



(12)发明专利

(10)授权公告号 CN 105451224 B

(45)授权公告日 2018.09.28

(21)申请号 201410406620.5

H04M 1/725(2006.01)

(22)申请日 2014.08.18

(56)对比文件

(65)同一申请的已公布的文献号

CN 101674583 A, 2010.03.17,

申请公布号 CN 105451224 A

CN 103634477 A, 2014.03.12,

(43)申请公布日 2016.03.30

EP 2357859 B1, 2013.06.19,

(73)专利权人 北京国基科技股份有限公司

审查员 刘红芹

地址 100085 北京市海淀区上地七街1号1
号楼1-A3F

(72)发明人 高林花 姬峰 李飞 何代钦
陈正伟 李燕舞

(74)专利代理机构 北京亿腾知识产权代理事务
所 11309

代理人 李楠

(51)Int.Cl.

H04W 12/00(2009.01)

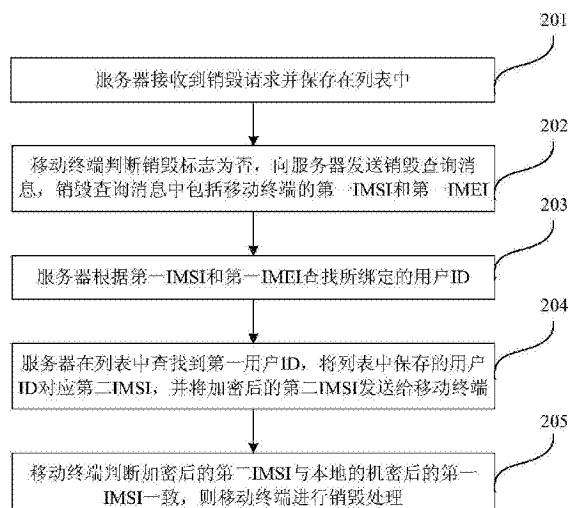
权利要求书1页 说明书4页 附图2页

(54)发明名称

销毁方法

(57)摘要

本发明涉及一种销毁方法,方法包括:用户通过移动终端首次成功登录后,将IMEI和IMSI保存在本地,并将第一广播添加到闹钟管理定时器中并广播;将成功登录变量设置为真;移动终端的广播接收器接收到第一广播,启动销毁服务;广播接收器接收到系统发送的开机自启动广播;判断成功登录变量是否为真,如是则发送第二广播;广播接收器接收到第二广播时,监听SIM;如无法识别到SIM,或第二IMEI与第一IMEI不一致,或第二IMSI与第一IMSI不一致则进行销毁处理。本发明的销毁方法可以方便的利用本地检测进行自销毁,或利用服务器侧启动销毁,将移动终端所保存的信息销毁,从而可以有效的保护移动终端的信息安全。



1.一种销毁方法,其特征在于,所述方法包括:

用户通过移动终端首次成功登录后,将所述移动终端的第一国际移动设备识别码IMEI和第一国际移动用户识别码IMSI保存在本地,并将第一广播添加到闹钟管理AlarmManager定时器中并广播所述第一广播;

用户开机时将成功登录变量设置为真;

移动终端的广播接收器接收到所述第一广播,启动销毁服务;

开机后,所述广播接收器接收到系统发送的开机自启动广播;

判断所述成功登录变量是否为真,如是则发送第二广播;

所述广播接收器接收到所述第二广播时,监听所述移动终端中客户识别模块SIM;

如果无法识别到所述SIM,或者获取到的所述移动终端的第二IMEI与本地保存的所述第一IMEI不一致,或者获取到的第二IMSI与本地保存的所述第一IMSI不一致则所述移动终端进行销毁处理。

2.根据权利要求1所述的方法,其特征在于,所述如是则发送第二广播具体包括:将所述第二广播添加到闹钟管理定时器中,以第一时间间隔发送所述第二广播。

3.根据权利要求1所述的方法,其特征在于,所述移动终端进行销毁处理具体包括:所述移动终端将本地保存的信息删除。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:所述移动终端将销毁标志设置为真,并将销毁处理时间发送给所述服务器。

5.一种销毁方法,其特征在于,所述方法包括:

服务器接收到销毁请求并保存在列表中,所述销毁请求中包括用户ID,所述用户ID与用户密码、IMIS和IMEI相绑定;

移动终端判断销毁标志为否,向所述服务器发送销毁查询消息,所述销毁查询消息中包括所述移动终端的第一IMSI和第一IMEI;

所述服务器根据所述第一IMSI和第一IMEI查找所绑定的用户ID;

所述服务器在所述列表中查找到第一用户ID,将所述列表中保存的所述用户ID对应的第二IMSI,并将加密后的第二IMSI发送给所述移动终端;

所述移动终端判断所述加密后的第二IMSI与本地的加密后的第一IMSI一致,则所述移动终端进行销毁处理。

6.根据权利要求5所述的方法,其特征在于,所述服务器接收到销毁请求并保存在列表中之后还包括,将所述用户ID设置为销毁状态。

7.根据权利要求5所述的方法,其特征在于,所述销毁查询消息中包括的所述移动终端的第一IMSI和第一IMEI具体为加密后的第一IMSI和加密后的第一IMEI。

8.根据权利要求5所述的方法,其特征在于,所述服务器根据所述第一IMSI和第一IMEI查找所绑定的用户ID之前还包括,验证所述第一IMSI和第一IMEI是否合法。

9.根据权利要求5所述的方法,其特征在于,所述移动终端进行销毁处理具体包括:所述移动终端将本地保存的信息删除。

10.根据权利要求5所述的方法,其特征在于,所述方法还包括:所述移动终端将销毁标志设置为真,并将销毁处理时间发送给所述服务器。

销毁方法

技术领域

[0001] 本发明涉及信息安全领域,尤其涉及一种销毁方法。

背景技术

[0002] 随着时代的发展,信息技术日新月异,人们对信息的需求也越来越大。而在信息化的社会中,信息的重要性和经济价值也越来越高。

[0003] 但是信息安全问题也因此产生,尤其对于一些保密要求高的行业或者领域,当所使用的移动终端丢失被人捡到就可能产生信息丢失和泄密的问题。

发明内容

[0004] 本发明的目的是针对现有技术的缺陷,提供一种销毁方法,用以实现当发现不安全情况时,启动销毁处理,可以有效防止信息泄露。

[0005] 为实现上述目的,本发明提供了一种销毁方法,所述方法包括:

[0006] 用户通过移动终端首次成功登录后,将所述移动终端的第一国际移动设备识别码IMEI和第一国际移动用户识别码IMSI保存在本地,并将第一广播添加到闹钟管理AlarmManager定时器中并广播所述第一广播;用户开机时将成功登录变量设置为真;

[0007] 移动终端的广播接收器接收到所述第一广播,启动销毁服务;

[0008] 开机后,所述广播接收器接收到系统发送的开机自启动广播;

[0009] 判断所述成功登录变量是否为真,如是则发送第二广播;

[0010] 所述广播接收器接收到所述第二广播时,监听所述移动终端中客户识别模块SIM;

[0011] 如果无法识别到所述SIM,或者获取到的所述移动终端的第二IMEI与本地保存的所述第一IMEI不一致,或者获取到的第二IMSI与本地保存的所述第一IMSI不一致则所述移动终端进行销毁处理。

[0012] 进一步的,所述如是则发送第二广播具体包括:将所述第二广播添加到闹钟管理中,以第一时间间隔发送所述第二广播。

[0013] 进一步的,所述移动终端进行销毁处理具体包括:所述移动终端将本地保存的信息删除。

[0014] 进一步的,所述方法还包括:所述移动终端将销毁标志设置为真,并将销毁处理时间发送给所述服务器。

[0015] 本发明还提供了一种销毁方法,所述方法包括:

[0016] 服务器接收到销毁请求并保存在列表中,所述销毁请求中包括用户ID,所述用户ID与用户密码、IMIS和IMEI相绑定;

[0017] 移动终端判断销毁标志为否,向所述服务器发送销毁查询消息,所述销毁查询消息中包括所述移动终端的第一IMSI和第一IMEI;

[0018] 所述服务器根据所述第一IMSI和第一IMEI查找所绑定的用户ID;

[0019] 所述服务器在所述列表中查找到所述第一用户ID,将所述列表中保存的所述用户

ID对应的第一IMSI，并将加密后的第二IMSI发送给所述移动终端；

[0020] 所述移动终端判断所述加密后的第二IMSI与本地的加密后的第一IMSI一致，则所述移动终端进行销毁处理。

[0021] 进一步的，所述服务器接收到销毁请求并保存在列表中之后还包括，将所述用户ID设置为销毁状态。

[0022] 进一步的，所述销毁查询消息中包括的所述移动终端的第一IMSI和第一IMEI具体为加密后的第一IMSI和加密后的第一IMEI。

[0023] 根据权利要求5所述的方法，其特征在于，所述服务器根据所述第一IMSI和第一IMEI查找所绑定的用户ID之前还包括，验证所述第一IMSI和第一IMEI是否合法。

[0024] 进一步的，所述移动终端进行销毁处理具体包括：所述移动终端将本地保存的信息删除。

[0025] 进一步的，所述方法还包括：所述移动终端将销毁标志设置为真，并将销毁处理时间发送给所述服务器。

[0026] 本发明的销毁方法可以方便的利用本地检测进行自销毁，或者利用服务器侧启动销毁，将移动终端所保存的信息销毁，从而可以有效的保护移动终端的信息安全。

附图说明

[0027] 图1为本发明销毁方法实施例一的流程图；

[0028] 图2为本发明销毁方法实施例二的流程图。

具体实施方式

[0029] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

[0030] 本发明的销毁方法就是利用自动销毁或者远程销毁来保证用户信息的安全，防止移动终端丢失后造成信息的意外泄漏。

[0031] 本发明具有两种处理模式，第一种模式适用于终端绑定，用户在第一次成功登录终端软件后，获取设备国际移动用户识别码 (International Mobile SubscriberIdentification Number, IMSI)、国际移动设备识别码 (International Mobile EquipmentIdentification Number, IMEI) 信息并保存在SharedPreferences中。销毁服务运行时根据已保存设备信息和现有设备IMEI、IMSI进行比较，确定是否需要销毁。

[0032] 图1为本发明销毁方法实施例一的流程图，如图所示，本实施例具体包括如下步骤：

[0033] 步骤101，用户通过移动终端首次成功登录后，将移动终端的第一IMEI和第一IMSI保存在本地；并将第一广播添加到闹钟管理AlarmManager定时器中并广播；

[0034] 步骤102，将成功登录变量设置为真；

[0035] 步骤103，移动终端的广播接收器接收到第一广播，启动销毁服务；

[0036] 具体的，用户第一次成功登录时，将设备的IMSI、IMEI信息保存在SharedPreferences中，同时将表示成功登录过软件的变量successedLogin设置为true。用户第一次手动登录成功后，将第一广播Constants.ACTION_ACTIVATE_DESTROY添加到闹钟管理AlarmManager中，并以间隔120秒的时间不断发送该广播，广播接收器收到该第一广播

后,立即启动销毁服务。

[0037] 步骤104,开机后,广播接收器接收到系统发送的开机自启动广播;

[0038] 步骤105,判断成功登录变量是否为真,如是则发送第二广播;

[0039] 具体的,之后移动终端再开机,则利用广播接收器收到开机自启动广播,即 android.intent.action.BOOT_COMPLETED广播,首先判断变量successedLogin的值是否为 true,如果满足条件,就将第二广播即Constants.ACTION_ACTIVATE_DESTROY添加到闹钟管理AlarmManager中,并以第一时间间隔,例如120秒的时间不断发送该广播。

[0040] 步骤106,广播接收器接收到第二广播时,监听移动终端中客户识别模块(Subscriber Identity Module,SIM);

[0041] 具体的,广播接收器收到第二广播后,立即启动销毁服务,监听SIM卡的状态。

[0042] 步骤107,如果无法识别到SIM,或者获取到的移动终端的第二IMEI与本地保存的第一IMEI不一致,或者获取到的第二IMSI与本地保存的第一IMSI不一致则移动终端进行销毁处理。

[0043] 具体的,如果无法识别到SIM卡,例如是无SIM卡状态,或是有SIM卡状态,但是获取到的第二IMSI或第二IMEI信息与SharedPreferences保存的第一IMSI或第一IMEI信息不一致,都开启自销毁处理。

[0044] 销毁处理就是将本地保存的信息删除,例如删除数据库文件中的信息,清空 SharedPreferences保存的所有变量(包括用户账号、密码、IMEI、IMSI、设置项),然后将销毁标志destroy设置为true,保存入SharedPreferences中。

[0045] 如果网络正常,则将软件销毁时间发送到服务器。杀死当前进程,以及正在运行的 view层、service层进程。

[0046] 如果下次希望再次登录的时候,则会提示“软件已经自毁,请卸载后重新安装!”,将无法进入本应用,软件禁止使用。

[0047] 本发明的第二种处理模式适用于服务器端绑定:在服务器端录入用户信息的时候,将用户ID、密码、IMSI、IMEI进行绑定,有远程销毁请求的时候,可以根据IMSI、IMEI去查找需要销毁的用户,然后进行相应的销毁操作。

[0048] 图2为本发明销毁方法实施例二的流程图,如图所示,本实施例具体包括如下步骤:

[0049] 步骤201,服务器接收到销毁请求并保存在列表中,销毁请求中包括用户ID,用户 ID与用户密码、IMIS和IMEI相绑定;

[0050] 具体的,如果对某个绑定的用户有销毁要求,则在调度台选中该用户,发送销毁请求CC2SS_KILL_USR_REQ给服务器,销毁请求携带被销毁用户ID。

[0051] 服务器收到调度台的销毁请求后,在这三个表中PTT_HEAP.ZXYongHu_Record, PTT_HEAP.YongHu_Record, PTT_DISK.YongHu_Info查找到该用户,并设置该用户的销毁状态。

[0052] 步骤202,移动终端判断销毁标志为否,向服务器发送销毁查询消息,销毁查询消息中包括移动终端的第一IMSI和第一IMEI;

[0053] 具体的,终端启动销毁服务后,若销毁标志destroy为false,则以第一时间间隔,例如120秒给服务器发送销毁查询消息询问有无销毁要求,发送的销毁查询消息包括第一

IMSI信息,以及第一IMEI信息,优选的是经MD5加密后的第一IMSI信息,以及第一IMEI信息。

[0054] 步骤203,服务器根据第一IMSI和第一IMEI查找所绑定的用户ID;

[0055] 具体的,服务器收到销毁查询消息后,通过消息中携带的第一IMSI信息,以及第一IMEI信息验证绑定关系,在验证合法后,通过绑定关系找到终端对应的用户ID,并在PTT_HEAP.YongHu_Record表中通过用户ID查找是否有销毁该用户的销毁请求记录。

[0056] 步骤204,服务器在列表中查找到第一用户ID,将列表中保存的用户ID对应的第二IMSI,并将加密后的第二IMSI发送给移动终端;

[0057] 步骤205,移动终端判断加密后的第二IMSI与本地的加密后的第一IMSI一致,则移动终端进行销毁处理。

[0058] 具体的,当移动终端得到服务器返回的销毁确认消息KILL_USR_CNF_MSG,判断服务器返回消息中携带的所要销毁手机的经MD5加密后第二IMSI信息是否与现有设备加密后的第一IMSI一致,如果相等且销毁标志位为1,则启动销毁流程。

[0059] 销毁处理就是将本地保存的信息删除,例如删除数据库文件中的信息,清空SharedPreferences保存的所有变量(包括用户账号、密码、IMEI、IMSI、设置项),然后将销毁标志destroy设置为true,保存入SharedPreferences中。

[0060] 如果网络正常,则将软件销毁时间发送到服务器。杀死当前进程,以及正在运行的view层、service层进程。

[0061] 如果下次希望再次登录的时候,则会提示“软件已经自毁,请卸载后重新安装!”,将无法进入本应用,软件禁止使用。

[0062] 本发明的销毁方法可以方便的利用本地检测进行自销毁,或者利用服务器侧启动销毁,将移动终端所保存的信息销毁,从而可以有效的保护移动终端的信息安全。

[0063] 专业人员应该还可以进一步意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0064] 结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执行的软件模块,或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0065] 以上所述的具体实施方式,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施方式而已,并不用于限定本发明的保护范围,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,均应包含在本发明的保护范围之内。

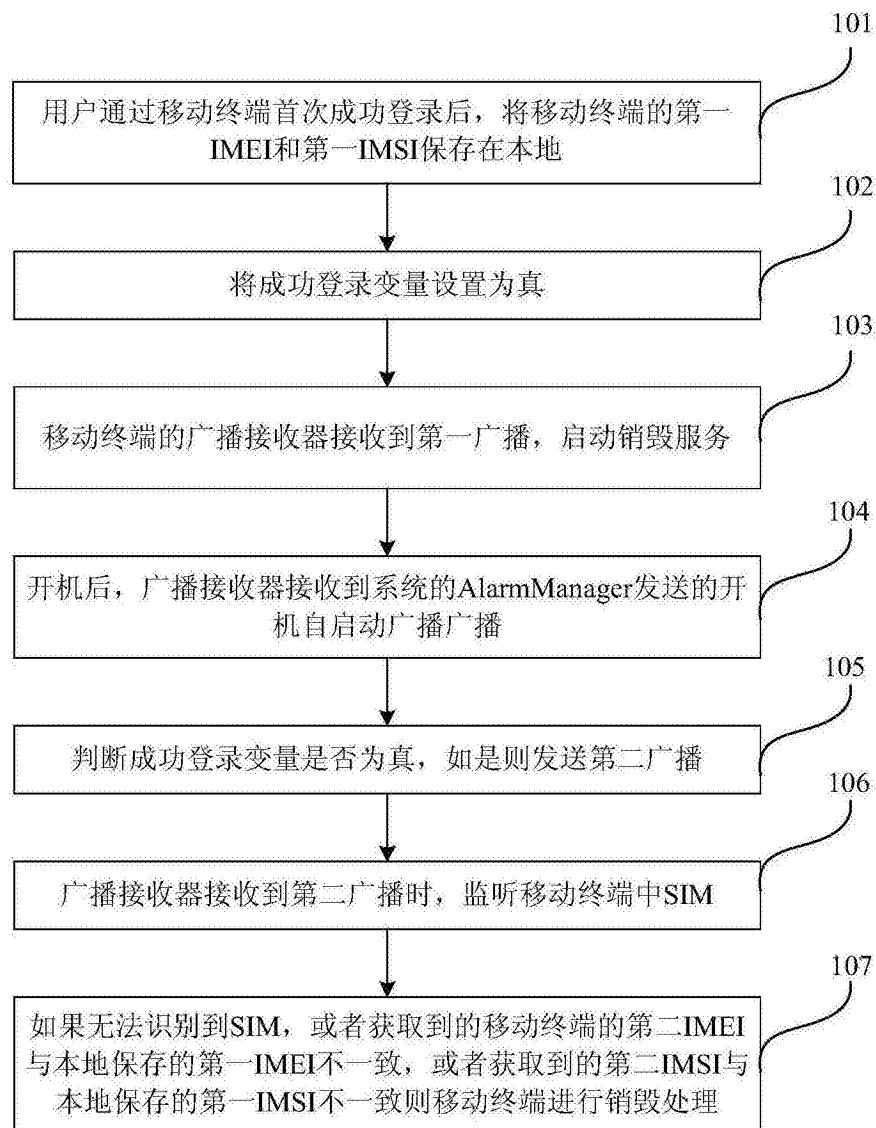


图1

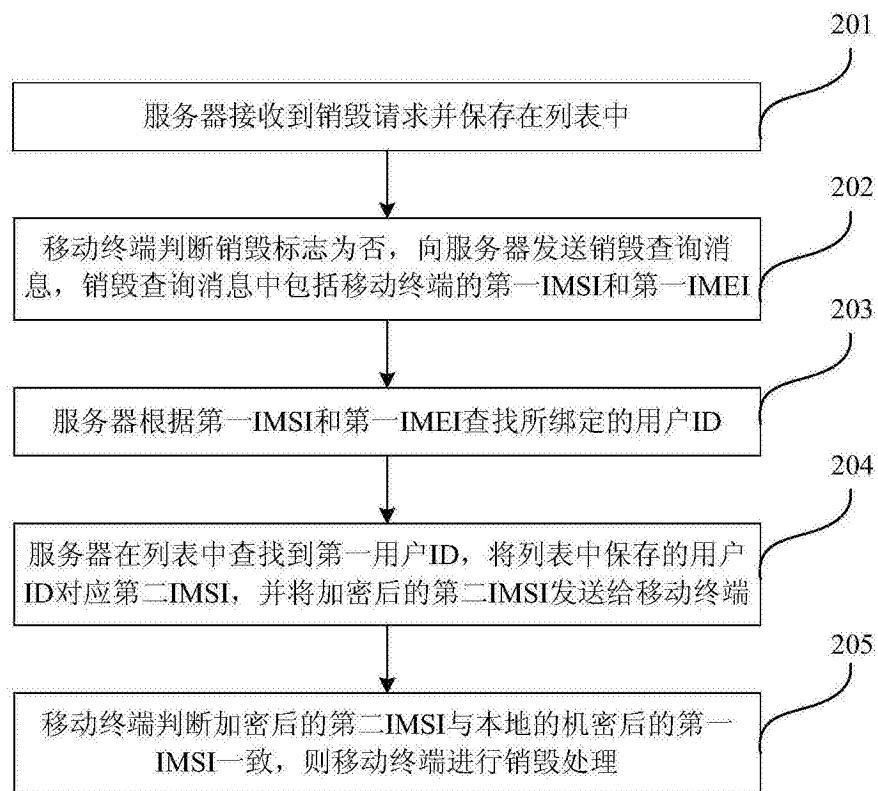


图2