保护企业网络安全重要方法
——软件资产管理（SWAM）

北京三博安科技有限公司

2021-9-20

目 录

保护企业网络安全重要方法——软件资产管理（SWAM）

引言

当今，近乎所有的网络安全事件均是软件实施的。软件可以定义网络，也可以摧毁网络。如果不有效管理软件，网络系统受恶意软件威胁将会越来越严重，加上现代软件的复杂性，有的软件产品包含数千个可执行文件，系统管理员对自己组织的网络系统安装、运行的软件数量不清楚、来源不清楚、版本不清楚，那就像习主席所说的：网络谁进来了不知道、是敌是友不知道、干了什么不知道。因此，一个企业或政府组织应该像管理其他资产一样对软件进行登记立账管理，即实施软件资产管理（Software Asset Management，SWAM）。

一、什么是软件资产？

一个计算机中的软件包括固件、基本输入/输出系统(BIOS)、操作系统、应用程序、恶意软件，如工具包、木马、病毒和蠕虫。

软件资产可以是一行源代码，也可以是一个由多个产品、数千个可执行文件以及无数行代码组成的软件套件。

软件资产一般有两种形式存在：一是产品，二是可执行文件。

1）软件产品：软件产品是一个由供应商、产品名、发布时间、补丁级别的组合，这些软件通常被授权，在注册表中列出进行安装，并由用户执行。

2）可执行文件：在永久存储器中的文件可被加载到活动内存，并由 CPU 执行。恶意软件可作为与产品没有关联的单个文件被引入，也可以通过将具有恶意功能的文件替换为授权产品中的授权可执行文件被引入。识别恶意软件重要方法是将可执行文件与产品链接起来，并验证可执行文件与供应商发布的是否相同。要消除恶意软件，必须关注可执行文件。

在解释语言的情况下，源代码可以被视为可执行文件，即使它在加载到内存中之前被解释。源代码文件的数字指纹可用于验证它是否是预期的代码。但是，如果源代码被编译成机器代码，并且只在产品运行的设备上加载机器代码，则编译后的代码应该是在目标设备上找到的唯一资产。

二、SWAM 解决软件安全的问题

- 软件授权和需要
- 软件从受信任的供应链获得，而不是从包含恶意代码的地方获得
- 软件安全配置，以降低特定目标吸引力，减少被成功攻击的可能性
- 使用最新的补丁，以降低特定目标的吸引力，减少被成功攻击的可能性

攻击者经常发现和利用系统弱点来危害设备。SWAM 解决了上述问题，特别是前两个问题造成的攻击场景，间接支持后两个问题解决。具有配置设置/补丁管理的授权软件，其配置设置(CCE)和补丁设置(CWE)的质量分别属于配置设置管理(CSM)和漏洞管理(VUL)能力。SWAM 支持 CSM 和 VUL 能力，确保组织知道有什么软件，并可正确配置和打补丁。

SWAM 可防止未经授权软件和恶意软件的攻击，SWAM 还降低基于不安全配置和过时补丁的攻击。

系统安全弱点	SWAM 措施
未经授权的软件产品	○ 给设备分配角色。 ○ 对于每个设备角色，知道已授权的软件产品。 ○ 阻止其他软件运行、删除或接受风险（通过特定设备授权）。
未经授权的可执行文件 ● 恶意软件作为未经授权的可执行文件插入 ● 将恶意软件插入到已授权的可执行文件中	○ 对于已授权的产品，知道与每个产品关联的可执行文件，通过每个可执行文件的字指纹来验证文件的完整性。 ○ 阻止与授权产品关联的没有正确指纹的文件执行。
未管理的安全设置、未管理的补丁	○ 确保指定一个具有适当技能和权限的管理员管理产品每个安装实例的这些因素。 ○ 如果没有明确指定这样的管理员，假定由设备管理员负责。 ○ 向指定的管理员报告所有缺陷，以便进行纠正或风险评估。

三、SWAM 技术方法

1）软件黑名单和白名单管理

从信任角度，软件可以分为：

- 白名单软件—“已知的好的”或可信的软件
- 黑名单软件—“已知的坏软件”或不可受信任的软件
- 灰名单软件—此刻不知是好还是坏的软件

白名单（阻止除可信软件以外的所有软件）和黑名单（阻止所有不受信任的软件）可以用作阻止恶意软件的策略。

灰名单可分为两种：

- 允许的灰名单—将认为是安全并允许执行的软件。例如，在分发软件配置控制板的代理上，由授权人员安装的新软件。
- 不允许灰名单—所有不允许运行的软件，包括授权安装程序未安装/下载的软件（例如，网络钓鱼攻击）。

2）不同设备使用黑名单和白名单

这些名单并不是通用的，不同类型设备有不同角色，需要不同的软件名单。例如：路由器、用户工作站和移动设备通常有不同操作系统，适用于 Windows 服务器上使用的软件（例如 MS-Exchange）不应该安装在用户工作站上（例如允许使用 MSOutlook）。

设备角色——是指设备所要执行的业务和/或技术功能，使该角色与设备所需的软件密切相关。

组织必须定义足够的设备角色，以便白名单和黑名单能够足够具体，限制设备上所需软件，而不需要大量例外。

3）白名单比黑名单更能阻止恶意软件

大多数杀毒软件属于黑名单，它屏蔽已知不良软件。防病毒软件定期更新识别新的已知不良软件特征，攻击者通过轻微修改恶意代码可防止病毒检测，使得黑名单失效，导致已知不良软件特征数据绝对数量增加。因此，黑名单作用越来越小。

白名单：只允许执行已知的好软件，因为组织控制其白名单，可将其保持在一定数量，所以白名单更容易管理。白名单不易被攻击者操纵，因为当软件在可执行级别被识别时新版本恶意软件被自动阻止。因此，白名单更有潜力阻止多数恶意软件，包括高级持续威胁（APT）和 0-day 恶意软件。

四、SWAM 期望状态和实际状态

1） SWAM 期望状态

软件资产管理的期望状态是，每个被授权的设备只包含分配角色所需的授权（已知好的）软件。在短期内，组织可能使用允许的灰名单执行选定的软件，但这不是理想状态，而期望状态是：

- 只有已知的好软件（白名单软件）和选定的灰名单软件（不知好坏的软件）才允许在设备上安装或执行。
- 提供管理软件的个人信息，以便将风险报告给负责人。

2） 期望状态的软件管理功能

组织机构不同，软件管理责任不同。简单情况下，每个设备管理器负责该设备上的所有软件管理功能。复杂情况下，不同的软件管理功能可以分配给不同的组，它们必须协调管理设备上的软件。每个软件产品的期望状态数据必须指定人负责该产品（在每个设备上）每个软件功能，以便向负责人报告风险/缺陷以达到问题解决。

软件产品管理功能：

- 软件产品管理（在整个组织范围内）
- 软件安装（按设备计）
- 软件配置设置管理（按设备计）
- 软件补丁管理（按设备计）

3） 软件管理功能和角色分配

组织应该为应用程序（角色或软件套件）选择一个主体专家，他了解系统和软件的依赖性、安全配置、补丁周期或如何正确安装软件。其可选择管理任务：

（1）自动或手动

在许多组织中，所有软件都是由在每个本地设备上运行安装软件管理员手动安装的。在有些组织中，从一个集中式控制台自动完成软件安装，该控制台使用软件安装工具将新软件推到所有设备。这两种方法或组合都是有效的，但它们通常会改变人的责任，这种责任的变化必须反映在期望状态数据中。当自动化工具在已知范围内管理安装时，该范围可用于记录自动化工具的责任。

（2）集中或分散

即使在使用手动安装程序的组织中，一些产品（例如，数据库管理系统）也可能需要一个中心主体专家来执行安装。同样，在补丁中，组织可以使用自动化软件包来安装软件，不是从中央控制台执行安装，而是从分布式位置执行安装。如果软件从中央控制台自动化进行集中管理，那么责任范围也可以改变负责特定职能的人。

（3）多面手（设备经理）或专家（例如，修补过程中的 SME，或产品中的 SME）

4） 期望状态资产目录

SWAM 的状态资产目录包括：

- 处于硬件资产管理（HWAM）期望状态的每个授权设备的角色列表；
- 每个角色列表，用于标识允许为每个设备角色安装/执行的软件产品和可执行文件；
- 按设备列出的所有授权软件清单，这些授权软件可在 HWAM 清单中每个设备上安装/执行。

软件配置文件是允许安装和运行的授权软件列表。

5） 在期望状态下应记录哪些数据

期望状态记录的最小软件资产管理数据应包括以下内容：

数据项	理由
批准软件注册内容（供应商、产品、版本、版本级别等）或软件标识（SWID）	● 报告设备类型 ● 供应链管理 ● 确定什么产品可能适用于设备
对每个软件注册内容管理职能的管理职责	确定管理职责，确保软件许可证、补丁和

	配置标准是最新的。（如果没有明确指定，假定其为设备管理员。）
软件产品预计将出现在白名单、黑名单、灰名单上的时间段	用于确定特定授权软件产品的使用寿命。(所有授权软件必须有“删除”日期。）
预期软件的数字指纹，包括已批准软件产品的可执行文件（组件、EXEs 、DLLs 等）。	标识可执行文件可能改变时，意味着它可能不再是“好”软件。

6） 如何确定 SWAM 期望状态？

SWAM 期望状态是由组织授权的软件资产清单，包括资产特性。

经授权的软件资产目录包括：

- 建立和维护在具有该角色的授权硬件设备上允许的授权软件产品和可执行文件的角色列表和相关配置文件。包括：
  - o 白名单软件
  - o 允许的灰名单软件
- 记录特定设备可能具有附加软件的例外情况（风险验收）
- 建立和维护网络上明确不允许列出的软件包、产品和文件（列入黑名单）的列表,不应安装在公司网络上的软件包（如色情、赌博），过时和脆弱的企业软件版本，在网络上安装不必要特性的侵入性软件包（例如，工具栏、间谍软件、密钥记录器）。注：只需要执行白名单软件，无需黑名单，增加的黑名单提供深入防御。

许多白名单工具可以识别具有行业认为已知好特征和已知坏特征的软件，这可帮助识别受信任的软件，避免在允许的灰名单上添加已知的坏软件特征。

通常，白名单产品会为大多数商业软件产品中的可执行文件提供数字指纹（或数字签名）。这可以帮助识别可能已被修改为包含恶意软件的软件可执行文件。对于自定义代码，组织应该对代码执行漏洞分析，并在经过验证的代码上计算数字指纹（或数字签名）。

7） 期望状态更改

许多事件会触发期望状态更改，组织必须及时识别并响应这些事件。示例如下：

事件	响应
经批准的安装程序安装了新的软件产品或可执行文件。	可以自动允许运行或阻止。通常，除非已经被归类为已知的“好”软件，否则它将被添加到灰名单中。因为灰名单应该很小（随着时间的推移应该会变小），软件产品应该被评估并迅速转移到白色或黑名单中。
在允许的灰名单中的遗留软件存在于设备	超过 12-24 个月，这样的软件必须被列入白

上。	名单或被列入黑名单。
未识别的软件出现在没有由授权安装程序放置的设备上，或以前可信的可执行更改的数字指纹。	这很可能是恶意软件。需要一种方法来阻止这些软件的执行，还必须有一种删除它的方法，并确定其来源。
已批准的软件产品的预期软件可执行文件(例如，组件、EXEs、dll)的数字指纹有改变。	必须使用数字指纹来识别可执行文件何时可能发生了变化，这意味着它可能不再是“好”软件，可能需要删除已更改的可执行文件。

8） SWAM 实际状态

软件资产管理的实际状态是：每个软件产品和企业网络上当前存在的每个可执行文件，包括可执行文件与其对应的软件产品相互关系。包括：

- 经授权和未经授权的软件
- 恶意和非恶意的软件
- 允许运行的软件和不允许运行的软件

9） 实际状态资产目录构成

软件资产管理的实际状态资产目录是通过已发现的设备列的清单，组织中每个设备上发现的所有的软件（产品和相应的可执行文件）。

实际状态记录的最小软件资产管理数据应包括：

数据项	理由
软件资产（产品和可执行文件）在硬件资产上检测到的数据	供将来比较白名单和黑名单的情况软件
软件（批准软件注册/可执行文件）的时间估计	确定软件被看到的时间以及最后一次在企业中看到的时间
有足够的数据，允许将实际的软件资产与授权的硬件资产进行比较	将授权软件连接到应该安装的设备上 ● 映射到批准软件注册、软件标识（SWID）等，为产品提供的信息 ● 可执行文件的数字指纹
数据，以唯一地标识正确的内容，将每个唯一的标识符关联到每个组成软件套件软件注册的可执行文件的每个数字对象（与数字指纹进行比较）	用于将每个唯一标识符关联到每个标识组成一个软件套件的可执行文件
从软件资产列表中（已识别的数字资产对象）推断出软件必要数据：批准软件注册数据(或SWID)	对于连接批准软件注册数据（或 SWID ）到一个特定的软件资产

10） 组织如何确定其实际状态

使用传感器来收集存在于网络的软件信息，这些传感器使用的技术包括注册表扫描、系统自我报告，定期执行软件发现和日志记录，以及单个文件分析等。

五、一个组织如何找到期望状态和实际状态之间的区别

如果正确设置了期望状态软件资产目录和实际状态软件资产目录，则检测这些潜在风险条件所需的所有数据都是可用的，可通过简单的数据库查询检测风险。查询后，查询结果可以报告给仪表盘，仪表盘可以记录发现每种风险状况的时间以及存在的时间。从期望状态软件资产目录和实际状态传感器接收数据后，由仪表盘自动处理。

期望状态和实际状态之间的差异被认为是一种可能导致缺陷的风险条件。主要示例如下表所示：

检测到期望状态和实际状态之间的差异	为什么是风险状况？	什么风险？
黑名单软件被允许存在或执行。	已知的坏软件通常会导致安全危害。	该软件很可能会导致安全危害。
灰名单中的软件被允许存在或执行。	未验证安全的软件可能被执行。	由于该软件尚未被验证是安全的，因此它将导致安全危害的风险就会增加。
存在未经授权的软件。	未以期望状态列出的软件被允许存在或执行。	由于该软件尚未被验证是安全的，因此它将导致安全危害的风险增加。由于该软件没有出现在所需的态列表中，因此它将导致安全危害风险增加。
存在非报告的设备。	由于该设备没有报告存在软件，因此存在恶意软件的风险较高。	通常，如果设备没有报告，软件管理器就不知道需要修复什么，因此缺陷会随着时间的推移而增加。 由于恶意软件或恶意内部人士干扰报告，设备可能无法报告。

六、解决实际状态和期望状态之间的差异

一旦网络安全仪表盘确定了实际状态资产目录和期望状态资产目录之间的差异，仪表盘将标记存在风险条件的软件资产，评分算法将被用于估计风险。如果风险状况较大，

风险评分可能会增加（随着时间的推移，妥协的可能性可能会增加）。某些类型的软件的风险评分也可能更高。

实际消除风险需要采取以下措施：

风险条件	检测规则	响应选项
黑名单软件被允许存在或执行。	软件出现在实际状态软件资产目录中，但被列入期望状态资产目录的黑名单，执行不被阻止。	1.阻止软件的执行 2.将其从实际状态中删除（请卸载）。 3.未将其列入黑名单。（这种反应是危险的。）
灰名单中的软件被允许存在或执行。	软件出现在实际状态软件资产目录中，但在所需状态软件资产目录中灰名单显示，不会阻止执行。	1.阻止软件的执行 2.将其从实际状态中删除（请卸载）。 3.未将其列入白名单。（这种反应是危险的。） 问题：这个缺陷开始时风险比以前的风险低，但风险会随着时间的推移而增加。
存在未经授权的软件。	软件出现在实际状态软件资产目录中，但不在期望状态。（注意：如果由批准的安装程序安装，组织可以自动列入灰名单软件，以避免此问题。）	将软件添加到期望状态，并将其列入白、灰/黑名单。
存在非报告的设备。	具有软件的硬件处于期望的或实际状态软件资产目录，但不处于软件实际状态及时的数据。	恢复报告，或在 HWAM 中声明设备丢失/卸载/退役。

防止未经授权的软件进入网络

从灰名单中删除未经授权的软件或授权软件理论上是不必要的。但在真正的运营网络中，这往往是不可避免的，最终是一项艰巨的任务。尽管如此，我们还是必须问，组织是否可以做些事情来减少发现和分类新发现的软件为授权软件所需的返工或恶意软件。

可以采取以下措施，减少整个企业系统上未经授权的软件数量：

1） **安全策略明确规定谁将在系统上拥有高级特权，以及他们可以使用这些特权做什么。**系统管理员经常向系统引入未经授权和潜在的恶意软件，因为他们能够在系统上安装新软件，并使用提高帐户的互联网，或者他们可能在可移动媒体方面使用不“卫生”

做法。适当地限制管理员拥有的特权，并定义授权和未经授权的活动，可大大地降低安全风险。

2） **日志记录可以跟踪何时安装了未经授权的软件以及由谁完成。**日志可以帮助确定原因（例如，配置管理过程中的故障、滥用特权）。一旦这个人被发现，让他们知道可防止这些风险条件产生的预期是什么。

3） 处罚。处罚那些经常通过滥用角色和特权而安装未经授权的软件的人，以及在收到警告后仍这样做的人。

七、SWAM 标准和机构

1） 通用平台枚举(CPE）规范

NIST 联合系列报告 Common Platform Enumeration (CPE)—Specification, Version 2.3, 2011.8。CPE 一种描述和识别企业计算资产中的应用程序、操作系统和硬件设备类别的标准化方法。CPE 可用作信息源，用于执行和验证与这些资产相关的 IT 管理策略，如漏洞、配置和补救策略。IT 管理工具可以收集有关已安装产品的信息，使用其 CPE 名称识别产品，并使用这些标准化信息来帮助对资产做出完全或部分自动化的决策。

CPE 名称提供了许多联邦政府安全内容自动化协议(SCAP)数据库之间的一个关键链接。最初构思时，CPE 命名过程假设软件发布商提供适当的 CPE 名称以包含在正式的 CPE 字典中。到目前为止，软件发布社区采用 CPE 命名过程受到限制，因此国家标准与技术研究所(NIST)和 MITRE 公司开发了一个程序，通过手动创建 CPE 名称并将其添加到 CPE 字典中。

2） 软件标识标(SWID)标准

ISO/IEC19770-2：2015--信息技术--软件资产管理--第二部分：软件标识标(SWID)。SWID 标准能够记录和报告组成产品的可执行文件列表和每个文件的数字指纹。该功能支持两个有意义的供应链分析：首先，SWID 中报告的可执行文件是否与产品的预期可执行文件相匹配，如果没有，则该产品在安装前可能已被篡改；第二，在当前设备上执行报告的可执行文件是否与 SWID 中的可执行文件相匹配。

3） 企业软件管控标准

中关村标准化协会 2016 年发布 T/ZSA 3001.01-2016 企业移动智能终端应用开发、安装、运行管控机制指南。本标准规定了企业移动应用软件（App）开发准入、软件开发、软件签名及验证、软件审核、软件发布、软件安装及运行监管等过程，为移动智能终端厂商、应用开发者、企业应用软件服务商实施企业移动应用软件（App）资产生命期管理提供指南。

4） TagVault.org

一个注册和认证组织，为软件发布商提供生成满足 CPE 及 SWID 标准的软件认证标签工具，并对认证标签进行数字签名，确保数据权威性，任何查看标签数据的人均可验证数据的来源，以满足 CPE 标准要求。

八、SWAM 实例

中国政企应用软件平台（China Government Enterprise Application Platform，cgeap.cn)依据网络安全等级保护标准 GB/T 22239-2019 网络安全等级保护基本要求、中关村标准 T/ZSA 3001.01-2016 企业移动智能终端应用开发、安装、运行管控机制指南，为政企单位提供 App 开发者审核、安全开发、数字签名、安全检测、运行管理等 App 资产全生命期管理服务，确保政企 App 资产合规、安全、绿色、高品质、责任可追溯。

1） GEAP 平台构成

GEAP 平台由五个子系统组成：政企软件开发管理、政企通用软件市场、政企软件仓库、APP 国密签名、GEAP 安全移动终端。见图 1。

图 1 GEAP 平台系统构成

2） 软件开发管理

为移动软件开发者提供软件开发和发布的平台。系统主要提供开发者（机构开发者）注册、登录、提交实名认证申请、身份审验（包括自动和人工）、证书申请、证书下载/更新/注销、软件签名、软件提交、版本管理、软件上架前审核等服务，实现软件实名化，保证开发者身份的可靠性，保证移动软件的安全性和完整性。

软件开发管理系统主要包括一套功能完备的 Web 网站，提供给平台运营团队以及所有开发者使用。同时系统还为开发者提供了专用的签名工具，用于线下代码签名。

3） 政企通用软件市场

为软件开发者提供软件推广、上架/下架、软件信息更新、软件售卖服务。为软件

用户提供合规、安全、绿色、高效、可靠的软件搜索、软件推荐、查看软件详情、软件下载/更新等服务。软件市场包括服务器端管理系统以及客户端 APP。如图 2 所示。

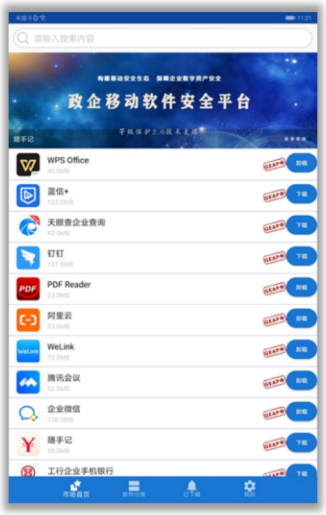

图 2 GEAP 平台政企通用软件市场

4） 政企软件仓库

为政企单位提供软件资产安全托管和软件运行管理服务，建立软件资产白名单、软件配置列表，降低软件管理成本，提高软件运维安全。政企移动软件仓库如图 3 所示。

图 3 政企软件仓库

5） APP 国密签名与验证

对 APP 进行国密算法多重代码签名与验证的功能模块，包含提供给开发者的签名工具、平台使用的自动签名服务和 SDK，手机用户可随时远程或本地验证 app 签名等。APP 国密签名与验证如图 4 所示。

图 4 GEAP 平台 APP 国密签名与验证

6） GEAP 安全移动终端

GEAP 安全移动终端是华为鼎桥通信技术有限公司与三博安科技有限公司合作开发的企业级移动智能终端，与“政企移动软件安全平台”（GEAP 平台）联合使用，GEAP 安全移动终端“只运行授权白名单 app”，为网络安全等级保护 2.0 实施提供技术支持。实现 SWAM 期望状态。GEAP 安全移动终端见图 5。

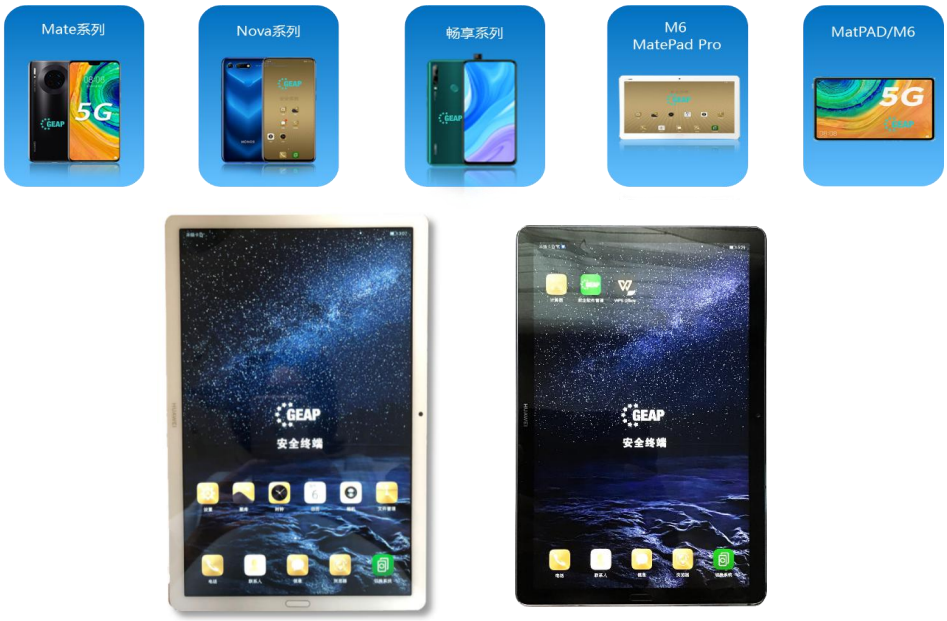

图 5 GEAP 安全移动终端

参考文献

[1] CDM Software Asset Management (SWAM) Capability, Department of Homeland Security Office of Cybersecurity and Communications Federal Network Resilience

[2] Certified SWID Tag Integration with Common Platform Enumeration names, https://register.mitre.org/devdays/certified_swid_tags_integration_cpe_names.pdf

[3] ISO/IEC 19770-1:2012 -- Information technology -- Software asset management -- Part 1: Processes and tiered assessment of conformance http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=56000

[4] ISO/IEC 19770-2:2009 -- Information technology -- Software asset management --Part 2:Software identification tag, http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670

[5] Common Platform Enumeration:Naming Specification Version 2.3, NIST Interagency Report 7695 http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf.

[6] T/ZSA 3001.01-2016 企业移动智能终端应用开发、安装、运行管控机制指南 https://www.cgeap.cn/uploadfile/2020/0715/20200715093411134.pdf