(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 107851157 A
(43)申请公布日 2018.03.27

(21)申请号 201680037858.2

(22)申请日 2016.05.25

(30)优先权数据
14/752901 2015.06.27 US

(85)PCT国际申请进入国家阶段日
2017.12.27

(86)PCT国际申请的申请数据
PCT/US2016/033977 2016.05.25

(87)PCT国际申请的公布数据
WO2017/003587 EN 2017.01.05

(71)申请人 迈可菲有限责任公司
地址 美国加利福尼亚州

(72)发明人 J.L.爱德华兹 J.R.斯普尔洛克

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张凌苗 陈岚

(51)Int.Cl.
G06F 21/56(2006.01)
G06F 21/57(2006.01)
H04L 29/06(2006.01)

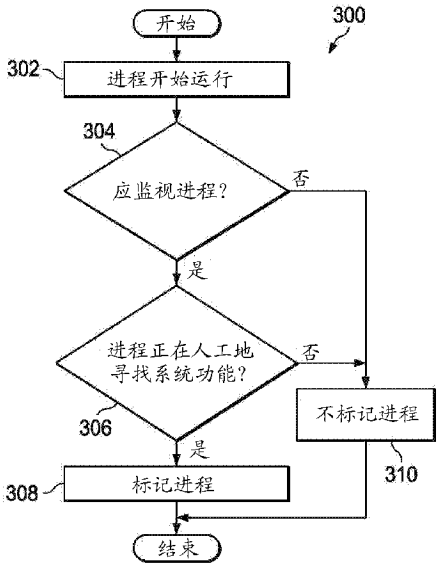
权利要求书2页 说明书9页 附图7页

(54)发明名称

恶意软件的检测

(57)摘要

在本文中描述的特定实施例提供了一种电子设备，所述电子设备可以被配置成监视进程、确定进程是否正在解析以寻找一个或多个系统功能、以及如果进程正在解析以寻找一个或多个系统系统功能则标记进程。在示例中，如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则可以确定进程正在解析以寻找一个或多个系统功能。在另一个示例中，如果进程调用GetProcAddress，则可以确定进程正在解析以寻找一个或多个系统功能。



CN 107851157 A

1.至少一种机器可读介质，其包括一个或多个指令，当由至少一个处理器执行所述一个或多个指令时，使得至少一个处理器：

监视进程；

确定进程是否正在解析以寻找一个或多个系统功能；以及

如果进程正在解析以寻找一个或多个系统功能，则标记进程。

2.如权利要求1所述的至少一种机器可读介质，其中，如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

3.如权利要求1和2中的任一项所述的至少一种机器可读介质，其中，如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

4.如权利要求1-3中的任一项所述的至少一种机器可读介质，其中，进程包括壳代码。

5.如权利要求1-4中的任一项所述的至少一种机器可读介质，进一步包括一个或多个指令，当由至少一个处理器执行所述一个或多个指令时，进一步使得至少一种机器可读介质：

针对恶意软件分析进程。

6.如权利要求1-5中的任一项所述的至少一种机器可读介质，进一步包括一个或多个指令，当由至少一个处理器执行所述一个或多个指令时，进一步使得至少一种机器可读介质：

如果在白名单中找到进程，则移除标记。

7.一种装置，其包括：

系统进程监视模块，其中所述系统进程监视模块被配置成：

监视进程；

确定进程是否正在解析以寻找一个或多个系统功能；以及

如果进程正在解析以寻找一个或多个系统功能，则标记进程。

8.如权利要求7所述的装置，其中，如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

9.如权利要求7和8中的任一项所述的装置，其中，如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

10.如权利要求7-9中的任一项所述的装置，其中，进程包括壳代码。

11.如权利要求7-10中的任一项所述的装置，其中，系统进程监视模块被进一步配置成：

针对恶意软件分析进程。

12.如权利要求7-11中的任一项所述的装置，其中，系统进程监视模块被进一步配置成：

如果在白名单中找到进程，则移除标记。

13.一种方法，其包括：

监视进程；

确定进程是否正在解析以寻找一个或多个系统功能；以及

如果进程正在解析以寻找一个或多个系统功能，则标记进程。

14.如权利要求13所述的方法，其中，如果进程解析可移植的可执行的头部以找到和解

释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

15.如权利要求13和14中的任一项所述的方法，其中，如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

16.如权利要求13-15中的任一项所述的方法，其中，进程包括壳代码。

17.如权利要求13-16中的任一项所述的方法，进一步包括：

针对恶意软件分析进程。

18.一种用于检测恶意软件的系统，所述系统包括：

系统进程监视模块，其中，所述系统进程监视模块被配置用于：

监视进程；

确定进程是否正在解析以寻找一个或多个系统功能；以及

如果进程正在解析以寻找一个或多个系统功能，则标记进程。

19.如权利要求18所述的系统，其中，如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

20.如权利要求18和19中的任一项所述的系统，其中，如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

恶意软件的检测

[0001] 相关申请的交叉引用

本申请要求题为“Detection of malware”的、2015年6月27日提交的美国非临时(实用新型)专利申请No. 14/752,901的权益和优先权,通过引用将其全文并入本文中。

技术领域

[0002] 本公开一般地涉及信息安全的领域,并且更特别地涉及恶意软件的检测。

背景技术

[0003] 在如今的社会中,网络安全的领域已经变得日益重要。因特网已经使能遍及世界的不同的计算机网络的互相连接。特别地,因特网提供了用于在经由各种类型的客户端设备连接到不同的计算机网络的不同的用户之间交换数据的介质。虽然因特网的使用已经改变了商业和个人通信,但是其也被用作了用于恶意操作者得到对计算机和计算机网络的未授权的访问以及用于敏感信息的有意的或无意的公开的媒介。

[0004] 感染主机计算机的恶意的软件(“恶意软件”)可能能够执行任何数量的恶意动作,诸如从与主机计算机相关联的商业或个体窃取敏感信息、向其他主机计算机传播和/或协助分布式服务拒绝攻击、从主机计算机发出垃圾邮件或恶意电子邮件等。因此,对于保护计算机和计算机网络免受恶意的软件和设备的恶意的和无意的利用而言,留下了重大的管理挑战。

附图说明

[0005] 为了提供对本公开以及其特征和优点的更完整的理解,结合附图,做出对以下描述的参考,其中相同的参考标号表示相同的部分,在其中:

图1是根据本公开的实施例的用于恶意软件的检测的通信系统的简化的框图;

图2是根据本公开的实施例的用于恶意软件的检测的通信系统的一部分的简化的框图;

图3是图示了根据实施例的可以与通信系统相关联的潜在操作的简化的流程图;

图4是图示了根据实施例的可以与通信系统相关联的潜在操作的简化的流程图;

图5是图示了根据实施例的以点对点配置来布置的示例计算系统的框图;

图6是与本公开的示例ARM生态系统片上系统(SOC)相关联的简化的框图;以及

图7是图示了根据实施例的示例处理器核心的框图。

[0006] 附图的图不一定按比例绘制,因为在不脱离本公开的范围的情况下,它们的尺寸可以是相当地不同的。

具体实施方式

[0007] 示例实施例

图1是根据本公开的实施例的用于恶意软件的检测的通信系统100的简化的框图。如在

图1中图示的那样，通信系统100的实施例可以包括电子设备102、云服务104和服务器106。电子设备102可以包括操作系统(OS)110、存储器112、处理器114、管理程序116、安全模块118和至少一个应用120。OS 110可以包括OS功能122和OS变量124。存储器112可以包括共享库126。安全模块118可以包括系统进程监视模块128、白名单130和黑名单132。云服务104和服务器106的每个可以包括网络安全模块134。网络安全模块124可以包括白名单130和黑名单132。电子设备102、云服务104和服务器106可以使用网络108通信。在示例中，恶意设备136可能尝试使用网络108或一些其他方式(例如，物理连接)来用恶意代码138感染电子设备102。

[0008] 在示例实施例中，通信系统100可以被配置成监视进程的线程并且确定线程是否正在尝试查找进程应当已经知道的功能。通常，是合法软件或合法应用的一部分的代码不需要寻找公共功能以与操作系统交互，因为在发布的库中公共功能是可用的，并且相对导出库链接公共功能，并且动态链接库(DLL)加载器可以自动地解析地址。然而，恶意代码常常不知道各种功能调用的位置，并且在恶意代码可以执行之前恶意代码必须首先找到功能。通过将涉及系统功能的某些文件和区标记为不可读，系统可以分析什么正在读文件和区以定位系统功能并且做出代码是可信任的还是恶意的确定。

[0009] 通过采用任何合适的连接(有线或无线)的一个或多个接口可以将图1的元件耦合到彼此，这为网络(例如，网络108)通信提供了可行的路径。另外，可以基于特定配置需要组合图1的这些元件中的任何一个或多个或将图1的这些元件中的任何一个或多个从架构移除。通信系统100可以包括有用于网络中的分组的传输或接收的传输控制协议/因特网协议(TCP/IP)通信能力的配置。在适当的情况下并且基于特定需要，通信系统100还可以结合用户数据报协议/IP(UDP/IP)或任何其他合适的协议操作。

[0010] 为了说明通信系统100的某些示例技术的目的，重要的是理解可能正在遍历网络环境的通信。以下基础的信息可以被视为基础，根据其可以正确地解释本公开。

[0011] 恶意代码138可以是感染主机计算机(例如，电子设备102)以执行任何数量的恶意动作的恶意软件或恶意的软件，所述恶意动作诸如从与主机计算机相关联的商业或个体窃取敏感信息、传播到其他主机计算机和/或协助分布式服务拒绝攻击、从主机计算机发出垃圾邮件或恶意电子邮件等。一个公共的恶意软件特征是使用壳代码(shellcode)来利用在机器上运行的软件中的弱点。壳代码是用作软件弱点的利用中的净荷的代码的片。将其称为“壳代码”，因为其通常开始攻击者可以从其控制损害的机器的命令壳。在壳代码可以有效地感染机器之前，其需要找到OS功能或例程(例如，LoadLibrary、CreateFile等)以执行其净荷。为了找到OS例程，壳代码可以调用GetProcAddress或解析可移植的可执行的(PE)头部(portable executable header)以找到和解释DLL的导入和导出表。需要的是提供检测壳代码和标识恶意活动的系统和方法的安全技术方案。

[0012] 如在图1中概述的那样，用于恶意软件的检测的通信系统可以解决这些问题(以及其他问题)。通信系统100可以被配置成使用基于管理程序(例如，管理程序116)存储器的监视来在代码正在执行和访问数据时监视代码。例如，可以在数据结构上使用存储器读监视，恶意软件需要读取所述数据结构以便找到在其可以执行之前恶意软件可能需要的OS功能。当DLL导出一些功能到进程时，可以找到关于功能的开始的位置的信息以及被存储在表(例如，导出表)中的功能的名称，在DLL的开始处由公知的结构指向所述表。通信系统100可以

被配置成使用管理程序来使那些结构和表不可读，使得当进程读它们时，系统可以分析进程并且查看访问的模式和正在访问结构或表的代码。根据被访问的模式和字节，系统可以确定正在寻找什么功能并且可以确定代码是否是找到功能的恶意尝试。

[0013] 例如，系统进程监视模块128可以被配置成分析正在查找OS功能(例如，OS功能122)和OS变量(例如，OS变量124)的代码(例如，来自应用120)。在系统的共享库(例如，共享库126)中，使得仅指示去哪里找到OS功能或OS变量的结构不可读，因为在使得代码不可读中没有益处。可以被保护和标记为不可读取的存储器的区域可以包括导入和导出表、DLL、PE文件等。

[0014] 转向图1的基础设施，示出了根据示例实施例的通信系统100。通常，可以在任何类型的网络或网络的拓扑中实现通信系统100。网络108表示用于接收和传输通过通信网络100传播的信息的分组的互相连接的通信路径的一系列点或节点。网络108提供节点之间的通信接口，并且可以被配置为任何局域网(LAN)、虚拟局域网(VLAN)、广域网(WAN)、无线局域网(WLAN)、城域网(MAN)、内联网、外联网、虚拟专用网(VPN)以及促进网络环境中的通信的任何其他适当的架构或系统、或其任何合适的组合，包括有线和/或无线通信。

[0015] 在通信系统100中，可以根据任何合适的通信消息收发协议来发送和接收包括分组、帧、信号、数据等的网络流量。合适的通信消息收发协议可以包括多层方案，诸如开放系统互连(OSI)模型或其任何衍生物或变型(例如，传输控制协议/因特网协议(TCP/IP)、用户数据报协议/IP(UDP/IP))。另外，可以在通信系统100中提供通过蜂窝网络的无线电信号通信。可以提供合适的接口和基础设施以使能与蜂窝网络的通信。

[0016] 如在本文中使用的术语“分组”指代可以在分组交换网络上的源节点和目的地节点之间路由的数据的单元。分组包括源网络地址和目的地网络地址。这些网络地址可以是TCP/IP消息收发协议中的因特网协议(IP)地址。如在本文中使用的术语“数据”指代任何类型的二进制的、数值的、语音、视频、文本的或脚本数据、或任何类型的源代码或目标代码、或可以从电子设备和/或网络中的一个点传送到另一个点的任何适当的格式的任何其他合适的信息。另外，消息、请求、响应和询问是网络流量的形式，并且因此可以包括分组、帧、信号、数据等。

[0017] 在示例实现中，电子设备102、云服务104和服务器106是网络元件，其意味着包含网络设备、服务器、路由器、交换机、网关、桥、负载平衡器、处理器、模块、或任何其他合适的设备、部件、元件、或可操作以在网络环境中交换信息的物体。网络元件可以包括促进其操作的任何合适的硬件、软件、部件、模块或物体以及用于在网络环境中接收、传输和/或否则传送数据或信息的合适的接口。这可以包括虑及数据或信息的有效的交换的适当的算法和通信协议。

[0018] 关于与通信系统100相关联的内部结构，电子设备102、云服务104和服务器106中的每个可以包括用于存储要在本文中概述的操作中使用的信息的存储器元件。电子设备102、云服务104和服务器106中的每个可以将信息保持在任何合适的存储器元件(例如，随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)、专用集成电路(ASIC)等)、软件、硬件、固件中，或在适当的情况下并且基于特定需要保持在其他合适的部件、设备、元件或物体中。应当将在本文中讨论的存储器条目中的任何存储器条目解释为被包含在广义术语‘存储器元件中。而且，可以在任何数据库、寄存

器、队列、表、高速缓存、控制列表或其他存储结构中提供在通信系统100中被使用、跟踪、发送或接收的信息，在任何合适的时间帧处可以引用其中的所有。可以在如在本文中使用的广义术语‘存储器元件’中包括任何此类存储选择。

[0019] 在某些示例实现中，可以通过编码在一个或多个有形介质(例如，要被处理器或其他类似的机器等执行的在ASIC中提供的嵌入式逻辑、数字信号处理器(DSP)指令、软件(潜在地包括目标代码和源代码))中的逻辑来实现在本文中概述的功能，其可以包括非暂态计算机可读介质。在这些实例中的一些中，存储器元件可以存储用于在本文中描述的操作的数据。这包括能够存储被执行以执行在本文中描述的活动的软件、逻辑、代码或处理器指令的存储器元件。

[0020] 在示例实现中，通信系统100的网络元件，诸如电子设备102、云服务104和服务器106可以包括软件模块(例如，安全模块118、系统进程监视模块128和网络安全模块134)以实现或以培养(foster)如在本文中概述的操作。可以以任何适当的方式合适地组合这些模块，其可以基于特定配置和/或供应需求。在示例实施例中，此类操作可以由硬件执行、在这些元件外部实现、或包括在一些其他网络设备中以实现期望的功能。此外，可以将模块实现为软件、硬件、固件或其任何合适的组合。这些元件还可以包括可以与其他网络元件协调以便实现如在本文中概述的操作的软件(或往复式(reciprocating)软件)。

[0021] 另外，电子设备102、云服务104和服务器106中的每个可以包括可以执行软件或算法以执行如在本文中讨论的活动的处理器。处理器可以执行与数据相关联的任何类型的指令以实现在本文中详述的操作。在一个示例中，处理器可以将元件或物品(例如，数据)从一个状态或事物变换成另一个状态或事物。在另一个示例中，可以用固定的逻辑或可编程逻辑(例如，由处理器执行的软件/计算机指令)来实现在本文中概述的活动，并且在本文中标识的元件可以是包括数字逻辑、软件、代码、电子指令或其任何合适的组合的一些类型的可编程处理器、可编程数字逻辑(例如，现场可编程门阵列(FPGA)、EPROM、EEPROM)或ASIC。应将在本文中描述的潜在的处理元件、模块和机器中的任何处理元件、模块和机器解释为被包含在广义术语‘处理器’中。

[0022] 电子设备102可以是网络元件并且包括例如台式计算机、膝上型计算机、移动设备、个人数字助理、智能电话、平板或其他类似的设备。云服务104被配置成向电子设备102提供云服务。通常可以将云服务定义为作为服务通过诸如因特网之类的网络传递的计算资源的使用。通常，在云基础设施中提供计算、存储和网络资源，有效地将工作负载从本地网络改变到云网络。服务器106可以是诸如服务器或虚拟服务器之类的网络元件并且可以与希望经由一些网络(例如，网络108)在通信网络100中发起通信的客户端、客户、端点或最终用户相关联。术语‘服务器’包括用于服务客户端的请求和/或在通信系统100中代表客户端执行一些计算任务的设备。虽然在图1中将安全模块118表示为被定位在电子设备102中，但是这仅是用于说明性的目的。可以以任何合适的配置来组合或分离安全模块118。此外，安全模块118可以与诸如是云服务104或服务器106之类的电子设备102可访问的另一个网络集成，或安全模块118可以分布在诸如是云服务104或服务器106之类的电子设备102可访问的另一个网络中。

[0023] 转向图2，图2是用于恶意软件的检测的通信系统100的一部分的简化的框图。如在图2中图示的那样，电子设备102可以包括OS 110、存储器112、安全模块118和应用120。OS

110可以包括OS功能122和OS变量124。存储器112可以包括DLL 140、导入和导出表142、一个或多个PE文件144和GetProcAddress 148。安全模块118可以包括系统进程监视模块128、白名单130和黑名单132。应用120可以包括壳代码146。每个PE文件144可以包括头部150。GetProcAddress 148可以从DLL 140取回导出的功能或变量的地址。

[0024] 如果应用是恶意的或者包括恶意的代码138，则在壳代码146可以有效地感染机器之前，其需要找到操作系统功能或例程(例如，示例LoadLibrary、CreateFile等)以执行其净荷。为了找到OS例程，壳代码可以调用GetProcAddress 148或解析以从PE文件144寻找PE头部以找到并且解释DLL的或导入和导出表142。例如，当DLL 140导出一些功能到进程时，可以找到关于功能的开始的信息以及功能的名称。可以将功能的名称存储在导入和导出表142中，在DLL 140的开始处由公知的结构指向导入和导出表142。白名单122可以包括已知干净的或信任的应用、代码、串等的条目，并且可以使用白名单122来减少假阳性(false positive)。黑名单124可以包括已知恶意的或不信任的应用、代码、串等的条目。

[0025] 转向图3，图3是图示了根据实施例的可以与恶意软件的检测相关联的流300的可能的操作的示例流程图。在302处，进程开始运行。在304处，系统确定是否应监视进程。如果不应监视进程，那么不标记进程，如在310中那样。例如，可以在白名单130中找到进程并且可以将进程分类为信任的。此外，进程可以是通常不针对恶意软件被监视的进程。如果应监视进程(例如，应用是未知的，或者在黑名单132中找到该应用)，那么系统确定进程是否正在人工地寻找(例如，解析以寻找)系统功能，如在306中那样。如果进程未正在人工地寻找(例如，解析以寻找)系统功能，那么不标记进程，如在310中那样。如果进程正在人工地寻找(例如，解析以寻找)系统功能，那么标记进程，如在308中那样。通过标记进程，可以由安全模块118针对恶意软件分析进程或者将进程发送到网络元件用于进一步分析(例如，通过网络安全模块134)。

[0026] 转向图4，图4是图示了根据实施例的可以与恶意软件的检测相关联的流程400的可能的操作的示例流程图。在402处，应用开始执行。在404处，应用开始解析PE文件以人工地(例如，解析以)找到和解释DLL表。在406处，标记应用用于进一步分析以确定应用是否是恶意的。例如，可以由安全模块118针对恶意软件分析进程或者将进程发送到网络元件用于进一步分析(例如，通过网络安全模块134)。

[0027] 图5图示了根据实施例的以点对点(PtP)配置来布置的计算系统500。特别地，图5示出了其中通过多个点对点接口将处理器、存储器和输入/输出设备互相连接的系统。通常，可以以与计算系统500相同或相似的方式配置通信系统100的网络元件中的一个或多个。

[0028] 如在图5中图示的那样，系统500可以包括若干处理器，为了清楚，示出了其中的仅两个，处理器570和580。虽然示出了两个处理器570和580，但是要理解，系统500的实施例还可以包括仅一个此类处理器。处理器570和580每个可以包括核心的集合(即，处理器核心574A和574B以及处理器核心584A和584B)以执行程序的多个线程。核心可以被配置成以与以上参考图1-5讨论的类似的方式执行指令代码。每个处理器570、580可以包括至少一个共享高速缓存571、581。共享高速缓存571、581可以存储由诸如处理器核心574和584之类的处理器570、580中的一个或多个部件利用的数据(例如，指令)。

[0029] 处理器570和580每个还可以包括集成的存储器控制器逻辑(MC)572和582以与存

储器元件532和534通信。存储器元件532和/或534可以存储由处理器570和580使用的各种数据。在替代实施例中，存储器控制器逻辑572和582可以是与处理器570和580分离的谨慎的(discreet)逻辑。

[0030] 处理器570和580可以是任何类型的处理器并且可以分别使用点对点接口电路578和588经由点对点(PtP)接口550交换数据。处理器570和580每个可以使用点对点接口电路576、586、594和598经由个别点对点接口552和554与芯片集590交换数据。芯片集590还可以使用接口电路592经由高性能图形接口539与高性能图形电路538交互数据，所述接口电路592可以是PtP接口电路。在替代实施例中，可以将在图5中图示的PtP链接中的任何或所有链接实现为多点(multi-drop)总线而不是PtP链接。

[0031] 芯片集590可以经由接口电路596与总线520通信。总线520可以具有通过其通信的一个或多个设备，诸如总线桥518和/或I/O设备516。经由总线510，总线桥518可以与其他设备通信，所述其他设备诸如键盘/鼠标512(或诸如触摸屏、轨迹球等的其他输入设备)、通信设备526(诸如调制解调器、网络接口设备或可以通过计算机网络560通信的其他类型的通信设备)、音频I/O设备514和/或数据存储设备528。数据存储设备528可以存储可以由处理器570和/或580执行的代码530。在替代实施例中，可以用一个或多个PtP链接来实现总线架构的任何部分。

[0032] 在图5中描绘的计算机系统是计算系统的实施例的示意性图示，可以利用所述计算系统来实现在本文中讨论的各种实施例。将会理解，可以将在图5中描绘的系统的各种部件组合在片上系统(SoC)架构中或者以任何其他合适的配置来组合在图5中描绘的系统的各种部件。例如，可以将在本文中公开的实施例并入包括移动设备的系统中，所述移动设备诸如智能蜂窝电话、平板计算机、个人数字助理、便携式游戏设备等。将会理解，在至少一些实施例中，可以为这些移动设备提供SoC架构。

[0033] 转向图6，图6是与本公开的示例ARM生态系统SOC 600相关联的简化的框图。本公开的至少一个示例实现可以包括在本文中讨论的恶意软件特征的检测和ARM部件。例如，图6的示例可以与任何ARM核心(例如，A-7、A-15等)相关联。而且，架构可以是任何类型的平板、智能电话(包括Android®电话、iPhones®)、iPad®、Google Nexus®、Microsoft Surface®、个人计算机、服务器、视频处理部件、膝上型计算机(包括任何类型的笔记本)、Ultrabook™系统、任何类型的触摸使能的输入设备等的部分。

[0034] 在图6的该示例中，ARM生态系统SOC 600可以包括多个核心606-607、L2高速缓存控制608、总线接口单元609、L2高速缓存610、图形处理单元(GPU)615、互相连接602、视频编解码器620和液晶显示器(LCD)I/F 625，其可以与耦合到LCD的移动行业处理器接口(MIPI)/高清晰度多媒体接口(HDMI)链接相关联。

[0035] ARM生态系统SOC 600还可以包括订户身份模块(SIM)I/F 630、引导只读存储器(ROM)635、同步动态随机存取存储器(SDRAM)控制器640、闪存控制器645、串行外设接口(SPI)主机650、合适的功率控制655、动态RAM(DRAM)660和闪存665。此外，一个或多个示例实施例包括一个或多个通信能力、接口和特征，诸如Bluetooth™ 670、3G调制解调器675、全球定位系统(GPS)680和802.11 Wi-Fi 685的实例。

[0036] 在操作中，图6的示例可以提供处理能力连同相对低的功耗以使能各种类型的计算(例如，移动计算、高端数字家庭、服务器、无线基础设施等)。此外，此类架构可以使能任

何数量的软件应用(例如,Android®、Adobe® Flash® Player、Java 平台标准版(Java SE)、JavaFX、Linux、Microsoft Windows Embedded、Symbian和Ubuntu等)。在至少一个示例实施例中,核心处理器可以实现具有耦合的低延迟级别-2高速缓存的无序的超标量管线(superscalar pipeline)。

[0037] 图7图示了根据实施例的处理器核心700。处理器核心700可以是用于任何类型的处理器的核心,诸如微处理器、嵌入式处理器、数字信号处理器(DSP)、网络处理器或执行代码的其他设备。虽然在图7中图示了仅一个处理器核心700,但是处理器可以替代地包括在图7中图示的处理器核心700中的多于一个。例如,处理器核心700表示参考图5的处理器570和580示出和描述的处理器核心574a、574b、584a和584b的一个示例实施例。处理器核心700可以是单线程核心,或对于至少一个实施例而言,处理器核心700可以是多线程的,因为其可以每个核心包括多于一个硬件线程上下文(或"逻辑处理器")。

[0038] 图7还图示了根据实施例的耦合到处理器核心700的存储器702。存储器702可以是广泛种类的存储器(包括存储器层级的各种层)中的任何存储器,其对于本领域技术人员而言是已知的或否则是可用的。存储器702可以包括代码704,其可以是要被处理器核心700执行的一个或多个指令。处理器核心700可以遵循由代码704指示的指令的程序序列。每个指令进入前端逻辑706并且由一个或多个解码器708处理所述每个指令。解码器可以生成作为其输出的微操作,诸如预定义格式的固定宽度微操作,或者可以生成其他指令、微指令、或反映原始代码指令的控制信号。前端逻辑706还包括寄存器重新命名逻辑710和调度逻辑712,其通常分配资源和使对应于用于执行的指令的操作排队。

[0039] 处理器核心700还可以包括具有执行单元716-1到716-N的集合的执行逻辑714。一些实施例可以包括专用于具体功能或功能的集合的多个执行单元。其他实施例可以包括可以执行特定功能的仅一个执行单元或一个执行单元。执行逻辑714执行由代码指令指定的操作。

[0040] 在由代码指令指定的操作的执行完成之后,后端逻辑718可以引退(retire)代码704的指令。在一个实施例中,处理器核心700允许乱序执行但是要求指令的按顺序引退。引退逻辑720可以采取多种已知形式(例如,重新排序缓冲器或者诸如此类)。以该方式,在代码704的执行期间,至少根据由解码器生成的输出、由寄存器重新命名逻辑710利用的硬件寄存器和表以及由执行逻辑714修改的任何寄存器(未示出)来变换处理器核心700。

[0041] 虽然在图7中未图示,但是处理器可以包括在具有处理器核心700的芯片上的其他元件,参考图5在本文中示出了和描述了其中的至少一些。例如,如在图5中示出的那样,处理器可以包括存储器控制逻辑连同处理器核心700。处理器可以包括I/O控制逻辑和/或可以包括与存储器控制逻辑集成的I/O控制逻辑。

[0042] 注意,对于在本文中提供的示例,可以在二个、三个或更多个网络元件方面中描述交互。然而,为了清楚和仅示例的目的已经完成这一点。在某些情况中,通过仅参考有限的数量的网络元件来描述流程的给定集合的功能中的一个或多个可能更容易。应当理解,通信系统100和其教导是可容易扩展的并且可以适应大量的部件,以及更复杂的/精致的(sophisticated)布置和配置。因此,提供的示例不应限制通信系统100的范围或抑制其广泛的教导,因为其潜在地适用于大量的其他结构。

[0043] 注意到以下内容也是重要的:在在前的流程图(即,图3-5B)中的操作图示了可能

的相关的场景和模式中的仅一些，所述场景和模式可以由通信系统100执行或在通信系统100内执行。在适当的情况下，可以删除或移除这些操作中的一些，或在不脱离本公开的范围的情况下，可以相当大地修改或改变这些操作。此外，已经将多个这些操作描述为与一个或多个附加操作同时地或并行地执行。然而，可以相当大地变更这些操作的定时。已经提供在前的操作流程用于示例和讨论的目的。由通信系统100提供大量的灵活性，因为在不脱离本公开的教导的情况下，可以提供任何合适的布置、时间顺序(chronologies)、配置和定时机制。

[0044] 虽然已经参考特定的布置和配置详细地描述了本公开，但是在不脱离本公开的范围的情况下，可以显著地改变这些示例配置和布置。此外，基于特定的需要和实现，可以组合、分离、消除或添加某些部件。另外，虽然已经参考促进通信进程的特定元件和操作图示了通信系统100，但是可以由实现通信系统100的期望的功能的任何合适的架构、协议和/或进程来替代这些元件和操作。

[0045] 多个其他改变、代替、变型、变更和修改对本领域技术人员来说是可以被查明的，并且旨在本公开包含如落入所附权利要求书的范围内的所有此类改变、代替、变型、变更和修改。在解释附于本申请的权利要求中为了协助美国专利和商标局(USPTO)以及另外在本申请上发布的任何专利的读者，申请人希望指出，申请人：(a)不旨在所附权利要求中的任何权利要求援引35 U.S.C第112节的第六段(6)，因为其在本文的提交日期存在，除非在特定权利要求中具体地使用措辞“用于……的装置”或“用于……的步骤”；以及(b)不旨在通过说明书中的任何声明来以否则不在所附权利要求中反映的任何方式限制本公开。

[0046] 其他注意和示例

示例C1是至少一种机器可读介质，其具有一个或多个指令，当由至少一个处理器执行所述一个或多个指令时使得至少一个处理器监视进程、确定进程是否正在解析以寻找一个或多个系统功能、以及如果进程正在解析以寻找一个或多个系统功能则标记进程。

[0047] 在示例C2中，示例C1的主题可以可选地包括其中如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

[0048] 在示例C3中，示例C1-C2中的任何一个的主题可以可选地包括其中如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

[0049] 在示例C4中，示例C1-C3中的任何一个的主题可以可选地包括其中进程包括壳代码。

[0050] 在示例C5中，示例C1-C4中的任何一个的主题可以可选地包括其中一个或多个指令，当由至少一个处理器执行所述一个或多个指令时进一步使得至少一个处理器针对恶意软件分析进程。

[0051] 在示例C6中，示例C1-C5中的任何一个的主题可以可选地包括其中一个或多个指令，当由至少一个处理器执行所述一个或多个指令时进一步使得处理器如果在白名单中找到进程则移除标记。

[0052] 在示例A1中，一种装置可以包括系统进程监视模块。所述系统进程监视模块可以被配置成监视进程、确定进程是否正在解析以寻找一个或多个系统功能、以及如果进程正在解析以寻找一个或多个系统功能则标记进程。

[0053] 在示例A2中，示例A1的主题可以可选地包括其中如果进程解析可移植的可执行的

头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

[0054] 在示例A3中，示例A1-A2中的任何一个的主题可以可选地包括其中如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

[0055] 在示例A4中，示例A1-A3中的任何一个的主题可以可选地包括其中进程包括壳代码。

[0056] 在示例A5中，示例A1-A4中的任何一个的主题可以可选地包括其中系统进程监视模块被进一步配置成针对恶意软件分析进程。

[0057] 在示例A6中，示例A1-A5中的任何一个的主题可以可选地包括其中系统进程监视模块被进一步配置成如果在白名单中找到进程则移除标记。

[0058] 示例M1是一种方法，其包括监视进程、确定进程是否正在解析以寻找一个或多个系统功能、以及如果进程正在解析以寻找一个或多个系统功能则标记进程。

[0059] 在示例M2中，示例M1的主题可以可选地包括其中如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

[0060] 在示例M3中，示例M1-M2中的任何一个的主题可以可选地包括其中如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

[0061] 在示例M4中，示例M1-M3中的任何一个的主题可以可选地包括其中进程包括壳代码。

[0062] 在示例M5中，示例M1-M4中的任何一个的主题可以可选地包括针对恶意软件分析进程。

[0063] 示例S1是一种用于检测恶意软件的系统，所述系统可以包括系统进程监视模块。所述系统进程监视模块可以被配置用于监视进程、确定进程是否正在解析以寻找一个或多个系统功能、以及如果进程正在解析以寻找一个或多个系统功能则标记进程。

[0064] 在示例S2中，示例S1的主题可以可选地包括其中如果进程解析可移植的可执行的头部以找到和解释动态链接库表，则确定进程正在解析以寻找一个或多个系统功能。

[0065] 在示例S2中，示例S1和S2中的任何一个的主题可以包括其中如果进程调用GetProcAddress，则确定进程正在解析以寻找一个或多个系统功能。

[0066] 示例X1是一种机器可读存储介质，其包括机器可读指令以实现如在示例A1-A6或M1-M5中的任一个中的方法或实现如在示例A1-A6或M1-M5中的任一个中的装置。示例Y1是一种装置，所述装置包括用于示例方法M1-M5中的任何方法的执行的装置。在示例Y2中，示例Y1的主题可以可选地包括用于执行方法的装置，所述装置包括处理器和存储器。在示例Y3中，示例Y2的主题可以可选地包括存储器，所述存储器包括机器可读指令。

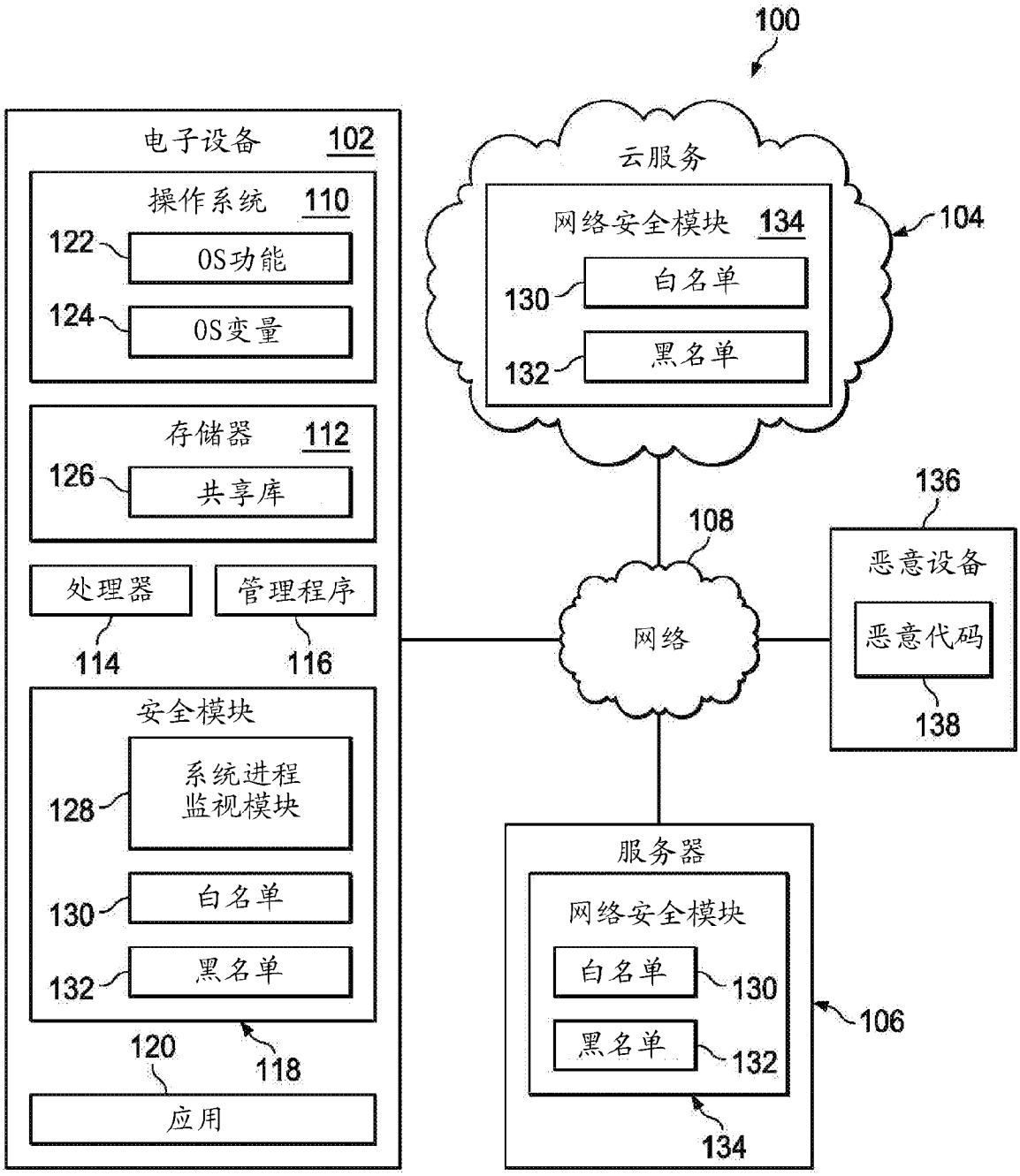

100
电子设备 102
操作系统 110
122
OS功能
124
OS变量
存储器 112
126
共享库
处理器
管理程序
114
116
安全模块
128
系统进程
监视模块
130
白名单
132
黑名单
120
118
应用
云服务
网络安全模块 134
104
130
白名单
132
黑名单
108
网络
136
恶意设备
恶意代码
138
服务器
网络安全模块
白名单
130
黑名单
132
106
134

图 1

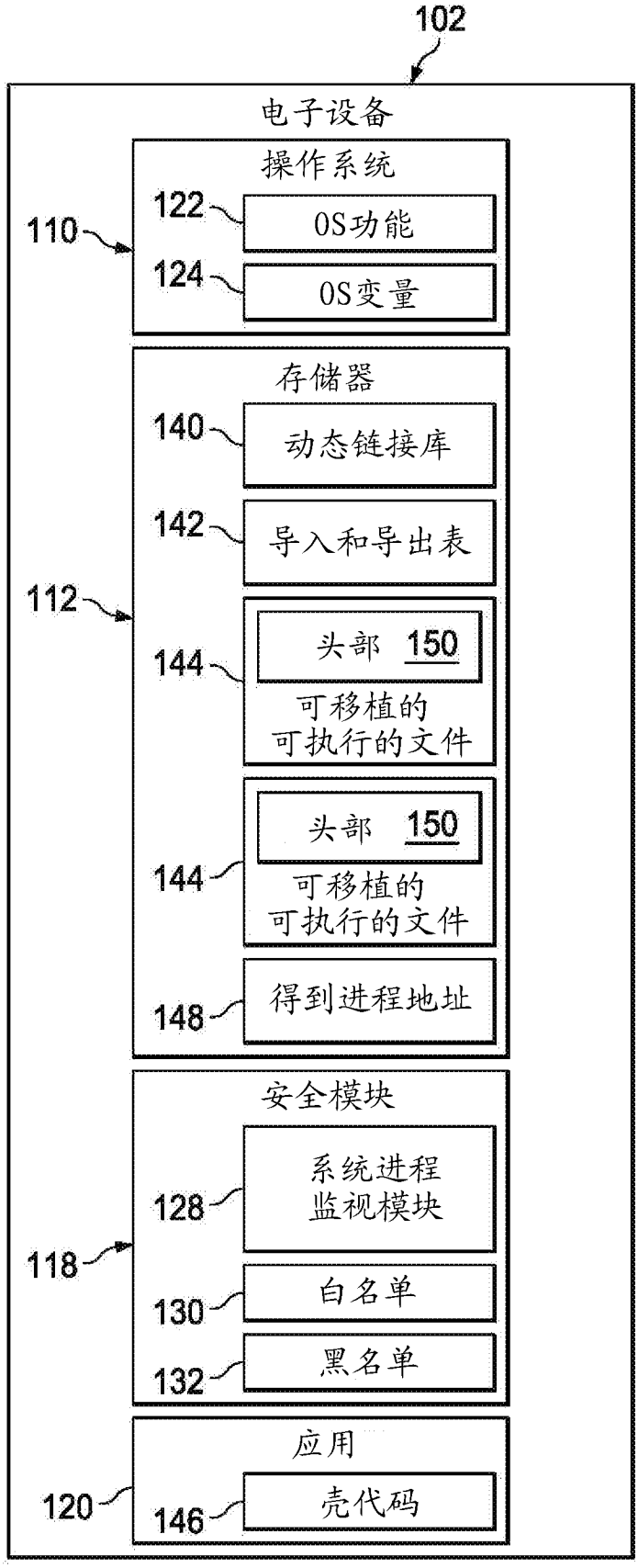

102
电子设备
操作系统
122
OS功能
110
124
OS变量
存储器
140
动态链接库
142
导入和导出表
112
头部 150
144
可移植的
可执行的文件
头部 150
144
可移植的
可执行的文件
148
得到进程地址
安全模块
系统进程
监视模块
128
118
130
白名单
132
黑名单
应用
120
146
壳代码

图 2

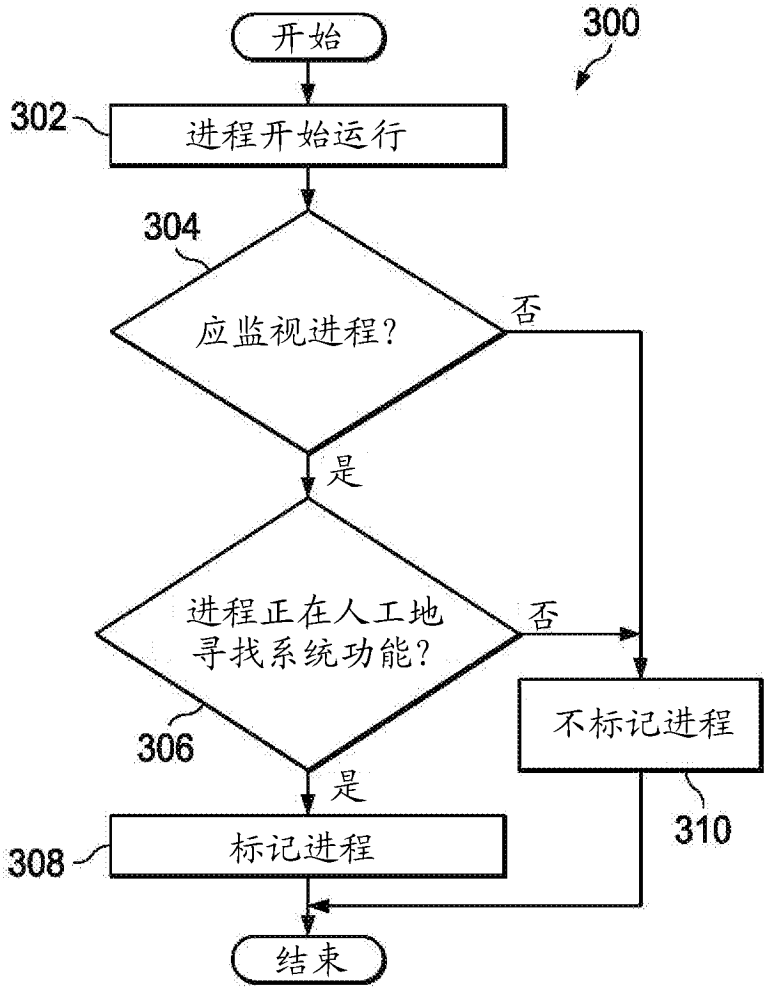

开始
300
302
进程开始运行
304
应监视进程?
否
是
进程正在人工地
寻找系统功能?
否
306
不标记进程
是
310
308
标记进程
结束

图 3

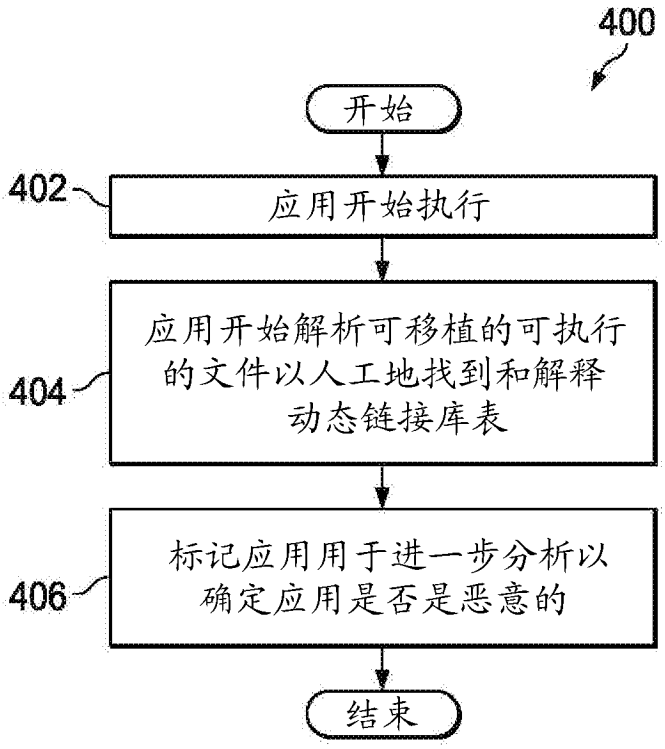

400
开始
402
应用开始执行
404
应用开始解析可移植的可执行的文件以人工地找到和解释动态链接库表
406
标记应用用于进一步分析以确定应用是否是恶意的
结束

图 4

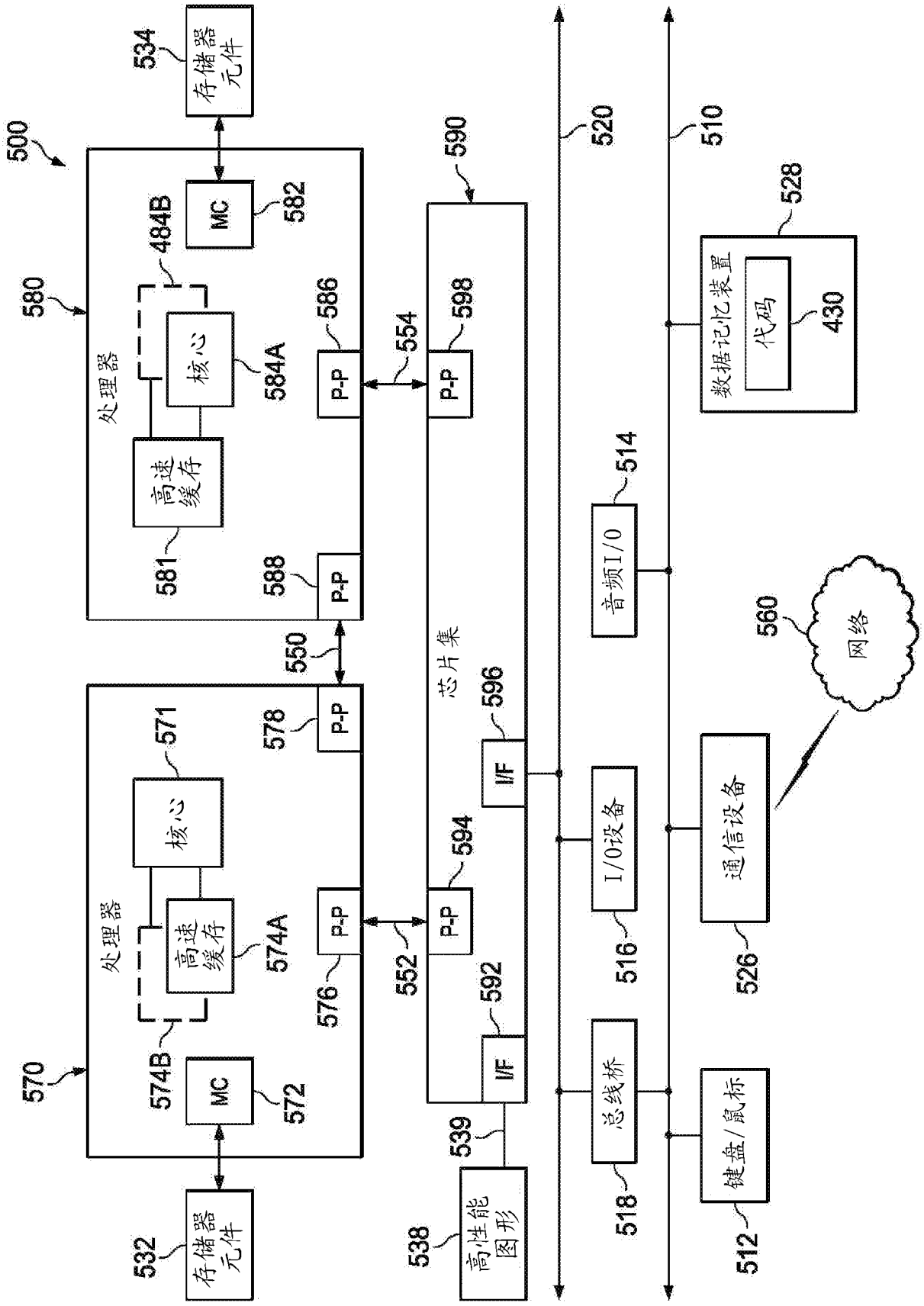

500
534
存储器元件
MC
582
484B
580
处理器
核心
584A
高速缓存
581
586
P-P
588
P-P
554
598
P-P
590
520
510
528
数据记忆装置
代码
430
514
音频I/O
550
578
P-P
596
I/F
芯片集
560
网络
571
核心
574A
高速缓存
处理器
576
P-P
552
P-P
594
592
I/F
516
I/O设备
526
通信设备
570
574B
MC
572
539
总线桥
518
键盘/鼠标
512
532
存储器元件
538
高性能图形

图 5

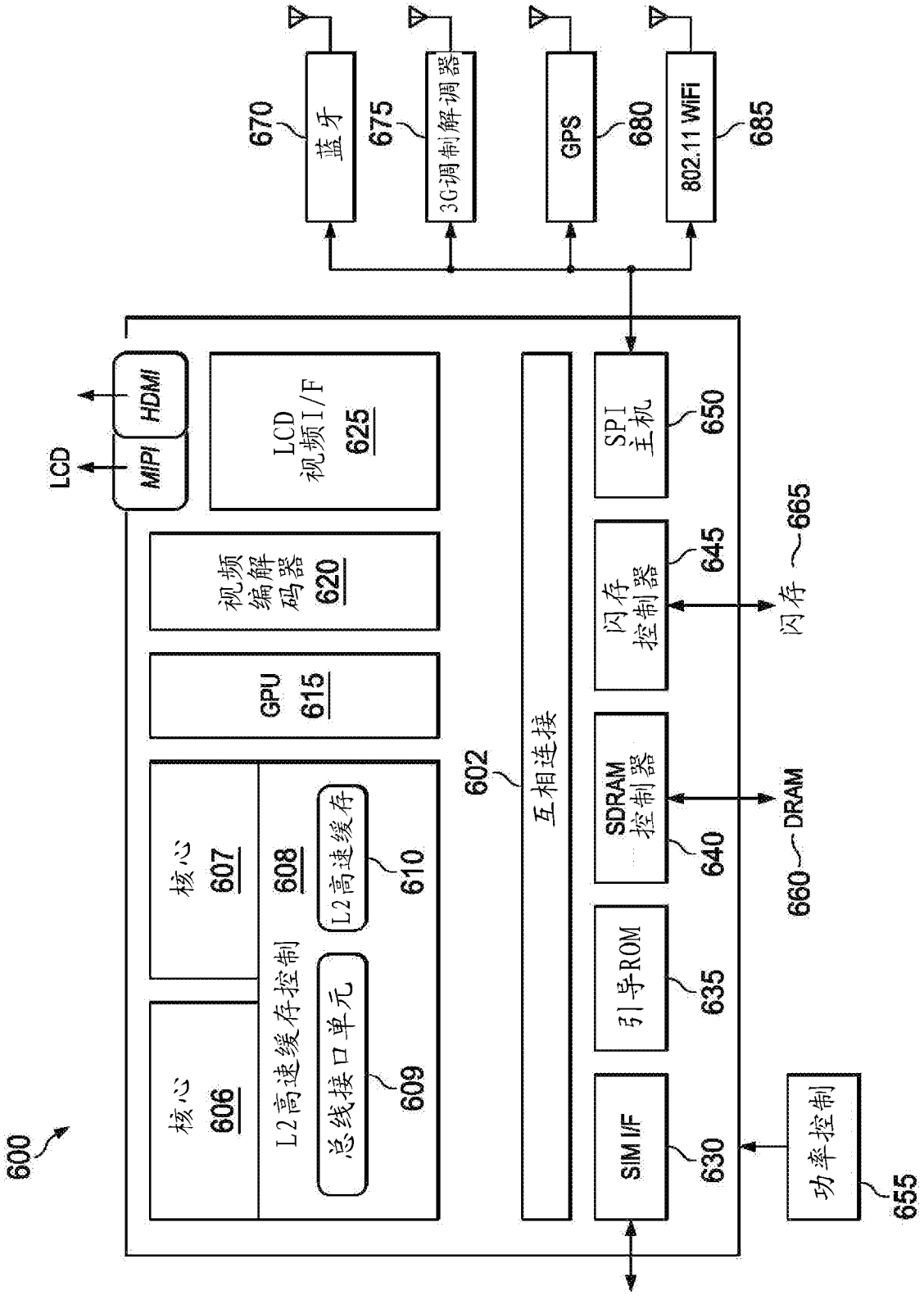

600
核心 606
L2高速缓存控制 608
总线接口单元 609
核心 607
L2高速缓存 610
GPU 615
视频编解码器 620
LCD 视频I/F 625
LCD
MIPI
HDMI
互相连接 602
SIM I/F 630
引导ROM 635
SDRAM 控制器 640
DRAM 660
闪存控制器 645
闪存 665
SPI 主机 650
功率控制 655
蓝牙 670
3G调制解调器 675
GPS 680
802.11 WiFi 685

图 6

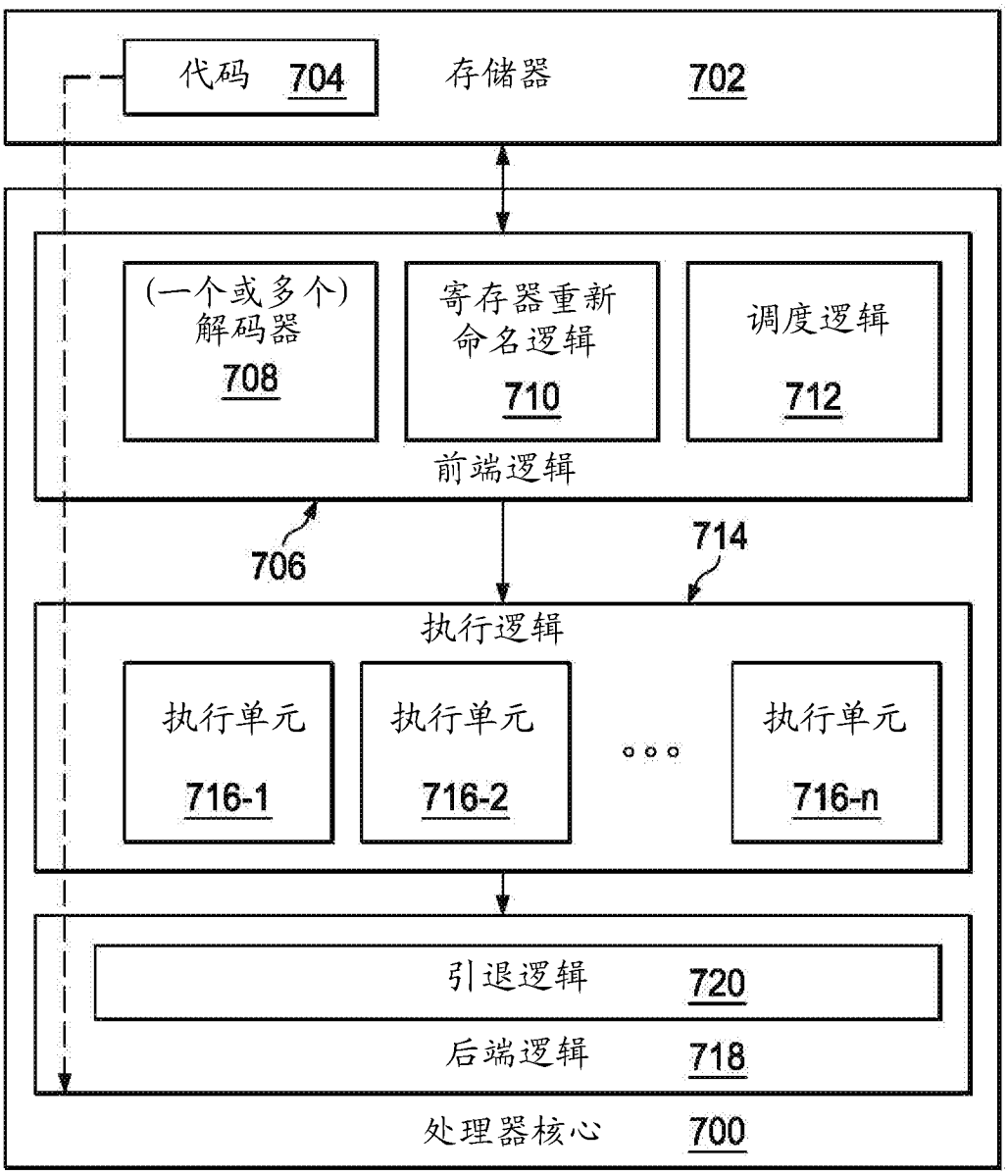

代码 704
存储器 702
(一个或多个)
解码器
708
寄存器重新
命名逻辑
710
调度逻辑
712
前端逻辑
706
714
执行逻辑
执行单元
716-1
执行单元
716-2
执行单元
716-n
引退逻辑 720
后端逻辑 718
处理器核心 700

图 7