的特征库总晚于恶意程序的发现, 面对新型病毒、木马时, 无法从根本上做到防范. 此外, 恶意程序驱动常借助系统权限来实现破坏、隐藏、嗅探等目的. 同处于系统内核中, 传统主动防御软件不具优势^[3]. 由于驱动可信度难以分析, 用户选择放行后, 主动防御软件便失去了主导, 后果是

自身保护机制被攻破, 用户群体尤其是政府、商业职员将可能面临严重的数据泄露、丢失等问题.

为解决传统主动防御软件的不足, 本文在硬件虚拟化的基础上, 提出了一个更有效的高安全主动防御模型.

2 主动防御模型设计

本文设计的主动防御模型是在 P2DR(Policy、Protection、Detection 和 Response)模型的基础上, 加入硬件虚拟化的支持并进行有效的精简和改进. 主要分为以下四个部分:

(1) 安全策略模块.

- (2)内核及自身防护模块.
- (3)行为监测模块.
- (4)处理响应模块.

通过自建的轻量级虚拟机管理器为以上功能模块提供硬件虚拟化的特权及保护支撑,使得本模型在应用硬件虚拟化特性的基础上,能够提供优于传统主动防御软件的安全服务.

各功能模块协作关系如图 1 所示.

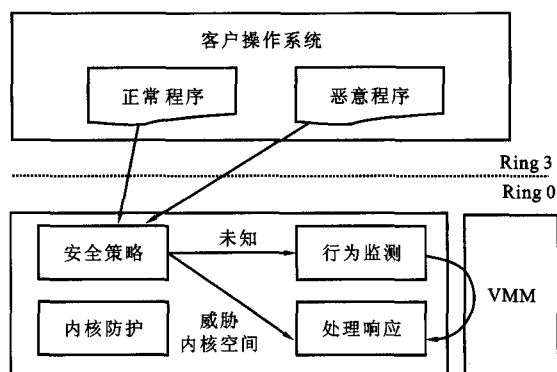


图 1 模块功能协作图

2.1 整体架构设计

为实现上述功能模块,本主动防御模型的整体架构如图 2 所示.

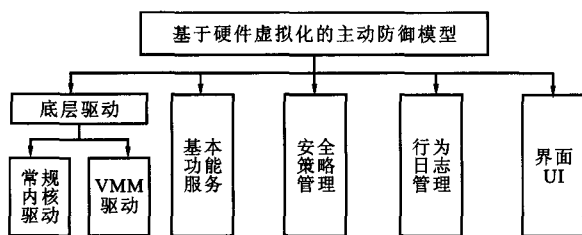


图 2 整体方案架构

各部分具体功能如下:

(1)底层驱动. 负责提供硬件虚拟化支持;负责在系统内核中对进程行为进行监测;负责对已定义的安全策略自动做出相应处理;负责实现内核环境的完整性及自我保护.

(2)基础功能服务. 负责加载驱动,响应驱动对上层应用的通知;负责提供基本功能接口;负责将驱动拦截的敏感操作信息呈献给用户,并通知用户处理.

(3)安全策略管理. 负责更新和维护安全策略;负责从行为特征中提取相应的安全策略;负责对单一程序或全局进行策略配置.

(4)行为日志管理. 负责记录程序敏感操作的行为轨迹,并进行针对性分类管理;负责为安全策略提供数据支持.

(5)界面 UI. 负责用户与功能模块的友好交互.

2.2 内核驱动

2.2.1 轻量级虚拟机管理器

这里,我们构建一个轻量级虚拟机管理器 LVMM,通过将本地操作系统迁移至非根操作模式使得虚拟机管理器具有比操作系统更高的权限.其作用是为常规内核驱动创造干净完整的内核环境,提供有效的保护机制,并利用 VT-x 技术特性针对特定的一些敏感操作进行拦截.

主动防御系统对进程行为的监控依赖于对内核系统调用的监控,为此,只有当处于一个完整、干净的内核环境中,才能够保证整个监控过程不被干扰.由于传统的主动防御系统与恶意驱动存在同级竞争,面对一些经过巧妙构造的恶意代码,主动防御软件可被其从系统底层进行篡改或强制结束,从而失去保护能力.通过虚拟机管理器,在影子页表中维护一份干净的内核镜像,必要时对客户机内核进行恢复以保证内核环境的完整性.

执行特定敏感操作后,将产生 VM Exit 事件而陷入 VMM,此时,控制权转交给 VMM,而客户机操作系统则处于“暂停”状态.针对引发 VM Exit 的不同情况,有相应的 Exit_Reason 用来进行分支判断.

这里所提到的特定敏感操作包括对重要寄存器 CR0、IDTR、MSR 等的写操作.一些病毒、木马等常常通过修改重要寄存器的手段来达到潜伏或是篡改内核代码的目的.通过配置虚拟机管理器的 VMCS 域,可以实现对其的拦截、欺骗等操作.

对于内存保护,其原理是在开启 CR0 保护机制的情况下,设置要保护的内存所在页面为只读,当系统进行写入操作时就会触发 #PF 页面异常.实现方式是在 VMM 中配置 EXCEPTION_BITMAP 数组,使页异常中断产生 VM Exit.当非法访问某个页表项或页目录项时就会触发,从而跳入到 VMM 中进行处理.需要进行内存保护的地址包括内核代码段、重要表、重要数据结构以及常规主动防御驱动.

对于常规驱动的保护,可针对该驱动所在的内存页进行内存保护.而要实现 VMM 驱动的自保护,则需要进行影子页表的处理.VMM 的运行依靠自建的一套页目录和页表,所指向的物理内存内容与操作系统相一致.通过修改影子页表中的页表项、页目录项属性,客户机操作系统中运行的程序将无法访问 VMM 的内存地址.

对 SLDT、SIDT、SGDT 等敏感指令的拦截 VT-x 尚未实现,可通过内存保护的手段来防止系

统的 IDT 表、GDT 表等重要数据不被恶意代码修改。

对于处于白名单中的程序,将放行其对内核空间进行的修改;未在名单中的程序,需要针对具体操作进行判别。

2.2.2 常规内核驱动

程序对 API 的调用最终归结为对内核中 SS-DT、SSDT Shadow 两张表的内核服务函数的调用。在进入内核的过程中,需要调用 KiFastCallEntry 函数进行函数的选择和传参等处理。通过嵌入 VM-CALL、CPUID 等指令以实现在每一次系统调用时转入 VMM 进行处理。为降低虚拟机管理器对计算机性能的影响,对程序执行过程中的 API 行为处理放在常规内核驱动中进行,且有选择地对系统调用进行陷入处理。与传统主动防御驱动不同的是,对于高危害的病毒木马,可通过主动陷入交予 VMM 再进行处理,从而避免其在内核同级竞争中对监测过程的干扰和影响。

2.3 Ring 3 级应用程序

通过 Ring 3 级应用程序,为用户提供一个好的交互界面。用户通过可视化窗口对主动防御系统进行控制。包括安全策略、行为日志的管理,以及对主动防御运行过程中所产生的必要控制处理。

安全策略包括对单一程序的执行控制、对全局的执行控制、以及黑白名单控制。执行控制包括程序对注册表的读写访问、对远程进程的访问、对重要文件的访问。通过预先对程序的安全策略进行配置从而在程序执行过程中直接应用并进行处理。对于未知程序,当执行敏感操作时询问用户是否将其放行或为其创建安全策略。

行为日志记录程序的敏感操作信息,同时为事后分析提供有效的数据支持。

2.4 整体运行流程

程序运行时首先加载 VMM 驱动,进行相关的初始化工作,并将当前操作系统迁至非根模式下,将自身所在内存页通过影子页表进行隐藏。虚拟机管理器启动成功后加载常规内核驱动。内核驱动加载后通知 VMM 对其所在内存页实施内存保护,防止驱动代码被病毒、木马恶意修改和破坏。

Ring 3 应用程序及内核驱动读取用户配置并根据当前设定的安全策略实施监控。对于已知进程,根据安全策略自动决定对用户系统的敏感操作是否放行;对于不能在安全策略中匹配到的进程,当执行敏感操作时首先判断是否为已知非法操作,若是

则直接对该进程进行强制性结束处理并通知用户,写入相关日志,否则将敏感操作内容呈递给用户,让用户自行判断,根据用户判断来决定对该进程的处理,并将其添加至安全策略中。

处理操作包括加入黑白名单、建立安全策略、强制结束、内存访问欺骗等。对于已列入白名单的程序,允许其调用系统功能函数或对内核进行可允许范围的修改;而对于黑名单中的程序,则禁止其通过调用相关 API 对用户敏感数据的访问。可将拦截进程所执行的敏感操作作为一条规则加入到相应的安全策略中,从而当该进程再次执行同一操作时自动进行判断从而减少用户处理次数,为用户提供良好的交互环境。对于已知位于黑名单中的程序或执行某些特定危险操作的程序,应予以强制性结束,防止该恶意程序在后续执行中带来的危害。

3 关键技术分析

3.1 内核完整性保护技术

由于病毒、木马等常借助自身的驱动对内核中系统服务函数或是重要的数据结构进行修改,考虑到内核 HOOK 的全局性,常规内核驱动调用系统服务函数对恶意程序进行检测和拦截是不可靠的。为了保证本模型的常规主动防御驱动能够运行在干净的内核环境中,需要对可能被修改的代码段及重要数据结构进行还原。

实现方法是模拟 PE 文件加载器的原理利用 VMM 将内核文件正确映射在内存中的一块区域中,根据 PE 结构找到其代码段及 IDT、SSDT 等重要数据结构。当需要进行内核代码还原时,通过 VM Exit 陷入 VMM 后将其恢复至相应的内核地址,同时还要将地址所在内存页进行内存保护,以防止病毒、木马的再次修改。

内核代码段包括 SSDT、SSDT Shadow 所涉及到的系统服务函数,需要还原并保护的还有表本身包含的函数地址索引。此外, IDT、GDT、ObjectType 结构等也应该进行内存保护。

3.2 影子页表技术

为了实现本主动防御系统对程序的透明化,达到自我保护的目的,需要使用影子页表技术将 VMM 对操作系统隐藏。影子页表实现的基本原理是为 VMM 构建访问内存的私有页表。该页表的用途包括对 VMM 所占用内存的管理;映射操作系统内核以便 VMM 能正确访问操作系统内核,并调用操作系统内核函数;隐藏 VMM 的存在,当私有页

表构建成功之后,通过修改操作系统固有页表中有关 VMM 的页表项以达到隐藏自己的目的。

3.3 行为特征视窗技术

针对单一进程,在 VMM 启动后为其创建一个大小合适的行为特征记录视窗,从而方便地提取敏感操作,应用安全策略。采用了有限状态机的模型来实现行为主动防御,在状态机流动的过程中匹配相应规则。从初态开始记录定长的系统调用,然后查询安全策略所对应的调用序列,若匹配则进行相关处理,状态迁移;或当进程触发某一特定的敏感操作,则直接进入处理,随后进程再次回到初态。安全策略包括对全局和局部的注册表、文件、进程启动、关键 API 调用等相关规则。每一条规则有一个特定的调用序列与之对应,也可以由敏感的操作字段和单一行为所触发。

3.4 黑白名单技术

在常规内核驱动的行为监控及 VMM 的特定操作监控过程中,首先需要对当前进程进行甄别。为降低虚拟机管理器所带来的性能损耗,对于可信的程序将加入到白名单中,而对于已知的具有潜在威胁的程序将加入到黑名单中,在进行对进程行为的安全策略审查过程中可以跳过,直接进入处理阶段。

4 结束语

目前国内出色的主动防御软件包括:360 安全卫士、金山卫士、微点等,无论是从功能上还是完善程度上都表现出了很高的水准。与上述产品相比,本文讨论的模型具有如下优点:

(1)软硬结合,利用硬件虚拟化技术提供强有力的保护。硬件虚拟化技术兴起不久,更多的潜力还有待挖掘。而当前使用虚拟化技术的病毒木马虽然已经出现但由于门槛较高,还不能造成较大的影响。

(2)充分利用 VT-x 技术的优势,提供高强度的自保护和有效的行为拦截。通过影子页表技术实现使 VMM 所在内存页对操作系统透明,操作系统中的恶意程序无法觉察到 VMM 的存在,从而提高了自身的安全性。利用内存保护手段,从更加底层的角度保护其他内核驱动的安全,有效防止恶意篡改和

破坏。基于 VT-x 两种操作模式的特性,陷入 VMM 后客户机操作系统处于“暂停”状态,不会对 VMM 实施的检测和处理过程造成干扰,保障了行为取证的准确性。

(3)采用轻量级虚拟机,代码量少,有效降低程序编写过程所带来的潜在的漏洞或逻辑错误,保障了 VMM 运行的稳定性。应用黑白名单技术,作为安全策略中的一部分,有效降低 VMM 带来的性能损失。

现在,随着云计算概念的流行,主动防御软件也在与时俱进,提出了“云安全”服务方案^[4]。基于其后台服务器强大的处理能力和丰富的特征库^[5],不仅能够为本地客户端在恶意程序查杀方面大幅提速,同时也提高了查杀的准确度。今后可以考虑将硬件虚拟化的主动防御与云安全概念相结合^[6],在融合 VT-x 所带来的高安全性和高隐蔽性同时^[7],也能够提高对进程行为监测的处理效率。

参考文献:

- [1] 贺卫红,高为民. 分布式蠕虫检测与主动防御系统的研究与实现[J]. 计算机工程与设计, 2008, (22): 5735-5747.
- [2] 陶芬,尹芷仪,傅建明. 基于系统调用的软件行为模型[J]. 计算机科学, 2010, (04): 151-157.
- [3] 孟令强,关勇,张向红,等. 基于可信计算的应用程序白名单管理系统[J]. 计算机安全, 2010, (10): 16-17.
- [4] 胡焕增,李志洁,郑海旭. 基于云规则的驱动级主动防御系统[J]. 微计算机信息, 2011, (05): 164-166.
- [5] 蒋万春,汤立,陈震. 虚拟化安全问题探析[J]. 信息网络安全, 2010, (08): 83-87.
- [6] 温研,赵金晶,王怀民. 基于硬件虚拟化技术的隐藏进程检测技术. 计算机应用研究, 2008, (11): 3460-3474.
- [7] 李珣,黄皓. 一个基于硬件虚拟化的内核完整性监控方法[J]. 计算机科学, 2011, (12): 68-73.

作者简介:

徐 鲲 男, (1990—), 研究方向为信息安全.

廖小飞 男, (1978—), 教授, 博士生导师. 研究方向为多核与虚拟化、移动互联网计算.