GohighSec
高鸿信安

基于可信计算和SGX技术的

软件保护白皮书

Gohighsec

大唐高鸿信安（浙江）信息科技有限公司

2018．05

版权所有 ©大唐高鸿信安（浙江）信息科技有限公司。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部内容，并不得以任何形式传播。

商标声明




商标为大唐高鸿信安（浙江）信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受大唐高鸿信安（浙江）信息科技有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，本公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

Copyright

联系方式

地址： 浙江省义乌市苏溪镇苏福路126号

北京市海淀区北坞村路23号北坞创新园中区2号楼

电话： 010-88465090 网站：www.gohighsec.com

Gohighsec

目 录

Cohighsec

1 背景情况

互联网产业的飞速发展产生了海量数据，同时，处理器的计算能力也伴随着摩尔定律而不断提升，这些因素都间接推动了深度学习技术在人工智能领域的普及，促进了语音识别、图像识别等技术的快速发展和产业化推进。1997 年，IBM 的“深蓝”超级电脑战胜国际象棋世界冠军卡斯帕罗夫，标志着人工智能领域发展迎来了一个里程碑时刻；2016 年，谷歌的“AlphaGo”击败围棋世界冠军李世石九段，进一步加速了人工智能的普及，并彻底引爆产业发展。

目前，人工智能已在多个领域开花结果。谷歌、微软、苹果、亚马逊等世界巨头，以及国内的百度、阿里、腾讯等领先企业纷纷结合自身业务情况开展了相关的研究，并在自动驾驶、智慧医疗、虚拟现实等场景下取得了丰硕成果，也为企业发展注入了新的力量，可以说，人工智能是引领企业未来发展的战略性技术突破。

与此同时，由于人工智能包含了企业的核心算法和数据，凝聚了企业的智力成果，包含相关成果和知识产权的软件如果被不法分子破解，进而窃取关键算法和重要数据，将给企业带来无法估量的损失。因此相关企业对人工智能的成果保护工作愈发重视，主要从两个方面开展工作，一方面是依赖于国家的知识产权保护规定，通过申请专利进行保护；另一方面是通过一些软件保护的措施，防止核心算法和数据被窃取。对于前者，各国规定不一而同，如美国专利局支持人工智能算法通过专利进行保护，而包含中国在内的部分国家，尚不支持智力活动的规则和方法申请专利；对于后者，保护形式多种多样，保护强度也差别较大。因此，

对于那些资源有限、经费有限的企业，在专利保护制度尚不能有效保护的条件下，更依赖于软件保护的方式。

2 通用软件保护

通用的软件保护方式有三类，一种是纯软件形式的加密保护，另一种是软硬件结合的加密保护，第三种是基于网络服务器的加密保护。

- **纯软件保护方式**

纯软件的保护方式不需要额外的硬件支持，因此在成本控制和易用性上有一定优势，常见的有注册码保护和时间限制保护两种。前者的原理是软件发行商对一个唯一串（一般包含了注册用户的个人相关信息，例如用户的姓名、生日、邮箱地址、网卡号、计算机名等）使用预先设计好的注册算法生成注册码，并发送给用户；后者保护依赖于软件的定时更新，每次更新都会导致旧版本的软件功能无法使用，这种“售后保障”是所有盗版者都不愿意做的。

- **软硬结合保护方式**

软硬结合的软件保护技术需要硬件支持，其保护策略主要包括身份认证、数据加密、访问控制、密钥生成、序列号唯一、数据的可靠传输以及硬件识别等，常见的保护形式是加密狗保护，加密狗（Special-Purpose Dongles）是一种智能化的加密产品，又被称作加密锁，通常安装在串口、并口以及 USB 接口上的硬件电路，内置相应的驱动程序和加密程序，通过和与其链接的计算机进行数据交换，并自动或手动运行密钥检测程序，判断用户是否合法。

Conlensec

- **基于网络服务器的保护方式**

此种保护方式需要用户在使用过程中保持对发行商服务器的实时访问。用户的客户端软件包含基本的数据和程序，而发行商的服务器中则包含软件使用必须的部分数据，如人工智能程序（AI）、部分关键的数字建模以及部分重要环境的设置。用户在使用该软件时，如果不访问发行商的服务器，就根本无法进行正常的操作，同时由于服务器中的数据量十分巨大庞杂，即使通过攻击服务器获取数据，也很难将其全部植入客户端内，因此这种方法在当前以及今后一段时间内是比较安全的。

总的来看，纯软件的保护方式虽然简单易用，但保护强度较低，容易被非法人员通过内存窃取、暴力破解等方式绕过保护；软硬件结合的保护方式虽然保护强度较高，但成本高、兼容性差、易用性差；基于网络服务器的保护方式保护强度高，但需要一定的先期投入，而且需要用户实时联网，不利于推广使用。

3 基于可信计算和 SGX 技术的软件保护

3.1 可信计算技术

“可信计算”始于 1999 年 Compaq、HP、IBM、Intel 和 Microsoft 牵头组织的 TCPA(Trusted Computing Platform Alliance)，2003 年 3 月 TCPA 改组为 TCG(Trusted Computing Group)，其目的是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性。TCG 组织制定了 TPM（Trusted Platform Module）标准，由于其从硬件角度实现安全防护，正逐渐成为 PC server、PC 以及便携式 PC 的标准配置。

2012 年，TCG 发布 TPM2.0 标准，兼容中国加密算法。2015 年，由 TCG 推动的 TPM2.0 规范已经被国际标准组织/国际电工委员会采纳并作为 ISO/IEC11889:2015 予以发布，该标准已获得包括中国在内的许多国家/地区支持。目前，符合国际可信计算规范的产品已经在市场上广泛应用。

可信计算是一种运算和防护并存主动免疫的新计算模式，可信计算安全的起点、基础以及强度相比传统安全技术有本质的区别，可信计算基于硬件密码芯片，从平台加电开始，到应用程序执行，构建完整的信任链，逐级认证，未获认证的程序不能执行，从而使信息系统实现自身免疫，构建起高安全等级的主动防御体系。相比于传统安全技术，可信计算对于“震网”、“火焰”、“心脏滴血”、APT 攻击、0Day 攻击、供应链攻击等一批新型网络攻击武器及攻击方式具有突出的优越性和强大的防御能力，从结构上大大增强系统的可信性和安全性。

3.2 SGX 技术

SGX（Software Guard Extension）技术是由 Intel 提出的，是 Intel 指令集架构（ISA）的扩展，用于增强软件的安全性。这种方式并不是识别和隔离平台上的所有恶意软件，而是将合法软件的安全操作封装在一个 Enclave 中，保护其不受恶意软件的攻击，特权或者非特权的软件都无法访问 Enclave。Enclave 也可以理解为一个可信执行环境 TEE（Trusted Execution Environment），一旦软件和数据位于 Enclave 中，即便操作系统或者和 VMM（Hypervisor）也无法影响 Enclave 里面的代码和数据，Enclave 的安全边界只包含 CPU 和它自身。

3.3 基于可信计算和 SGX 技术的软件保护

基于可信计算和 SGX 技术的软件保护包括三个步骤，首先，通过可信计算

技术增强目标软件运行环境的安全性；其次，基于 TCM/TPM2.0 可信芯片进行密钥管理以及加解密运算，实现对目标软件的静态保护；最后，通过 SGX 技术对目标软件进行动态保护。通过以上步骤，构建一个安全保护闭环，显著提升系统的安全保护强度。

1. 可信环境

在目标主机上，以 TCM/TPM2.0 可信芯片或 fTPM （Firmware-based TPM 2.0 Implementation）为信任根，构建从 BIOS、OS Loader 到 OS Kernel 的信任链，对主机软硬件完整性、配置状态等进行逐级度量，实现从加电启动到应用执行全过程安全防护，从而构建一个安全可信的软件运行环境，可以抵御未知漏洞、木马和病毒的攻击和入侵，为后续的静态保护和动态保护提供环境安全保障和可信功能支持。

2. 静态保护

静态保护主要针对存储在磁盘上的目标软件及其重要数据，降低其被窃取或反编译分析的可能性。通过基于 TCM/TPM2.0 可信芯片提供的可信计算功能接口，实现对目标软件可执行程序的压缩、封装，提升其安全性，即使其被拷贝到其他环境下，也无法加载执行，也难以被反汇编或静态分析；基于 TCM/TPM2.0 可信芯片的加解密及密钥管理功能，对目标软件的重要数据进行加密存储，实现静态保护，当程序运行时，进行解密处理，并与下一步基于 SGX 的动态保护进行对接，使得整个保护过程可靠衔接。

3. 动态保护

目标软件被执行时，将会以明文形式存在内存中，非法用户可借助专业的工

具将内存 dump 出来，进行分析并提取出重要信息。目标软件及重要数据的动态保护依赖于 Intel 的 SGX 技术，可以在程序运行时建立一个 Enclave 安全空间，将需要保护的程序或数据放置到该 Enclave 安全空间，由于该 Enclave 安全空间是被 CPU 加密的，只有 CPU 自身有权限访问，OS、VMM、及第三方程序等都无法获取该空间的信息，因此即使该 Enclave 内存区域被 dump 出来，由于数据是加密的，也无法获取原始信息，从而实现对目标程序及重要数据的动态保护。

4. 扩展保护

在某些业务场景，用户除了对目标软件有具体的保护需求之外，还对程序执行环境、软件更新过程等有着更加严格的要求，对于前者，可在主机可信环境基础上，通过多因子身份认证、区域隔离控制等手段，结合多元分权管理、软件白名单管理等机制来实现；对于后者，可在主机可信基础上，通过数据完整性校验、可信远程证明等手段，结合可信服务中心实现。

4 环境要求

基于可信计算和 SGX 技术的软件保护对目标软件的运行环境有一定要求，具体配置如下表所示。

表 1 环境配置要求

序号	项目	配置要求
1	处理器	Intel 至强 E3，支持 SGX 技术

		Intel 酷睿系列，支持 SGX 技术
3	内存	8GB 以上
4	可信芯片	TCM/TPM2.0/FTPM
5	操作系统	操作系统可信增强系统 CTRUST HTE_V3.0
6	程序保护软件	可信知识产权保护系统 CTRUST DRM V2.0

5 方案优势

基于可信计算和 SGX 技术的软件保护方式较通用的方式保护有着明显的优势，与纯软件的保护方式相比，其保护强度明显增强；与网络服务器的保护方式相比，其对产品发行商不存在依赖关系，同时成本投入不高；与常用的软硬结合的加密狗保护方式相比，具有以下优势：

1. 存储空间大：加密狗保护方式是将应用程序的一段代码放置在其存储空间，通过 API 接口将导入的数据进行计算，将结果返回给应用程序，但其存储空间有限，一般只有几十 KB；本方案保护方式是将所有待保护数据加密后存储于用户硬盘，使用时实时解密，可满足大容量数据的保护需求。

2. 算法丰富：加密狗保护方式仅支持几种有限的加解密算法，本方案保护方式除了支持 RSA、ECC、AES、SHA256 等国际算法外，还支持 SM2、SM3、SM4 等中国商用密码算法，便于用户进行选择。

3. 防静态分析：加密狗保护方式仅对应用程序的核心代码或数据进行保护，

但并不支持对应用程序进行整体保护，他人可能通过反汇编等方式进行静态分析；本方案保护方式对应用程序整体进行进行压缩、封装、保护，可显著提升他人通过反汇编等手段进行静态分析的难度，从而掌握程序结构和设计机制。

4. 防动态破解：加密狗保护方式并不能对运行数据进行实时保护，因此存在被动态破解的隐患；本方案保护方式通过基于 CPU 的硬件级功能支持，将重要数据放置在内存的受保护区域，显著降低外部用户或手段非法获取数据的可能性，因此可有效提升应用程序在动态运行阶段的安全性。

5. 硬件平台绑定：加密狗保护方式将应用程序和硬件进行绑定，但受硬件自身性能、接口速度等影响，应用程序的运行性能可能受到影响甚至显著降低；本方案保护方式将应用程序和硬件平台进行一对一绑定，通过优化适配，几乎不影响应用程序的运行性能，同时能够防止应用程序被拷贝到其他平台上使用，保护用户知识产权。

6. 性能可以优化：加密狗保护方式由于加密狗本身硬件的限制，无法为应用提供性能上的优化，反而会让性能受到一定的损失；本方案可以很好的利用服务器的硬件资源、软件优化方案，使诸如 AI 应用能够发挥最佳的性能优势，提高处理速度和准确性。

6 典型案例

某医疗影像科技公司研究开发了针对甲状腺结节、肺结节、肝脏三维建模等疾病辅助诊断的 AI 应用，并进行了临床测试，根据实测效果，诊断正确率在国内同行中处于领先地位，具有很好的市场前景和经济效益。但是，在该产品推向

市场时，该公司非常担心其软件被破坏从而影响客户体验，或者研究成果被窃取导致公司利益受损。因此，迫切需要对其 AI 应用进行有效保护。

高鸿信安根据客户的实际需求，考虑使用可信计算和 SGX 技术对其 AI 诊断程序进行保护。首先，将 AI 诊断程序绑定到特定可信设备上，使得应用只能在该设备上运行，即使被非法复制到别的设备上程序也无法启动；其次，结合可信计算和 SGX 技术，对 AI 诊断程序进行存储状态的静态保护和运行状态的动态保护，从而显著降低核心信息被泄露的可能性。经过原理分析和实际测试，高鸿信安提供的安全保护强度符合客户预期目标，客户可以放心地进行市场推广和销售。

7 应用场景

高鸿信安基于可信计算和 SGX 技术的软件保护方法可以对客户软件进行高级别安全保护，软硬结合的保护方案覆盖程序的静态存储阶段和动态运行阶段，保护其软件的安全性和完整性，显著降低其核心知识成果被窃取的风险。同时，结合高鸿信安的 CTRUST SERVER 可信服务器、CTRUST NTU 可信终端/单元，可为用户提供更加安全的执行环境，并通过设备绑定提供更高级别的保护。

该方案可应用于智慧医疗、自动驾驶、智能机器等人工智能典型应用场景，也可应用于其他常规的应用场景，对包含客户核心算法和重要数据的程序进行高级别保护，避免客户智力成果遭受损失。

GoTrustSec