计算生命周期保障（CLA）对零信任的重要性

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The importance of compute lifecycle assurance in a zero-trust world		
原文作者	卡米尔·莫哈特（Camille Morhardt）	**原文发布日期**	2021 年 8 月 3 日
作者简介	卡米尔·莫哈特是 Intel 安全计划和通信总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/08/03/compute-lifecycle-assurance/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	随着物联网（IoT）中攻击面激增、基于固件的硬件攻击增加，以及系统在整个生命周期中面临的威胁不断增加，企业开始采用“零信任”模型。在促进零信任模型的部署方面，CLA 发挥着越来越重要的作用。CLA 是一个框架，可帮助分析和解决系统及其组件在整个生命周期中的安全性和完整性问题。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

计算生命周期保障（CLA）对零信任的重要性

卡米尔·莫哈特

2021 年 8 月 3 日

随着物联网（IoT）中攻击面激增、基于固件的硬件攻击增加，以及系统在整个生命周期中面临的威胁不断增加，企业开始采用“零信任”模型。

计算生命周期保障（CLA）

在过去的十年中，IT 部门通常要求最终用户在被授予系统或网络访问权限之前对其进行身份验证。但在零信任模型中，这一要求不仅针对用户。在任何给定时间，系统本身及其组件都被假定是“不安全的”。这促使企业不仅要在生命周期的每个阶段验证系统用户的身份，还要验证系统本身的完整性。

在促进零信任模型的部署方面，CLA 发挥着越来越重要的作用。CLA 是一个框架，可帮助分析和解决系统及其组件在整个生命周期中的安全性和完整性问题。

生命周期分为四个阶段——构建、传输、运行和退役。因伪造或篡改，甚至过时的固件版本问题，企业的系统（例如 CPU 或其他计算元件）面临着风险。此外，在许多情况下，IT 部门不具备可见性。攻击可能发生在“构建阶段”的制造过程中，也可能发生在“运行阶段”的系统日常使用过程中。

根据 IBM 的统计数据，在 2020 年，企业识别漏洞所需的平均时间为 228 天。在这种情况下，CLA 能够提供另一个重要的安全层。

但是，CLA 框架的每个阶段是如何帮助实现零信任模型的呢？在下文中，我们将详细进行分析。

构建

在制造和组装过程中，企业面临收到假冒或替换零件的风险，这些零件本身可能是恶意的，或者容易受到未来攻击。举例来说，由于供应短缺，企业再次担心会出现假冒芯片。

CLA 建议企业采用一种方法来验证他们收到的东西是真的——不仅包括系统，还包括组件（如果组件运行活动固件）。活动固件可以成为进入硬件的途径，因此企业要保证它们

不被篡改，并且是最新的。

企业如何在构建阶段进行验证呢？一种方法是，获取从车间控制单元构建的组件硬件信息，然后将其安全且唯一地存储在每个设备上，使客户能够自行检索数据，并查看完整的材料清单和溯源报告。

企业也可以使用分类账簿或数据库模型方法。以笔记本电脑制造商为例：通过捕获所有生产信息并将其安全地发送到远程服务器，他们可以验证组件（例如主板或服务器中的组件）、安装的固件和系统配置的真实性，以备后用。

传输

在数字时代，“抢劫勒索”不同于以往。如今，系统在从制造地点到最终位置的物理运输过程中可能会被篡改或破坏。例如，将固态硬盘运送到原始设计制造商进行集成的过程中，通过将硬盘中的固件替换为恶意版本，可以篡改计算机系统中的数据。

企业通过各种方法来应对这类问题，包括设施安全要求（如闭路监控、访问控制等）以及运输安全要求（如防篡改包装、运输路线安全审查、上锁、集装箱完整性、GPS 跟踪等）。

在这方面，戴尔使用“运输资产保护协会”（TAPA）要求，惠普使用“供应商管理系统”要求。此外，CLA 建议，在构建和传输阶段后，企业应现场验证收到的系统是否与所订购的完全相同。

运行

该阶段包括几个子阶段，每个子阶段都有其自身的风险，例如分配（包括现场或远程）、日常使用和更新。CLA 建议，在将系统配置到网络或将其分配给最终用户之前，至少要验证系统的完整性。为了获得更高的安全性，企业可以要求系统在每次尝试访问网络时进行自我验证，以确保它们处于已知良好状态。这意味着，在使用过程中验证系统固件是最新的且未被篡改，以及系统上的物理组件（如固态硬盘）未被替换。

如何才能做到这一点？一种方法是使用分类账簿和数据库模型。例如，通过使用分类账簿模型，一旦将计算系统交付给客户，客户就可以验证初始构建记录，并持续维护更改记录。另一种方法是自我报告。

一旦设备交付给最终客户，设备就可以提供其所有智能组件当前配置的加密报告（或综

合系统级报告）。

退役

通常系统或其组件会重复使用。在重用之前，尤其是在重新配置给不同用户或用于不同目的之前，企业需要完全擦除数据。CLA 建议，企业应验证系统是否以与使用之前相同的状态返回给 IT 部门。企业应记录系统运行时对系统进行的任何物理组件或固件更改，包括升级，并对每一次更改进行说明。

如何才能做到这一点？企业需要对资产进行唯一标识，且在处理资产时进行跟踪。但是，很多企业在未验证数据已被擦除的情况下就处理了硬件。销毁证书是可以伪造的，因此，保护证据和监管链信息是很重要的。

硬件供应商应该投资于其生态系统中的实践、工具和技术，以帮助客户和合作伙伴在生命周期的每个阶段验证系统的完整性。CLA 框架旨在帮助企业实现该目标。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com