(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113641997 A
(43)申请公布日 2021.11.12

(21)申请号 202110812804.1

(22)申请日 2021.07.19

(71)申请人 青岛海尔工业智能研究院有限公司
地址 266510 山东省青岛市黄岛区团结路2877号中德生态园管委会257房间
申请人 海尔数字科技(青岛)有限公司
海尔卡奥斯物联生态科技有限公司

(72)发明人 黄玉宝 孙明 林宏 于海东

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孔凡红

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 16/903(2019.01)

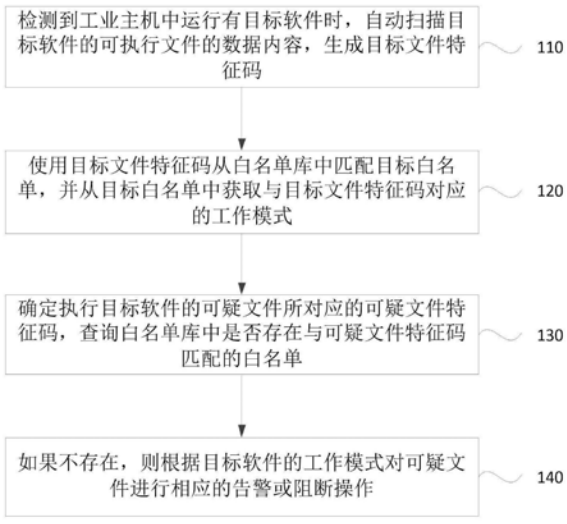
权利要求书2页 说明书8页 附图3页

(54)发明名称

工业主机的安全防护方法、装置、系统及存储介质

(57)摘要

本发明实施例公开了一种工业主机的安全防护方法、装置、系统及存储介质。该方法应用于安装在工业主机上的安全防护系统客户端，包括：检测到工业主机中运行有目标软件时，自动扫描目标软件的可执行文件的数据内容，生成目标文件特征码；使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获取与目标文件特征码对应的工作模式；确定执行目标软件的可疑文件所对应的可疑文件特征码，查询白名单库中是否存在与可疑文件特征码匹配的白名单；如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻断操作。本发明实施例的技术方案，通过进行轻量级的白名单匹配，禁止异常程序在工业主机中运行，实现对工业主机的安全防护。



CN 113641997 A

1.一种工业主机的安全防护方法,其特征在于,应用于安装在工业主机上的安全防护系统客户端,包括:

检测到工业主机中运行有目标软件时,自动扫描所述目标软件的可执行文件的数据内容,生成目标文件特征码;

使用所述目标文件特征码从白名单库中匹配目标白名单,并从所述目标白名单中获取与所述目标文件特征码对应的工作模式;

确定执行所述目标软件的可疑文件所对应的可疑文件特征码,查询白名单库中是否存在与所述可疑文件特征码匹配的白名单;

如果不存在,则根据所述目标软件的工作模式对所述可疑文件进行相应的告警或阻断操作。

2.根据权利要求1所述的方法,其特征在于,所述工作模式包括告警模式和防护模式;

所述告警模式,用于在异常程序执行被保护的可执行文件时,进行实时告警,但不阻断异常程序执行;

所述防护模式,用于在异常程序执行被保护的可执行文件时,进行实时告警,并阻断异常程序执行。

3.根据权利要求2所述的方法,其特征在于,还包括:

如果检测到工业主机下载或者开启使用新软件,则为新软件设置工作模式,并自动扫描新软件的可执行文件的数据内容,生成新的文件特征码;

使用新的文件特征码和工作模式生成新的白名单,并将新的白名单存储到白名单库中更新生效。

4.根据权利要求1所述的方法,其特征在于,还包括:

当检测到外部存储设备接入时,基于所述外部存储设备的唯一标识判断所述外部存储设备是否具有接入权限;

如果有接入权限,则根据所述外部存储设备的唯一标识匹配获取设备操作权限,并根据设备操作权限响应所述外部存储设备的操作。

5.一种工业主机的安全防护装置,其特征在于,应用于安装在工业主机上的安全防护系统客户端,包括:

文件扫描模块,用于检测到工业主机中运行有目标软件时,自动扫描所述目标软件的可执行文件的数据内容,生成目标文件特征码;

白名单匹配模块,用于使用所述目标文件特征码从白名单库中匹配目标白名单,并从所述目标白名单中获取与所述目标文件特征码对应的工作模式;

查询模块,用于确定执行所述目标软件的可疑文件所对应的可疑文件特征码,查询白名单库中是否存在与所述可疑文件特征码匹配的白名单;

告警模块,用于如果不存在,则根据所述目标软件的工作模式对所述可疑文件进行相应的告警或阻断操作。

6.根据权利要求5所述的装置,其特征在于,所述工作模式包括告警模式和防护模式;

所述告警模式,用于在异常程序执行被保护的可执行文件时,进行实时告警,但不阻断异常程序执行;

所述防护模式,用于在异常程序执行被保护的可执行文件时,进行实时告警,并阻断异

常程序执行。

7.一种工业主机安全防护系统,其特征在于,所述系统包括:安装在工业主机上的客户端以及安装在服务器上的控制中心;

所述客户端,用于执行如权利要求1-4中任一项所述的工业主机的安全防护方法;

所述控制中心,用于对联网情况下的多个工业主机上的客户端进行集中管理。

8.根据权利要求7所述的系统,其特征在于,所述工业主机安全防护系统包括单机版本和网络版本;

单机版本的工业主机安全防护系统用于对隔离情况下孤立的工业主机进行安全防护,系统包括:安装在工业主机上的客户端;

网络版本的工业主机安全防护系统用于对联网情况下的多个工业主机进行集中管控,系统包括:安装在工业主机上的客户端以及安装在服务器上的控制中心。

9.根据权利要求7所述的系统,其特征在于,

所述控制中心,用于收集各客户端上报的日志数据进行分析,如果发现网络攻击事件,则切断网络攻击事件的传播路径,并生成安全防护策略下发至所有工业主机上的客户端。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-4中任一所述的工业主机的安全防护方法。

工业主机的安全防护方法、装置、系统及存储介质

技术领域

[0001] 本发明实施例涉及工业安全技术领域，尤其涉及一种工业主机的安全防护 方法、装置、系统及存储介质。

背景技术

[0002] 现有技术中，工业主机相对普通的IT系统主机，在安全防护方面存在以下 特点：1)工业主机在投运后会运行很多年，硬件资源受限，往往不能安装杀毒 软件；2)工业主机不会随意升级或增加新的软件、插件，工控系统中的防病毒 库也不能定期升级；3)安装的普通杀毒软件可能会误杀关键进程，造成工控系 统运行异常的事件；4)杀毒软件一般会使用本地引擎或云端病毒库对工业主机 进行病毒查杀，可能会对造成工业软件的处理延时。这些特点导致对工业主机 进行全面的安全防护比较困难。

[0003]

发明内容

[0004] 本发明实施例提供一种工业主机的安全防护方法、装置、系统及存储介质，通过进行轻量级的白名单匹配，禁止异常程序在工业主机中运行，实现对工业 主机的安全防护。

[0005] 第一方面，本发明实施例提供了一种工业主机的安全防护方法，应用于安 装在工业主机上的安全防护系统客户端，包括：

[0006] 检测到工业主机中运行有目标软件时，自动扫描目标软件的可执行文件的 数据内容，生成目标文件特征码；

[0007] 使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获 取与目标文件特征码对应的工作模式；

[0008] 确定执行目标软件的可疑文件所对应的可疑文件特征码，查询白名单库中 是否存在与可疑文件特征码匹配的白名单；

[0009] 如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻 断操作。

[0010] 可选的，工作模式包括告警模式和防护模式；

[0011] 告警模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，但不阻断异常程序执行；

[0012] 防护模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，并阻断异常程序执行。

[0013] 可选的，还包括：

[0014] 如果检测到工业主机下载或者开启使用新软件，则为新软件设置工作模式，并自动扫描新软件的可执行文件的数据内容，生成新的文件特征码；

[0015] 使用新的文件特征码和工作模式生成新的白名单，并将新的白名单存储到 白名

单库中更新生效。

[0016] 可选的，还包括：

[0017] 当检测到外部存储设备接入时，基于外部存储设备的唯一标识判断外部存 储设备是否具有接入权限；

[0018] 如果有接入权限，则根据外部存储设备的唯一标识匹配获取设备操作权限，并根据设备操作权限响应外部存储设备的操作。

[0019] 第二方面，本发明实施例还提供了一种工业主机的安全防护装置，应用于 安装在工业主机上的安全防护系统客户端，包括：

[0020] 文件扫描模块，用于检测到工业主机中运行有目标软件时，自动扫描目标 软件的可执行文件的数据内容，生成目标文件特征码；

[0021] 白名单匹配模块，用于使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获取与目标文件特征码对应的工作模式；

[0022] 查询模块，用于确定执行目标软件的可疑文件所对应的可疑文件特征码，查询白名单库中是否存在与可疑文件特征码匹配的白名单；

[0023] 告警模块，用于如果不存在，则根据目标软件的工作模式对可疑文件进行 相应的告警或阻断操作。

[0024] 可选的，工作模式包括告警模式和防护模式；

[0025] 告警模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，但不阻断异常程序执行；

[0026] 防护模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，并阻断异常程序执行。

[0027] 第三方面，本发明实施例还提供了一种工业主机安全防护系统，系统包括：安装在工业主机上的客户端以及安装在服务器上的控制中心；

[0028] 客户端，用于执行本发明实施例提供的工业主机的安全防护方法；

[0029] 控制中心，用于对联网情况下的多个工业主机进行集中管理。

[0030] 可选的，工业主机安全防护系统包括单机版本和网络版本；

[0031] 单机版本的工业主机安全防护系统用于对隔离情况下孤立的工业主机进行 安全防护，系统包括：安装在工业主机上的客户端；

[0032] 网络版本的工业主机安全防护系统用于对联网情况下的多个工业主机进行 集中管控，系统包括：安装在工业主机上的客户端以及安装在服务器上的控制 中心。

[0033] 可选的，控制中心，用于收集各客户端上报的日志数据进行分析，如果发 现网络攻击事件，则切断网络攻击事件的传播路径，并生成安全防护策略下发 至所有工业主机上的客户端。

[0034] 第四方面，本发明实施例还提供了一种计算机可读存储介质，其上存储有 计算机程序，该程序被处理器执行时实现本发明任意实施例提供的工业主机的 安全防护方法。

[0035] 本发明实施例中，工业主机安全防护系统客户端检测到工业主机中运行有 目标软件时，自动扫描目标软件的可执行文件的数据内容，生成目标文件特征 码；使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获 取与目标文件特征码对应的工作模式；确定执行目标软件的可疑文件所对应的 可疑文件特征码，查询白名单库中是

否存在与可疑文件特征码匹配的白名单；如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻断操 作，解决了现有技术中对工业主机进行安全防护困难的问题，通过进行轻量级 的白名单匹配，禁止异常程序在工业主机中运行，实现对工业主机的安全防护。

附图说明

[0036] 图1a是本发明实施例一中的一种工业主机的安全防护方法的流程图；

[0037] 图1b是本发明实施例一中的一种白名单架构示意图；

[0038] 图1c是本发明实施例一中的一种异常程序的拦截流程图；

[0039] 图2是本发明实施例二中的一种工业主机的安全防护装置的结构示意图；

[0040] 图3a是本发明实施例三中的一种工业主机安全防护系统的结构示意图；

[0041] 图3b是本发明实施例三中的一种网络版本的工业主机安全防护系统的架 构图。

具体实施方式

[0042] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此 处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需 要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结 构。

[0043] 实施例一

[0044] 图1a是本发明实施例一中的一种工业主机的安全防护方法的流程图，本实 施例可适用于对工业主机进行全面的安全防护的情况，该方法可以由工业主机 的安全防护装置来执行，该装置可以由硬件和/或软件来实现，并一般可以集成 在提供工业安全防护服务的工业主机安全防护系统客户端中。如图1a所示，该 方法包括：

[0045] 步骤110、检测到工业主机中运行有目标软件时，自动扫描目标软件的可 执行文件的数据内容，生成目标文件特征码。

[0046] 本实施例中，为了检测客户端所在工业主机中是否有异常程序，可以实时 检测工业主机中是否有软件在运行，如果捕获到正在运行的目标软件，则通过 全盘自动扫描将目标软件的可执行文件形成唯一的目标文件特征码。其中，文 件特征码不依赖于可执行文件的文件名称、文件路径或扩展名等信息，只依赖 于可执行文件本身的数据特征，只要可执行文件发生变化，文件特征码就相应 变化。

[0047] 步骤120、使用目标文件特征码从白名单库中匹配目标白名单，并从目标 白名单中获取与目标文件特征码对应的工作模式。

[0048] 本实施例中，白名单中包括预先设置的允许在工业主机中运行的可执行文 件的文件特征码以及工作模式。在确定目标文件特征码之后，可以使用目标文 件特征码在白名单库中查询匹配的白名单，如果查询到包括目标文件特征码的 目标白名单，则认为目标软件是被保护的常规软件，需要从目标白名单中获取 与目标文件特征码对应的工作模式，确定目标软件的安全防护等级。如果没有 查询到包括目标文件特征码的白名单，则认为目标软件未受保护，不对其进行 安全防护操作。

[0049] 可选的，工作模式包括告警模式和防护模式；告警模式，用于在异常程序 执行被保护的可执行文件时，进行实时告警，但不阻断异常程序执行；防护模 式，用于在异常程序

执行被保护的可执行文件时，进行实时告警，并阻断异常 程序执行。

[0050] 本实施例中，可以根据重要性，将要保护的软件的工作模式设置为告警模 式或者防护模式。其中，当工作模式为告警模式时，如果被保护的可执行文件 被异常程序执行，会根据可执行文件和异常程序的相关信息进行实时告警，但 不会阻断异常程序的执行；当工作模式为防护模式时，如果被保护的可执行文 件被异常程序执行，会进行告警同时进行阻断，使得异常程序无法运行。

[0051] 本实施例中，当在工业主机中安装系统客户端时，会选择工业主机使用的 软件，并自动扫描软件的可执行文件生成文件特征码加入白名单，然后为软件 设置相应的工作模式加入白名单，将白名单加入白名单库中应用生效，如图1b 所示，以便于后续根据白名单库中的白名单判断主机中的软件是否允许运行。

[0052] 步骤130、确定执行目标软件的可疑文件所对应的可疑文件特征码，查询 白名单库中是否存在与可疑文件特征码匹配的白名单。

[0053] 本实施例中，在确定目标软件为受保护软件后，需要进一步验证目标软件 的执行者是否是异常程序。可以先获取执行目标软件的程序作为可疑文件，扫 描该可疑文件的数据内容生成可疑文件特征码，在白名单库中根据可疑文件特 征码进行白名单匹配，如果匹配到白名单，则认为目标软件的执行者不是异常 程序，可以正常运行。

[0054] 步骤140、如果不存在，则根据目标软件的工作模式对可疑文件进行相应 的告警或阻断操作。

[0055] 本实施例中，如果白名单库中找不到与可以文件特征码匹配的白名单，则 认为目标软件的执行者为异常程序，需要进行相应的防护处理，此时，如果目 标软件的工作模式为告警模式，则根据可执行文件和异常程序的相关信息进行 实时告警，但不用阻断异常程序的运行；如果工作模式为防护模式，则会在进 行告警的同时阻断异常程序运行。

[0056] 可选的，还可以包括：如果检测到工业主机下载或者开启使用新软件，则 为新软件设置工作模式，并自动扫描新软件的可执行文件的数据内容，生成新 的文件特征码；使用新的文件特征码和工作模式生成新的白名单，并将新的白 名单存储到白名单库中更新生效。

[0057] 本实施例中，如图1b所示，当工业主机要使用新的软件，需要进行白名单 软件更新时，可以进行追加目录或追加文件进行白名单放行，也可设置信任目 录或信任文件进行完全信任和放行。当白名单进行更新后，需要存到白名单库 中进行应用生效。其中，新软件的白名单可以导入生成，也可以扫描生成。导 入生成，可以直接将已生成的白名单导入客户端中；扫描生成，可以通过自动 扫描新软件的可执行文件的数据内容生成新的文件特征码，并将新软件的工作 模式以及新的文件特征码加入新的白名单。其中，白名单库支持对白名单进行 查询、导入、导出以及显示列表等操作。

[0058] 可选的，还可以包括：当检测到外部存储设备接入时，基于外部存储设备 的唯一标识判断外部存储设备是否具有接入权限；如果有接入权限，则根据外 部存储设备的唯一标识匹配获取设备操作权限，并根据设备操作权限响应外部 存储设备的操作。

[0059] 本实施例中，如图1c所示，为了更加全面的对工业主机进行防护，可以预 先为外部存储设备设置接入权限，防止非授权的外部存储设备引入病毒。从而， 在发现有外部存储设备接入工业主机时，可以根据该设备的设备标识判断其是 否具有接入权限，如果没有

被授权，则不允许该设备接入，如果确定有授权，则继续使用该设备的设备标识查询具体的操作权限，只对开放权限的操作进行 响应。

[0060] 本实施例中，在对外部存储设备进行接入授权之外，还可以通过系统内置 “永恒之蓝”漏洞的网络防御引擎和专杀工具，对“永恒之蓝”及其变种网络 攻击实时拦截。利用“漏洞利用分析-流量解析对比-可疑攻击阻断”等技术，无需为工业主机打补丁、关端口，即可进行“永恒之蓝”勒索病毒的预判与防 御。

[0061] 本实施例中，工业主机安全防护系统以轻量级“白名单”的技术方式，全 方位地保护主机的资源使用。根据白名单策略，工业主机安全防护系统会禁止 非法进程的运行，并通过基于设备唯一标识的USB移动存储外设管控，禁止非 法USB设备的接入，同时对合法USB设备进行权限管控，还可以结合漏洞防御、网络防护等安全防护措施，切断病毒和木马的传播与破坏路径。

[0062] 本发明实施例中，工业主机安全防护系统客户端检测到工业主机中运行有 目标软件时，自动扫描目标软件的可执行文件的数据内容，生成目标文件特征 码；使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获 取与目标文件特征码对应的工作模式；确定执行目标软件的可疑文件所对应的 可疑文件特征码，查询白名单库中是否存在与可疑文件特征码匹配的白名单； 如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻断操 作，解决了现有技术中对工业主机进行安全防护困难的问题，通过进行轻量级 的白名单匹配，禁止异常程序在工业主机中运行，实现对工业主机的安全防护。

[0063] 实施例二

[0064] 图2是本发明实施例二中的一种工业主机的安全防护装置的结构示意图，本实施例可适用于对工业主机进行全面的安全防护的情况，该装置可以由硬件 和/或软件来实现，并一般可以集成在提供工业安全防护服务的工业主机安全防 护系统客户端中。如图2所示，该装置包括：

[0065] 文件扫描模块210，用于检测到工业主机中运行有目标软件时，自动扫描 目标软件的可执行文件的数据内容，生成目标文件特征码；

[0066] 白名单匹配模块220，用于使用目标文件特征码从白名单库中匹配目标白 名单，并从目标白名单中获取与目标文件特征码对应的工作模式；

[0067] 查询模块230，用于确定执行目标软件的可疑文件所对应的可疑文件特征 码，查询白名单库中是否存在与可疑文件特征码匹配的白名单；

[0068] 告警模块240，用于如果不存在，则根据目标软件的工作模式对可疑文件 进行相应的告警或阻断操作。

[0069] 本发明实施例中，工业主机安全防护系统客户端检测到工业主机中运行有 目标软件时，自动扫描目标软件的可执行文件的数据内容，生成目标文件特征 码；使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获 取与目标文件特征码对应的工作模式；确定执行目标软件的可疑文件所对应的 可疑文件特征码，查询白名单库中是否存在与可疑文件特征码匹配的白名单； 如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻断操 作，解决了现有技术中对工业主机进行安全防护困难的问题，通过进行轻量级 的白名单匹配，禁止异常程序在工业主机中运行，实现对工业主机的

安全防护。

[0070] 可选的，工作模式包括告警模式和防护模式；

[0071] 告警模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，但不阻断异常程序执行；

[0072] 防护模式，用于在异常程序执行被保护的可执行文件时，进行实时告警，并阻断异常程序执行。

[0073] 可选的，还包括：

[0074] 更新模块，用于如果检测到工业主机下载或者开启使用新软件，则为新软 件设置工作模式，并自动扫描新软件的可执行文件的数据内容，生成新的文件 特征码；

[0075] 使用新的文件特征码和工作模式生成新的白名单，并将新的白名单存储到 白名单库中更新生效。

[0076] 可选的，还包括：

[0077] 接入检测模块，用于当检测到外部存储设备接入时，基于外部存储设备的 唯一标识判断外部存储设备是否具有接入权限；

[0078] 如果有接入权限，则根据外部存储设备的唯一标识匹配获取设备操作权限，并根据设备操作权限响应外部存储设备的操作。

[0079] 本发明实施例所提供的工业主机的安全防护装置可执行本发明任意实施例 所提供的工业主机的安全防护方法，具备执行方法相应的功能模块和有益效果。

[0080] 实施例三

[0081] 图3a是本发明实施例三中的一种工业主机安全防护系统的结构示意图，本 实施例可适用于对工业主机进行全面的安全防护的情况。如图3a所示，该系统 包括：安装在工业主机上的客户端310以及安装在服务器上的控制中心320；

[0082] 客户端310，用于执行本发明任意实施例提供的工业主机的安全防护方法；

[0083] 控制中心320，用于对联网情况下的多个工业主机上的客户端进行集中管 理。

[0084] 本实施例中，客户端310部署在需要被保护的工业主机上，执行最终的白 名单扫描和防护、外设管控、漏洞防御等安全防护操作，并与控制中心通信，提供控制中心管理所需的相关安全告警信息。

[0085] 可选的，控制中心320，用于收集各客户端上报的日志数据进行分析，如 果发现网络攻击事件，则切断网络攻击事件的传播路径，并生成安全防护策略 下发至所有工业主机上的客户端。

[0086] 本实施例中，如图3b所示，控制中心采用B/S架构，允许随时随地通过浏 览器进行访问，来对客户端进行管理和控制，主要包括分组管理、策略制定下 发、统一白名单扫描(及定时扫描)、客户端软硬件资产管理等。此外，控制中 心还可以提供系统运维的基础服务，如：客户端升级服务、数据服务、通讯服 务等。其中，单个控制中心可并发管理6000多个主机客户端，可基于用户组织 架构进行安全风险管理。同时，针对每个客户端可进行灵活的模块配置、权限 配置、页面配置、扫描时间配置，满足工业主机现场定制化安全策略需求。

[0087] 本实施例中，控制中心可以了解全网客户端的告警信息，掌握全网威胁状 况，预先设置安全防护策略，比如拦截常见网络攻击事件或者病毒等。如果控 制中心通过对客户

端的日志数据进行分析,发现网络攻击事件或者病毒等,则 切断其传播与破坏路径,并将对应的安全防护策略下发到所有主机的客户端进 行安全防护。

[0088] 可选的,工业主机安全防护系统包括单机版本和网络版本;单机版本的工 业主机安全防护系统用于对隔离情况下孤立的工业主机进行安全防护,系统包 括:安装在工业主机上的客户端;网络版本的工业主机安全防护系统用于对联 网情况下的多个工业主机进行集中管控,系统包括:安装在工业主机上的客户 端以及安装在服务器上的控制中心。

[0089] 本实施例中,考虑到工业主机可能由于联网情况或者其他原因导致无法与 外界通信,设计了单机版本和网络版本的工业主机安全防护系统。系统可以在 服务器上安装控制中心,对于隔离情况下孤立的工业主机,由于其无法连接控 制中心,因此,可以将工业主机上安装的系统客户端单独看作一个工业主机安 全防护系统,即系统切换为单机版本,来实现对孤立的工业主机进行安全防护。对于可联网的工业主机,由于主机上的客户端可以与控制中心连接,因此,系 统可以切换为网络版本,通过控制中心对网内所有工业主机上的客户端进行安 全策略管理、配置下发等,实现统一管控和安全风险分析。

[0090] 本实施例中,工业主机安全防护系统是一款工控环境专用的软件产品,通 过在工业主机上安装系统的客户端,在服务器上安装系统的控制中心,可以基 于智能匹配的白名单技术和基于设备标识的USB移动存储管控,对工业主机进 行入口拦截、运行拦截、扩散拦截等关卡式病毒拦截,能够防范恶意程序的运 行和非法外设接入,可以对多个工业主机进行全面集中管理和安全风险管理等, 实现对工业主机全面的安全防护。

[0091] 另外,工业主机安全防护系统针对工业设备搬迁、工业更替等引起的安全 防护软件授权无法替换使用的情况,可以通过授权回收机制,保证购买点数在 设备替换等情况下不会丢失和额外增加投资成本,从而节约用户成本。

[0092] 本实施例中,工业主机安全防护系统的软硬件适配能力较强,支持各种操 作系统,以及企业版、专业版等各类系统版本,硬件资源仅需256M内存、400M 可用硬盘空间,适配100多种工业软件。

[0093] 本发明实施例中,工业主机安全防护系统包括安装在工业主机上的客户端 以及安装在服务器上的控制中心;通过客户端,对外部存储设备进行接入鉴权, 使用轻量级白名单的智能匹配技术拦截运行中的恶意程序;通过控制中心,对 客户端上报的日志数据进行分析,如果发现网络攻击事件,切断网络攻击事件 的传播路径,并生成安全防护策略下发至所有工业主机上的客户端,实现对联 网情况下的多个工业主机上的客户端进行集中管理和安全风险分析,解决了现 有技术中对工业主机进行安全防护困难的问题,通过进行轻量级的白名单匹配, 禁止异常程序在工业主机中运行,实现对工业主机的安全防护。

[0094] 实施例四

[0095] 本发明实施例四还公开了一种计算机存储介质,其上存储有计算机程序, 该程序被处理器执行时实现一种工业主机的安全防护方法,应用于安装在工业 主机上的安全防护系统客户端,包括:

[0096] 检测到工业主机中运行有目标软件时,自动扫描目标软件的可执行文件的 数据内容,生成目标文件特征码;

[0097] 使用目标文件特征码从白名单库中匹配目标白名单,并从目标白名单中获 取与目标文件特征码对应的工作模式;

[0098] 确定执行目标软件的可疑文件所对应的可疑文件特征码,查询白名单库中 是否存在与可疑文件特征码匹配的白名单;

[0099] 如果不存在,则根据目标软件的工作模式对可疑文件进行相应的告警或阻 断操作。

[0100] 本发明实施例的计算机存储介质,可以采用一个或多个计算机可读的介质 的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储 介质。计算机可读存储介质例如可以是,但不限于电、磁、光、电磁、红外线、 或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的 更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式 计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程 只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光 存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可 读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系 统、装置或者器件使用或者与其结合使用。

[0101] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据 信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种 形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读 的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算 机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用 或者与其结合使用的程序。

[0102] 计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不 限于无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0103] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计 算机程序代码,程序设计语言包括面向对象的程序设计语言,诸如Java、 Smalltalk、C++,还包括常规的过程式程序设计语言,诸如”C”语言或类似的 程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算 机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算 机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形 中,远程计算机可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN), 连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供 商来通过因特网连接)。

[0104] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员 会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进 行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此,虽 然通过以上实施例对本发明进行了较为详细的说明,但是本发明不仅仅限于以 上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例, 而本发明的范围由所附的权利要求范围决定。

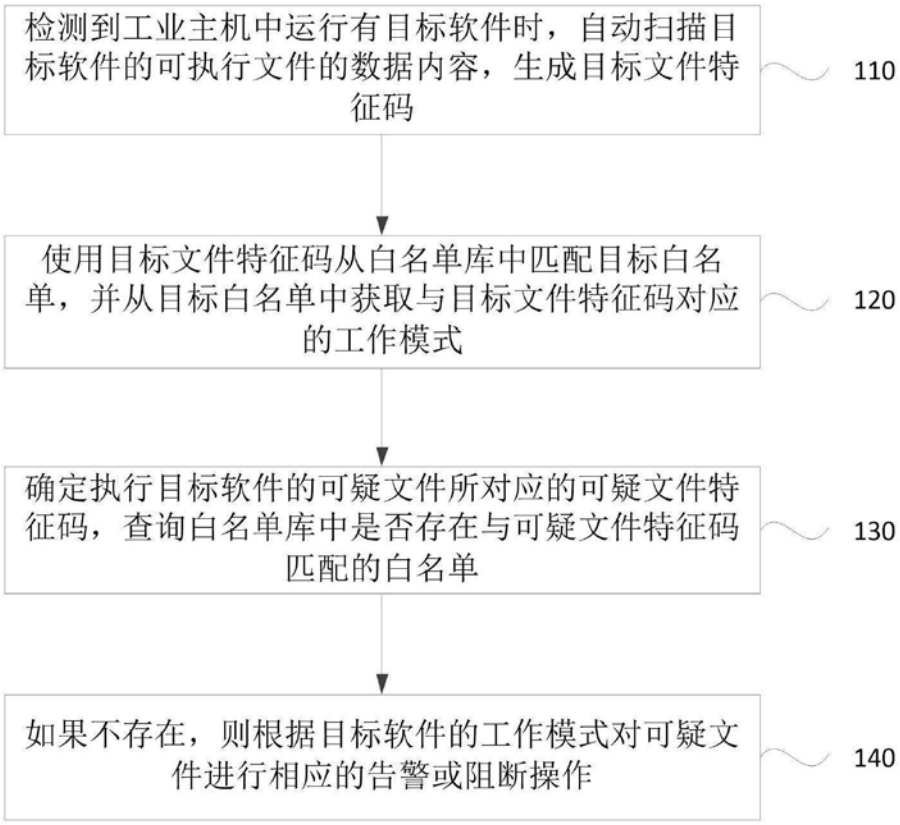

检测到工业主机中运行有目标软件时，自动扫描目标软件的可执行文件的数据内容，生成目标文件特征码
110
使用目标文件特征码从白名单库中匹配目标白名单，并从目标白名单中获取与目标文件特征码对应的工作模式
120
确定执行目标软件的可疑文件所对应的可疑文件特征码，查询白名单库中是否存在与可疑文件特征码匹配的白名单
130
如果不存在，则根据目标软件的工作模式对可疑文件进行相应的告警或阻断操作
140

图1a

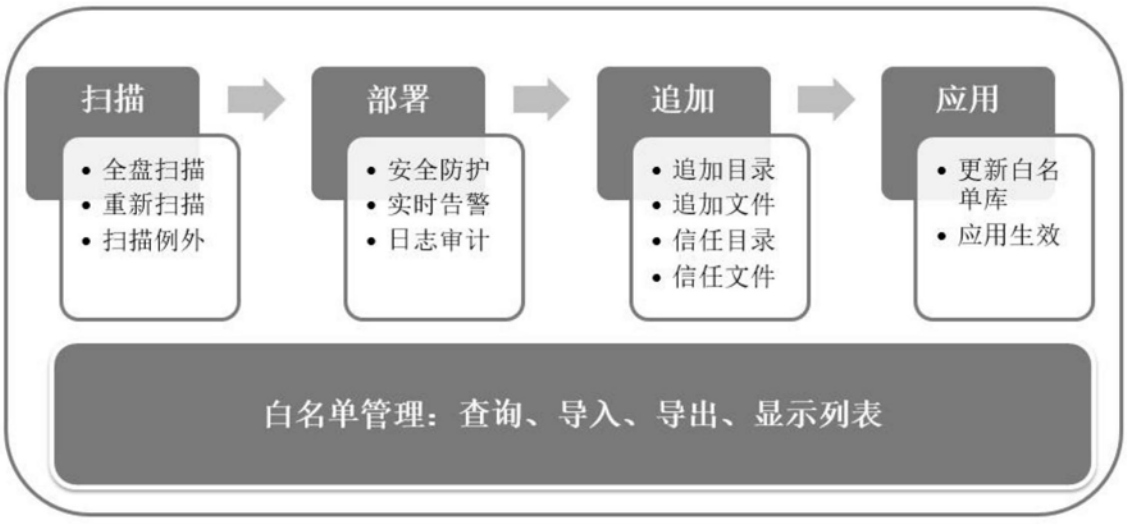

扫描
• 全盘扫描
• 重新扫描
• 扫描例外
部署
• 安全防护
• 实时告警
• 日志审计
追加
• 追加目录
• 追加文件
• 信任目录
• 信任文件
应用
• 更新白名单库
• 应用生效
白名单管理：查询、导入、导出、显示列表

图1b


“永恒之蓝”超前防御，防蓝屏
一键设置白名单，无需升级
网络防护，主机中毒后防止扩散
100%
入口拦截
运行拦截
扩散拦截
U盘管控，防止非授权外设引入病毒
三种模式一键切换，保障生产连续性
日志审计，溯源攻击主机和恶意程序
注册
授权
审计
关闭
告警
防护
白名单漏洞防御日志
IP端口应用程序
溯源主机恶意软件

图1c

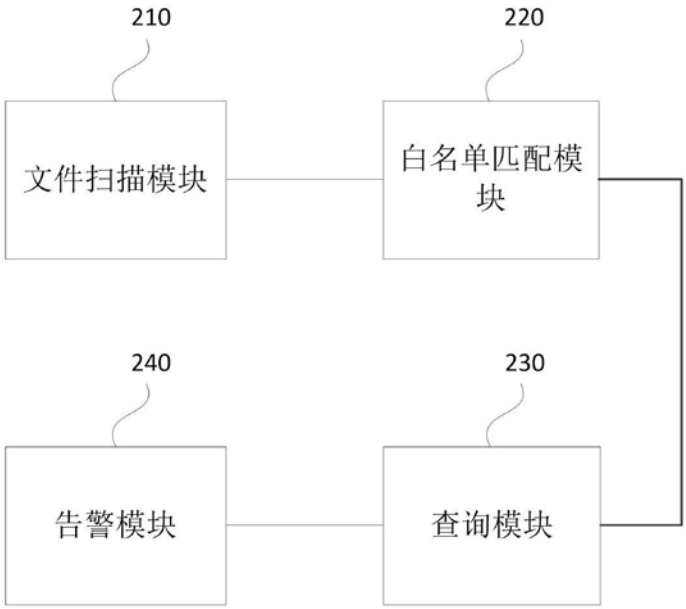

210
220
文件扫描模块
白名单匹配模块
240
230
告警模块
查询模块

图2

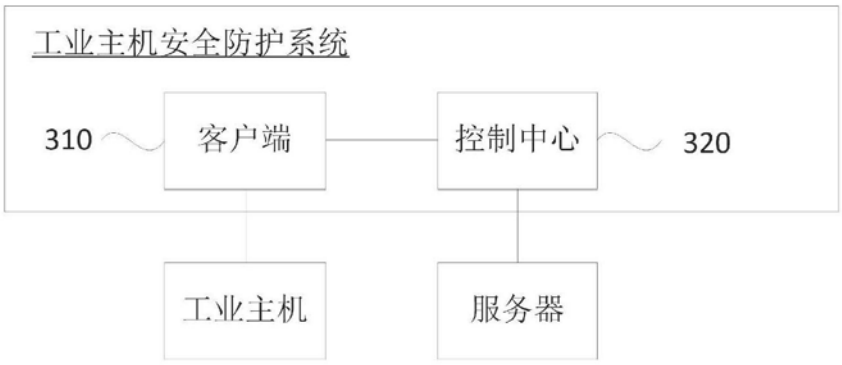

工业主机安全防护系统
310
客户端
控制中心
320
工业主机
服务器

图3a

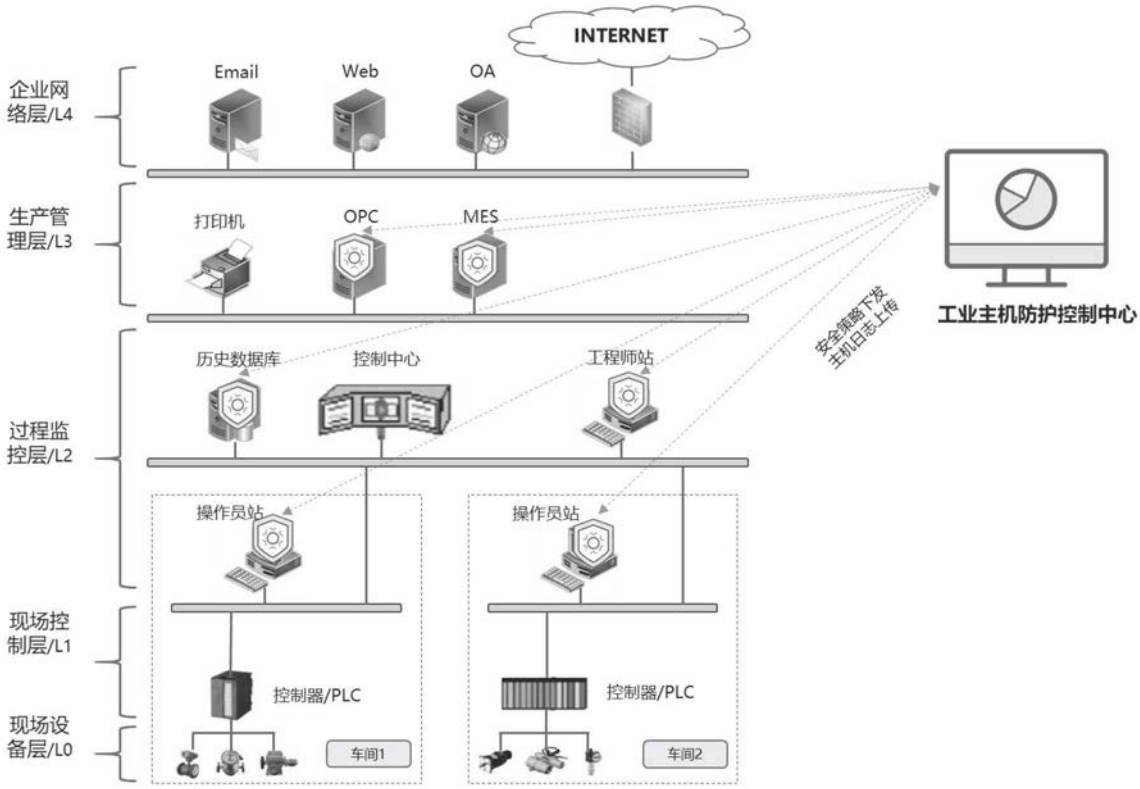

INTERNET
企业网络层/L4
Email
Web
OA
生产管理层/L3
打印机
OPC
MES
过程监控层/L2
历史数据库
控制中心
工程师站
现场控制层/L1
现场设备层/L0
操作员站
操作员站
控制器/PLC
控制器/PLC
车间1
车间2
安全策略下发
主机日志上传
工业主机防护控制中心

图3b