**基于二进制动态翻译的ROP攻击检测方法研究与实现**

**技术方案**

**\*\*\*项目组**

\*\*\*

**目录**

[1 概述 1](#_Toc327454798)

[1.1 项目基本情况简介 1](#_Toc327454799)

[1.2 术语和缩写词 1](#_Toc327454800)

[2 参考资料 2](#_Toc327454801)

[3 功能概述与技术指标 2](#_Toc327454802)

[3.1 功能要求 2](#_Toc327454803)

[3.1.1 云服务器的可信引导功能 2](#_Toc327454804)

[3.1.2 虚拟可信根创建以及可信根与虚拟机的绑定 2](#_Toc327454805)

[3.1.3 虚拟机可信引导功能 2](#_Toc327454806)

[3.1.4 虚拟机可信监控功能 3](#_Toc327454807)

[3.1.5 可信软件栈功能 3](#_Toc327454808)

[3.2 技术指标 3](#_Toc327454809)

[4 系统运行平台 4](#_Toc327454810)

[5 技术方案设计 4](#_Toc327454811)

[5.1 总体设计 4](#_Toc327454812)

[5.1.1 系统构成 4](#_Toc327454813)

[5.1.2 工作原理 5](#_Toc327454814)

[5.2 虚拟可信机制内部模块设计方案 5](#_Toc327454815)

[5.2.1 可信引导模块 5](#_Toc327454816)

[5.2.1.1 功能概述 5](#_Toc327454817)

[5.2.1.2 组成结构 7](#_Toc327454818)

[5.2.1.3 工作流程 8](#_Toc327454819)

[5.2.1.4 重要数据结构 10](#_Toc327454820)

[5.2.1.5 接口 11](#_Toc327454821)

[5.2.2 Dom0可信管理模块 12](#_Toc327454822)

[5.2.2.1 功能概述 12](#_Toc327454823)

[5.2.2.2 组成结构 12](#_Toc327454824)

[5.2.2.3 工作流程 12](#_Toc327454825)

[5.2.2.4 重要数据结构 13](#_Toc327454826)

[5.2.2.5 接口 13](#_Toc327454827)

[5.2.3 虚拟可信根模块 13](#_Toc327454828)

[5.2.3.1 功能概述 13](#_Toc327454829)

[5.2.3.2 组成结构 13](#_Toc327454830)

[5.2.3.3 工作流程 14](#_Toc327454831)

[5.2.3.4 重要数据结构 16](#_Toc327454832)

[5.2.3.5 接口 18](#_Toc327454833)

[5.2.4 可信根通信模块 20](#_Toc327454834)

[5.2.4.1 功能概述 21](#_Toc327454835)

[5.2.4.2 组成结构 22](#_Toc327454836)

[5.2.4.3 工作流程 35](#_Toc327454837)

[5.2.4.4 主要数据结构 37](#_Toc327454838)

[5.2.4.5 接口设计 40](#_Toc327454839)

[5.2.5 DomU可信监控模块 42](#_Toc327454840)

[5.2.5.1 功能概述 42](#_Toc327454841)

[5.2.5.2 组成结构 42](#_Toc327454842)

[5.2.5.3 工作流程 42](#_Toc327454843)

[5.2.5.4 重要数据结构 42](#_Toc327454844)

[5.2.5.5 接口 42](#_Toc327454845)

修订表

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 时间 | 修改内容 | 修改者 |
|  |  |  |  |

# 概述

## 项目基本情况简介

本课题的任务目标是实现能够检测和防御ROP攻击及其变种攻击的软件，该软件基于动态检测框架，用户可选择开启多种攻击检测机制，对目标应用程序进行保护，提高操作系统中运行的应用程序的安全性。

## 术语和缩写词

ROP:返回导向编程 (Return Oriented Programming)

COP:调用导向编程 (Call Oriented Programming)

JOP:跳转导向编程 (Jump Oriented Programming)

ELF:可执行与可链接格式 (Executable and Linkable Format)

PLT:延迟绑定表 (Procedure Linkage Table)

GOT:全局偏移表 (Global Offset Table)

# 参考资料

* 《可信计算密码支撑平台功能与接口规范》
* 《核高基重大专项课题任务合同书——可信子系统研发》
* 《可信计算平台选型技术说明》

# 功能概述与技术指标

## 功能要求

### 程序信息获取功能

获取elf文件和共享库libc的信息，供pintools分析，具体功能如下：

1. 读取elf文件的plt、got表，获取符号名及对应内存地址。
2. 获取操作系统libc版本，获取其中各个函数的偏移量。

### 攻击检测功能

检测程序运行时受到的攻击，具体功能如下：

1. 通过PIN提供的插桩API，检测指令是否合法。
2. 记录程序控制流，检测控制流异常。
3. 记录程序中call指令和ret指令的执行次数。

### 程序保护功能

攻击发生后，为了阻止攻击，进行一系列处理，具体如下：

1. 保护got表，防止用户对其进行二次修改。
2. 检测到攻击后，关闭进程，报告程序存在漏洞。

### 日志功能

在受保护的程序被攻击者攻击后，记录相关信息，供程序员分析并修补软件漏洞。其基本功能为：

1. 记录进程上下文、程序控制流。
2. 显示漏洞位置。
3. 记录攻击信息。

## 技术指标

* 支持32位及64位Linux操作系统。
* 实现实时保护用户进程。
* 实现对可执行文件的保护。
* 提供图形化的安全展示界面。
* 支持对ROP攻击等代码复用攻击的主动防御。
* 支持对系统中运行的进程的尝试攻击进行审计记录。
* 对系统性能影响不超过15%。

# 系统运行平台

通用计算机。

各Linux桌面操作系统。

# 技术方案设计

## 总体设计

### 系统构成

虚拟可信机制由可信引导程序、Dom0可信管理模块、虚拟可信根模块、可信根通信模块和DomU可信监控模块组成，其框架如下图所示。



图1 虚拟可信机制框架图

可信引导程序在可信Grub基础上实现，实现云服务器物理平台的可信启动过程。

Dom0可信管理模块由可信管理程序、Dom0 TSS、Dom0 内核监控模块组成，其中Dom0 TSS直接使用开源trousers软件。该模块提供Dom0的虚拟机与VTPM绑定、VM镜像可信管理等功能。

虚拟可信根模块由VTPM管理器和VTPM实例组成，实现虚拟可信根的创建和管理操作。

可信根通信模块由VTPM前端通信和VTPM后端通信组成，实现虚拟机对虚拟可信根的信息传递。

DomU可信监控模块由DomU可信管理程序、DomU TSS、DomU 内核监控模块和Dom U安全守护进程组成，其中DomU TSS直接使用开源trousers软件。该模块提供DomU 的可信监控功能。

### 工作原理

## 虚拟可信机制内部模块设计方案

### 可信引导模块

#### 功能概述

为防止因计算机启动相关文件被篡改而导致的系统破坏，本模块提供对启动过程中涉及的引导程序和引导文件进行度量验证，禁止使用不可信的本地配置启动；同时提供初始化、更新启动过程相关的预期度量值功能；允许用户关闭可信引导模块。

该模块包含的子模块以及相关功能如下：

* 1. 配置及模式切换

本模块支持关闭可信子系统（含可信引导模块）功能，其开关配置存放于可信引导程序的Stage1.5中。

子系统的关闭及子系统开启与更新均由可信管理模块发起。除子系统关闭功能外，其它功能的实现均需可信管理模块提供度量文件列表。

* 1. 度量验证

用于度量和验证操作系统内核启动之前加载的模块和重要文件的完整性。

1. OS内核加载前进行可信引导：度量验证OS内核加载前的启动代码。

基于软算法对Stage 2、MCF进行度量与代码验证。度量算法暂定为国标算法SMS3，验证方式是比较实际度量值与度量文件中的预设值，不同则执行以下操作：禁止引导，提示禁止原因，要求使用操作系统恢复光盘恢复系统。

本段功能代码添加在stage1.5的cmain函数中的最开始位置。即在stage1.5一开始运行时，先运行本段代码，在运行stage1.5自身的代码。其中使用了grub的一个全局变量config\_file，变量存储stage2的路径。

1. OS内核的可信引导：度量验证OS内核以及重要系统文件。

在装载用户选择的OS内核前，根据度量配置文件对不同的内核文件、初始盘文件等OS加载文件及其他关键系统文件进行度量与代码验证。度量及失败处理方式同上。

这段代码添加在stage2的cmain函数中。在stage2初始化一些变量后，运行添加的代码。结束后，运行stage2自身代码。其中使用了grub的一个全局变量config\_file，变量存储stage2的路径。根据stage2的路径找到MCF的路径。

* 1. 预期值初始化、系统配置与更新

可信子系统开关标志位存放于Stage1.5中。

用于对系统内核、初始盘、配置文件、内核模块等文件进行验证的预期值存储于度量配置文件（MCF，Measurements Configuration File）中。而对于度量配置文件与Grub的Stage2的预期值分的处理：

默认认为MBR及Stage1.5可信。

1. Stage2及MCF的预期值存放于Stage1.5中。
2. 当度量配置文件等相关内容发生变化时，可信度量模块（内核层）通知可信管理模块（应用层）需修改文件列表，可信管理模块据此更新策略文件，并根据策略文件更新MCF及Stage1.5中存放的预期值。

注：可信引导模块其它功能同GRUB。

GRUB功能说明：

GRUB含有几个images文件，两个必需的文件stage1和 stage2，可选的为stage1.5和两个网络引导的文件nxgrub和pxegrub。stage1 是用于引导GURB的一个必须的映象文件。通常它是被嵌入到 MBR。或者一个分区的引导扇区之中。因为 PC 的引导扇区是 512 字节，所以 stage1也是512字节。stage1的作用就是从一个本地磁盘加载stage 2 或者stage1.5。

Stage1可以加载stage1.5再加载stage2，也可以直接加载stage2。（本启动模块建立在stage1加载stage1.5再加载stage2方式上。）Linux默认安装下，stage1装到MBR，stage1.5作为grub的文件系统的驱动程序，直接装到stage1的后面，也就是0磁道的第二个，到第64个簇。然后，stage1.5在系统安装的时候通常都做了处理，这样他就直接能找到stage2的文件了。

#### 组成结构

在原有grub的基础上增加了可信引导模块，使得grub在启动时加载文件前度量该文件。可信引导模块由可信度量验证子模块、可信度量值初始化与更新子模块组成。可信度量验证模块工作于操作系统启动阶段（GRUB中），对操作系统进行可信引导，可信度量值初始化与更新子模块模块能够扫描/boot目录生成MCF文件，同时计算stage2和MCF摘要值并写入引导区标记后。



图3 可信引导模块架构图

每个模块的功能分别为：

1. 可信度量验证子模块

* Stage1.5运行，计算stage2摘要值并与自身所存摘要值对比。
* 相同继续下一步，不同提示启动失败，按Esc键停止引动，按其他键忽略错误继续引导。
* 计算MCF摘要值并与自身所存摘要值对比
* 相同继续下一步，不同提示启动失败，按Esc键停止引动，按其他键忽略错误继续引导。

1. 可信度量值初始化与更新子模块

* 扫描文件，计算文件摘要值，生成MCF文件。
* 计算stage2和MCF文件摘要值写入引导区（stage1.5中）。
* 初始化与更新过程一样。

#### 工作流程

##### 总体流程

使用安装脚本安装含有可信引导模块的grub。可信管理模块在调用可信度量值初始化与更新子模块，命令行参数是1。可信度量值初始化与更新子模块扫描/boot下文件，计算文件摘要值，生成MCF文件，由于MCF文件最大为8KB，所以/boot下文件较多是，可生成多个MCF文件，文件名为MCF0到MCF9，最多10个。然后分别计算stage2和MCF文件的摘要值，MCF文件有多个时，分别计算每个MCF文件，然后异或成一个摘要值。以二进制形式读取引导区前32KB内容到文件，然后查找文件中字符为BJUTKXAQKXQDM的标志，写入结构体s1struct。结构体s1struct中包含了标志位和stage2、MCF文件摘要值。重启系统，grub引导系统，stage1.5运行，计算stage2的摘要值，与自身存储stage2摘要值对比，不同提示启动失败，按Esc键停止引动，按其他键忽略错误继续引导。相同则度量MCF，方式同度量stage2。不同提示启动失败，按Esc键停止引动，按其他键忽略错误继续引导。相同stage2运行，根据MCF的内容度量/boot下的文件。所有文件度量完毕，提示文件度量数量，文件度量失败数量。若失败数量不为0，提示按Esc键停止引动，按其他键忽略错误继续引导。为0，则继续grub后续步骤，内核运行。可信引导到此结束。

可信引导模块总体运行流程如下图所示：



图4 可信引导模块运行流程图

##### 可信度量验证子模块工作流程

1. stage1.5运行，度量stage2，失败按Esc键停止引动，按其他键忽略错误继续引导。成功进行下一步。
2. 度量MCF，失败按Esc键停止引动，按其他键忽略错误继续引导。成功进行下一步。
3. stage2运行，根据MCF内容进行度量其他文件。
4. 所有文件度量完毕，提示文件度量数量，文件度量失败数量。若失败数量不为0，提示按Esc键停止引动，按其他键忽略错误继续引导。为0，则继续grub后续步骤，内核运行。

##### 可信度量值初始化与更新子模块工作流程

1. 扫描/boot目录下文件并计算摘要值，生成MCF。
2. 计算stage2和MCF摘要值
3. 以二进制形式读取引导区前32KB内容到文件，然后查找文件中字符为BJUTKXAQKXQDM的标志。
4. 写入结构体s1struct。结构体s1struct中包含了标志位和stage2、MCF文件摘要值。

#### 重要数据结构

MCF文件结构

MCF是度量配置文件（Measurements Configuration File）的简称，存放于引导分区上，用于保存引导模块需要度量的文件列表。该列表包含内核文件列表、初始盘文件列表、OS内核启动之后而OS动态度量模块未启动之前需验证的文件列表和上述诸文件的摘要值。

MCF文件中的数据按以下格式组成：

文件Hash值+文件名称（全路径）

文件Hash值+文件名称（全路径）

……

其中，文件名称为带设备信息的绝对路径格式，应使用GRUB可以识别的格式，即：分区标记（如(hd0,0)） + 文件完整路径，文件Hash值长度视最终确定的摘要算法的要求而定（SM3算法为256比特。

Stage1.5标志结构

struct {

uint8 start\_mark[13]={}; //开始标志

uint8 on\_off; //可信开关标志，1开0关

uint8 soft\_hard;//软硬件模式标志，1软0硬

uint8 MCFcount;//MCF文件个数

uint32 s2\_hash[8];//stage2摘要值

uint32 mcf\_hash[8];//MCF文件摘要值

}\_attribute\_((packed)) s1struct;

该结构用于保存可信引导模块的相关标识信息和度量预期值。其中，start\_mark[13]为应用层的查找标志，用于查找标志位和摘要值在stage1.5中的写入位置；on\_off是可信开关标志，1为开启可信引导，0为关闭可信引导，关闭可信引导后grub与普通grub功能相同。soft\_hard是用于保存使用模式信息，标识当前是使用可信芯片硬件接口或软算法接口，目前为保留标识，1为使用软件模式，即摘要值的计算使用软件算法sms3。0为硬件模式，如果得到grub下tcm的驱动，即可以使用tcm内置的sms3计算芯片计算摘要值。 MCFcount记录MCF文件的个数，因为MCF文件最大为8KB，所以当有多个MCF文件是，必须计算每个MCF文件摘要，再异或运算形成一个摘要值再对比。s2\_hash[8]、 mcf\_hash[8]分别为存储stage2和MCF文件的摘要值。

#### 接口

##### 启动/关闭可信启动功能

描述：由可信管理模块以脚本形式调用初始化与更新子模块实现。

参数：命令行参数形式，0为关闭可信启动功能，1为开启可信启动功能。

返回结果：成功返回0，失败打印错误信息，返回-1。

##### 更新预期度量值

描述：由可信管理模块在后台调用初始化与更新子模块实现。

参数：命令行参数形式，只能为1。

返回结果：成功返回0，失败打印错误信息，返回-1。

##### 文件被篡改，可信启动失败

描述：可信启动失败后，提示用户关闭系统后使用中标麒麟操作系统恢复光盘恢复系统。

参数：键入Esc或者其他键。

返回结果：用户键入Esc键，停止启动。按其他键，可忽视错误，继续启动。

### Dom0可信管理模块

#### \*\*\*

### 虚拟可信根模块

\*\*\*

### DomU可信监控模块

#### \*\*\*