毒酒：软件供应链混合样本攻击和防御

Poisoned Wine: Software Supply Chain Mixed Sample Attack and Defense

个人简介

吴鹤意，东南大学网络安全专业毕业，拥有丰富的安全工作经验，参与过多个中央部委级网络安全体系建设以及攻防演练和实战，先后在华为2012实验室和深信服创新研究院担任安全技术专家，从事AI安全，数据安全，云安全，安全开发，情报狩猎等领域的研究和产品端到端落地。在国内外知名网络安全会议发表演讲，例如HITB，BSides，看雪SDC，XCon，Geekpwn，FB AI安全讲师等，参与了国内外多个安全标准的编制（IEEE P2841-AI安全相关评估标准，国产化操作系统安全等），发表了多篇EI/SCI论文和专利，拥有国内外多项安全证书（CISP，CCSK，CDPSE等），给监管部门提交过若干0day漏洞，国产化操作系统通用安全问题和高级攻击狩猎溯源报告。

本次议题内容仅代表个人观点

1、背景介绍

2、混合样本思路

3、测试效果

4、防御手段

背景介绍

混合样本指的是：跨平台的恶意样本。此类样本风险涉及软件供应链，之前就存在，例如通过　　　在ΩΓΓ褢平台上运行偾Γ平台的恶意软件，在偾Γ平台上通过vii yΩ运行ヸΓΓ褢平台的样本，通过ᄼΓΓ犭ジ徲在ヸΓΓ褢平台上运行ᄼΓΓ∨mifの应用。也有人研究过相关的问题，例如右边所示：

Linux Malware Could Run Undetected on Windows: Researchers

By Ionut Arghire on September 12, 2017

Share　Tweet　推荐 0　RSS

A new Windows 10 feature that makes the popular Linux bash terminal available for Microsoft's operating system could allow for more malware families to target the operating system, Check Point researchers claim.

Called Windows Subsystem for Linux (WSL), the feature exited beta a couple of months ago and is set to become available to all users in the upcoming Windows 10 Fall Creators Update (FCU), set to be released by Microsoft in October 2017.

包括学术界机构也发表过此领域的研究，例如如下所示：

相关的攻击成功率如下所示：

Security implications of running windows software on a Linux system using Wine: a malware analysis study

Rory Duncan[1] · Z. Cliffe Schreuders[1]

Received: 13 April 2017 / Accepted: 22 March 2018
© The Author(s) 2018

不过由于这类场景之前出现的不多，所以并未引起大家足够的关注。相关的厂商对此也不是很积极。

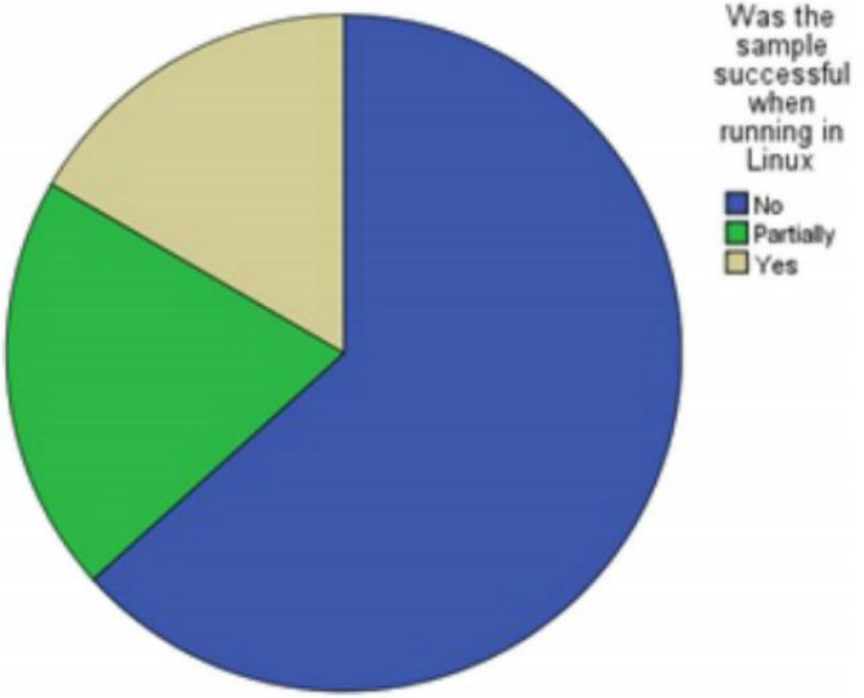


Fig. 3 The success rate of windows malware in wine

但是目前情况发生了变化，在中国，近些年，越来越多支撑跨平台的操作系统和产品进入大家的日常工作中。例如UOS，目前在中国已经有了可观的使用率（市场占有率超过70%），而且支持win和android平台的应用在linux上运行。例如如下所示：

UOS简介

良好兼容性

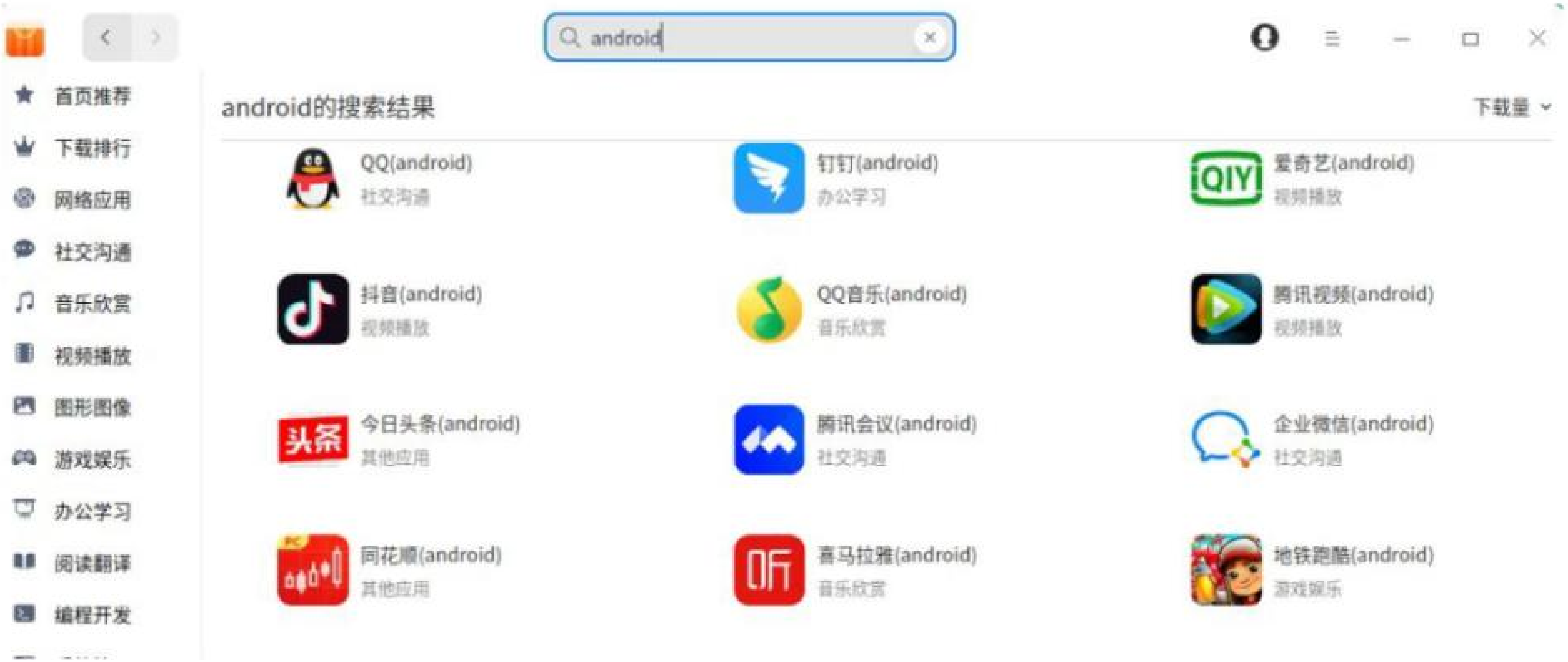
兼容x86、ARM、MIPS、SW架构；支持七大国产CPU品牌：龙芯、申威、鲲鹏、麒麟、飞腾、海光、兆芯；与40多个国产桌面整机厂商达成合作；适配了180多款桌面类整机型号（笔记本、台式机、一体机、平板）

软件，商店已上架800多应用；与讯飞、金山、网易等300多家国内软件开发商达成合作；适配超过600款桌面商用软件；基于Wine技术，无缝迁移Windows常规应用

外设，兼容主流的打印机、扫描仪、高拍仪、读卡器、Raid卡、HBA卡等外设；与超过80家外设厂商达成合作；适配超过1300款第三方外设产品

在x86平台上运行ARM平台应用

!!!!!’Ë y在x86平台上运行ARM平台应用，不仅软件厂商，包括中国的一些T e’ 生产商也在积极开发相关功能，例如龙芯就支持硬件二进制翻译能力，如右所示：



龙芯3A5000/3B5000 产品参数

主频 2.3GHz–2.5GHz	**峰值运算速度** 160GFlops
核心个数 4	**处理器核** 支持LoongArch®指令系统；支持128/256位向量指令；四发射乱序执行；4个定点单元、2个向量单元和2个访存单元
高速缓存 每个处理器核包含64KB私有一级指令缓存和64KB私有一级数据缓存；每个处理器核包含256KB私有二级缓存；所有处理器核共享16MB三级缓存	**内存控制器** 2个72位DDR4-3200控制器；支持ECC校验
高速I/O 2个HyperTransport3.0控制器；支持多处理器数据一致性互连（CC-NUMA）	**其它I/O** 1个SPI、1个UART、2个I2C、16个GPIO接口
功耗管理 支持主要模块时钟动态关闭；支持主要时钟域动态变频；支持主电压域动态调压	**典型功耗** 35W@2.5GHz

龙芯简介

龙芯支持硬件二进制翻译，所以以前被大家忽视的软件供应链跨平台样本问题是时候引起大家的关注了。

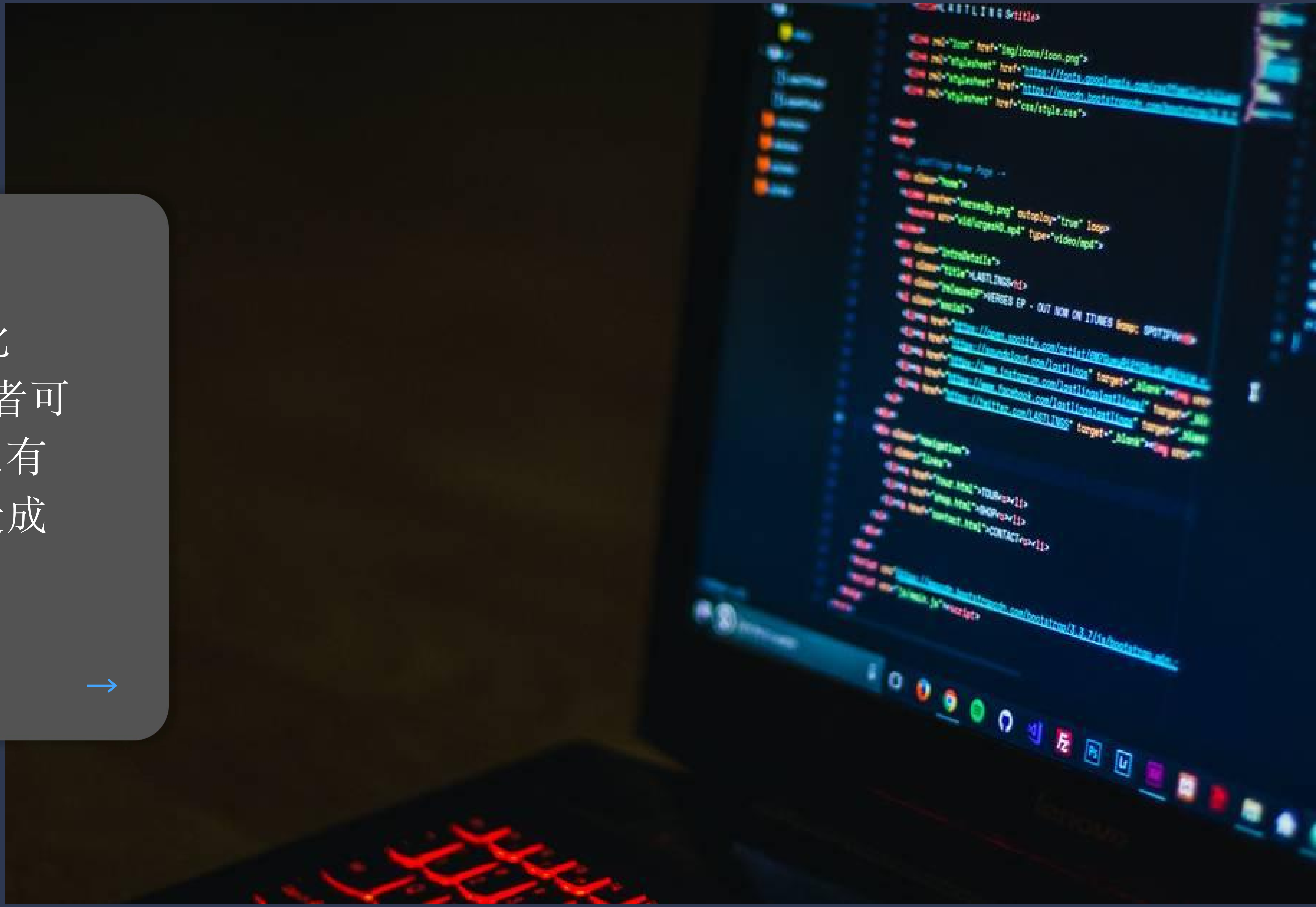
混合样本思路

我们在三个中国国内都具有可观使用量的操作系统上进行了测试。使用了偾ሰ⺀和两个偾ሰ平台上知名的勒索恶意软件：V 刂ᕫ⼆U 世ᕪ和 vii ⼦ሰሰ⼦ŭ⺀ሰ。三个平台和相关配置如下所示：

供应商	版本	版本	防御手段
机	（专业版㗊㗊）		终端安全㗊㗊
阿里云	位!' d 㗊版		主机安全
华为云			主机安全

目前虽然[illegible]平台上的样本相比侦[illegible]平台还不是很多，但是攻击者可以通过上述的思路，迅速利用已有的大量样本，快速进行攻击，造成严重的破坏

→



测试效果

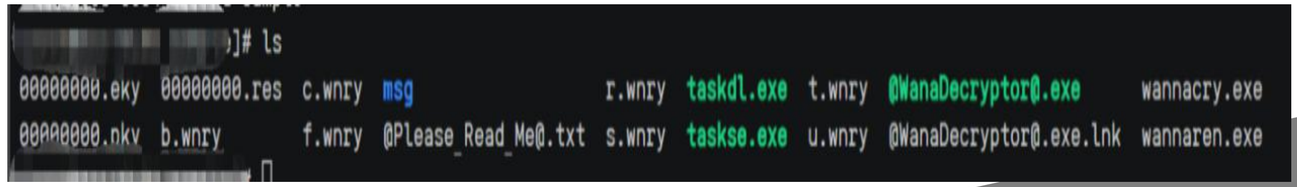
测试结果汇总如下：

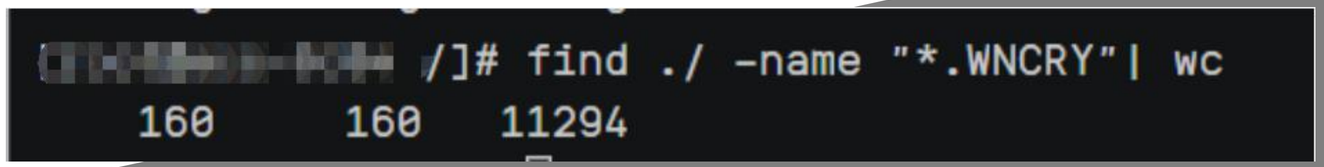
供应商			其他样本	防御告警
机	攻击成功	攻击未成功	部分成功（占比[illegible]）	文件隔离
阿里云	攻击未成功	攻击成功	部分成功（占比[illegible]）	文件落盘和后缀告警
华为云	攻击成功	攻击成功	部分成功（占比[illegible]）	暴力破解

其他样本为随机抽取的12个真实win平台样本

华为云测试结果举例：
WannaCry攻击共加密文件160个，主机安全告警暴力破解

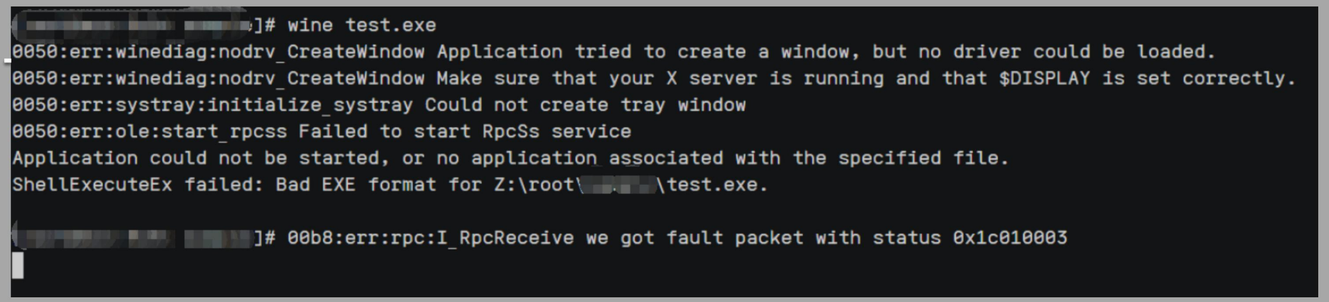
文件加密情况





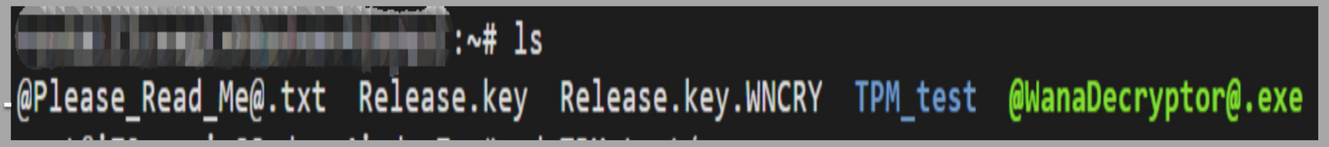
加密文件统计

主机安全告警

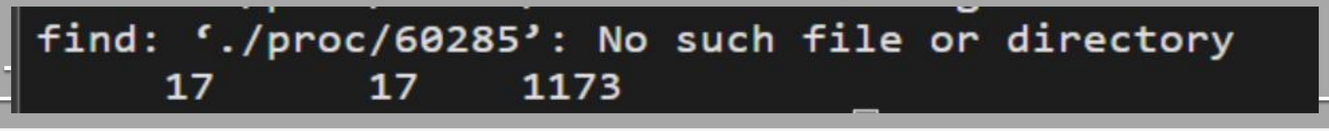


其他样本运行举例阿里云测试结果举例：

WannaCry攻击共加密文件17个，主机安全告警暴力破解



文件加密情况



文件加密情况 ----------

```
find: ‘./proc/60285’: No such file or directory
     17      17    1173
```

加密文件统计 ----------

恶意软件-勒索病毒 待处理

该告警由如下引擎检测发现：

文件路径：/root/.wine/dosdevices/z:/@WanaDecryptor@.exe

恶意文件md5：7bf2b57f2a205768755c07f238fb32cc

扫描来源方式：落盘文件扫描

检测方式：云查杀

精准防御- 可疑勒索行为 拦截成功

该告警由如下引擎检测发现：

ATT&CK攻击阶段：影响破坏

恶意行为：写勒索特征后缀文件

执行命令的进程：/usr/lib/wine/wineserver64

进程id：55091

执行命令：/usr/lib/wine/wineserver64 -p0

读写的目标文件：/usr/bin/@Please_Read_Me@.txt

主机安全告警 ----------

```
[redacted]:~/TPM_test/sample# wine hello.exe
hello world!
Press any key to continue... [redacted]~/TPM_test/sample# wine nc.exe
Cmd line: ls
```

其他样本运行举例 ----------

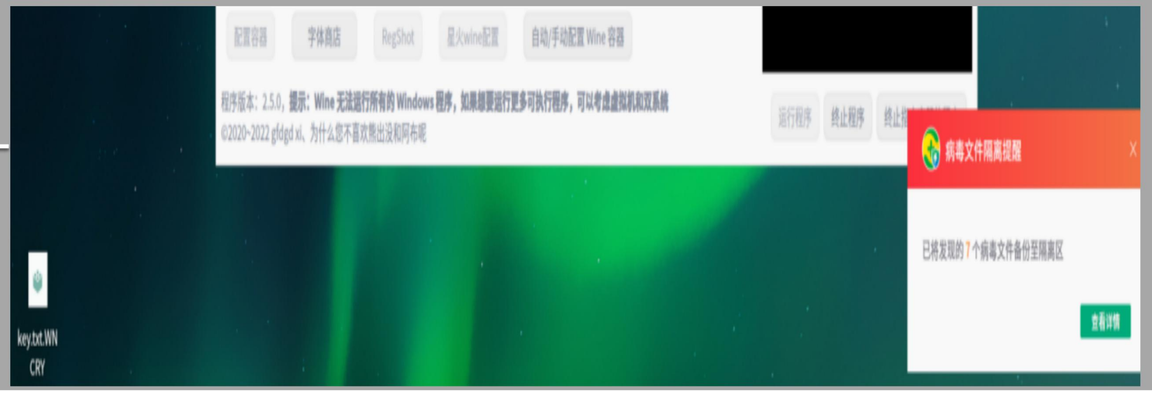
UOS真机测试结果举例：

攻击成功示例

WannaCry攻击共加密文件62个，主机安全告警进行文件隔离

```
find: './media/loongson/f51479c1-e
      62      102     5134
```

加密文件统计

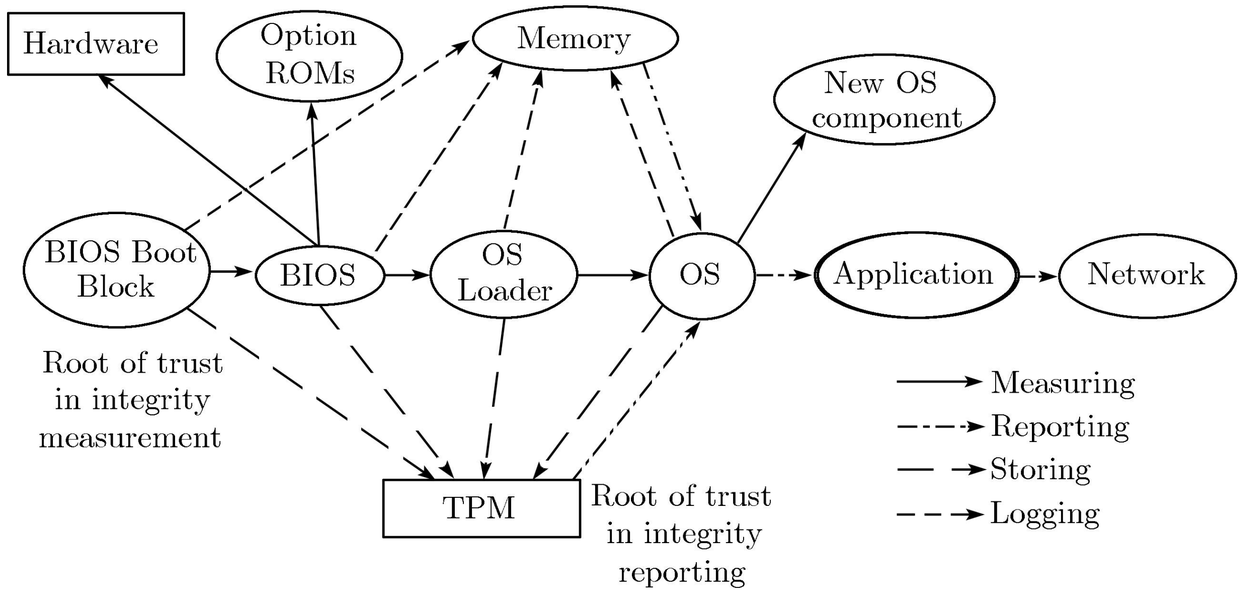


从上述测试可知，有部分的样本可以在linux平台上运行成功并生效，其中WannaCry和WannaRen两个知名勒索软件也在一定程度上逃过了主机安全的防御，对部分文件进行了加密破坏，说明我们不能忽视此类问题。

防御手段

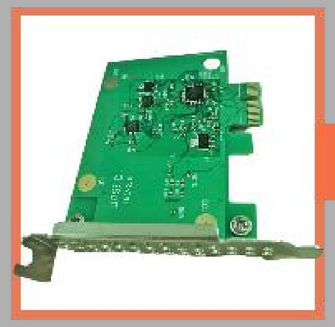
目前各家服务商对于此类混合样本还是基于以往的落盘查杀和文件后缀规则，或者暴力破解来判断，普遍存在防御盲区和滞后性。针对此种新型攻击手法，我们提出了基于TPM EDR的防御方案，下面进行介绍：

受信任的平台模块（TPM）技术旨在提供基于硬件的安全相关功能。TPM芯片是一种安全的加密处理器，旨在执行加密操作。该芯片包含多个物理安全机制以使其防篡改，并且恶意软件无法篡改TPM的安全功能。TPM的可信链如右图所示：



目前一些服务商已经提供了TCM（中国国内版本的TPM）功能，例如阿里云就提供了vTCM产品，如右所示：

USB



PCIE

阿里vTCM模块
但是目前提供的TCM功能并未覆盖应用层保护，没有充分发挥可信计算的全部能力。以前因为TPM功能还未大规模使用，导致很多用户必须通过外置的TPM模块来尝试和体验，如下所示：

在之前测试中也已经开启：

```
:~/TPM_test# ls /dev/tpm*
/dev/tpm0  /dev/tpmrm0
```

The Unfortunate Reality

In the vast majority of situations, ELAM vendors don't meet Microsoft's recommendations. In 2021, Maxim Suhanov published a blog post, "Measured Boot and Malware Signatures: exploring two vulnerabilities found in the Windows loader," wherein he compared 26 vendors' ELAM drivers. He noted that only 10 used signatures at all; of these, only two used them to affect Measured Boot in the way intended by Microsoft. Instead, these vendors use their ELAM drivers nearly exclusively to create protected processes and access the Microsoft-Windows-Threat-Intelligence ETW provider discussed in the next chapter.

各种外置TPM模块
因为目前TPM芯片在Win11中必须开启，说明技术准备已经成熟，所以我们提出了TPM EDR这个概念，通过将可信计算与EDR结合，提供原生的安全防御能力，例如下表所示：

	防护软件	可信计算防护
木马	防御	免疫
广告推广	防御	免疫
勒索程序	防御	免疫
蠕虫	防御	免疫
RootKit	防御	免疫
WebShell	防御	免疫
恶意软件	防御	免疫
病毒	防御	防御
后门	防御	防御
漏洞利用	防御	防御

TPM EDR=UEFI TPM Agent + Linux TPM Agent，包括了可信启动方案、应用程序白名单、基于路径的访问控制、基于标签的访问控制、基于系统调用的访问控制、远程证明方案、可信管理平台等功能。

可信启动方案细节和UEFI TPM Agent实现要点：

（1）SecureBoot使用自定义证书，在BIOS里导入
（2）自研UEFI放置在磁盘上，安全性由自定义证书对应密钥签发（由我们掌握密钥）签名，SecureBoot会校验签名
（3）自研UEFI校验GRUB签名，GRUB签名由自定义证书对应密钥签发
（4）GRUB对Linux Kernel和Initramfs进行校验，校验通过再进行加载
（5）之后靠initramfs内的tpm agent用户态对其他程序进行度量
（6）自研UEFI有两个模式：强制模式和宽容模式，宽容模式下只告警，不拦截
（7）“模式”保存在TPM内

应用程序白名单要点：

（1）Linux TPM Agent的基本框架参考Fedora的fapolicyd的实现方式
（2）fapolicyd需要4.15+内核
（3）可以实时扫描二进制文件、脚本文件（仅以MIME判断，不考虑复杂的攻击脚本绕过）
（4）同样具备强制模式和宽容模式

基于路径的访问控制要点：

（1）同样以fanotify为基础，以主体（进程路径）和客体（访问文件路径）的规则标记主体是否访问客体
（2）Fanotify可以得到主体pid和客体路径
（3）默认规则考虑可操作性，对系统文件不做约束，对第三方文件重点约束
（4）具备强制模式和宽容模式和学习模式，学习模式对单一进程进行学习（类似tomoyo模块）

基于标签的访问控制要点：

（1）同样以fanotify为基础，以主体（进程路径对应的文件系统元属性）和客体（访问文件对应的文件系统元属性）做为规则，类似smack的基础规则
（2）Fanotify可以得到主客体的元属性，但需要考虑加速缓存来存储元属性
（3）默认规则考虑可操作性，对系统文件不做约束，对第三方文件重点约束
（4）具备强制模式和宽容模式

可信管理平台要点：

（1）统一管理所有可信设备，实现TCM/TPM身份登记、证书颁发、可信策略下发配置、可信状态校验（远程证明）等功能
（2）管理可信启动链上涉及的固件更新的配套可信策略（关系RTM）
（3）管理可信应用程序白名单的可信策略
（4）实体/虚拟TPM/TCM证书颁发
（5）实现等保2.0中，关于“在检测到其可信性收到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心”的要求

基于系统调用的访问控制要点：

（1）以对auditd的配置为基础，考虑将对重点程序的高危系统调用进行审计，并转发审计日志到本机UDP端口（快速原型开发）
（2）宽容模式下只记录警告
（3）强制模式下通过外部kill信号杀死高危进程
（4）对socket的审计可以带来按进程的网络活动监控，理论上可以得到比iptables更细粒度的网络访问控制（配合netlink）

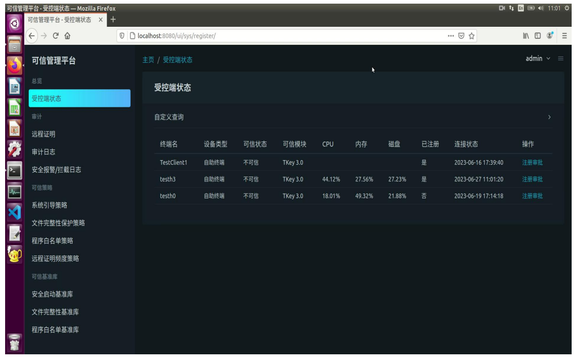
远程证明方案要点：

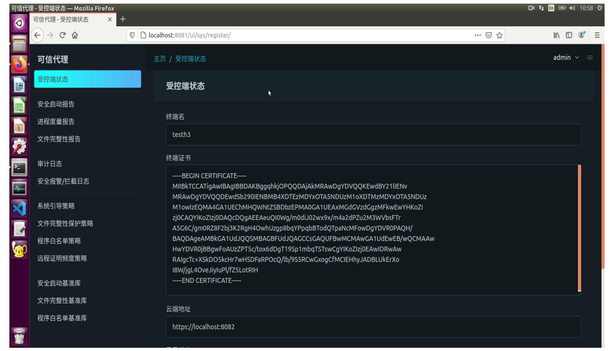
（1）可信启动时滚PCR，并记录启动日志，按TPM标准执行
（2）应用程序白名单滚PCR并记录日志：只记录未在日志中的度量，此时方才滚PCR（此即IMA模式）
（3）各访问控制：只记录未在日志中的访问轨迹，此时方才滚PCR（可能拖累系统速度，解决方案待调研）

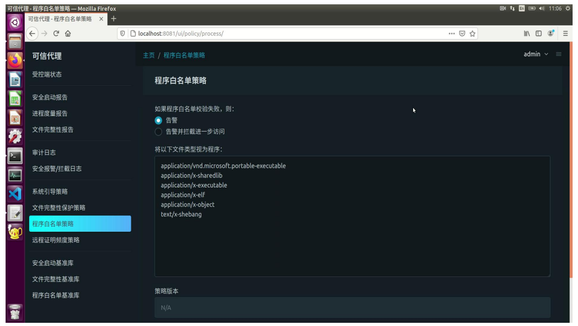
TPM EDR效果演示

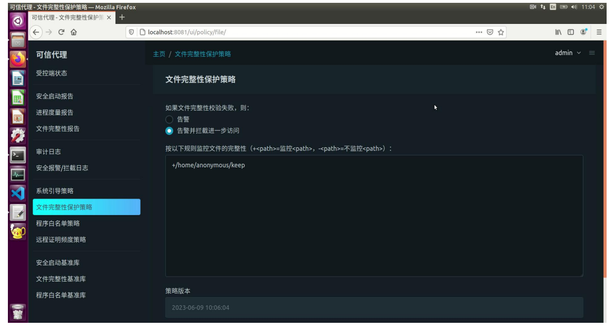
内存消耗7M，CPU 3%以内

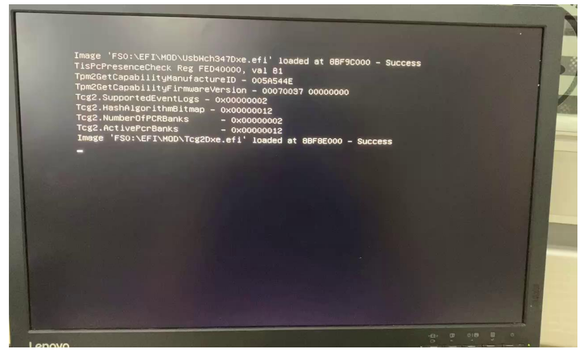
1.可信管理平台界面概览
2.可信代理程序界面概览
3.可信代理程序——通过启动校验
4.可信代理程序——启动校验失败
5.可信代理程序——对未知可执行文件拦截或告警
6.可信代理程序——阻止对受保护的文件进行修改





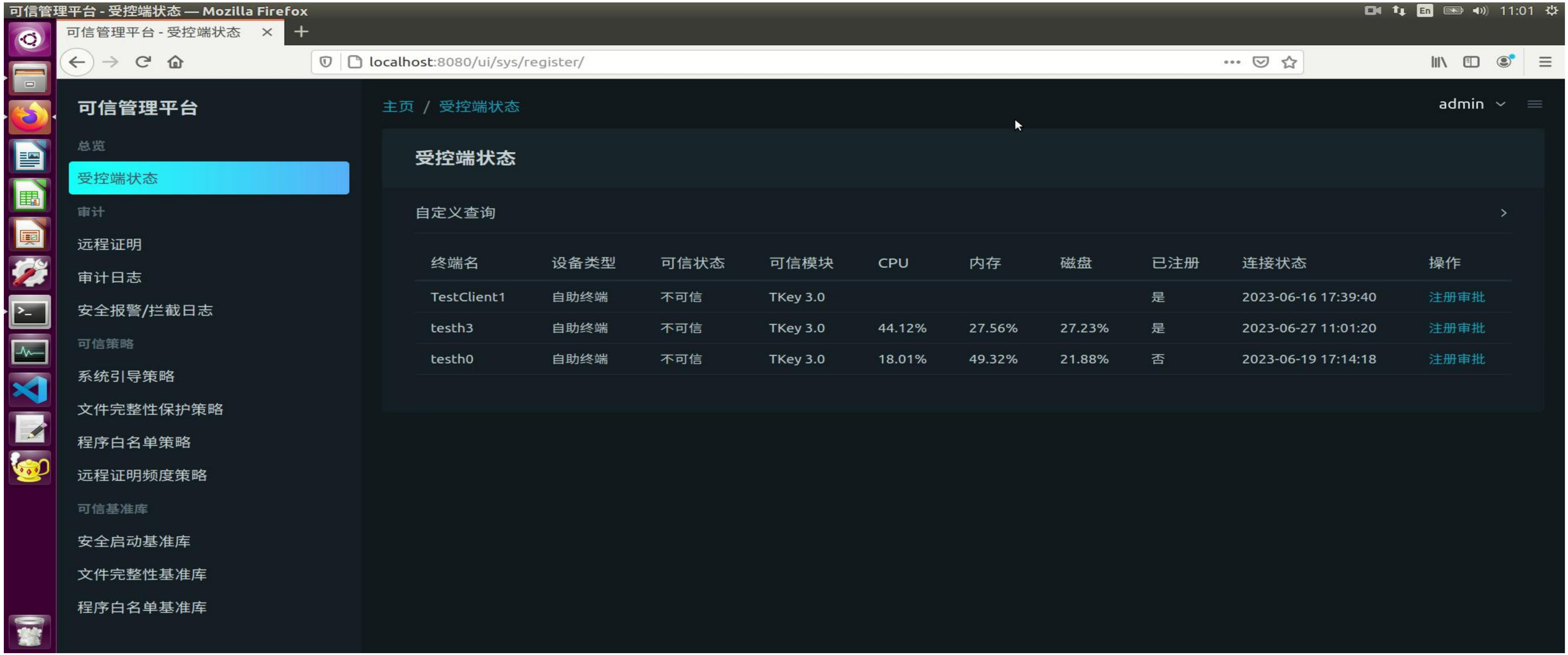






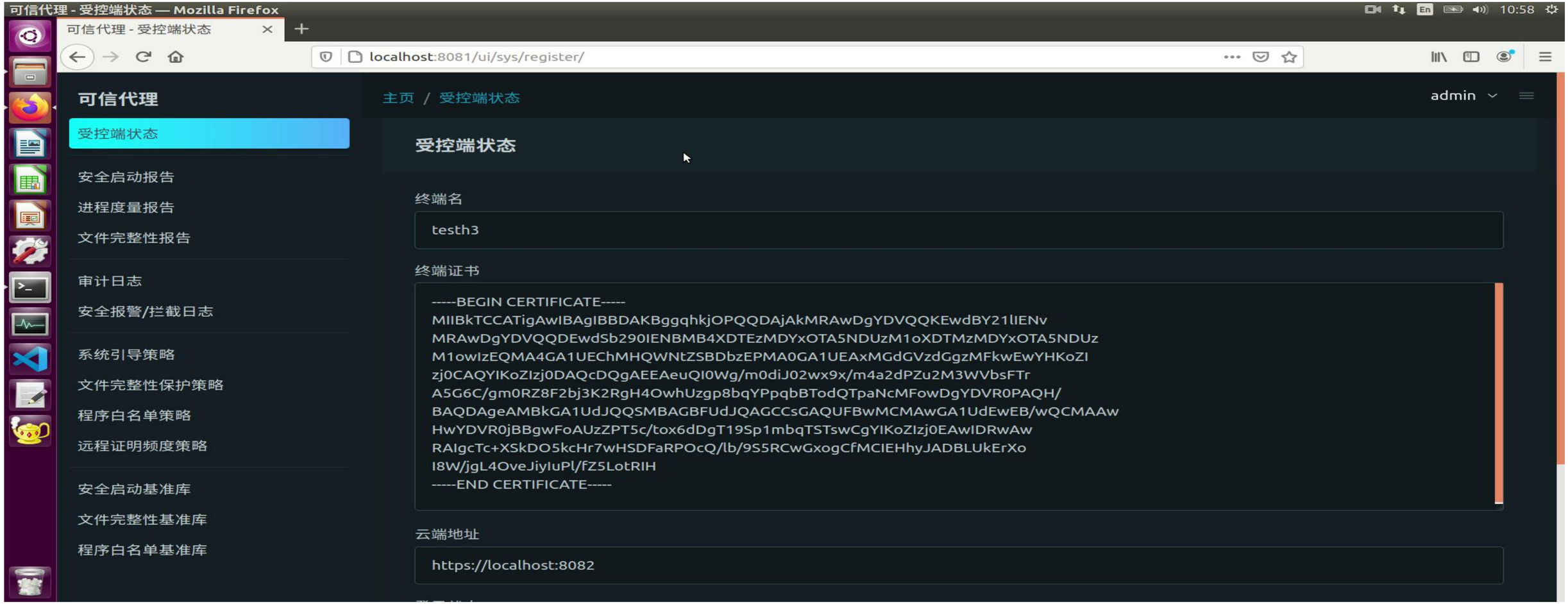
TPM EDR效果演示

1.可信管理平台界面概览



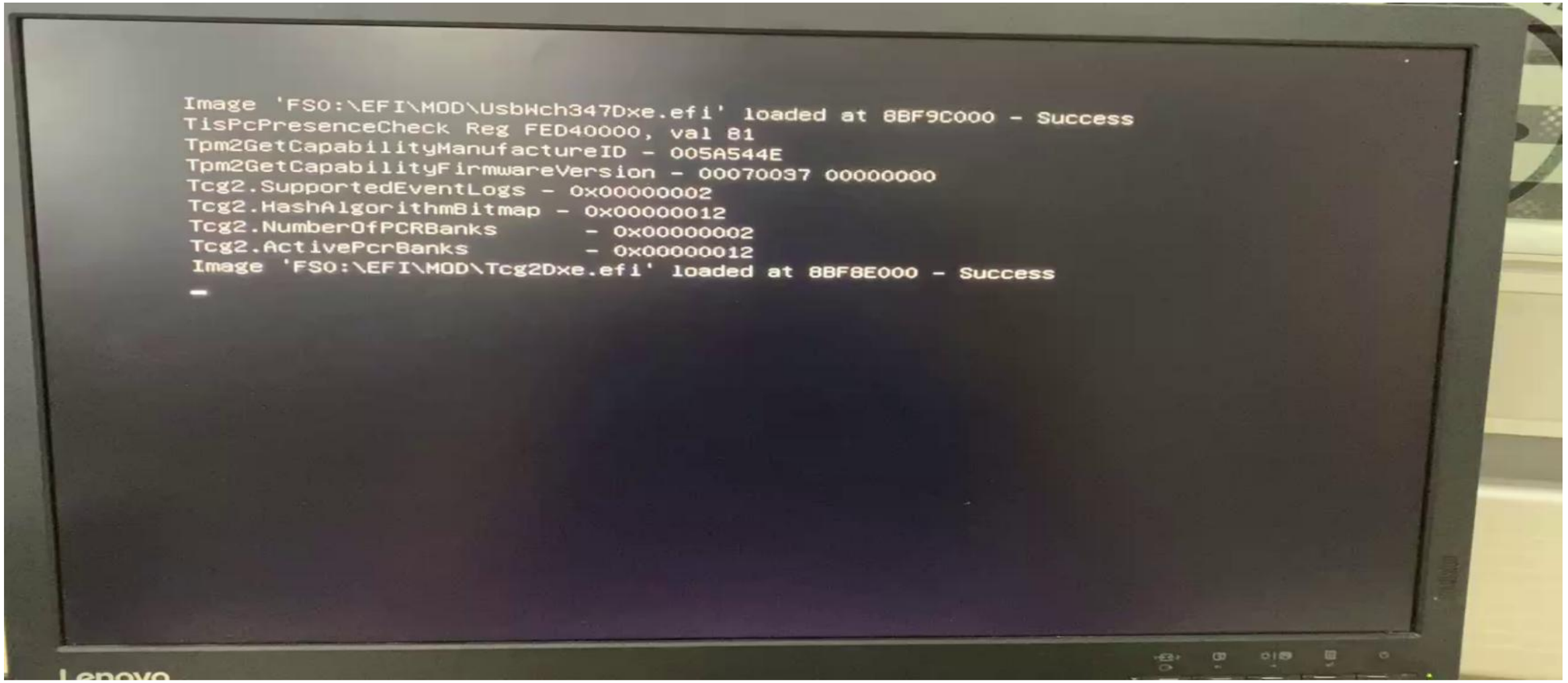
TPM EDR效果演示

2.可信代理程序界面概览



TPM EDR效果演示

3.可信代理程序——通过启动校验

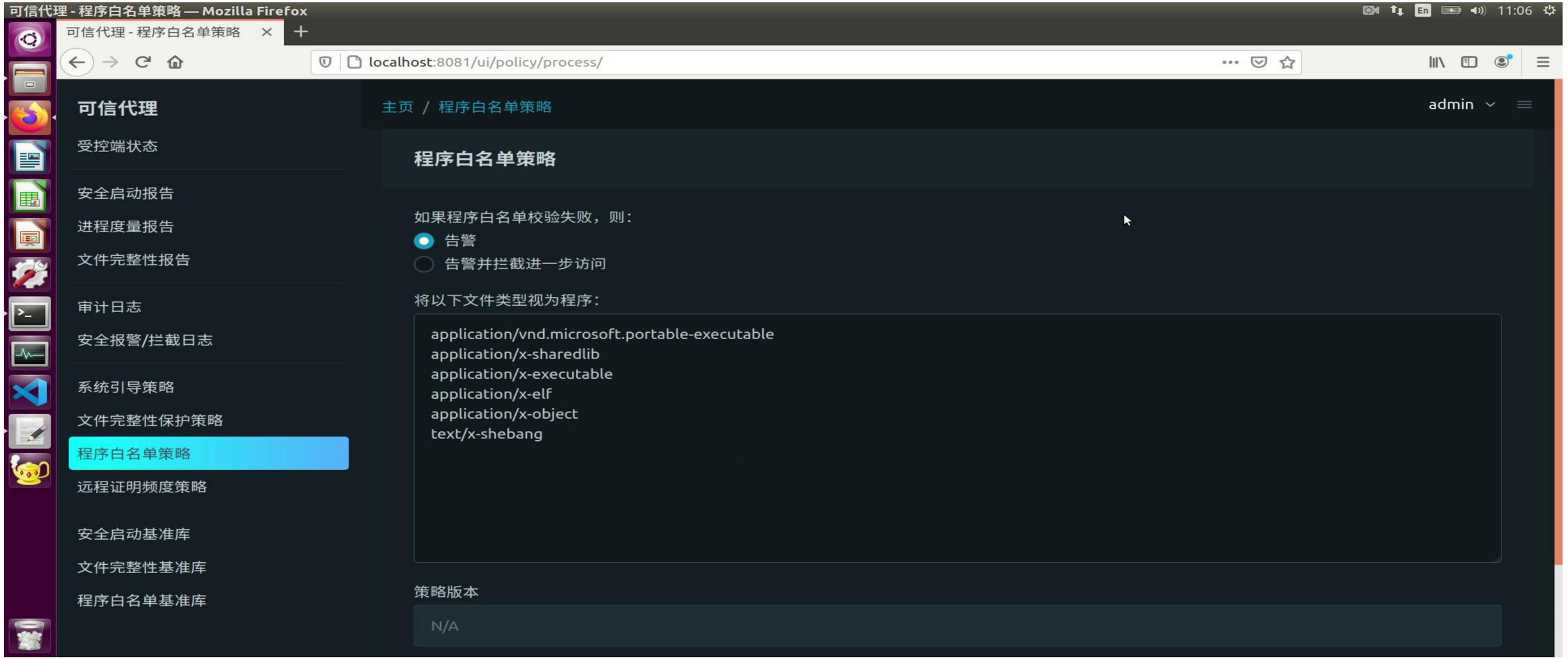


TPM EDR效果演示

4.可信代理程序——启动校验失败

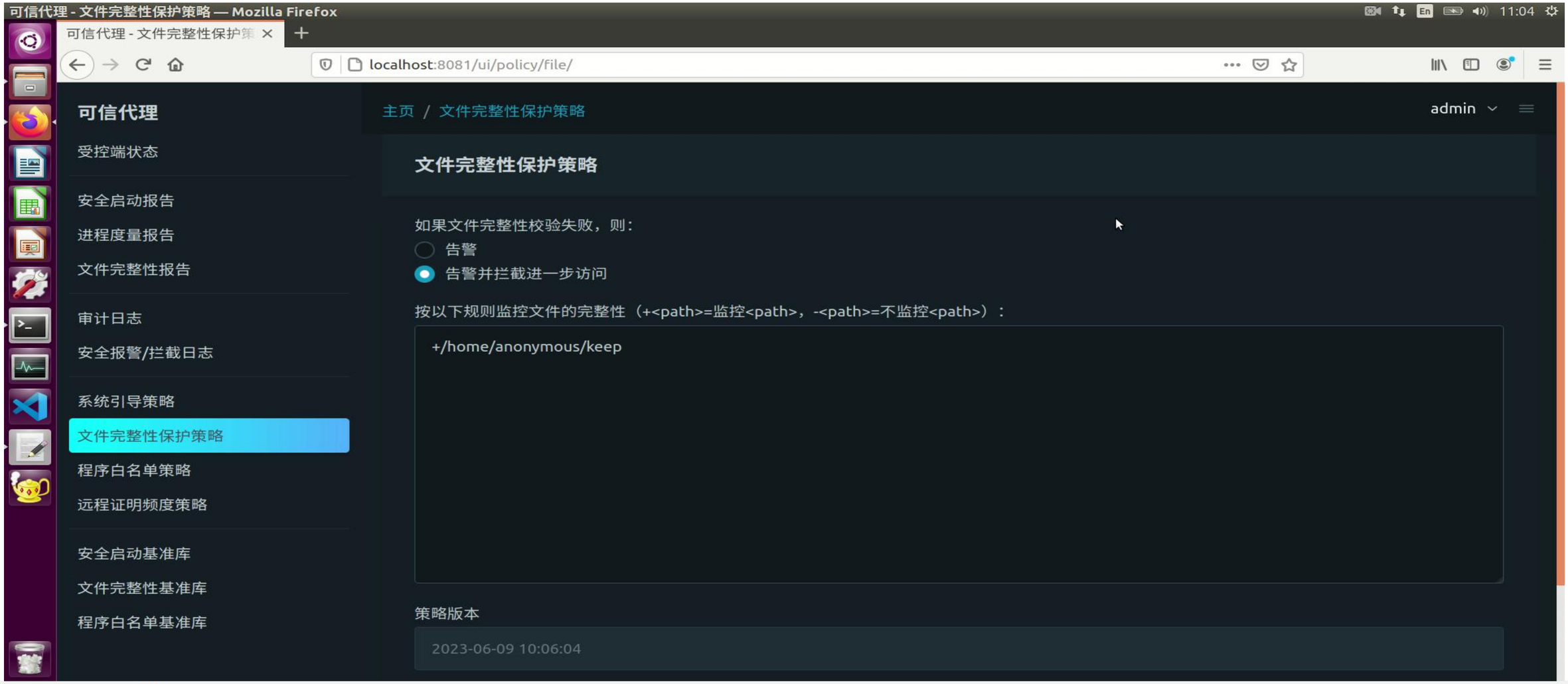
TPM EDR效果演示

5.可信代理程序——对未知可执行文件拦截或告警



TPM EDR效果演示

6.可信代理程序——阻止对受保护的文件进行修改



通过上述的设计，我们希望可以利用可信计算的技术来提高针对软件供应链混合样本的防御能力，补足之前忽视的一个安全威胁。我们认为随着跨平台的场景越来越多，以前的异构安全理念，也会被新的安全威胁挑战，我们应该提前规划，做好防御准备，保护用户的安全。

想一想，我该如何把这些技术应用在工作实践中？

THANKS