2021 年度 CCF-深信服伏羲基金申报课题

目录

（1）大数据探索性数据分析的研究与应用

背景

随着大数据的发展，在不断的膨胀数据中，依赖人工数据分析师来分析数据会具有一定的局限性，而突破人工的思维定式，才可以从海量数据中发现隐藏的信息。因此，自动的进行探索性数据分析(Exploratory Data Analysis (EDA))就变得越来越重要，即通过数据分析和探索来获取隐藏在数据中的有意义、有用和可操作的信息，发现有趣的数据模式逐渐变成一种常见且重要的分析需求。而目前在多维数据中进行自动探索仍然具有挑战性，构建自动、高效、准确、使用统一框架、抽取结构化知识的探索性数据分析系统还是一个亟待解决的难题。

目标

针对上述提到的问题，结合业界与学界最新研究成果，探索方案或者算法设计：

1、探索一种新的探索性数据分析(Exploratory Data Analysis (EDA))分析方法，具有自动、高效、准确、使用统一框架、方便抽取结构化知识等特征，可以应用到数据仓库中。

2、发表 CCF-A/CCF-B 以上的高水平学术合作论文至少 1 篇。

3、形成可以落地的技术方案，在真实客户业务侧落地。

相关研究课题

1、数据挖掘 2、图学习 3、数据库系统

（2）数据质量与数据治理智能化研究与应用

背景

大数据分析在商业决策和商业活动分析中起着至关重要的作用。尽管大数据处理技术层出不穷，用户从数据中获得知识的过程依然困难重重：（1）用户数据质量差，没有系统的方法和技术提升用户数据质量，无法保证用户获取的知识是否可靠；（2）用户的业务数据流复杂，且可能存在性能问题，没有一套系统的方法，能够帮助用户改善业务流程，提升业务数据处理的效率；（3）用户对数据不了解，可能开发的业务不能完全发挥数据价值，需要一套技术方案和解决方法，帮助用户发现数据中可能存在的规律，并辅助用户发现有价值的数据应用。

目标

针对数据质量、数据治理相关问题，结合业界与学界最新研究成果，研究满足用户需求的方案：

1、探索智能化提升用户数据质量的技术方案，或智能化改善用户业务流程的技术方案，或智能化发现用户业务盲区并推荐有价值的数据规律

2、产出能解决用户痛点的智能数据质量或智能数据治理工具。

3、发表 CCF-A/CCF-B 以上的高水平学术合作论文至少 1 篇。

4、形成可以落地的技术方案，在真实客户业务侧落地，产生实际业务价值。

相关研究课题

1、数据挖掘

2、数据库&数据仓库

3、算法

4、数据发现（data discovery）、数据清洗（data cleaning）

（3）大数据 OLAP 引擎性能及易用性增强研究与实践

背景

随着大数据业务的复杂性，对 OLAP 引擎的能力从原始的单一场景的性能要求，逐步的朝着复合场景的需求演进，也即是全场景的 OLAP 引擎的诉求。然而，现有的开源 OLAP 引擎或者商业版的 OLAP 引擎面对大数据的体量，在不少的场景上还无法完全满足客户的极速性能诉求，例如多维数据分析、数据实时更新等等。与此同时，随着系统的复杂化，易用性也成为了用户关注的重点，例如分析 SQL 执行计划的性能瓶颈、SQL 智能优化等等。因此，本课题希望就 OLAP 引擎在性能和易用性上达成研究合作，并促成成果落地，能够提升深信服 OLAP 引擎的能力

目标

针对 OLAP 引擎相关的问题，结合业界与学界最新研究成果，研究和落地相应的性能优化、易用性改造的核心技术点：

1、构建具有业界领先的大数据 OLAP 性能和易用性相关的核心技术，例如：高性能实时更新、增量物化视图、分布式 Join 算法优化、聚合分析性能优化等等。

2、发表 CCF-A/CCF-B 以上的高水平学术合作论文至少 1 篇。

3、形成可以落地的技术方案，在真实客户业务侧落地。

相关研究课题

1、OLAP 优化

2、实时更新

3、物化视图

4、分布式 Join

（4）敏感数据地图

背景

当前企业的业务系统越来越复杂，业务系统之间的数据交流更频繁，对于这些业务系统对敏感数据的访问关系的梳理是一件非常复杂而且繁琐的事情，用户在做数据安全相关的建设的前提就是要能够梳理出这些敏感数据地图的访问关系，针对这些访问关系才可以做下一步的计划和安排。敏感数据地图的自动化梳理可以做成我们数据安全产品的一个非常重要的核心竞争力。

目标

1、通过流量自动的检测数据在采集、使用、分享、流转、存储、销毁等阶段的访问关系

2、能够对分类数据的访问关系进行自动化的展示，不同数据类型在业务系统之间是如何流转和使用的，自动识别非法的数据访问关系

相关研究课题

数据安全、数据地图

（5）Stream Algorithms 在生产环境下大数据分析中的应用

背景

现代 IT 系统变得越来越复杂，随之网络故障原因也千奇百怪。快速的网络故障定位和诊断可以大大缩短故障的影响时间，从而提升用户的业务体验。随之云计算的引入，IT 规模也变得越来越大，因而，网络监控所收集的数据量也指数级的增加。云计算的网络故障诊断将越来越依赖大数据处理技术，并且需要高实时性。Stream algorithms 可以实时快速地进行大数据的分析，如计数估计，异常值检测等，并且计算资源（CPU 和内存）消耗一般而言也会很低。但该类算法本身是一种近似算法，需要可以从理论上来对误差给出数学上下界，以保证算法的效果。

目标

针对上述提到的问题，结合业界与学界最新研究成果，完成如下方案或者算法设计:

1、提出一种新的 Stream Algorithm，可以应用到网络故障或者异常检测中，并给出算法误差的数据上下届。算法需要应用到主流的大数据计算引擎如 spark，flink 中。

2、发表 CCF-A/CCF-B 的学术论文至少 1 篇。

相关研究课题

1、大数据

2、近似算法

3、云计算网络排障

（6）软硬件一体化探索

背景

随着当前 X86 算力持续提升，且 intel 开源的 dpdk 应用层包处理框架越来越完善。

之前多用在服务器场景的 x86 体系结构，近来在工控机场景也得到了越来越多的应用。

利用应用层处理包框架，可以大幅降低开发难度和排障成本，从而极大的缩短了项目周期。

目前随着智能网卡、可编程 ASIC 在云场景持续演进，有可能探索出一套异构的方案，

将对网络业务流 L4/L7 的处理卸载到专用硬件之上，特定场景下进一步提高工控机的性能和性价比。

目标

1、离线异构架构

工控机集成不带网口的硬件加速模块，卸载必要的 L4/L7 业务流，从而提高性价比。

2、在线异构架构

工控机集成带网口的硬件加速模块，卸载必要的 L4/L7 业务流，从而提高性价比。

相关研究课题

1、智能网卡

2、可编程 ASIC

（7）终端攻击行为推理

背景

随着企业边界逐渐模糊，终端成为企业防护攻击的最后防线。近几年出现了大量在终端上基于 Provenance Graph 和用户/进程行为分析的入侵检测方法，但这些方法限制于有限的数据集，并且有很强的前提假设，不具备普适性，难以解决现实世界中的位置威胁检测问题。基于终端用户/进程行为的入侵检测，可以从已知的行为和场景推理未检测到的恶意/可疑行为、攻击意图、攻击源头等。

目标

1、提出、设计和实现适用于企业环境的、基于用户/进程/行为/身份的终端入侵检测、攻击预测方法；

2、在实际企业环境中测试并取得预期效果

额外目标：相关的高水平会议或者期刊论文一篇（CCF-B 及以上）

相关研究课题

1、Reasoning

2、因果关联分析

3、大数据分析推理等

（8）终端行为知识图谱

背景

在网络安全领域，知识是至关重要的。正是因为攻击者拥有防守方不知道的知识(漏洞、钓鱼、攻击工具)，攻击才如此容易成功。也是因为这个原因，MITRE 公司才提出并维护了 CVE 漏洞库、ATT&CK 攻击矩阵以及其他的知识库。然而现在的终端安全攻防知识库都是基于人工建立。

目标

1、提出、设计和实现自动化终端行为知识图谱构造系统，从非结构化数据中收集安全攻防知识；

2、通过将各种终端安全攻防的知识和经验表述为机器可以理解并处理的形式，基于这些可机读的知识库可以为用户提供检测结果可解释性和处置建议等；

3、在实际企业环境中测试并取得预期效果

额外目标：相关的高水平会议或者期刊论文一篇（CCF-B 及以上）

相关研究课题

1、知识图谱

2、攻防知识库

3、自然语言处理

4、AI 等。

（9）云端 WEB 应用自动化攻击解决方案

背景

当前的网络环境中充斥着大量的由自动化工具发起的 bots 机器人攻击流量，这种攻击是通过工具或者程序脚本对应用系统进行探测和攻击，通常这种攻击流量没有明显的特征，传统技术无法检测，它们更多的是利用业务逻辑漏洞。

目前，这种机器流量接近世界互联网流量的一半，而对于一些资源抢占类和信息公示类的系统中，机器流量甚至超过了 80%，并且自动化的攻击这些年来也一直在保持着高增长的态势，新兴的攻击中 90%都为自动化攻击。同时在移动互联网、O2O（线上到线下）、移动支付、电子政务新趋势下，伴随着业务不断蓬勃发展的需要，政府或企业需要对外/合作方/内提供越来越多的 API，互联网上关于 API 的访问流量占比越来越多，Bot 和 API 结合的攻击越演越烈。

目标

1、 通过行为分析的方式识别高级的自动化攻击

2、 实现设备指纹，实现细力度的管控，减少设备指纹的碰撞率。

3、 通过建立 API 访问行为基线，识别 API 的越权滥用、异常访问等行为

相关研究课题

1、API 异常行为分析

2、自动化攻击行为检测

（10）设计稿的网页元素识别与检测

背景

随着近几年人工智能发展，该技术已经在各行各业都有着深入的应用，前端开发这个领域也不例外。前端智能化这个新兴的概念在迅速的发展，通过设计稿直接生成代码、交互图识别视觉稿、页面还原度自动判断等都有一些公司在尝试。随着公司的业务规模不断扩大，前端资源慢慢的变得紧缺，为了解决这个问题也正在采取一些方案，如业务组件、UI 中台、标准化组件库等。但是这些还不够，为了进一步提升前端开发的工程能力和开发效率，需要在前端智能化方面进行探索。目前有一些被使用广泛的前端 UI 组件库，如 ElementUI、antDesign 等。这些 UI 组件库规范性很强，假设有一个图片是按照其中一种 UI 组件库进行设计的，想要通过目标检测，文字检测等技术识别图片的组件和文字信息。

目标

针对上述提到的问题，结合业界与学界最新研究成果，完成如下的方案：

1、能够识别一张图片中 WEB 组件，并结合一些算法和图像处理技术得到完整的组件信息。

2、通过一定的算法，能够得到组件的层级结构与包含关系。

能够识别一张图片中文字内容和文字信息（坐标、文字颜色、文字大小、文字字体）

相关研究课题

1、目标检测

2、文字识别

（11）扫描攻击日志识别

背景

客户的防火墙、态势感知等安全设备每天产生大量的 SQL 注入、XSS 注入、账号爆破、漏洞利用等攻击日志，这些攻击日志除极少数是具有针对性或人参与的攻击之外，大部分是监管单位扫描、扫描器定期扫描、黑客随机扫描等产生的，导致真正的有效攻击被大量无效的告警淹没掉，给安全运营人员正常工作造成大量额外的工作量，甚至关键告警由于未被识别造成系统被攻陷的安全事故。

目标

针对上述提到的问题，设计一套机器学习算法，自动对客户的安全日志进行学习：

1、把监管单位扫描、扫描器定期扫描、黑客随机扫描等产生的安全日志识别出来，并对日志打上对应的标签。

2、外到内的安全日志，具备 PB 基本的全网数据的分析能力

相关研究课题

近似算法

（12）定向攻击识别

背景

客户的防火墙、态势感知等安全设备每天产生大量的 SQL 注入、XSS 注入、账号爆破、漏洞利用等攻击日志，这些攻击日志除极少数是具有针对性或人参与的攻击之外，大部分是监管单位扫描、扫描器定期扫描、黑客随机扫描等产生的，这些攻击一般不具备太大的威胁。真实的攻防对抗或者 APT 一般具有以下特点：

1、采用代理池，短时间内更换不同的攻击 IP，避免被发现或被安全设备封锁掉。

2、长时间针对某个客户或目标站点进行攻击，并且攻击速度是相对比较慢的

3、采用多种攻击手段

4、前后攻击或访问之间具有相关性

由于上述特点，运营人员很容易把这类具有针对性的攻击当做普通的攻击给忽略掉，导致最终客户网络被攻陷。

目标

针对上述问题，结合业界与学界最新研究成果，从以下几个方面(包括但是不限于)研究定向攻击的识别：

1、采用机器学习算法，根据源 IP 地理分布、数据包指纹等把采用了代理池的攻击数据关联到一起。

2、按照攻击时间线，能够实现 2 周以上攻击数据的关联，并根据攻击行为，识别出定向攻击，并预测当前的攻击阶段。

预期产出：

定向攻击识别的算法

相关研究课题

近似算法

（13）神经网络编译器在国产芯片上的适配和加速

背景

随着 AI 产业的发展，出现了越来越多的 AI 芯片架构和 AI 算法，在 AI 价值落地的过程中，需要兼顾算法效果和计算效率的问题。如何灵活、高效的将各种新出现的算法快速适配到不同异构 AI 计算平台上并生成接近专家手工设计的算子性能，成为 AI 产品竞争力的核心要素之一。

目标

1、设计实现通用神经网络模型编译器（可以参考 TVM、XLA 等）技术架构;
2、在 nvidia GPU, X86 CPU，国产 NPU 等 AI 芯片的某一种或几种特定架构进行研究;
3、产出设计文档和相关核心代码并通过验收

相关研究课题

1、神经网络模型编译器
2、异构 AI 芯片适配与算子自动优化

（14）Windows 平台 UWP 应用进程链识别技术突破

背景

UEM PC 端沙箱，Windows 沙箱还不支持 UWP 应用（只支持 win32 应用），原因是因为 UWP 应用启动方式都是通过 svchost RPC 通信代理启动，启动的进程链没有明确的父子进程关系（或者没有可识别的桌面特征），导致沙箱内启动的 UWP 应用，没有明确的启动进程链关系，所以导致沙箱内启动的 UWP 应用无法识别为安全进程。同时微软也在大力推广 UWP 应用，UEM 沙箱未来，会面对越来越多的 UWP 应用，所以 Windows 沙箱支持 UWP 应用越来越迫切，Windows 沙箱需要尽快支持解决。

目标

针对上述问题，需要给出沙箱能识别 UWP 应用的解决方案，具体可行解决思路和技术要求如下:
1、提出一种能够在沙箱内启动 UWP 进程，能准确识别进程启动链关系的解决方案，因为 UWP 应用通过 svchost 代理启动，所以可行技术方案为逆向分析 svchost 代理启动流程，hook 代理客户端进行辅助识别;
2、进程识别技术方案要求能精准识别沙箱内安全进程，方案不存在场景遗漏（或方案漏洞伪造安全进程特征），技术方案要求支持 windows7、windows10、windows11 所有版本。

相关研究课题

UEM 沙箱 UWP 应用

（15）iOS 应用级禁止截屏和录屏技术突破

背景

UEM 移动端沙箱，iOS 平台无法做应用级禁止截屏和录屏，iOS 平台在此项应用级安全能力上存在短板。当前业界也没有什么很好的技术方案，现在 Apple 苹果提供的解决方案为 MDM 管控，实现整个终端禁止截屏方案，此方案可以做到全设备禁止截屏，无法灵活的做到正对应用和终端环境，动态开启和关闭应用级防截屏和录屏。

目标

针对上述提到的问题，需要实现 iOS 平台，禁止截屏和录屏 SDK（或者应用 UI 截屏、录屏内容为空），具体 SDK 技术要求如下：

1、实现一个禁止截屏、录屏 SDK，SDK 功能可以动态设置禁止/允许对 SDK 宿主应用进程截屏和录屏（形态也可以为对宿主 UI 截屏录屏内容为空白，只要能达到禁止截屏效果）。

2、SDK 技术方案需要能支持 iOS 所有 UI 框架，不能额外引入兼容性问题，该技术方案要求能上架 AppStore，iOS 系统版本未 11、x-15、x。

相关研究课题

iOS 应用安全

（16）云安全场景下的防虚拟机逃逸技术研究

·**背景**

虚拟机逃逸是指利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的。我们希望识别和防范云上的虚拟机逃逸事件，为用户提供安全保障，同时尽可能降低对虚拟机性能的影响，令用户无感享受安全防护机制。能够增强云的安全防护机制力度，保障云用户业务的安全，防止失陷虚拟机中的恶意攻击者进行横向移动等攻击。

目标

1、探索较为深入的云上的虚拟机逃逸技术，提出、设计和实现系统化的防虚拟机逃逸的解决方案。

2、在真实场景中，解决方案要能够满足安全性、准确性以及性能等要求，能够用实际的攻击案例等方式验证解决方案的有效性。

3、满足信息安全等级保护、中华人民共和国国家标准中云计算、虚拟化等标准合规要求。

相关研究课题

1.虚拟化安全

2.云安全

（17）PB 级别的事后攻击链路异常事件检测的底层存储和计算的框架

背景

运营人员在判断某个告警是否为真实的时候，通过单个告警比较难去判断，需要手动了调查很多的信息，例如进程的关系、网络访问的关系、出现的频率等，这个对运营人员的要求比较高，效率低，在海量数据里面去做单个告警的调查是比较困难的。

目标

1、做自动化的攻击链溯源分析，能够基于某个异常指标，逐层的把与他相关的数据关联出来，并且在架构上支持数据源的关联扩展

2、支持多级关联，能满足超过 4 层以上的关联存储

3、支持 PB 级别数据的存储，支持查询秒级别的返回

相关研究课题

1、近似存储和计算的算法

（18）资产识别效果关键技术研究

背景

目前网络空间资产测绘中的资产信息依赖于指纹识别，大量的指纹信息主要来源于人工收集补充，其准确性和覆盖广度还不够，并且收集到的开源指纹在实际场景中存在较大的误报，期望有方案能够全面保障资产识别的准确性和覆盖面。资产测绘技术主要是针对网络空间中的 IP 进行网络资产发现，在实际用户角度比较关注于物理资产，需要一种远程探测的技术手段能够进行网络资产和物理资产的关联识别（比如虚拟化，多网卡，NAT 转发等场景的识别）

目标

1、 覆盖常见网络环境中（互联网，办公网，物联网，视频网，医疗网等）的 95%以上资产识别，准确率达到 90%以上

2、 提供远程探测技术方案解决网络资产和物理资产的关联映射识别

相关研究课题

网络空间测绘

（19）数据库系统性能卡慢的诊断和根因分析

背景

让数据库系统持续发挥出较高效能，对于企业和应用开发者而言充满挑战。数据库系统性能卡慢问题时有发生，往往会对业务造成一定的影响，但对于非专业人士难以在短时间内进行诊断和处理，这是客户反映的一个痛点。引起性能卡慢的原因很多，如 CPU、内存、IO 等系统资源瓶颈；锁或者其他数据库内部资源争抢阻塞；突发的流量高峰；系统参数配置问题；查询负载特性等。如何快速分析和解决类似的问题，并保障数据库服务的稳定、安全是数据库管理平台需要考虑的问题。此外，智能化技术和数据库场景的结合能够帮助消除数据库管理和人工操作的复杂性，保障数据库服务的稳定、安全及高效，因此客户在数据库智能化运维和管理上的需求越来越强烈。

目标

针对上述提到的数据库系统性能卡慢问题，结合业界与学界相关研究成果，数据库管理平台希望能够设计一套结合数据和算法的系统，智能化分析和诊断数据库系统的性能卡慢问题。目标为自动识别出性能卡慢的特征和原因，并提供解决该类卡慢问题的处置方式和建议，帮助用户能够快速定位和处理问题，恢复数据库系统的稳定运行。

预期产出：

设计一套基于数据和算法的性能根因诊断方法，用于自动识别和处理对数据库系统造成性能卡慢的问题，完成下面的相关工作：

1、能够主动识别出数据库运行过程中典型的性能卡慢或相关性能异常的场景，完成原因诊断分析。

2、能够针对上述问题提供有效的处置建议，快速帮助用户解决问题，恢复系统稳定。

3、针对的目标数据库产品优先为 Oracle，其次为 MySQL。

相关研究课题

1、数据库故障诊断

2、数据库性能优化

（20）图像压缩关键技术突破

背景

随着当今社会技术的不断发展，桌面云技术也得到了很大的提升。在使用桌面云的过程中，人们对网络传输质量的需求越来越高（即网络传输图像或视频的高质量与高流畅）。然而主流的视频编码标准在网络带宽严重受限的情况下，不能提供给用户优良的服务，如何降低网络传输过程对高带宽的依赖，越来越引起人们的关注。一种有效的方法是，可以先对输入信号进行分辨率的插值下采样处理，然后对处理后的信号进行压缩编码，并进行网络传输，这样能有效地减少码流，降低对网络带宽的要求，最后在解码端对重建信号进行插值上采样恢复高分辨率，但是这种方法在传输特征较少的情况下(如小文字)会出现边缘模糊的问题。

目标

针对上述提到的问题，结合业界与学界最新研究成果，在 CPU 单核情况下，完成如下目标：

1、在现有编码标准框架上，按照上述思路进行算法优化，解决解码端重建信号出现的边缘模糊问题；或者提出更高效的图像压缩技术，降低网络传输对高带宽的依赖；

2、图像压缩技术的引入需确保视频编码满足实时性需求（当前基于 AI 的多数算法，难以在当前硬件环境下满足实时性要求）。

相关研究课题

视频编码、图像压缩、AI 超分

（21）桌面云场景视频会议体验优化技术

背景

现代办公场景下，跨地域协作越来越普遍，而视频会议是跨地域协作的一种常见手段，能有效提升沟通的有效性和及时性。桌面云场景下，在虚拟机中使用视频会议软件时，期望会议体验能与同等配置物理机的接近，且其资源（CPU，网络带宽等）开销与物理机相近或更低。

目标

1、 确保桌面云视频会议场景的体验优良（如：视频流畅，无卡顿，花屏；音频流畅，无杂音或语音丢失等）

2、 视频会议体验达到或接近同等配置物理机的体验，同时 CPU 等资源开销与物理机接近

3、 在 Host 主机（运行虚拟机的服务器主机）的 CPU 利用率在 80%时，也能有良好的体验

4、 发表高水平会议长文至少一篇（CCF-B 及以上）

相关研究课题

实时音视频技术

（22）桌面云场景暗水印技术

背景

为了保护办公场景下的数据安全，对抗拍照、截屏等数据窃取手段，常使用水印技术，在数据泄露后进行溯源，并对泄密人员进行追责。水印技术常分为明水印和暗水印。当前桌面云已实现明水印，但未实现暗水印。期望提供桌面云的暗水印技术，确保较高的溯源能力。

目标

1、 桌面云的办公桌面叠加暗水印后，不能影响人眼的视觉体验

2、 暗水印对拍照、截屏、录屏等常规手段下，能有效进行溯源，期望溯源成功率达到60%

3、 发表高水平会议长文至少一篇（CCF-B 及以上）

相关研究课题

明水印，暗水印

（23）高兼容性的 windows 驱动重定向方案

背景

企业对泄密风险越来越重视，传统的中间人解密对设备的性能影响大，需要企业升级替换硬件，大幅提企业的 SSL 治理成本，但不解密又存在很多数据泄露的风险。在 PC 上做中间人代理解密，首先要解决的问题就是如何 NAT 客户的 https 连接(客户无感知的方式，不需要配置浏览器代理)到我们的代理程序；目前我们在 windows，主要是通过 WPF 框架来进行改包，从而实现 NAT 功能。PC 端代理程序每次启动都会监听一个随机的端口，然后 WPF 框架通过改包来实现 NAT 到这个端口上；中间人代理的实现方式具体可以参考开源的 mitmproxy 工程（https://github.com/mitmproxy）

WPF 框架在实际使用过程中发现，有部分网卡驱动(典型的 intel 杀手网卡)或者杀毒软件，会提前截获并处理处理数据包，从而导致这些数据不再经过 WPF 驱动，也就无法进行代理解密；这里主要的原因，是 WPF 框架本身是比较靠后的数据包处理点，如果有其他的驱动模块提前截获的数据包，那么就无法跑到 WPF 框架了，从而功能失效；

目标

针对上述提到的问题，结合业界与学界最新研究成果，给出能够达成如下目标的方案：

1、能够最大程度兼容当前的 mimtproxy 代理逻辑，在尽可能不改或者少改动的前提下完成对 WPF 的替换（不一定是替换，能解决当前每个 https 连接均能 NAT 到 PC 代理程序即可）；由于 PC 代理程序自身是跨平台的，所以最好不要为了 win 做太多特性化的东西；

2、新的方案，要能兼容所有 WPF 能够兼容的 win 系列；

3、能够兼容所有的杀毒软件、网卡等，不再出现功能失效的情况；

相关研究课题

1、SSL 中间人

2、解密性能

（24）高兼容性的 U 盘只读控制技术方案

背景

终端侧办公安全对企业信息安全显得尤为重要，与网络安全并驾齐驱。对 USB 外设的信息安全防护可以保障用户的私密信息不被泄漏及防止病毒通过外设横向传播，其中对外设的只读访问是比较常用的场景。终端上对外设中的文件进行读写的软件种类繁多，需要有轻量且稳定的方案，在软件对外设文件进行写入时进行拒绝并给用户恰当提示，并对软件的其他功能不造成影响。另外，要着重考虑方案在各平台下的兼容性及维护性，可以根据擅长的平台方向，实现覆盖 windows，国产化 linux，MAC 等平台的任意多种（尽量多的覆盖）。

目标

针对上述问题背景，USB 设备只读方案设计需满足以下目标：

1、方案轻量级，稳定性高，终端环境兼容性好

2、对各类型的 USB 设备有良好兼容性

3、方案尽可能的覆盖多种平台（单独解决某一个平台也可以）

相关研究课题

1、设备管理

2、设备驱动

（25）基于行为分析的身份可信评估方案

背景

在零信任安全框架下，所有数据访问都需要身份化，身份的可信识别就成为其中最重要的一环，即谁是谁，当前的身份识别可以基于多因素认证、生物认证、手机即身份等，但是依然存在各类风险，如设备盗用、内部泄密风险等，我们希望有一套基于用户行为分析的检测模型方案，能够准确识别身份可信风险。

当前的技术可以通过 UEBA 技术思路，收集多种类型信号，训练基线，实施规则或算法检测。

目标

1、探索一套较为完整的身份威胁场景，包括身份账号威胁与数据访问威胁，如账号被盗、设备被盗、异地登录、异常下载等。

2、探索身份可信评估的模型检测方案，针对威胁场景进行细化，能够检测准确，减少误判，平衡体验与安全方面体现优势。

3、方案尽可能的轻量级，可用于实时分析场景。

相关研究课题

1、零信任安全

2、身份安全

（26）智能化自动适应权限技术方案研究

背景

在零信任的安全框架下，建议实施细粒度的权限授权，建立身份与资产的细粒度权限关系，身份与资产两个维度在企业中都是灰频繁变化的，如何更加智能的构建身份与资产的权限关系就成为了一个重要课题，我们希望能有一套自适应的权限构建方案，提升安全性与生产力。

目标

探索业界的权限自适应方案，设计一套智能化的自适应身份权限方案，包括但不限适用于权限学习、权限回收、权限收缩、权限优化等。

相关研究课题

1、零信任

2、权限管理设计