(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102214134 B
(45)授权公告日 2015.08.12

(21)申请号 201010150156.X

(22)申请日 2010.04.12

(73)专利权人 腾讯科技（深圳）有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室

(72)发明人 谷沉沉 何健 吕静

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 谢安昆 宋志强

(51)Int.Cl.
G06F 11/28(2006.01)
G06F 21/56(2013.01)

(56)对比文件
CN 101226570 A,2008.07.23, 权利要求第 8 项,说明书第 5 页第 10-14 段,第 15 页第 6-7 段.
US 2004123137 A1,2004.06.24, 全文.
JP 2008546077 A,2008.12.18, 全文.
杨玉兰.《从系统进程的角度防治病毒》.《计算机安全》.2006,(第 7 期),
杨玉兰.《从系统进程的角度防治病毒》.《计算机安全》.2006,(第 7 期),

审查员 崔岩

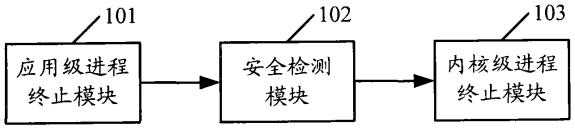
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种计算机进程终止系统和方法

(57)摘要

本发明提供了一种计算机进程终止系统和方法。该系统包括应用级进程终止模块、安全检测模块和内核级进程终止模块；所述应用级进程终止模块，用于对待终止的程序进程执行应用级模式终止操作；所述安全检测模块，用于对应用级进程终止模块终止失败的程序进程进行安全性检测；所述内核级进程终止模块，用于根据安全检测模块的安全性检测结果，判断是否对该终止失败的程序进程执行内核级模式强制终止操作。应用本发明可以保证计算机系统可以安全稳定地运行。



CN 102214134 B

1. 一种计算机进程终止系统，其特征在于，该系统包括应用级进程终止模块、安全检测模块和内核级进程终止模块；

所述应用级进程终止模块，用于对待终止的程序进程执行应用级模式终止操作；

所述安全检测模块，用于对应用级进程终止模块终止失败的程序进程进行安全性检测；

所述内核级进程终止模块，用于根据安全检测模块的安全性检测结果，判断是否对该终止失败的程序进程执行内核级模式强制终止操作；该系统进一步包括用户交互模块；

所述用户交互模块，接收用户选定待终止的程序进程的命令，向应用级进程终止模块发送对该待终止的程序进程执行终止操作的指示，以及输出或显示安全检测模块的检测结果，接收用户是否强制终止该程序进程的命令；

所述内核级进程终止模块，用于根据安全检测模块的安全性检测结果，以及用户交互模块接收的命令，判断是否对该终止失败的程序进程执行内核级模式强制终止操作；在有效终止内核级危险进程的同时，保证系统稳定运行；

该系统进一步包括进程详细信息配置文件；

所述进程详细信息配置文件，用于存储进程名称与进程描述信息、进程的安全级别以及建议操作的对应关系；所述安全级别包括关键进程、安全进程和可疑进程，对应的建议操作分别为不能终止关键进程、建议不终止安全进程和建议终止可疑进程；

所述安全检测模块，用于根据待终止的程序进程名称，依据进程详细信息配置文件中的对应关系，查找进程描述信息，并判断该待终止的程序进程的安全级别，以及对该待终止的程序进程的建议操作；

所述内核级进程终止模块，在安全检测模块的安全性检测结果是该待终止的程序进程是操作系统的关键进程时，内核级进程终止模块判定不对该待终止的程序进程执行终止操作，在安全检测模块的安全性检测结果是该待终止的程序进程不是操作系统的关键进程时，如果用户交互模块接收的命令是终止该程序进程则对该程序进程执行内核级模式强制终止操作，如果用户交互模块接收的命令是不终止该程序进程则不对该程序进程执行内核级模式强制终止操作。

2. 根据权利要求 1 所述的系统，其特征在于，该系统进一步包括进程枚举模块；

所述进程枚举模块，根据当前正在运行的进程状态形成进程列表，并根据进程终止情况更新进程列表。

3. 一种计算机进程终止方法，其特征在于，该方法包括：

接收用户选定待终止的程序进程的命令，利用应用级进程终止系统对待终止的程序进程执行应用级模式终止操作，在终止操作失败时，对该待终止的程序进程进行安全性检测，输出或显示检测结果，接收用户是否强制终止该程序进程的命令，根据安全性检测结果以及接收的命令，利用内核级进程终止模块对该程序进程执行内核级模式强制终止操作；在有效终止内核级危险进程的同时，保证系统稳定运行；

所述对该待终止的程序进程进行安全性检测包括：

检测待终止的程序进程的名称，依据预设的程序进程的名称、描述信息与安全级别的对应关系，判定待终止的程序进程的安全级别；

所述安全级别包括关键进程、安全进程和可疑进程，所述根据安全性检测结果以及接

收的命令，利用内核级进程终止模块对该程序进程执行终止操作包括：

检测出待终止的程序进程是关键进程时，判定不终止该关键进程；

检测出待终止的程序进程是安全进程或可疑进程时，如果用户命令指示终止该程序进程，则利用内核级进程终止模块对该程序进程执行内核级模式强制终止操作。

4. 根据权利要求 3 所述的方法，其特征在于，该方法进一步包括：

下载存储有程序进程的名称与进程描述信息、安全级别以及建议操作的对应关系的配置文件。

一种计算机进程终止系统和方法

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种计算机进程终止系统和方法。

背景技术

[0002] 目前广泛应用的 Intel X86 处理器是通过权限级别来进行访问控制的，其权限级别具体分为四级 :Ring0、Ring1、Ring2 和 Ring3。其中，Ring0 级拥有最高的访问权限，Ring3 级拥有最低的访问权限。例如 Windows 等操作系统只使用两个级别，即 Ring0 和 Ring3，Ring0 级存放操作系统数据，工作在 Ring0 级别的内核级程序拥有和操作系统同样的权限，可以访问所有级别的数据，执行所有级别的指令，而一般的应用级程序只能工作在 Ring3 级别，受到操作系统的限制，只能访问 Ring3 级别的数据，执行 Ring3 级别的指令。

[0003] 目前的进程终止系统有应用级进程终止系统和内核级进程终止系统。应用级进程终止系统可以终止工作在 Ring3 的应用级程序的进程，无法终止工作在 Ring0 级的内核级程序的进程。内核级进程终止系统可以终止内核级程序等任何级别的程序，但是如果结束了操作系统中不应被结束的进程，将导致整个操作系统瘫痪。

[0004] 由于内核级程序运行在操作系统信任的 Ring0 环境下，可以访问和控制所有的系统资源，目前病毒和木马等恶意程序多数都属于内核级程序，具有很强的破坏性和隐蔽性。

[0005] 结束恶意程序进程可以对计算机起到一定的保护作用，但是，由于多数恶意程序是内核级程序，因此采用应用级进程终止系统无法结束恶意程序进程，如果采用内核级进程终止系统，又容易由于用户结束了操作系统进程等非恶意程序进程，而导致系统瘫痪，不利于操作系统的稳定运行。

发明内容

[0006] 有鉴于此，本发明提供了一种计算机进程终止系统和方法，以保证计算机系统可以安全稳定地运行。

[0007] 一种计算机进程终止系统，该系统包括应用级进程终止模块、安全检测模块和内核级进程终止模块 ；

[0008] 所述应用级进程终止模块，用于对待终止的程序进程执行应用级模式终止操作 ；

[0009] 所述安全检测模块，用于对应用级进程终止模块终止失败的程序进程进行安全性检测 ；

[0010] 所述内核级进程终止模块，用于根据安全检测模块的安全性检测结果，判断是否对该终止失败的程序进程执行内核级模式强制终止操作。

[0011] 一种计算机进程终止方法，该方法包括 ：

[0012] 利用应用级进程终止系统对待终止的程序进程执行应用级模式终止操作，在终止操作失败时，对该待终止的程序进程进行安全性检测，根据安全性检测结果，利用内核级进程终止模块对该程序进程执行内核级模式强制终止操作。

[0013] 由上述技术方案可见，本发明首先利用应用级进程终止模块终止程序进程，对于

终止失败的程序进程进行安全性检测，然后根据安全性检测结果利用内核级进程终止模块终止不安全的进程，一方面对于病毒木马等工作在内核级的恶意程序，在应用级进程终止模块无法终止该恶意程序时，可以通过安全性检测得知其是恶意程序，从而利用内核级终止模块终止该恶意程序，保证了计算机系统的安全性，另外，对于应用级的程序进程，由于采用应用级进程终止模块可以即可终止，因此不需启动内核级进程终止模块，从而减少了利用内核级进程终止模块出错而引起的系统瘫痪等问题，提高了计算机系统的稳定性。

[0014] 另外需要说明的是，由于大部分恶意程序都是工作在内核级的，因此首先利用应用级进程终止模块结束待终止的程序进程，如果无法终止该程序进程，则也可判定该程序是恶意程序的概率较大，因此首先利用应用级进程终止模块终止程序进程所起的作用不仅是结束应用级的程序进程，其还起到了对待终止程序进行安全性检测的作用，在此基础上再利用安全检测模块对程序进行进行安全性检测，也可以提高安全性检测结果的准确性。

[0015] 总之，本发明涉及的计算机进程终止系统，提供了一种安全可靠的内核级进程终止模块，对系统进程达到完全控制，有效地强制终止内核级的危险进程，同时又能最大限度地保证操作系统运行的稳定性。

附图说明

[0016] 图 1 是本发明提供的计算机进程终止系统结构图。

[0017] 图 2 是本发明提供的计算机进程终止系统的优选实施例结构图。

[0018] 图 3 是本发明提供的计算机进程终止方法的流程图。

具体实施方式

[0019] 本发明提供了一种安全可靠的计算机进程终止系统，在终止进程时优先采用应用级模式终止进程，若遇到应用级模式无法终止的内核级进程，经过进程安全性检测和用户交互确认，可采用内核级模式强制终止进程，达到有效终止内核级危险进程的目的，同时又能最大限度地保证系统运行的稳定性。下面将详细描述该技术方案的装置实施例和方法实施例。

[0020] 图 1 是本发明提供的计算机进程终止系统结构图。

[0021] 如图 1 所示，该系统包括应用级进程终止模块 101、安全检测模块 102 和内核级进程终止模块 103。

[0022] 应用级进程终止模块 101，用于对待终止的程序进程执行应用级模式终止操作。

[0023] 安全检测模块 102，用于对应用级进程终止模块 101 终止失败的程序进程进行安全性检测。

[0024] 内核级进程终止模块 103，用于根据安全检测模块 102 的安全性检测结果，判断是否对该终止失败的程序进程执行内核级模式强制终止操作。

[0025] 该系统还可以进一步包括用户交互模块，用于接收用户选定待终止的程序进程的命令，向应用级进程终止模块发送对该待终止的程序进程执行终止操作的指示，以及输出或显示安全检测模块的检测结果，接收用户是否强制终止该程序进程的命令。

[0026] 相应地，所述内核级进程终止模块，用于根据安全检测模块的安全性检测结果，以及用户交互模块接收的命令，判断是否对该终止失败的程序进程执行内核级模式强制终止

操作。

[0027] 该系统还可以进一步包括进程详细信息配置文件，用于存储进程名称与进程描述信息、进程的安全级别以及建议操作的对应关系。

[0028] 相应地，所述安全检测模块，用于根据待终止的程序进程名称，依据进程详细信息配置文件中的对应关系，查找进程描述信息，并判断该待终止的程序进程的安全级别，以及对该待终止的程序进程的建议操作。

[0029] 具体地，所述进程详细信息配置文件中的安全级别包括关键进程、安全进程和可疑进程，对应的建议操作分别为不能终止关键进程、建议不终止安全进程和建议终止可疑进程。

[0030] 相应地，所述内核级进程终止模块，在安全检测模块的安全性检测结果是该待终止的程序进程是操作系统的关键进程时，内核级进程终止模块判定不对该待终止的程序进程执行终止操作，在安全检测模块的安全性检测结果是该待终止的程序进程不是操作系统的关键进程时，如果用户交互模块接收的命令是终止该程序进程则对该程序进程执行内核级模式强制终止操作，如果用户交互模块接收的命令是不终止该程序进程则不对该程序进程执行内核级模式强制终止操作。

[0031] 该系统还可以进一步包括进程枚举模块，用于根据当前正在运行的进程状态形成进程列表，并根据进程终止情况更新进程列表。

[0032] 图 2 是本发明提供的计算机进程终止系统的优选实施例结构图。

[0033] 如图 2 所示，在该优选实施例中，该计算机进程终止系统包括进程枚举模块 201、应用级进程终止模块 202、安全检测模块 203、进程详细信息配置文件存储模块 204、用户交互模块 205 和内核级进程终止模块 206。

[0034] 进程枚举模块 201，用于枚举当前正在运行的进程，形成进程列表，并根据进程终止情况更新进程列表。用户可在进程枚举模块 201 形成的进程列表中选定需要终止的进程。

[0035] 应用级进程终止模块 202，用于对用户选定需要终止的进程执行应用级模式终止操作，如果终止失败，则安全检测模块 203 对该终止失败的进程进行安全性检测，具体根据进程详细信息配置文件存储模块 204 中存储的配置文件以及该终止失败的进程名称查找该进程的描述信息，检测该进程的安全级别，并根据检测结果通过用户交互模块 205 输出该进程的相关信息，建议用户执行相应的操作，例如，如果检测结果是关键进程，则通过用户交互模块 205 提示用户该进程不允许被终止，如果检测结果是安全进程，则通过用户交互模块 205 提示用户建议不终止该进程，如果检测结果是可疑进程，则通过用户交互模块 205 提示用户建议终止该进程。内核级进程终止模块 206 根据安全检测模块 203 的检测结果和用户交互模块 205 接收的用户指令执行相应的操作，例如，在安全检测模块 203 的检测结果是关键进程时，无论用户交互模块 205 接收的用户命令是怎样的，内核级进程终止模块 206 都不终止该关键进程，在安全检测模块 203 的检测结果是安全进程或者可疑进程时，根据用户交互模块 205 接收的用户命令执行相应的操作。

[0036] 图 3 是本发明提供的计算机进程终止方法的流程图。

[0037] 如图 3 所示，该流程包括 ：

[0038] 步骤 301，根据用户在进程列表中选定的程序进程，采用应用级进程终止模块终止

程序进程。

[0039] 步骤 302，判断程序进程是否终止成功，如果是，执行步骤 310，如果否，执行步骤 303。

[0040] 步骤 303，检测该终止失败的进程的安全性。

[0041] 步骤 304，根据检测结果判断该进程是否是关键进程，如果是，执行步骤 305，如果否，执行步骤 306。

[0042] 步骤 305，提示用户该关键进程不能被终止，结束本流程。

[0043] 步骤 306，向用户提示该进程的信息以及建议的操作。

[0044] 本步骤中，如果安全检测结果为该进程是安全进程，则提示用户建议不终止该进程，如果安全检测结果为该进程是可疑进程，则提示用户建议终止该进程。

[0045] 步骤 307，判断用户是否允许采用强制方式终止该进程，如果是，执行步骤 308，否则结束本流程。

[0046] 步骤 308，采用内核级进程终止模块强制终止该进程。

[0047] 步骤 309，判断该进程是否终止成功，如果是，执行步骤 310，否则结束本流程。

[0048] 步骤 310，更新进程列表。

[0049] 可见，本发明的进程终止系统包含内核级进程终止方式，能够达到对进程的完全控制，有效终止对系统有害的内核级进程。

[0050] 在执行内核级进程终止模块强制终止进程前，本发明的进程终止系统优先采用应用级进程终止模块终止进程，并保护内核级的系统关键进程不被终止，最终再由用户选择是否执行进程的强制终止，在有效终止内核级危险进程的同时，能够最大限度地保证系统稳定运行。

[0051] 采用应用级进程终止模块终止进程失败后，再进行进程安全性检测，据此对用户操作进行提示，避免用户选择操作的盲目性。同时，终止应用级进程时由于不需要执行安全性检测而具有较高的执行效率。

[0052] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

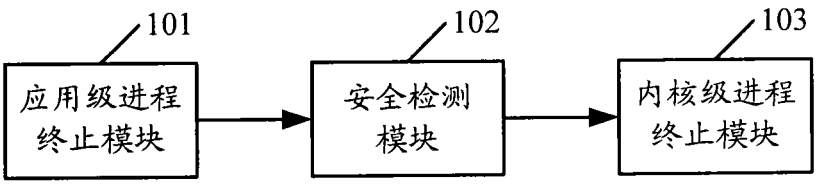

101
应用级进程终止模块
102
安全检测模块
103
内核级进程终止模块

图 1

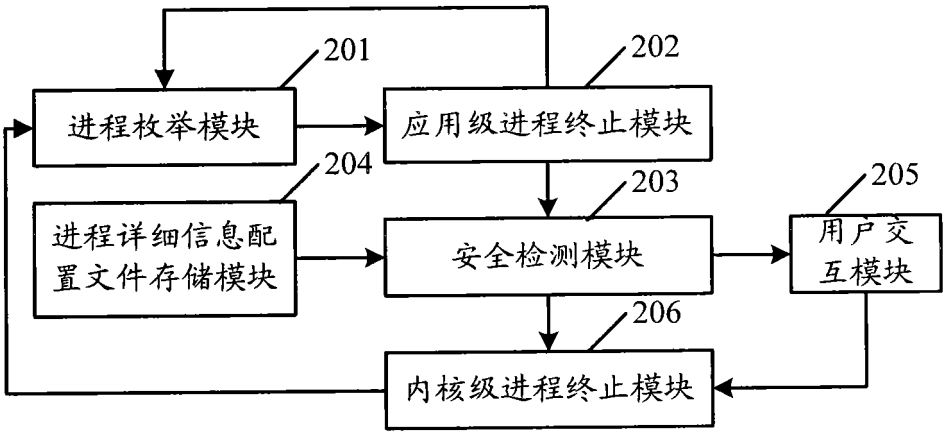

201
进程枚举模块
202
应用级进程终止模块
204
进程详细信息配置文件存储模块
203
安全检测模块
205
用户交互模块
206
内核级进程终止模块

图 2

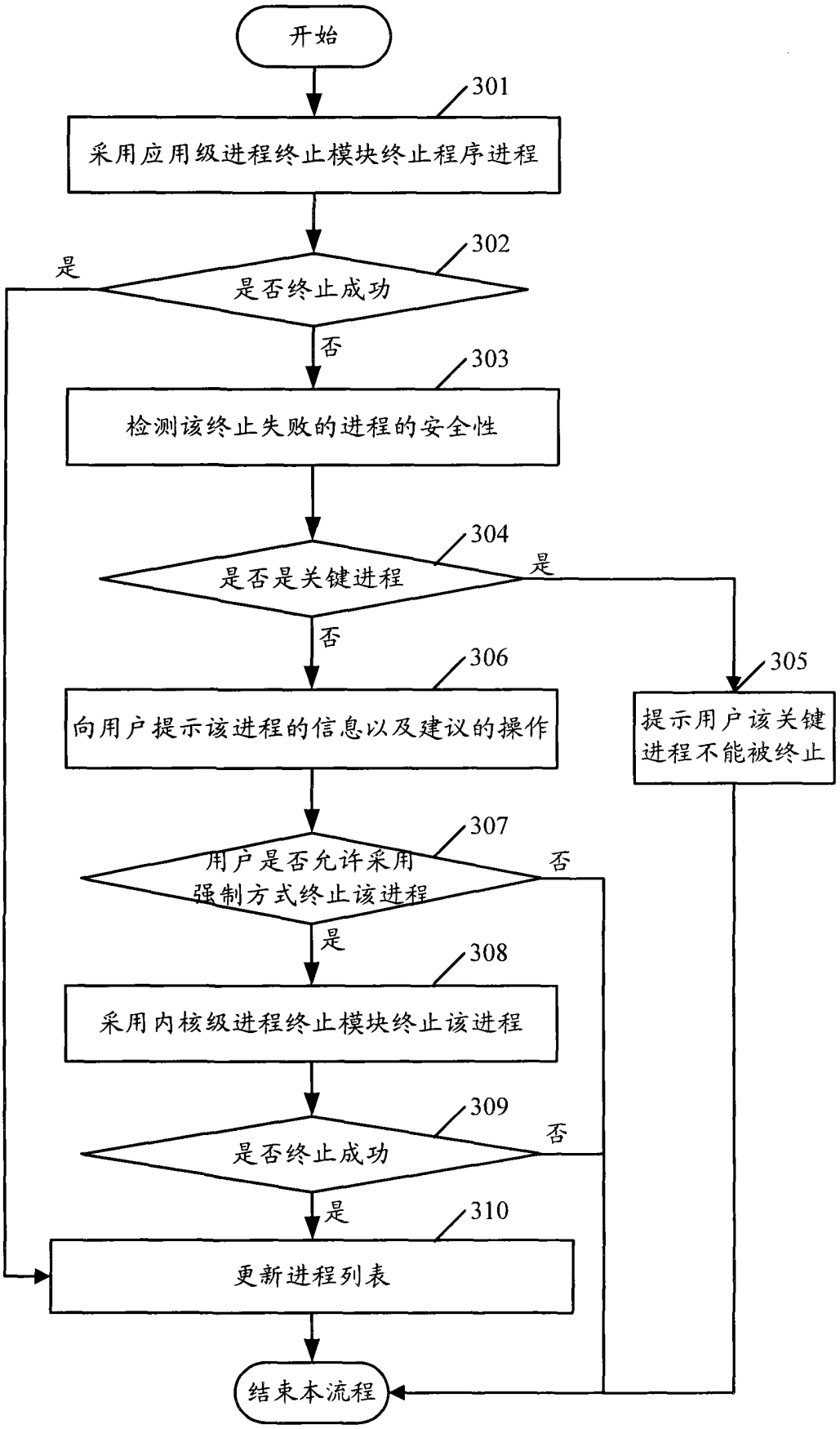

开始
301
采用应用级进程终止模块终止程序进程
302
是否终止成功
是
否
303
检测该终止失败的进程的安全性
304
是否是关键进程
是
否
305
提示用户该关键进程不能被终止
306
向用户提示该进程的信息以及建议的操作
307
用户是否允许采用强制方式终止该进程
否
是
308
采用内核级进程终止模块终止该进程
309
是否终止成功
否
是
310
更新进程列表
结束本流程

图 3