(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 103067246 B
(45)授权公告日 2015.11.25

(21)申请号 201110317166.2
(22)申请日 2011.10.18
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼岛资本大厦一座四层847号邮箱
(72)发明人 邵有石
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘
(51)Int.Cl.
H04L 12/58(2006.01)
H04L 9/00(2006.01)

(56)对比文件
CN 101959193 A,2011.01.26,
CN 102184356 A,2011.09.14,

审查员 张俊杰

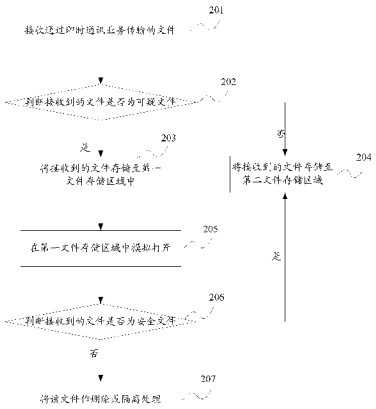
权利要求书3页 说明书9页 附图2页

(54)发明名称

对基于即时通讯业务接收到的文件进行处理的方法及装置

(57)摘要

本申请公开了一种对基于即时通讯业务接收到的文件进行处理的方法，包括：判断接收到的通过即时通讯业务传输的文件是否为带有病毒的可疑文件；如果是带有病毒的可疑文件，则将接收到的文件存储到第一文件存储区域，文件在所述第一文件存储区域中运行时不会对终端的系统安全造成影响；并在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；根据文件模拟打开的执行结果，在确定出该被模拟打开的文件不是安全文件时，将该被模拟打开的文件做删除或隔离处理。从而较好地控制通过即时通讯业务传输的带有病毒的文件被终端打开后，对终端系统的安全性造成的破坏。



CN 103067246 B

1. 一种对基于即时通讯业务接收到的文件进行处理的方法，其特征在于，包括：

判断接收到的通过即时通讯业务传输的文件是否为可疑文件；

如果判断结果是可疑文件，则将接收到的文件存储到第一文件存储区域，所述第一文件存储区域为文件隔离运行区域，文件在所述第一文件存储区域中运行时不会对终端的系统安全造成影响；如果判断结果不是可疑文件，则将接收到的文件存储至用于存储安全文件的第二文件存储区域；并

在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；

根据文件模拟打开的执行结果，在确定出该被模拟打开的文件不是安全文件时，将该被模拟打开的文件做删除或隔离处理。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

在确定出该被模拟打开的文件是安全文件时，将该被模拟打开的文件由第一文件存储区域转存至第二文件存储区域。

3. 如权利要求 1 所述的方法，其特征在于，判断接收到的通过即时通讯业务传输的文件是否为可疑文件，包括：

根据接收到的通过即时通讯业务传输的文件的文件后缀名，判断该文件是常态类型文件还是非常态类型文件，如果是常态类型文件，则确定该接收到的文件不是可疑文件，如果是非常态类型文件，则确定该接收到的文件是可疑文件；或者

根据接收到的通过即时通讯业务传输的文件的文件内容，判断该接收到的文件是否承载了有关病毒的代码，如果承载了有关病毒的代码，则确定该接收到的文件是可疑文件，如果没有承载有关病毒的代码，则确定该接收到的文件不是可疑文件；或者

在接收到的通过即时通讯业务传输的文件是以压缩包形式传送的文件时，获得接收到的压缩包中包含的文件的文件类型，判断获得的文件类型是常态类型还是非常态类型，如果是常态类型，则确定该接收到的文件不是可疑文件，如果是非常态类型，则确定该接收到的文件是可疑文件；或者

根据接收到的通过即时通讯业务传输的文件的文件内容，判断该文件是否具有公认安全的数字签名，如果具有公认安全的数字签名，则确定该接收到的文件不是可疑文件，如果不具有公认安全的数字签名，则确定该接收到的文件是可疑文件；或者

在接收到通过即时通讯业务传输的文件时，采用哈希函数对接收到的文件的内容进行计算，将计算得到的计算结果与预先存储的对应安全文件和不安全文件的计算结果进行比对，如果比对结果相同，则确定该接收到的文件是安全文件或者是不安全文件，如果比对结果不相同，则确定该接收到的文件是可疑文件。

4. 如权利要求 1 所述的方法，其特征在于，将接收到的文件存储到第一文件存储区域，包括：

对接收到的通过即时通讯业务传输的文件进行设置密码及其压缩处理；并

将压缩后的文件存储到第一文件存储区域。

5. 如权利要求 1 所述的方法，其特征在于，将指示打开的文件在所述第一文件存储区域中模拟打开，包括：

针对指示打开的文件创建一个进程，所述进程用于打开存储在第一文件存储区域的该

被指示打开的文件，或者用于执行打开存储在第一文件存储区域的该被指示打开的文件的程序；

使用创建的进程，将指示打开的文件在所述第一文件存储区域中模拟打开。

6. 如权利要求 4 所述的方法，其特征在于，将指示打开的文件在所述第一文件存储区域中模拟打开，包括：

将存储在第一文件存储区域的被指示打开的压缩文件做解压缩处理，并将解压缩后的文件存储在第一文件存储区域的临时目录下；

创建一个进程，所述进程用于打开存储在所述临时目录下的文件，或者用于执行打开存储在所述临时目录下的文件的程序；

使用创建的进程，将指示打开的文件在所述第一文件存储区域中模拟打开。

7. 如权利要求 1、5 或 6 所述的方法，其特征在于，将指示打开的文件在所述第一文件存储区域中模拟打开的过程中，还包括：

创建一个独立的窗口站，使指示打开的文件在所述第一文件存储区域中模拟打开的过程中，在所述创建的窗口站中创建或者访问终端系统的窗口资源。

8. 如权利要求 5 或 6 所述的方法，其特征在于，所述创建的进程，被赋予的权限包括下述中的至少一项：

禁止写磁盘；

禁止修改注册表；

禁止访问网络资源；

禁止更改浏览器资源；

禁止访问系统公共资源。

9. 如权利要求 6 所述的方法，其特征在于，将解压缩后的文件存储在第一文件存储区域的临时目录下之后，创建一个进程之前，还包括：

运行病毒扫描软件对存储在第一文件存储区域的临时目录下的解压缩后的文件做病毒扫描处理。

10. 如权利要求 1 所述的方法，其特征在于，根据文件模拟打开的执行结果，确定该被模拟打开的文件是否为安全文件，包括：

在文件模拟打开过程中，记录与终端系统安全有关的应用程序编程接口 API 函数被调用的模式，当记录的 API 函数被调用的模式与预先设定的模式不一致时，判断该被模拟打开的文件不是安全文件，否则判断该被模拟打开的文件是安全文件。

11. 如权利要求 1 所述的方法，其特征在于，将该被模拟打开的该文件做删除或隔离处理之后，还包括：

将该被模拟打开的文件是带有病毒的文件和 / 或将该被模拟打开的文件做删除或隔离处理的信息上报。

12. 一种对基于即时通讯业务接收到的文件进行处理的装置，其特征在于，包括：

可疑文件判断单元，用于判断接收到的通过即时通讯业务传输的文件是否为可疑文件；

文件存储单元，用于在可疑文件判断单元判断出所述文件是可疑文件时，将接收到的文件存储到第一文件存储区域，所述第一文件存储区域为文件隔离运行区域，文件在所述

第一文件存储区域中运行时不会对终端的系统安全造成影响；在可疑文件判断单元判断出所述文件不是可疑文件时，将接收到的文件存储至用于存储安全文件的第二文件存储区域；

文件模拟打开执行单元，用于在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；

安全文件判断单元，用于根据文件模拟打开执行单元对文件模拟打开的执行结果，确定该被模拟打开的文件是否为安全文件；

执行单元，用于在安全文件判断单元判断出被模拟打开的文件不是安全文件时，将该被模拟打开的文件做删除或隔离处理。

对基于即时通讯业务接收到的文件进行处理的方法及装置

技术领域

[0001] 本申请涉及互联网信息安全处理技术领域，尤其涉及一种对基于即时通讯业务接收到的文件进行处理的方法及装置。

背景技术

[0002] 随着计算机及互联网技术的迅速发展，各种业务数据的电子传输方式已经在整个社会中占据了主导地位。即时通讯（IM，Instant messaging）业务，是一种能够即时发送和接收互联网消息的业务。近几年随着互联网技术的发展，即时通信业务不再是单纯的聊天工具，其功能日益丰富，成为了包含电子邮件、博客、音乐、电视、游戏和搜索等多种功能集成在一起的综合业务，并且被发展成集交流、资讯、娱乐、搜索、电子商务、办公协作和企业客户服务等为一体的综合化信息平台。通过即时通讯技术进行文件传输，已经成为终端通过网络进行业务数据电子传输的重要手段之一。

[0003] 由于目前即时通讯业务都具备文件传输功能，使用同一种即时通讯业务的终端之间可以传输一个或多个文件。然而存在一些的使用者，通过即时通讯业务传输带有病毒、木马、脚本等对终端系统安全具有威胁的文件，这些文件如果在终端上被打开或者运行，会对终端系统的安全造成破坏，从而使存储在终端上的信息丢失，甚至直接造成终端用户的经济损失。因此如何保证通过即时通讯业务传输的文件在被终端接收后能够被安全打开是提高网络安全的必须选择。

[0004] 现有技术中将通过即时通讯业务传输的文件被接收后安全打开的方法有：

[0005] 第一种方法：针对接收到的文件，获取该文件的属性信息，如果接收到的文件的后缀名为可执行类文件，则采取将可执行类的文件后缀名自动重命名的方法，将接收到的可执行文件改名为非可执行的文件，从而不允许终端执行或者打开这些文件；

[0006] 第二种方法：利用杀毒软件对接收到的文件进行病毒和木马扫描，在终端系统中嵌入杀毒模块，对接收到的文件进行扫描，查看该文件是否承载了破坏终端系统安全的代码。

[0007] 上述第一种方法，在终端没有接收到任何指令的情况下自动修改接收到的文件的文件属性，可能导致最终找不到接收到的文件或者不知道如何打开该文件，在后续操作中，如果想要运行该文件，必须将文件类型重新更改回原来的类型，然后再运行，这时很可能依然会导致承载在该文件当中的代码被执行，从而对终端系统安全造成破坏。并且如果文件是以压缩包的形式进行传输的，就不能够采用重命名的方式保证终端系统的安全。

[0008] 上述第二种方法，依赖于杀毒模块的病毒库和特征码，杀毒模块需要及时更新，由于代码的生命周期很短，如果杀毒模块的更新不够及时，则对接收到的文件进行病毒扫描时，不能够及时判断出接收到的文件是否会对终端系统的安全造成影响，尤其是对于一些通过压缩形式传输的文件（特别是已经加密过的压缩包），杀毒模块不一定能够扫描到文件内容，从而无法识别文件的安全性。

[0009] 由此可见，现有技术中对通过即时通讯业务进行传输的文件，如果该文件为带有

病毒或恶意脚本程序等不良内容的文件，并不能较好地控制该接收的文件被终端打开后对终端系统的安全性造成的破坏。

发明内容

[0010] 本申请实施例提供一种对基于即时通讯业务接收到的文件进行处理的方法及装置，用以较好地控制通过即时通讯业务传输的文件在被终端打开后，不会对终端系统的安全性造成的破坏。

[0011] 本申请实施例技术方案如下：

[0012] 一种对基于即时通讯业务接收到的文件进行处理的方法，包括：判断接收到的通过即时通讯业务传输的文件是否为可疑文件；如果判断结果是可疑文件，则将接收到的文件存储到第一文件存储区域，所述第一文件存储区域为文件隔离运行区域，文件在所述第一文件存储区域中运行时不会对终端的系统安全造成影响；并在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；根据文件模拟打开的执行结果，在确定出该被模拟打开的文件不是安全文件时，将该被模拟打开的文件做删除或隔离处理。

[0013] 一种对基于即时通讯业务接收到的文件进行处理的装置，包括：可疑文件判断单元，用于判断接收到的通过即时通讯业务传输的文件是否为可疑文件；文件存储单元，用于在可疑文件判断单元判断出所述文件是可疑文件时，将接收到的文件存储到第一文件存储区域，所述第一文件存储区域为文件隔离运行区域，文件在所述第一文件存储区域中运行时不会对终端的系统安全造成影响；文件模拟打开执行单元，用于在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；安全文件判断单元，用于根据文件模拟打开执行单元对文件模拟打开的执行结果，确定该被模拟打开的文件是否为安全文件；执行单元，用于在安全文件判断单元判断出被模拟打开的文件不是安全文件时，将该被模拟打开的文件做删除或隔离处理。

[0014] 本申请的有益效果如下：

[0015] 本申请实施例提出的对基于即时通讯业务接收到的文件进行处理的方法及装置，通过对接收到的通过即时通讯业务传输的可疑文件模拟打开的方法，确定该接收到的文件是否为安全文件，如果是安全文件，则存储至用于存储安全文件的第二文件存储区域，如果不是安全文件，则做删除或隔离处理，从而较好地控制通过即时通讯业务传输的文件在被终端打开后，不会对终端系统的安全性造成的破坏。

附图说明

[0016] 图 1 为本申请实施例一中，提出的对基于即时通讯业务接收到的文件进行处理的系统架构图；

[0017] 图 2 为本申请实施例二中，提出的对基于即时通讯业务接收到的文件进行处理的方法流程图。

具体实施方式

[0018] 针对现有技术中存在的对接收到的通过即时通讯业务进行传输的文件，如果该文

件为带有病毒的文件，不能较好地控制该接收到的文件被终端打开后对终端系统的安全性造成的破坏的问题，本申请实施例提出一种对基于即时通讯业务接收到的文件进行处理的方法及装置，通过对接收到的通过即时通讯业务传输的可疑文件模拟打开的方法，确定该接收到的文件是否为安全文件，如果是安全文件，则存储至用于存储安全文件的第二文件存储区域，如果不是安全文件，则做删除或隔离处理，从而较好地控制通过即时通讯业务传输的带有病毒的文件被终端打开后，对终端系统的安全性造成的破坏。

[0019] 下面将结合各个附图对本申请实施例技术方案的主要实现原理、具体实施方式及其对应能够达到的有益效果进行详细地阐述。

[0020] 实施例一

[0021] 如图 1 所示，其为本申请实施例一中提出的对基于即时通讯业务接收到的文件进行处理的系统架构图。其中本申请权利要求保护的对基于即时通讯业务接收到的文件进行处理的装置就可以基于该系统架构来实现，具体地，该系统架构包括文件接收沙箱、第一文件存储区域、第二文件存储区域、文件存储单元、文件模拟打开执行单元、安全文件判断单元、执行单元和人机交互界面，其中：

[0022] 文件接收沙箱，包括可疑文件判断单元，用来判断接收到的通过即时通讯业务传输的文件是否为可疑文件。其中可疑文件是指可能带有恶意程序、病毒等不良内容的文件。其中，可疑文件判断单元判断接收到的通过即时通讯业务传输的文件是否为可疑文件，可以但不限于通过以下五种方式进行：

[0023] 第一种方式：根据接收到的通过即时通讯业务传输的文件的文件后缀名，判断该文件是常态类型文件还是非常态类型文件，如果是常态类型文件，则确定该接收到的文件不是可疑文件，如果是非常态类型文件，则确定该接收到的文件是可疑文件。其中，常态文件类型的文件后缀名可以但不限于为 txt、MP3、AVI、JPEG、MPEG 等，非常态文件类型的文件后缀名可以但不限于为 exe、SCR、JS、VBS 等。

[0024] 第二种方式：根据接收到的通过即时通讯业务传输的文件的文件内容，判断该接收到的文件是否承载了有关病毒的代码，如果承载了有关病毒的代码，则确定该接收到的文件是带有病毒的可疑文件，如果没有承载有关病毒的代码，则确定该接收到的文件不是带有病毒的可疑文件。例如，可以通过查看接收到的通过即时通讯业务传输的文件的文件头或者文件尾，判断该接收到的文件是否是恶意伪装成安全文件类型的文件或者是该文件中是否嵌入了其他文件的恶意代码。例如，对于通过即时通讯业务传输的文件类型为“EXE”和“DLL”的文件，在文件头存在“MZ”或“MZP”的标识，在标识之后文件会存在特定的结构，用于存储相关的执行文件信息，如代码段位置、代码段长度和入口地址等信息。

[0025] 第三种方式：在接收到的通过即时通讯业务传输的文件是以压缩包形式传送的文件时，通过对接收到的压缩包进行解压缩或通过查看接收到的压缩包内的文件列表信息，查看压缩包内的文件内容，获得接收到的压缩包中包含的文件的文件类型，判断获得的文件类型是常态类型还是非常态类型，如果是常态类型，则确定该接收到的文件不是带有病毒的可疑文件，如果是非常态类型，则确定该接收到的文件是可能带有病毒的可疑文件。其中，常态文件类型的文件后缀名可以但不限于为 txt、MP3、AVI、JPEG、MPEG 等，非常态文件类型的文件后缀名可以但不限于为 exe、SCR、JS、VBS 等。

[0026] 第四种方式：根据接收到的通过即时通讯业务传输的文件的文件内容，判断该文

件是否具有公认安全的数字签名，如果具有公认安全的数字签名，则确定该接收到的文件不是可疑文件，如果不具有公认安全的数字签名，则确定该接收到的文件是可疑文件。其中，公认安全的数字签名可以但不限于为：接收到的文件的文件内容中包含一些制作该文件的企业标识，如果该企业标识是比较知名的企业标识，则可以将该企业标识认为是公认安全的数字签名。

[0027] 第五种方式：在接收到通过即时通讯业务传输的文件时，采用哈希函数对接收到的文件的内容进行计算，将计算得到的计算结果与预先存储的对应安全文件或不安全文件的计算结果分别进行比对，如果比对结果相同，则确定该接收到的文件是安全文件或者是不安全文件，如果比对结果不相同，则确定该接收到的文件是可疑文件。

[0028] 具体地，判断接收到的通过即时通讯业务传输的文件是否为可疑文件时，可以采用上述五种方式中的至少一种判断方式或者采用至少两种方式的组合。例如，可以综合利用第二种判断方式和第四种判断方式对接收到的文件进行判断，根据接收到的通过即时通讯业务传输的文件的文件内容，判断出该接收到的文件是可疑文件，但是该接收到的文件的文件内容具有公认安全的数字签名，那么可以直接判断该文件是安全文件。综合利用上述五种判断方式，能够较好的节省终端的处理资源。

[0029] 第一文件存储区域，具体包括文件存储沙箱和执行环境沙箱，其中文件存储沙箱，具体用于存储文件接收沙箱中的可疑文件判断单元判断出的通过即时通讯业务传输的文件为可疑文件。

[0030] 第二文件存储区域，是用来存储安全文件的区域，用户可以对存储在第二文件存储区域的文件进行操作，并且可以指定文件存储在第二文件存储区域中的任一存储位置。

[0031] 文件存储单元，用于在文件接收沙箱中的可疑文件判断单元判断出通过即时通讯业务接收到的文件不是可疑文件时，则将接收到的文件存储至用于存储安全文件的第二文件存储区域。以及在可疑文件判断单元判断出该接收到的文件是可疑文件时，则将接收到的文件存储到第一文件存储区域中的文件存储沙箱中。

[0032] 进一步地，文件存储单元可以对通过即时通讯业务传输的可疑文件设置密码并进行压缩处理，然后将压缩后的文件存储在文件存储沙箱中的特定目录下，并且，压缩后的文件可以但不限于维护文件的名称、类型以及路径等信息。其中，文件存储单元对可疑文件进行压缩处理时，使用的压缩算法可以但不限于为 LZ77 算法和 / 或 LZMA 算法等。

[0033] 进一步地，文件存储沙箱还用于存储解压缩后的文件，然后将解压缩后的文件存储在文件存储沙箱的临时目录下。

[0034] 其中，第一文件存储区域中还包括执行环境沙箱，用于将指示打开的文件在执行环境沙箱中模拟打开，由于文件存储沙箱中存储有带有可疑文件，因此可以选择将文件存储沙箱中存储的可疑文件在执行环境沙箱中模拟打开，其中执行环境沙箱相当于一个文件隔离运行区域，文件在该执行环境沙箱中运行时不会对终端的系统安全造成破坏和影响。

[0035] 文件模拟打开执行单元，用于在接收到用于指示打开第一文件存储区域中存储的文件的指令时，在第一文件存储区域中的文件存储沙箱中查找到指示打开的文件，然后将该查找到的文件在执行环境沙箱中模拟打开；

[0036] 进一步地，文件模拟打开执行单元还可以创建一个独立的窗口站，使指示打开的文件在执行环境沙箱中模拟打开的过程中，在该创建的窗口站中创建或者访问终端系统的

窗口资源。

[0037] 其中，文件模拟打开执行单元还可以具体包括进程创建子单元和执行子单元。其中，进程创建子单元，用于针对指示打开的文件在执行环境沙箱中创建一个进程，用于打开存储在文件存储沙箱中被指示打开的文件，或者用于执行打开存储在文件存储沙箱中该被指示打开的文件的程序。执行子单元，用于使用进程创建子单元创建的进程，将指示打开的文件在第一文件存储区域中的执行环境沙箱中模拟打开。

[0038] 进一步地，文件模拟打开执行单元还可以将存储在文件存储沙箱中的被指示打开的压缩文件做解压缩处理，并将解压缩后的文件存储在文件存储沙箱中的临时目录下，然后利用进程创建子单元创建一个进程，用于打开存储在所述临时目录下的文件，或者用于执行打开存储在所述临时目录下的文件的程序，之后执行子单元使用创建的进程，将指示打开的文件在执行环境沙箱中模拟打开。可选地，在创建该进程之前还可以运行病毒扫描软件对存储在临时目录下的解压缩后的文件进行病毒扫描处理。

[0039] 更进一步地，进程创建子单元创建的进程，可以通过 Windows API 函数将所述进程赋予较低的权限，例如，禁止写磁盘、禁止修改注册表、禁止访问网络、禁止更改浏览器资源以及禁止访问系统公共资源等，从而可以较好的控制被模拟打开的文件中可能携带的病毒、恶意脚本程序等对终端系统安全造成破坏的问题。

[0040] 更进一步地，执行子单元在使用进程创建子单元创建的进程将指示打开的文件在执行环境沙箱中模拟打开的过程中，可以创建一个独立的窗口站，使指示打开的文件在执行环境沙箱中被模拟打开的过程中，在所述创建的窗口站中创建或者访问终端系统的窗口等 UI 资源。可选地，执行子单元将文件在独立窗口站中创建或者访问终端系统的窗口等 UI 资源的行为在人机交互界面上显示，使用户可以直接看到所述被模拟打开的文件的运行结果。

[0041] 安全文件判断单元，用于根据文件模拟打开执行单元对文件模拟打开的执行结果，确定该被模拟打开的文件是否为安全文件；

[0042] 进一步地，安全文件判断单元可以在执行环境沙箱中将文件模拟打开的过程中，记录与终端系统安全有关的应用程序编程接口 API 函数被调用的模式，当记录的 API 函数被调用的模式与预先设定的模式不一致时，则可以判断该被模拟打开的文件不是安全文件，否则判断该被模拟打开的文件是安全文件。所述 API 函数被调用的模式可以但不限于为以下几种：API 函数被单独调用的次数、调用的时间等模式，至少一个 API 函数被调用的次数、调用的时间的组合模式。下面以 X 和 Y 两个 API 函数调用次数为例，阐述基于 API 函数被调用的次数是否大于预先设定的阈值来进而判断被模拟打开的文件是否为安全文件。X 和 Y 预先设定的模式如下述表格 1 所示：

[0043] 表 1

[0044]

调用次数	判断结果
X ＞ 5	非安全文件
Y ＞ 4	非安全文件

X＞1 且 Y＞2	非安全文件
……	非安全文件
X＞2 且 Y＞1	非安全文件

[0045] 从上述表 1 中可以看出，在文件被模拟打开的过程中，当 X 函数单独被调用的次数为 4 次时，则可以确定该被模拟打开的文件为安全文件，但是在文件被模拟打开的过程中，X 函数被调用了 2 次，同时 Y 函数也被调用了 4 次，则可以确定此时该被模拟打开的文件不是安全文件。

[0046] 执行单元，用于在安全文件判断单元判断出被模拟打开的文件不是安全文件时，则对第一文件存储区域中的文件存储沙箱中存储的该被模拟打开的文件做删除处理或隔离处理。

[0047] 进一步地，执行单元还可以将该被模拟打开的文件是带有病毒的文件和 / 或将该被模拟打开的文件做删除或隔离处理的信息上报给系统服务器处理。

[0048] 此外，文件存储单元在安全文件判断单元判断出被模拟打开的文件是安全文件时，还可以将第一文件存储区域中的文件存储沙箱中存储的该被模拟打开的文件转存至第二文件存储区域，以使文件存储沙箱中存储的最终被确定为安全的文件转存到用于存储安全文件的第二文件存储区域，以使用户可以在第二文件存储区域中正常打开和使用该文件。

[0049] 人机交互界面，用于展示存储在第一文件存储区域中的文件被模拟打开的运行情况。可选地，在人机交互界面上展示的界面可以但不限于采用下述几种情况：

[0050] 第一种情况：将文件被模拟打开的运行过程在人机交互界面上展示，由终端接收操作命令进行每一步的操作。

[0051] 第二种情况：在文件被模拟打开的过程中，将文件在独立窗口站中创建或者访问终端系统的窗口等 UI 资源的行为在人机交互界面上展示。

[0052] 第三种情况：将文件被模拟打开的判断结果的提示信息在人机交互界面上展示，所述提示信息可以但不限于为：该文件是带有病毒的文件，可能会对终端系统安全造成破坏，请选择做删除或保留等操作。

[0053] 第四种情况：在人机交互界面上展示提示信息，该提示信息可以但不限于为：该文件是安全文件，不会对终端系统安全造成破坏，请转存到其他磁盘目录下存储。

[0054] 实施例二

[0055] 如图 2 所示，其为本申请实施例二中提出的对基于即时通讯业务接收到的文件进行处理的方法流程图。

[0056] 步骤 201，接收通过即时通讯业务传输的文件。

[0057] 步骤 202，判断步骤 201 接收到的通过即时通讯业务传输的文件是否为带有病毒的可疑文件，如果判断结果为该接收到的文件是可以文件，进行步骤 203，反之，进行步骤 204；

[0058] 判断接收到的通过即时通讯业务传输的文件是否为可疑文件的方法请参见上述实施例一中的详细论述，这里不再赘述。

[0059] 步骤 203，基于步骤 202 的判断结果为该接收到的文件是可疑文件，则将接收到的文件存储到第一文件存储区域中，其中第一文件存储区域为文件隔离运行区域，文件在所述第一文件存储区域中运行时不会对终端的系统安全造成影响。可选地，在文件存储到第一文件存储区域中之后，还可以将存储信息发送到人机交互界面上进行提示，例如提示信息可以是：该接收到的文件为可疑文件，以存储到隔离文件区域中。

[0060] 具体地，为防止文件被直接访问，还可以对接收到的通过即时通讯业务传输的文件进行设置密码及其压缩处理，然后将压缩后的文件存储到第一文件存储区域中的特定目录下。并且，压缩后的文件可以但不限于维护文件的名称、类型以及路径等信息。其中，对接收到的通过即时通讯业务传输的文件进行压缩处理时，使用的压缩算法可以但不限于为 LZ77 算法和 / 或 LZMA 算法。

[0061] 步骤 204，如果步骤 202 的判断结果为该接收到的文件不是可疑文件，则将接收到的文件存储至用于存储安全文件的第二文件存储区域；

[0062] 具体地，将文件存储至第二文件存储区域之后，在人机界面上展示提示信息，提示用户可以对该文件进行相关操作。其中，在第二文件存储区域，用户可以根据需要选择任一位置存储该文件，并且在存储之后可以可以打开该存储的文件。

[0063] 步骤 205，在接收到用于指示打开第一文件存储区域中存储的文件的指令时，将指示打开的文件在所述第一文件存储区域中模拟打开；

[0064] 具体地，可以创建一个进程，用于打开存储在第一文件存储区域中被指示打开的文件，或者用于执行打开存储在第一文件存储区域中该被指示打开的文件的程序，然后使用创建的进程，将指示打开的文件在第一文件存储区域中模拟打开。

[0065] 更具体地，对打开压缩算法压缩后存储在第一文件存储区域中的文件时，需要首先将存储在第一文件存储区域中的被指示打开的压缩文件做解压缩处理，然后将解压缩后的文件存储在第一存储区域中的临时目录下，然后创建一个进程，用于打开存储在所述临时目录下的文件，或者用于执行打开存储在所述临时目录下的文件的程序，最后使用创建的进程，将指示打开的文件在第一文件存储区域中模拟打开。

[0066] 可选地，还可以在创建用于打开被指示的文件的进程之前，运行病毒扫描程序对存储在临时目录下的解压缩后的文件进行病毒扫描处理，以使文件打开过程更为安全，以对终端的系统安全进行更进一步地保证。

[0067] 更具体地，创建的进程通过 Windows API 函数将所述进程赋予较低的权限，例如，禁止写磁盘和注册表、禁止访问网络、禁止更改浏览器资源以及禁止访问系统公共资源等。从而可以较好的控制被模拟打开的文件中可能携带的病毒对终端系统安全造成破坏的问题。

[0068] 更具体地，在使用创建的进程将指示打开的文件模拟打开的过程中，还可以进而创建一个独立的窗口站，使指示打开的文件在所述第一文件存储区域中模拟打开的过程中，在所述创建的窗口站中创建或者访问终端系统的窗口等 UI 资源。可选的，将文件在独立窗口站中创建或者访问终端系统的窗口等 UI 资源的行为在人机交互界面上显示，使用户可以直接看到所述被模拟打开的文件的运行结果。

[0069] 步骤 206，基于步骤 205 中文件在第一存储区域中被模拟打开的运行结果，判断该被模拟打开的文件是否为安全文件，如果是安全文件则返回执行步骤 204，将该被模拟打开

的文件由第一文件存储区域转存至第二文件存储区域。反之，执行步骤 207 ；

[0070] 具体地，在文件模拟打开过程中，记录与终端系统安全有关的应用程序编程接口 API 函数被调用的模式，当记录的 API 函数被调用的模式与预先设定的模式不一致时，判断该被模拟打开的文件不是安全文件，否则判断该被模拟打开的文件是安全文件。

[0071] 步骤 207，对第一文件存储区域中存储的该被判定为不是安全文件的文件做删除或者隔离处理 ；

[0072] 更进一步地，将该被模拟打开的文件是带有病毒的文件和 / 或将该被模拟打开的文件做删除或隔离处理的信息上报给系统服务器处理，比如上报给即时通讯业务服务商或者安全服务提供商处理。

[0073] 可选地，还可以在人机交互界面上展示将该被模拟打开的文件做删除或者隔离处理的结果信息，并提示用户该文件是带有病毒的文件，会对终端系统安全造成破坏。

[0074] 实施例三

[0075] 本实施例在上述实施例一基础上进一步地以接收的通过即时通信业务传输的文件名属性为“.exe”格式的文件为例，介绍本申请的具体实现过程。

[0076] 步骤一，文件接收沙箱接收到通过即时通讯业务传输的文件 ；

[0077] 步骤二，基于步骤一中接收到的文件，文件接收沙箱中的可以文件判断单元判断该文件后缀名为“.exe”格式，则确定该接收到的文件属于非常态类型文件是可疑文件，则将该接收到的文件转存到第一文件存储区域中的文件存储沙箱中 ；

[0078] 步骤三，文件存储沙箱为防止文件自动运行，对接收到的后缀名为“.exe”格式的文件设置密码，采用 LZ77 压缩算法，将该文件进行压缩处理，并将压缩后的文件存储在特定的目录下。压缩后的文件保存该文件的名称、类型以及存储路径等信息，并在人机交互界面上展示该些信息。

[0079] 步骤四，文件模拟打开执行单元接收到将经过压缩处理后的存储在文件存储沙箱中的特定目录下的文件打开的指令，使用解压缩算法，对该文件进行解压缩处理，解压缩后的文件存储在文件存储沙箱的临时目录中。文件模拟打开执行单元在执行环境沙箱中创建一个进程，使用创建的进程执行打开存储在所述临时目录下的“.exe”文件。其中，采用 Windows API 函数赋予该进程较低的权限，禁止该进程进行写磁盘、禁止修改注册表、禁止访问网络资源、禁止更改浏览器资源以及禁止访问系统公共资源。

[0080] 由于该文件在被模拟打开的过程中，需要访问终端系统资源，修改注册表，因此在执行环境沙箱中创建一个独立的窗口站，使该文件在创建的独立窗口站中访问终端的系统资源。并将该文件在创建的独立窗口站中访问终端系统资源和修改注册表的行为信息展示在人机交换界面上。

[0081] 步骤五，根据步骤四中文件被模拟打开的执行结果，确定该该被模拟打开的文件不是安全文件，则将该文件做删除处理，并将删除该接收到的“.exe”文件的处理结果上报给即时通讯业务服务提供商。

[0082] 使用本申请实施例提出的对基于即时通讯业务接收到的文件进行处理的方法和装置，通过对接收到的通过即时通讯业务传输的可疑文件模拟打开的方法，确定该接收到的文件是否为安全文件，如果是安全文件，则存储至用于存储安全文件的第二文件存储区域，如果不是安全文件，则做删除或隔离处理，从而较好地控制通过即时通讯业务传输的带

有病毒的文件被终端打开后，对终端系统的安全性造成的破坏。并且，在实际应用中可以综合使用本申请实施例提出的对接收到的通过即时通讯业务传输的可疑文件的判断方法，能够更好的节省终端的处理资源，提高处理效率。

[0083] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0084] 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0085] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0086] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0087] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0088] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

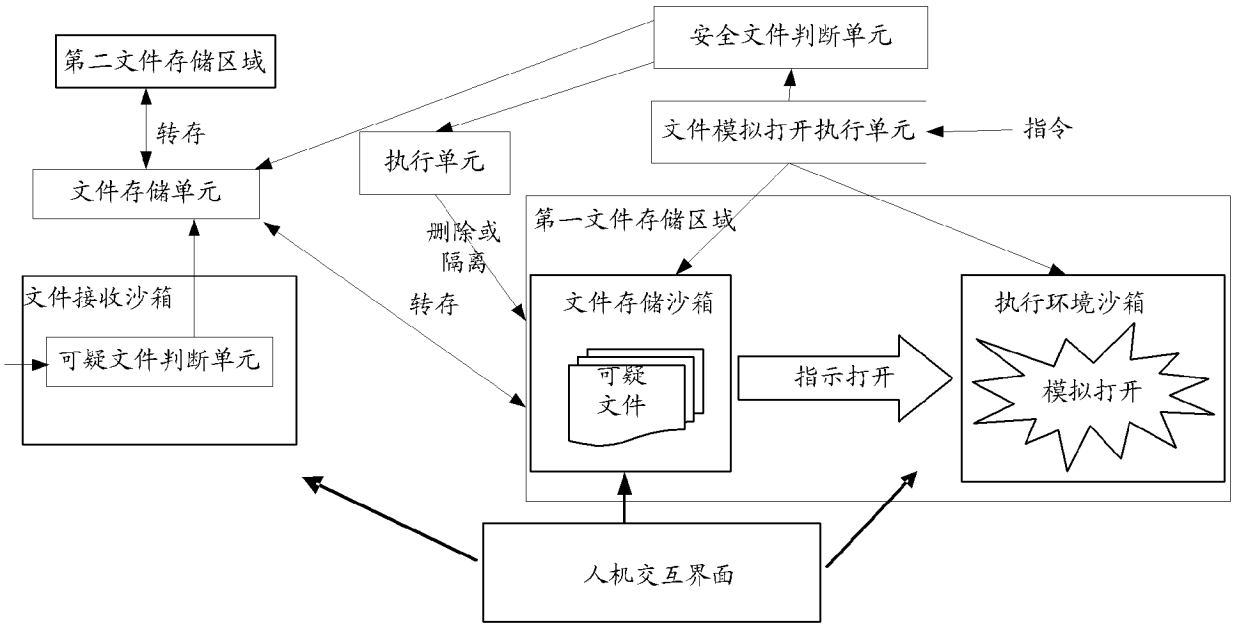

安全文件判断单元
第二文件存储区域
转存
文件模拟打开执行单元
指令
执行单元
文件存储单元
删除或
隔离
第一文件存储区域
文件接收沙箱
转存
文件存储沙箱
执行环境沙箱
可疑文件判断单元
可疑
文件
指示打开
模拟打开
人机交互界面

图 1

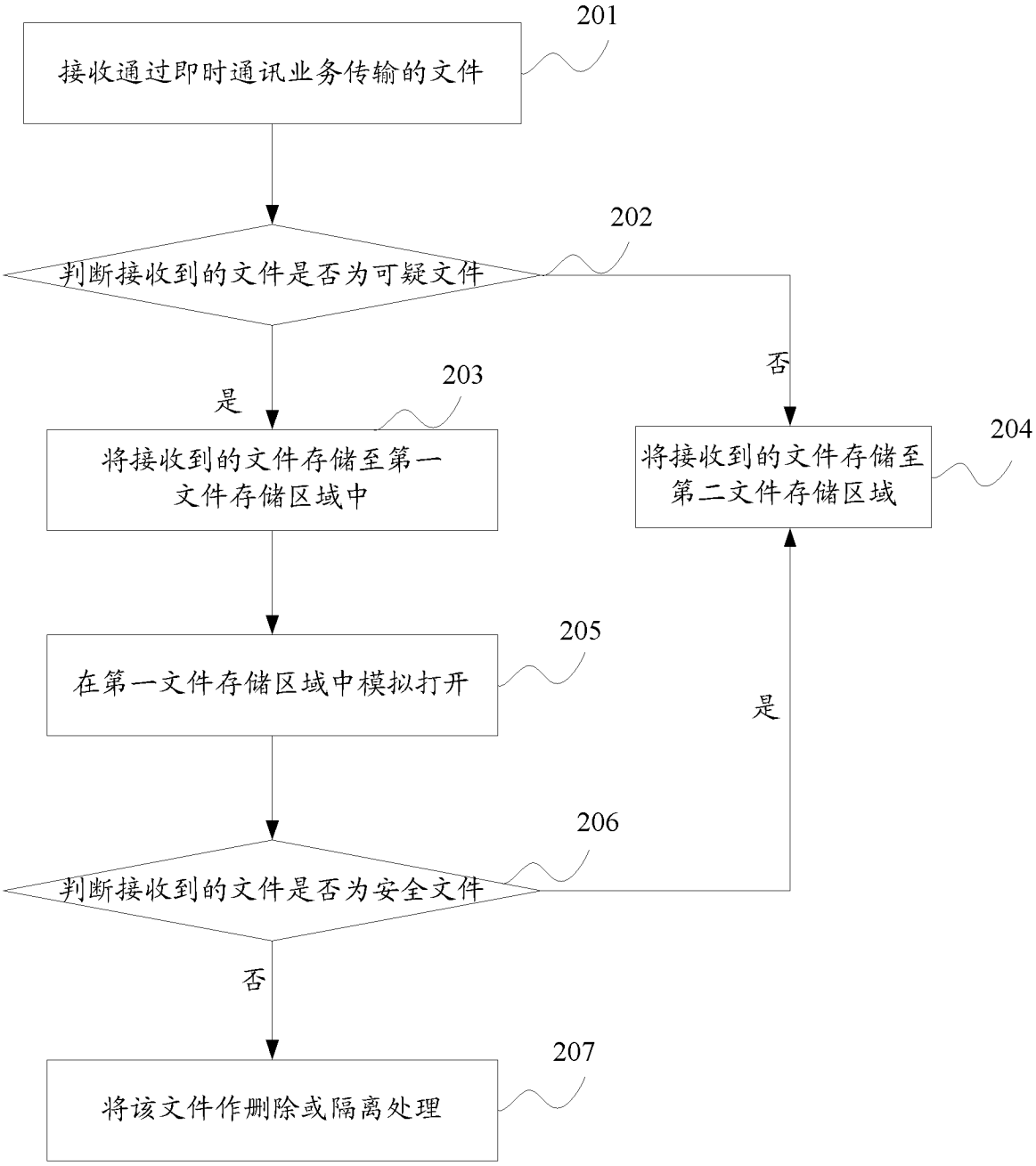

201
接收通过即时通讯业务传输的文件
202
判断接收到的文件是否为可疑文件
是
否
203
将接收到的文件存储至第一文件存储区域中
204
将接收到的文件存储至第二文件存储区域
205
在第一文件存储区域中模拟打开
是
206
判断接收到的文件是否为安全文件
否
207
将该文件作删除或隔离处理

图 2