

手机监控防盗模型的研究

石彦华,孔国利

(中州大学 信息工程学院,河南 郑州 450000)

摘要:如何找回被盗手机和手机中的被盗信息,一直是困扰手机用户的难题。基于此问题,文中提出了监控防盗法,帮助被盗手机用户找回被盗手机和被盗手机的重要信息,减少用户的重大损失。依据当前手机防盗策略的现状,首先给出了密码防盗法、报警防盗法、终端防盗法的相关概念和目的及其优缺点;然后基于上述三种防盗法优缺点,提出了监控防盗法及其基本思想和优点;接着从监控防盗模型和技术逻辑架构角度,阐释了技术的实现方案,并给出了监控防盗模型、逻辑架构和实现过程等;最后结合具体的项目案例,使用监控防盗法,用户只需上网注册即可实时查找被盗或被丢的手机和手机信息,给用户带来极大的安全感,验证了监控防盗模型的有效性和灵活性。

关键词:监控;手机;防盗;盗贼

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2016)03-0126-04

doi:10.3969/j.issn.1673-629X.2016.03.030

Research on Phone Monitoring Anti-theft Model

SHI Yan-hua, KONG Guo-li

(College of Information Engineering, Zhongzhou University, Zhengzhou 450000, China)

Abstract:How to recover the stolen mobile phone and its stolen information is still an open issue, which has troubled users always. Based on this, a Monitoring Anti-Theft (MAT) way is proposed to help mobile phone users for recovery of stolen mobile phones and stolen important information to reduce the significant losses. First, the concept, aim, and merits and demerits of Password Security Method (PSM), Alarm Security Method (ASM) and Terminal Security Method (TSM) are given based on the phone anti-theft situation. And then MAT way and its basic thought and merits is proposed based on the advantages and disadvantages of the above three kinds of anti-theft method. Thirdly, from the point of view of the security model and the technical logic structure, the implementation scheme of the technology is explained, and specific MAT mode, logical architecture and implementation processes are given. Finally, an application example is given to show the flexibility and validity of MAT model, which is that user can search to the stolen or lost mobile phone and its information to bring a great sense of security by using monitoring anti-theft method.

Key words: monitoring; phone; anti-theft; robber

0 引言

伴随着社会的发展,手机已经进入人们的生活。据官方数据统计,到2015年,世界上有手机的用户量将达到全球人口的一半,而中国作为全球最大的手机市场,手机用户量在今年的第三季度将突破五亿大关。手机的发展突飞猛进,给人们的生活带来了便捷和效率,但是手机的丢失和被盗,同时也给用户造成了重大损失。

如今如何找回被盗手机和手机中的被盗信息,成为当前人们面临的一个重要课题^[1]。

1 相关研究

当前手机被盗或手机意外丢失是经常发生的事情,这给手机用户造成了重大损失^[2-3]。针对此种情况,人们采用了不同的方法,归纳起来有三种:密码防盗法、报警防盗法、终端防盗法。

(1)密码防盗法。该方法主要是在被盗手机的软件中附加一段防盗程序,一旦手机被盗,被盗用户立即发送一条防盗信息,激活防盗程序,进而使被盗手机的全部功能锁定,无法使用该手机,除非有相应的密码进行解锁。该方法的优点是保密性比较强,缺点是防盗程序容易被破解或被格式化,进而起不到防盗功能,用

户无法获知被盗手机的位置信息和盗贼者信息^[4-5]。

(2)报警防盗法。这种手机本身具有防盗报警功能。一旦手机被盗或丢失,按下随身携带遥控器的防盗键可就近寻找手机;当机主处于危险境地可按遥控器上的触发器,触发被盗手机自动拨打报警号码。该方法的优点是实用性强、操作方便、隐蔽性好。缺点是一旦被盗手机没电、电池被拔掉或超出报警防盗范围圈,报警功能全部无效;用户无法获知被盗手机的位置信息和盗贼者信息^[6-7]。

(3)终端防盗法。该方法主要是通过在手机终端启用安防措施,获取盗贼信息和被盗者信息并发送给真正的用户,从而达到防盗的目的。关键的步骤有两步:怎样启用安防措施、怎样获取盗贼信息和被盗者信息并发送给真正的用户。目前启用安防措施主要是通过身份验证的方式实现;获取被盗信息和盗贼信息主要通过第三方软件实现。该方法的优点是实时性强、方便、快捷性好。其缺点是安防措施容易被盗贼禁用,从而使终端防盗法无效;或由于预设号码无效或被修改,造成用户无法收到被盗者信息^[8-9]。

2 基本思想

文中针对此三类情况,提出监控防盗法。监控防盗法主要通过手机监控平台对被盗手机进行实时监控,然后监控平台向被盗用户报告被盗手机的信息和盗贼的信息。它的优点是盗贼无法禁用安防措施,一旦手机上电就会和手机监控平台建立监控关系;其次是盗贼无法修改预设号码或使它无效,因预设号码不是设置在被盗手机中,而是设置在监控平台中;最后,用户查询被盗手机信息的方式多样化,通过网页、短信、彩信或电话的方式向用户报告被盗手机信息和盗贼信息^[10]。

3 监控防盗平台设计

从监控防盗的模型和逻辑架构角度阐释技术方案,最后给出具体实现步骤^[11]。

3.1 监控防盗模型

监控防盗法的模型包括四部分:用户、手机监控平台、被盗手机、公安机关。它的模型结构如图1所示。

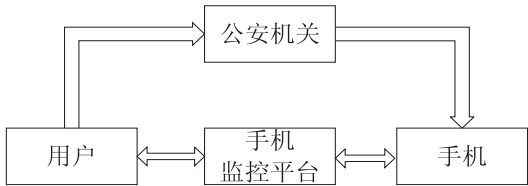


图1 监控防盗模型

用户是指被盗手机的用户,他需要向手机监控平台提供手机的相关参数信息,比如手机型号、入网许可

号、监控编号等。这些信息在手机说明书中都可查到。

手机监控平台包括三部分:服务容器、数据库、后台监控。它主要负责查找被盗手机的信息和盗贼的相关信息,同时向用户和公安机关报告。

服务容器中包括日志服务、注册服务和运行管理服务。日志服务主要负责记录被盗手机终端和监控平台中心的交互信息、各个服务代理的状态和操作信息和用户的注册相关信息;注册服务负责对用户的注册信息进行管理和整理;运行管理服务负责对各个服务代理进行管理和操作。数据库模块负责汇集整理并存储手机监控平台的各种信息和资源。后台监控部门负责对数据库中的被盗手机的监控信息进行分类管理和以网页的形式向用户进行展示,包括被盗手机的存储信息、盗贼的监控信息、服务代理的信息、相关日志和服务注册的信息。这样用户在有网络的地方就能实时查看自己被盗手机的信息和盗贼信息,从而弥补自己因手机被丢所造成的重大损失^[12]。

被盗手机中有监控模块终端,手机只要上电它就会自动启动运行。该监控模块终端存储了手机型号、入网许可号、监控编号等手机说明书中重要参数信息。一旦手机监控平台向它发出信号,它就会自动和监控平台建立监控关系,并报告当前的手机卡信息,联系人,通话记录、短信,基站地理信息,以及通过摄像头采样的图片信息等^[13]。

公安机关是辅助部门,负责帮助用户找回被盗手机。

3.2 监控防盗的逻辑架构

监控防盗法的逻辑架构包括四个阶段:手机注册服务、启动后台服务、手机数据库服务、后台监控服务。它的总体逻辑架构如图2所示。

(1)手机注册服务阶段。用户需要向手机监控平台提供手机说明书中相关参数信息,例如手机型号、入网许可号、监控编号、预设号码、身份证号、住址、姓名等。用户注册完成后手机监控平台会自动生成一个服务代理,它在运行管理服务器启动时被启动,专门负责查找该被盗手机。

(2)启动后台服务阶段。主要是在手机监控平台上启动三个服务:日志服务、注册服务和运行管理服务。日志服务主要负责记录被盗手机终端和监控平台中心的交互信息、各个服务代理的状态和操作信息和用户的注册相关信息;注册服务负责对用户的注册信息进行管理和整理;运行管理服务负责对各个服务代理进行管理和操作。启动日志服务主要是记录各个服务代理的操作信息,以便系统查找还原;启动注册服务主要是让各个服务代理(每个服务代理就是一个线程)运行起来,去完成各自的工作;启动运行管理服务

主要是让它管理各个服务代理,如启动、暂停、删除、激活等。

(3)手机数据库服务阶段。主要是记录手机的数

据信息,包括注册服务器记录信息、日志服务器记录信息、运行管理服务器记录信息等。

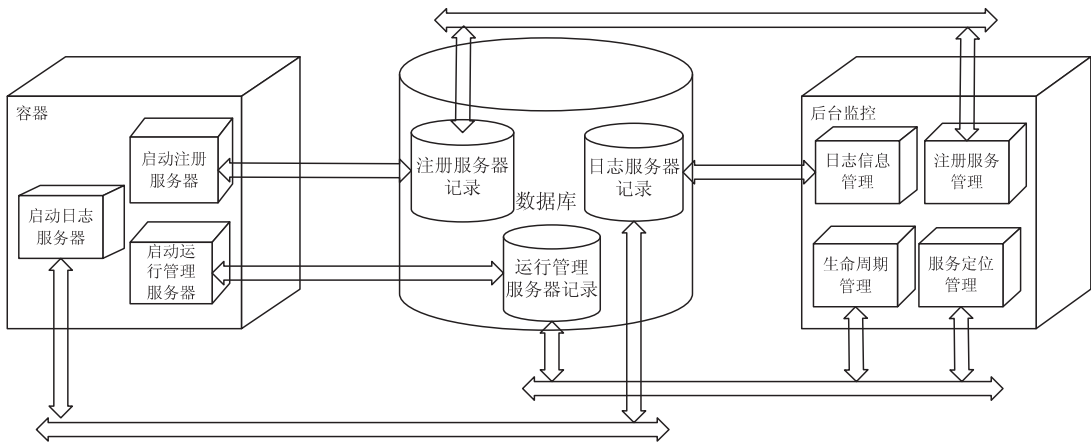


图 2 监控防盗逻辑架构

(4)后台监控服务阶段。以网页的形式,手机监控管理员负责对注册服务器记录信息、日志服务器记录信息、运行管理服务器记录信息进行管理。同时,对服务代理的生命周期、执行状态、执行结果查看监控。最后,以网页、短信、彩信或电话的方式向用户报告被盗手机信息和盗贼信息。

3.3 监控防盗的实现步骤

- 监控防盗法的具体执行过程如下：
- Step1: 用户向手机监控平台注册被盗手机信息, 自动生成一个新的服务代理；
 - Step2: 启动后台监控服务包括日志服务、注册服务和运行管理服务；
 - Step3: 被盗手机终端一旦上电开启, 新的服务代理就开始监控该被盗手机；
 - Step4: 手机监控平台查找到该被盗手机并记录手机信息和盗贼信息；
 - Step5: 以网页、短信、彩信或电话的方式向用户报告被盗手机信息和盗贼信息；
 - Step6: 用户通过公安机关找回被盗手机。

4 应用实例

监控防盗法相对其他防盗法而言,具有方便、快捷、实时性强的特点。一旦用户手机被盗或丢失,即可上网进行注册,登记手机相关信息。然后就可以在网上实时查询自己手机上存储的重要信息和盗贼的相关信息,或者向手机监控中心打电话进行咨询。最后用户通过公安机关,找回自己被盗的手机。下面给出具体说明。

当用户手机被盗后,可以上网注册被盗手机信息。监控后台会自动为你生成相应的服务代理,时刻监控被盗手机的相关信息。用户注册页面如图 3 所示。



图 3 用户注册

用户注册的各个服务代理,都运行在监控后台服务器中。为了激活各个服务代理,需要在监控后台启动相关服务后,各个服务代理才具有相应的生命周期,在监控后台中执行任务。在监控后台启动的服务有日志服务、注册服务和运行管理服务。

启动监控后台服务后,用户注册的各个服务代理开始查找被盗手机信息和盗贼信息。后台监控管理员可以对各个服务代理进行启动、暂停、删除、激活等管理操作,同时也可以查看到各个服务代理的信息、盗贼信息和被盗手机信息。而用户只有注册缴费后才可以查看到其手机信息和盗贼信息。图 4 给出了服务操作管理页面。

5 结束语

使用监控防盗法,可实时获取自己手机上的重要信息,以免造成重大损失;同时实时监控盗贼信息,以便及时获取自己贵重手机^[14]。使用监控防盗法,用户



图 4 服务操作管理

只需上网注册即可实时查找到被盗或被丢的手机和手机信息,实时性强、方便、快捷性好,给用户带来极大的安全感。

参考文献:

[1] Wiegand T, Sullivan G J. Overview of the H. 264/AVC video coding standard[J]. Transactions on Circuits and Systems for Video Technology, 2003, 7(13): 560-576.

[2] 杨鑫, 牛建伟, 胡建平. 一种基于 H. 264 的智能手机监控系统设计与实现[J]. 微电子学与计算机, 2006, 23(9): 118-119.

[3] 李曙光, 张琼声, 李文琳. 嵌入式 Linux 系统智能手机防盗追踪功能的实现[J]. 微计算机应用, 2007, 28(11): 1229-1232.

[4] 李海宁. 基于 H. 264 的智能手机监控系统的设计与实现[D]. 大连: 大连理工大学, 2009.

[5] Harrison R. Symbian OS C++ for mobile phones (vol1)[M]. London: Symbian Press, 2004.

[6] 钟萃芳. Windows Mobile 平台手机防盗系统的设计与实现[D]. 北京: 北京邮电大学, 2010.

[7] Richardson I E. H. 264 and MPEG-4 video compression video coding for next-generation multimedia[M]. London: John Wi-

ley & Sons Ltd, 2004.

[8] 高鹏. Symbian 平台手机防盗系统的设计与实现[D]. 北京: 北京邮电大学, 2010.

[9] 莫哈飞, 王春东, 冯超然, 等. 基于安卓的手机防盗追踪与隐私控制系统的研究[J]. 天津理工大学学报, 2014, 30(3): 21-25.

[10] Ohana D J, Phillips L, Chen Lei. Preventing cell phone intrusion and theft using biometrics[C]//Proc of security and privacy workshops. San Francisco: IEEE Press, 2013: 173-180.

[11] 赵银龙, 宋晖, 任建军, 等. 基于手机传感器的智能防盗与用户认证[J]. 智能计算机与应用, 2015, 5(1): 101-104.

[12] Buhlmann P, Hothorn T. Boosting algorithms: regularization, prediction and model fitting[J]. Statistical Science, 2007, 22(4): 477-505.

[13] 周非, 叶超龙, 张贵棕. 一种利用 IMSI 检测和人脸识别的手机防盗追踪系统研究[J]. 计算机应用研究, 2015, 32(3): 895-899.

[14] Zhang Dedong, Ma Zhaofeng, Niu Xinxin, et al. Anonymous authentication scheme of trusted mobile terminal under mobile Internet[J]. The Journal of China Universities of Posts and Telecommunications, 2013, 20(1): 58-65.