2022 年 CCF-绿盟科技“鲲鹏”科研基金-申报方向与课题

1. 工业互联网和车联网安全方向

1.1 面向工控系统的智能攻击检测和防御控制技术

研究背景：

针对电力行业的工控系统的恶意攻击，设计智能检测和识别机制，并设计控制器使得系统安全的同时达到期望控制性能指标。

研究内容：

1）研究模型数据混合驱动的恶意攻击智能检测机制；

2）研究面向恶意攻击的分布式工控系统安全控制器，安全控制器需保持工控系统稳定。

考核指标：

1）完成攻击检测器技术原型系统 1 套，并提供源代码；

2）设计的攻击检测器具备对数据混合驱动的恶意攻击智能检测，对攻击的检测精度达到 90%以上；

3）面向恶意攻击的工控系统安全控制算法 1 个；

4）面向工控系统的智能攻击检测和防御控制技术报告 1 份；

5）完成高水平论文 1 篇，发明专利 1 项。

1.2 侧信道故障注入绕过芯片保护的固件提取技术

研究背景：

智能设备厂商为了保护自己的核心技术，会在量产的设备中利用硬件特性对

固件实施读写保护，提升了安全风险发现的门槛。侧信道故障注入是指攻击者通过专用实验装置来破坏电子设备所处的安全物理环境，从而影响电子设备的正常工作并对其刻意引入故障，导致电路的错误输出。

研究内容：

1）研究利用侧信道注入获取电子设备密钥的方法；

2）研究利用毛刺电压和电磁故障注入，改变瞬态电压和电流、实现芯片内部逻辑值改变的方法；

3）研究芯片的时序逻辑和固件保护逻辑，实现利用侧信道注入方式进行改变电路状态，即绕过芯片保护，提取芯片固件；

4）研究固件验证技术，保证提取后的固件功能和原始设备功能一致。

考核指标：

1）完成侧信道故障注入绕过芯片保护的固件提取技术原型工具 1 套（不限制软硬件），并提供源代码。工具支持提取不少于两个厂商的芯片（例如:STMicroelectronics、NXP、Philips 等厂商），开启读写保护后的固件提取并验证功能一致；

2）完成侧信道故障注入绕过芯片保护的固件提取技术研究报告 1 份，过程实验报告若干，功能一致性验证报告 2 份；

3）完成发明专利 1 项。

1.3 VXWORKS 设备固件虚拟执行关键技术研究

研究背景：

VxWorks 设备繁多，面对通过购买设备不能解决 VxWorks 设备安全的查、防、控问题，需要进行 VxWorks 设备固件虚拟执行关键技术的研究。

研究内容：

1)研究 VxWorks 系统框架，实现系统可以拆分到系统最小运行单元（例如独立可运行的程序）；

2)研究 VxWorks 运行机制，实现硬件检测绕过方案；

3)研究设备虚拟化执行技术，支持全量虚拟和局部虚拟两种方式，支持开放虚拟执行设备的管理员权限。

考核指标：

1)完成研制 1 套基于 VxWorks 设备固件的虚拟执行的系统，并提供源代码。系统支持 2 个不同厂商的 VxWorks 设备固件虚拟执行，需要有目标设备的管理权限；

2）完成研究报告 1 份，相应过程实验报告，发明专利 1 项。

1.4 车联网虚拟攻防靶场技术

研究背景：

智能网联汽车已经成为汽车产业转型升级的重要战略方向，车联网安全能力需要在实战中进行检验，针对车联网系统中各种安全威胁和防护的研究、学习、测试、评价，需要在完全可控的车联网虚拟攻防靶场环境中进行实施，满足主管单位、科研机构、高等院校等针对车联网网络攻防过程的呈现、演练等需求，全面提升车联网网络安全防御能力。

研究内容：

1）研究车机、TBOX、网关、域控制器在内的汽车关键零部件的虚拟化技术；

2）研究车身 USB、OBD、以太网等接口的虚拟化技术；

3）研究汽车车内网络的虚拟化技术，支持车内网络虚拟设备的互联互通；

4）研究蓝牙、Wi-Fi、GPS、胎压等汽车无线网络的虚拟化或部署技术；

5）研究汽车电子控制技术，支持车联网虚拟攻防靶场的控制展示。

考核指标：

1）完成研制软硬件原型系统 1 套，并提供源代码；

2）系统实现对汽车电子攻防过程的模拟，可以呈现出汽车通信、物理接口，集成攻击技术；

3）至少支持座舱域控制器、自动驾驶域控制器、TBOX、网关 4 种实车零部件的模拟集成，并具备对应的实车功能；

4）至少完成对汽车的 USB 接口、OBD 接口/汽车以太网接口、Wi-Fi 接口、蓝牙接口的呈现，且保证车内网络、物理接口基本功能可用；

5）完成至少 10 种攻击脚本，包括但不限于基于 USB 接口、Wi-Fi、蓝牙等攻击方式；

6）完成技术报告、实验手册各 1 份，发明专利 1 项。

2. 智能威胁分析与攻防对抗方向

2.1 网络软件流量特征自动抽取技术

研究背景：

网络中恶意软件流量中加密、压缩流量占比逐年提高，基于内容特征的恶意软件流量识别方法适用范围快速缩小。通过分析恶意软件流量通信过程中呈现的通信行为规律特征，进行自动识别、抽取、建模形成检测特征。

研究内容：

1）提出恶意软件流量特征描述、检测方法和验证方法；

2）研究多维周期特征、多源数据特征等智能抽取技术；

3）研究通信中使用了加密或压缩技术的主流 RAT 类恶意软件通信行为特征自动提取技术。

考核指标：

1）完成网络软件流量特征自动抽取原型系统 1 套，并提供源代码；

2）提出不少于 20 维的基于逆向分析的流量特征描述的方法；

3）建立至少 10 个描述周期性特征模型，能够提取周期性通信软件特征不少于 20 个，支持协议不少于 20 种；

4)至少覆盖 20 个使用了加密或压缩技术的 RAT 类恶意软件家族的典型样本，能自动提取对应网络特征，并验证有效性；

5）流量特征自动抽取研究分析技术报告 1 份；

6）完成高水平论文 1 篇，发明专利 1 项。

2.2 网络终端和设备抗识别技术

研究背景：

针对网络空间大规模设备信息探测，漏洞利用横行的现状，研究面向终端和设备对抗探测的方法。

研究内容：

1）研究对抗信息探测，特征分析等网络终端和设备识别的方法；

2）研究保护网络空间关键节点，通信链路的抗识别关键技术；

3）研究网络终端和设备特征欺骗干扰的抗识别关键技术；

4）研究网络空间识别与抗识别的对抗博弈关系及演化机制；

5）提出网络空间抗识别动态演化方法。

考核指标：

1）构建完整的网络空间终端和设备对抗识别的方法与评估体系，包含技术原型系统和验证环境 1 套，并提供源代码；

2）支持可对抗至少 5 种网络空间终端和设备识别方法；

3）网络对抗中受保护节点识别成功率不低于 30%；

4）支持不少于 3 类网络终端和设备特征欺骗干扰方法，如安全设备、服务

器、网络通信设备等；

5）提出网络空间识别与抗识别动态演化模型 1 个；

6）网络终端和设备抗识别技术分析报告 1 份；

7）完成高水平论文 1 篇，发明专利 1 项。

2.3 未知网络攻击行为的检测技术研究

研究背景：

未知攻击手段在实战攻防中被普遍应用，由于缺乏有效的防御技术，攻击者利用掌握的技术，能够快速突破传统的安全防线，达成战术目的，给客户带来很大的损失,如何有效发现未知攻击尤为重要。传统基于 payload 特征的检测技术对未知攻击的检测效果欠佳,利用 AI 算法模型对未知威胁的发现有一定的作用，但同时也需要解决模型结果的解释性问题。

本课题旨在通过对典型 web 业务资产以及访问者行为的深度挖掘分析,建立起行为特征画像模型，进而识别出高可疑的未知攻击者和受害者。

研究内容：

1）通过对海量访问者行为的建模分析，建立访问者行为画像，识别出其中的高可疑攻击者；

2）受害者视角，建立受害者资产画像（包括静态特征和动态行为特征），研究资产在遭受到漏洞攻击后的画像变化，从而发现资产在遭受攻击的线索、痕迹；

3）研究未知攻击在后渗透阶段的典型攻击行为，并针对后渗透阶段的攻击行为设计可行的检测机制。

考核指标：

1）完成从海量访问数据中识别出可疑未知攻击行为的原型系统 1 套，包括数据集、设计文档、源代码等相关材料，并提供源代码；

2）原型系统检测效果：准确率>80%,检出率>80%；测试数据包括业务日常访问日志、资产终端行为日志，以及混杂其中的 100 个 Web 漏洞的攻击流量日志；

3）完成发明专利 1 项。

2.4 面向高隐匿威胁的攻击溯源技术

研究背景：

IT 技术的飞速发展，为企业带来的越来越便捷的基础设施；同时，也为攻击者提供了便利。攻击者利用 VPS、云函数、域前置等等多种或手段，在达到攻击意图的同时，也极大的隐藏了自身。如何溯源这些攻击者，构建攻击者画像对于防守方持续有效防御至关重要。

研究内容：

1）研究覆盖云函数、域前置等国内外高频使用的高隐匿威胁攻击方式；

2）研究基于云函数、域前置等隐匿威胁检测技术；

3）研究这些隐匿威胁的溯源技术，构建攻击者画像。

考核指标：

1）完成面向隐匿威胁的溯源防护原型系统 1 套，包括攻击路径溯源、攻击者身份溯源和攻击者团伙溯源等，并提供源代码；

2）完成高水平论文 1 篇，发明专利 1 项。

2.5 网络攻击下多智能体系统的分布式安全控制技术

研究背景：

多智能体系统通过通信网络实现信息交互和协作,但其网络也易受到精心设计的恶意攻击。面向智能攻击建立攻击防御机制并设计安全控制器使得多智能体系统完成协同任务。

研究内容：

1）设计基于强化学习框架的智能攻击防御机制；

2）设计基于神经网络的多智能体系统分布式安全协同控制器。

考核指标：

1）实现多智能体系统分布式安全协同控制器和模拟验证场景 1 套，并提供源代码；

2）设计的智能攻击防御机制对攻击的拦截率相比传统方法提升 5%；

3）完成分布式安全控制算法 1 个，分布式安全控制技术实现报告 1 份；

4）完成高水平论文 1 篇，发明专利 1 项。

2.6 自动攻击模拟技术

研究背景：

自动化、智能化、高仿真的攻击模拟，有助于提升对风险识别、攻防技战法推演的验证效率，可有效降低攻防演练成本，解决网络攻击动作覆盖不完整、人工执行效率低、基于脚本模拟的攻击逻辑及表现失真等问题。重点研究突破攻击技战法原子化模拟的知识表征、高价值目标自主优选、攻击链自动识别、攻击方案自主决策、多步网络攻击自动仿真执行等问题。

研究内容：

1）攻击技战法原子化仿真模拟的知识表征技术。基于现实网络特征，结合技战法适用场景，研究覆盖作战环境属性、原子攻击前置条件及执行结果、技战法逻辑关系等标准化知识表征方法，为规划攻击路径提供知识空间；

2）高价值目标自主优选、攻击链自动识别、攻击方案自主决策技术。利用机器学习等算法自主优选高价值攻击目标，自主构建攻击路径，解决复杂场景下鲁棒自适应攻击策略生成问题，为自动化仿真执行攻击链动作提供决策；

3）构建仿真技战法原子实现多步网络攻击的自动仿真执行。研究并实现能够覆盖完整攻击链阶段的攻击原子用例，包含攻击载荷、漏洞利用及命令控制等。

实现可统一调度的自动化任务执行框架，完成自动化加载和远程仿真执行。

考核指标：

1)完成自动攻击模拟技术完整方案,含技术原型系统和配套测试靶场 1 套，并提供源代码；

2）攻击战术能够覆盖完整攻击链阶段，攻击技术原子实现不少于 200 个；

3）攻击场景技战法知识表征及实现能够覆盖目标网络信息、终端情报、执行载荷、漏洞利用、技战法逻辑等基础知识，关系判断准确率≥70%；

4）目标自主优选、攻击链识别、攻击方案自主决策的静态和动态生成算法各 1 种；

5）配套测试靶场，并实现自动化攻击模拟执行，攻击成功率≥60%；

6）完成高水平论文 1 篇，发明专利 1 项。

2.7 攻击技战术模拟仿真技术

研究背景:

当前在攻防验证和安全攻防对抗技术研究方向都存在对靶场平台和其内置的攻防场景及攻击技战术模拟的大量需求。

研究内容:

本课题旨在绿盟靶场平台上实现对典型攻击场景与具体攻击技战术的模拟仿真：

1)典型边界突破攻击场景的自动化模拟仿真，如：邮件钓鱼、微信钓鱼、国产/信创系统攻击、供应链攻击等；

2）典型内网渗透攻击场景的自动化模拟仿真，如：无文件攻击技术、隐匿通信技术、域渗透技术、工控系统渗透技术、云/虚拟化系统渗透技术、信令系统攻击技术等；

3）典型攻击路径，如：利用攻击技战术，组建红蓝对抗经典场景/路径、APT 组织攻击场景/路径，如突破->内网漫游->数据窃取。

考核指标：

1)在绿盟靶场平台上实现自动化攻击模拟仿真场景与工具集，至少具备批量模拟、选择模拟、可扩展、反馈执行结果。提供仿真所需工具、流量、仿真样本以及仿真环境，提供仿真工具使用文档与《攻击场景仿真报告》；

2)能模拟典型边界突破攻防场景不少于 5 类，模拟内网典型渗透攻击场景不少于 3 类，覆盖典型攻击路径不少于 10 种；

3）鼓励参考 ATT&CK 框架，攻击阶段覆盖攻击全流程，TTPs 技术覆盖不低于 70%，每项技术实现包含子技术原子模拟不少于 3 个；

4）完成发明专利 1 项。

2.8 开源软件源代码识别技术

研究背景：

在当今的软件开发中，开发者会使用大量开源组件或参考开源代码编写产品功能，这些直接或间接引入的开源代码可能存在安全隐患。通过源代码审计可以识别引用的开源组件，但是，在软件开发过程中软件开发企业或最终用户也会遇到无法获得供应链上游的源代码的情况，如开源软件中不提供源代码的库、第三方提供的二进制 SDK、Docker 内已编译的二进制可执行文件等。本课题旨在对二进制文件进行开源组件代码识别的技术，期望能在大规模数据的场景下，实现多种语言编译后的文件检测。

研究内容：

1）二进制程序码纹技术研究；

2）基于开源组件编译后二进制码纹的实体特征表示工程；

3）二进制程序中的开源组件定位方法。

考核指标：

1）完成技术原型系统 1 套，并提供源代码；

2）实现从二进制程序中分析、识别开源组件的方法，能识别二进制文件中

使用的开源组件名称、版本；

3）支持编程语言 C/C++的开源组件识别，对 GitHub 上使用 C/C++的热点开源项目（如 star 大于 1000）识别率不低于 80%；

4）完成发明专利 1 项。

2.9 开源代码恶意语义建模与识别技术

研究背景：

对恶意软件的研究受限于难以获得源代码，难以深入。在代码开源平台兴起的当下，一方面黑客团伙积极的通过代码开源平台发布恶意代码，以展示其能力；另一方面更多的开源项目或红队工具开源项目也正在被黑客使用。本课题旨在通过结合开源代码中存在的恶意软件，研究源代码中的原生语义信息与代码行为的映射关系，实现自动化的代码行为推演与归纳方法。深入研究源代码的泛语义信息，充分刻画人与恶意代码之间的深层联系，实现由代码到人，又从人回归代码的恶意语义判别方法。

研究内容：

1）设计基于语义消歧的完备性代码范式；

2）面向原生语义的代码行为推演框架与归纳方法；

3）研究代码特征的图嵌入表示方法；

4）构建面向开源代码情报的知识图谱；

5）研究基于泛语义信息的实体特征表示工程；

6）研究基于语义融合的恶意代码定位方法。

考核指标：

1）完成技术原型系统和数据集 1 套，并提供源代码；

2）完成代码范式设计，支持当前主流编程语言，如 C/C++,C#,Java,Python,JS 范式形式的自动生成；

3）建立代码行为总表，支持自动化生成目标代码与代码行为总表中各个行为的关联性。同时，能够在不同上下文环境下动态的生成代码行为总表中各个行为的隐式相关性；

4）面向代码特征的图嵌入技术在当前代码补全、变量误用、漏洞识别、代码搜索等主流检验任务中达到学术界先进水平，检测准确率超过当前主流模型5%以上；

5）建立代码贡献者间的关联性图谱，完成代码贡献者的分类。代码贡献者的属性刻画超过 20 个维度，图谱包含的代码贡献者数量超过 100 万。基于图谱设计的代码贡献者分类方法准确率超过 90%；

6）建立样本数量超过 10 万的恶意代码数据集，基于该数据集训练的代码恶意性检测方法对于恶意代码的综合指标（定位率*分类准确率）超过 90%。实际发现开源代码中的恶意软件仓库不少于 10000 个；

7）完成发明专利 1 项。

2.10 开源组件提取技术

研究背景：

在开源社区的驱动下，开源力量的不断发展，开源软件被广泛复用在实际工程项目中，其数量也在不断攀升，如 Maven、NPM、GitHub、Gitee 等开源社区或仓库都已到达千万以上级别；开源软件版本迭代相对频繁，其内部成分及关系也会发生复杂改变，如增加、更新依赖组件库或版本、复用其他组件源码、调用其他组件类库等。如今企业为了提高软件开发效率，大量引用开源组件实现业务功能，然而却忽略了开源组件的安全性带来的风险。从企业安全管理出发，理清企业内部应用产品或项目的开源软件引用依赖关系，开源软件存在的安全漏洞等成为了一个亟待解决的安全难题。

研究内容：

本课题旨在实现从主流开源组件仓库自动提取组件信息及依赖关系的方法，并通过构建开源组件和标准漏洞库的知识图谱，应用组件多维信息和知识图谱表

示研究开源组件生态环境的安全性，提出有效的安全评估方法。

考核指标：

1）完成技术原型系统 1 套，含数据集，并提供源代码；

2）实现 Java、Golang、Python、nodejs 组件仓库中开源组件数据自动获取，从组件流行程度，组件漏洞（威胁程度、数量等）出发，每个生态提取不少于 1 万种组件（非版本），并解析组件上下游关系；

3）从开源漏洞库（如 CVE/CNVD 等）获取主流开源组件的漏洞数据并与组件建立关系，每个组件生态漏洞数不少于 500 个（其中优先考虑高中级别漏洞）；

4）结合 1 和 2 中数据集形成组件图谱，形成一个知识图谱应用原型。实现开源组件知识图谱自动化构建流程，周期性（天/周）获取新开源组件和漏洞信息构建图谱；上层应用实现组件信息、漏洞信息进行查询功能，实现子图检索、路径查找功能，实现在线图下钻分析（1-3 度）；

5）完成发明专利 1 项。

2.11 二进制程序语义分析技术研究

研究背景：

CodeQL 是一个开源的代码分析平台，通过对源代码进行分析来获取其语义信息并且生成数据库，从而可以使用查询语言 QL language 进行查询来发现潜在的安全风险。CodeQL 只能对源代码进行分析，不能处理二进制程序。本项目对 CodeQL 进行扩展，实现对二进制程序语义信息的分析与提取，生成语义信息数据库，以便通过 QL language 进行查询来发现其中的安全风险。

研究内容：

1）研究二进制程序语义信息建模技术，建立二进制程序的语义信息模型，定义描述该语义信息的数据结构；

2）二进制程序语义信息提取，定义从指定二进制程序中提取语义信息的方法；

3）语义信息数据库生成，设计语义信息的数据库，定义语义信息入库的规范；

4）查询语言扩展，对 QL language 进行扩展，以匹配对二进制程序语义信息的查询；

5）查询引擎原型系统。

考核指标：

1）完成技术原型系统 1 套，含示例集，并提供源代码；

2）支持单个二进制文件大小在 100MB 以上；

3）单个项目支持 1000 个以上文件；

4）提供 10 个以上漏洞的查询示例，需要包括 Stack Buffer Overflow、Heap Buffer Overflow、OOB read/write、UAF、Double Free 等类型；

5）完成发明专利 1 项。

3. 威胁情报与网空测绘方向

3.1 多源情报融合与补全技术

研究背景：

针对重要防御目标暴露面情报多源、多样化、不完全性、不确定等问题，实现面向网络空间人物、机构、资产的目标数据修复、补全多源数据融合，提升对重要防御目标的安全状况刻画能力。

研究内容：

1）多源数据融合技术。对防御目标网络资产对象，语义关系、逻辑关联、隐含关联等多种关联关系挖掘和推理，实现隐形关系抽取和数据融合；

2）多源数据融合技术在不完全信息条件下的推理和补全技术研究。

考核指标：

1）完成多源情报融合与补全技术原型系统 1 套，含数据集，并提供源代码；

2）融合的多源情报来源不少于 10 家；

3）隐性关联挖掘维度不低于 15 种；

4）多源数据融合模型支持推理框架不少于 3 种；

5）多源情报融合与补全技术研究报告 1 份；

6）完成高水平论文 1 篇，发明专利 1 项。

3.2 网络空间组织聚类和动态识别技术

研究背景：

针对长期活跃在网络空间并持续发起认知作战的人员进行组织刻画和组织动态识别的问题，突破对不同组织的属性划分和组织特征表征提取技术，突破基于确定型属性和基于非确定型属性与源组织集合的组织动态识别等关键技术。

研究内容：

1）研究组织背景属性的划分的方法；

2）研究基于确定型属性和非确定型属性的组织特征表示方法；

3）研究识别攻击行为和攻击动态的组织聚类算法；

4）研究基于确定型属性聚类算法生成源组织集合技术；

5）研究非确定型属性与源组织集合的组织动态识别技术。

考核指标：

1）完成网络空间组织聚类和动态识别技术原型系统 1 套，含数据集，并提供源代码；

2）支持对攻击组织、黑灰产团伙等非法组织的各团体组织中 TOP20 成员识别覆盖率不低于 80%；

3）对组织核心组织人员的识别准确率不低于 75%；

4）对组织的活动与舆论引导话题变化的预测准确率不低于 60%；

5）对组织人员变动的监测成功率不低于 65%；

6）网络空间组织聚类和动态识别技术研究报告 1 份；

7）完成高水平论文 1 篇，发明专利 1 项。

3.3 网络空间攻击者与物理空间人员身份协同关联技术

研究背景：

针对网络空间高级定向网络攻击隐蔽性、匿名性、持久性和复杂性高，难以映射物理空间真实组织人员的问题，研究网络空间攻击者与物理空间人员身份协同关联的方法。

研究内容：

1）研究网络空间中的攻击者、攻击组织复杂关系和行为模式分析方法；

2）研究网络空间攻击者行为标准表征关键技术；

3）研究物理空间人员关系图谱构建与推理关键技术；

4）提出网络空间攻击者虚拟身份与物理空间真实身份的映射方法并验证。

考核指标：

1）完成网络空间攻击者与物理空间人员身份协同关联完整技术方案和技术原型系统 1 套，并提供源代码；

2）支持不少于三种攻击组织关系与行为模式分析方法；

3）支持不少于三种网络空间攻击者行为标准表征类型；

4）支持物理空间人员关系挖掘与不少于三种挖掘方法；

5）物理空间已知人员关系识别准确率不低于 90%，未知关系识别率不低于 70%；

6）网络空间攻击者与物理空间人员身份协同关联关系识别算法 2 套；

7）完成高水平论文 1 篇，发明专利 1 项。

3.4 网络空间拓扑结构测绘技术

研究背景：

面对不完备拓扑结构场景下，研究高效识别网络空间拓扑结构特征等关键技术，测控大型目标网络空间拓扑结构。构建远程目标拓扑结构模型。

研究内容：

1）研究远程目标拓扑结构特征挖掘技术；

2）研究识别骨干路由节点、连接关系的相应技术；

3）研究远程目标链路发现分析技术。

考核指标：

1）完成互联网拓扑测绘原型系统 1 套，并提供源代码；

2）支持探测识别的假象不少于 20 个，拓扑结构属性信息不少于 10 种；

3）具备对远程目标基本信息、互联网交换点、边界路由器等关键路由节点的探测识别能力；

4）互联网拓扑测绘技术研究报告 1 份；

5）完成高水平论文 1 篇，发明专利 1 项。

4. 隐私计算与 5G 安全方向

4.1 基于 Windows 机密虚拟机的可信隐私计算

研究背景：

为了实现 Windows QEMU 虚拟机（称作 WinVM）在 AMD SEV 环境中的机密运行，以及基于 AMD SEV 的可信隐私计算。

研究内容：

1）用户 Guest Owner（GO）对 WinVM 进行 VeraCrypt 和 BitLocker 加密（假设密钥为 SK），得到加密的虚拟机，交给虚拟机持有者 Platform Owner（PO）；

2）GO 将解密密钥以机密的形式传递给 PO，PO 可以启动加密的 Windows 虚拟机。具体实现方式可以是 AMD SEV 安全注入协议、USB TPM 硬件模块或其它安全可行方案；

3）在安全启动之后的 WinVM 虚拟机中执行“无可信第三方”的联邦学习、高效安全多方计算算法。对有（无）TEE 环境下可能导致的隐私风险/信息泄露进行量化评估。

考核指标：

1）完成技术原型系统 1 套，并提供源代码；

2）支持 Windows 10 机密启动，须确保 PO 无法偷窥加密密钥 SK；

3）设计“无可信第三方”的联邦学习算法、高效安全多方计算算法，设计联邦学习隐私泄露量化方法，输出 2 篇以上高水平论文以及相关发明专利。

4.2 5G N1/N2 口安全研究技术

研究背景：

从安全事件上来看，基于 5G 的网络攻击事件频频出现，5G 网络属于最新一代的移动通信技术，安全防护的经验并没有深厚的积累，势必会遭受到来自各方的安全挑战。

研究内容：

1）研究移动设备通信与基站空口、UE 与 AMF 通信 N1 口、RAN 与 AMF 通信 N2 口的相关安全问题；

2）研究 5G 环境复现 NAS、NGAP 协议的安全问题，同时提出相应的防护措施；

3）研究 5GC 网元服务异常检测具体策略实现与优化配置，对 5G 全流量数据

进行分析处理，建立检测基线，利用配置基线检测异常流量，提前预警攻击行为；

4）研究 5GC 开放的 API 接口存在的脆弱性，通过 API 实现数据窃取、注册/注销网元等攻击目的。

考核指标：

1）完成研制可对 5GC 网元通信行为检测工具 1 套，并提供源代码；

2）完成 N1、N2 接口及相关协议的安全分析，形成安全分析报告并在报告中提出相应的风险应对措施；

3）针对 5GC 网元挖掘漏洞数量不少≥2 个，其中未公开漏洞≥1 个，漏洞类型不限于命令注入、拒绝服务、非授权访问；

4）提出基于 5GC 网元及网元接口的攻击战法≥2 种，形成攻击武器≥2 个；

5）完成技术报告、实验手册各 1 份，发明专利 1 项。