企业 iOS 移动设备管理（MDM）的研究与实现

文/涂源源　黄坚

摘要

近年，移动智能终端在企业信息化进程中得到迅速的普及和应用，提高了企业办公效率，但也引发了一系列安全问题。企业移动设备及应用的管理已成为迫在解决的问题。本文对该问题所涉及的的两大核心技术进行了分析；对研究问题进行剖析，提出解决方案，并最终加以实现。

【关键词】移动互联　企业信息化　iOS　APNS　MDM

1 前言

随着移动互联的快速发展，同时 iOS 操作系统的易操作、安全等特点，企业内部办公系统也从原来传统的 PC 台式机走向各大 iOS 智能终端；使用户可以随时随地进行办公。但安装了企业内部应用的移动设备会包含大量企业、商业及私人信息，设备的遗失或被盗将可能给企业和个人带来灾难性的损失，因此实现对移动设备的管理显的异常重要。

实现对移动设备的管理，需要相应的后台 MDM（移动设备管理）系统，负责移动设备的信息采集和管理。此时研究和解决的难点包括：建立设备和服务器之间的长连接，实现 MDM 消息的推送，设备的认证，抹去移动设备上的数据等。

2 APNS及MDM技术

实现对 iOS 移动设备的管理，需要 APNS（苹果消息推送）和 MDM 两大核心技术，本节将对二者进行扼要分析。

2.1 APNS技术

APNS 是苹果的一种消息推送机制，它能够向指定的设备推送指定的消息，设备令牌与电话号码类似，通过设备令牌就可在 APNS 注册的设备中找到对应的设备，然后向该设备推送消息。推送的消息是一个 JSON 格式的数据，其有规整的格式，各 Key 有着不同的含义，设备在接受到消息后会相应响应一些操作。iOS 消息推送的工作机制概括如图 1：

2.2 MDM技术

图 1：iOS 消息推送机制

图 2：MDM 移动客户端功能框架

MDM 使企业 IT 部门能完全控制和管理员工各类的移动设备群，通过它，企业可以安全、有效地管理所有 iOS 设备，并能确保所有移动设备及其所安装的应用和所保存信息的安全，同时可对数据进行一系列操作，实现一个企业内部的 AppStore。

iOS MDM 架构需要移动设备进行通信，移动设备管理服务器使用苹果推送服务。它是一个轻量级的可扩展服务，提供了一种唤醒设备的方式，该服务可以登录 MDM 服务器进行查询挂起的操作、未应答的询问等。同时借助苹果推送通知服务，MDM 服务器不但能与设备保持长连接的通讯，而且不会影响设备性能和电池的使用时间。

3 企业iOS移动设备管理研究问题的分析

本节将会对本文研究问题进行分析，首先，介绍 iOS MDM 基本控制流程，对五大关键步骤进行说明；然后做进一步分析，提炼出解决该研究问题的核心点，得出基本解决思路和方法。

iOS MDM 基本控制流程，分为五大步骤：

第一步：MDM 服务器发送一个 MDM 推送信息给推送服务器，该信息需推送服务器中转给设备，通知设备此时服务器需要该设备执行相关命令了，设备根据命令做出相应的判断和反应。

第二步：推送服务器通知 iOS 移动设备。

第三步：当设备空闲，且处于连网状态时，会去连接 MDM Server 并告诉服务器移动设备的状态。

第四步：MDM Server 根据设备状态返回给设备需要执行命令。命令是 xml 格式的 plist 文件。

步骤五：设备实行了命令，并将执行情况连接 MDM Serverf，反馈给 MDM Server。

其中难点主要集中在如何搭建推荐服务器、MDM 服务器以及终端的设备的认证。关键点包括 MDM Server 与终端的通信方式、SCEP（简单证书注册协议）。实现 MDM 后台对移动终端或应用安全管控的前提条件，就是建立 MDM 平台与终端之间的通信。

从消息的可靠性、经济性、及时性、设备资源开销等方面考虑。使用各手机平台自带的 push 服务是最方便、最可靠的方式。对于那些没有提供 push 服务的移动平台，我们可搭建单独的推送服务器来实现消息推送的功能。

同时，在一个 MDM 平台整个设备管理过程中，都需要通过数字证书服务的方式，来实现对终端用户的身份认证；通过锁屏、恢复出厂设置等来实现终端的认证和管理。SCEP 是 PKI（公钥加密技术）协议体系的一部分，它

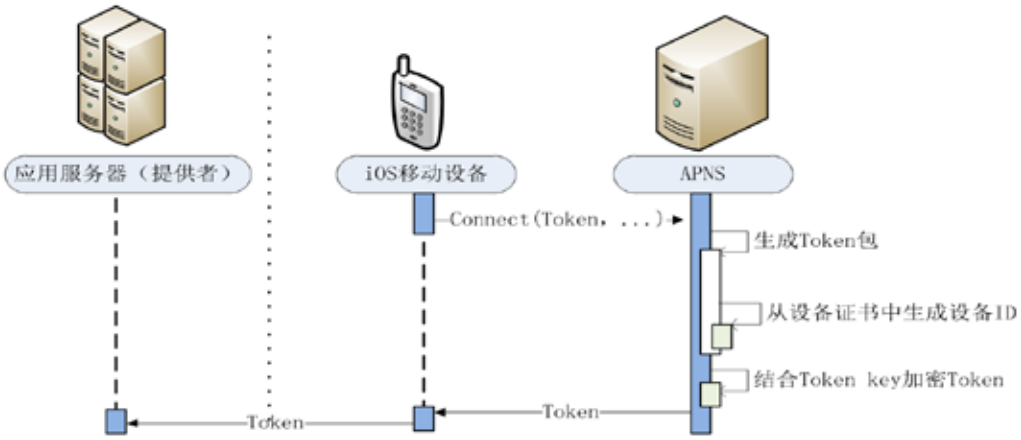

图 3：MDM 中 iOS 设备注册流程

能够安全可靠地为网络设备提供数字证书，通过它可以实现 MDM 平台对移动终端设备的身份认证。

综上，我们将通过推送服务技术来实现 MDM Server 和 iOS 终端设备的通信，通过 SCEP 来实现移动终端设备身份的认证。

4 企业iOS移动设备管理的实现

本节主要在前文对本研究问题分析的基础上，首先介绍 MDM 移动客户端功能框架，如图 2 所示，然后对 iOS 移动设备管理给出具体解决方案，并加以实现。

iOS 客户端 MDM 的主要功能如下：

（1）收发消息：负责通过 APNS 服务器与终端建立的长连接接收和发送消息。

（2）解析及封装通信协议：确保 MDM 服务器和 iOS 客户端可通过网络进行通讯，负责解析与封装二者之间通信协议。

（3）终端控制管理：实现 iOS 移动终端对移动端指令的管理和相应操作，如，恢复出厂设置、删除数据、密码设置、加密存储等。

（4）管理 Certificate 及策略文件。终端欲实现 MDM 功能，此时需要从 MDM 服务器下载和安装相关证书及管理设备的策略文件，那么此时我们需要对它们进行管理，该功能就可以实现这些。

（5）任务管理与分发。在 iOS 客户端获取了若干任务指令后，那么如何按照时间的先后顺序对这些任务进行管理和分发，让各项任务在客户端顺序执行，任务的执行预示着将执行相应命令完成相应的工作，同时每执行完一个任务需要进行反馈，如此迭代直至客户端收到的任务命令全部执行完毕。

iOS 平台可以通过在浏览器输入 MDM 平台下发的 URL 地址，进行证书、预置描述文件和管理策略文件的下载，同时可以完成对证书与预置描述文件的安装，最终实现了移动客户端 MDM 应有的功能，我们不需要额外开发 MDM 终端。

4.1 iOS平台实现MDM的前提工作

首先，我们注册 Apple 企业者账号（需花费 299 美元），成功一位企业级开发者，申请创建 MDM 证书；然后，搭建 MDM 服务器 https 环境；最后，通过借助“钥匙串工具”生成 MDM 推送 格式证书和描述文件（服务器要借助着两个文件完成对接 APNS）。

4.2 搭建MDM服务器和推送服务

通过上文的分析，本文的 MDM 整体框架包括三部分：MDM Server、推送服务器和移动终端。所以要想实现对 iOS 移动设备的管理，在已经实现移动终端 MDM 功能的前提下，还需要搭建 MDM 服务器和推送服务器。

本文的 MDM 服务器是采用 .Net 语言开发和实现的，实现了用户的注册和管理，实现对移动设备的注册，信息采集，移动设备的管理，同时可以向移动终端提供各种设备操作的指令，如：锁定设备、抹去应用数据、注销设备、强制退出；实现了对证书、设备管理决策文件、预置描述文件的管理等；实现了 MDM 服务器和推送服务器的对接，实现二者之间的通信。

本文的推送服务器是借助于苹果的 APNS 加以实现，APNS 也在前文进行了解释说明，此处不再细述，通过这种方式来实现 MDM 服务器与设备的长连接通信，此以保证终端接受平台指令。

4.3 设备注册和令牌Token的获取及传递

实现 MDM 功能，iOS 设备需要在我们自己的服务器和苹果服务器上完成设备的注册。iOS 移动端和 服务器以及 APP 应用服务器和 服务器都需要通过证书才能建立有效的连接，完成各自的功能等。证书的获取和配置由于篇幅在此不作说明。

当 iOS 程序配置了 MDM 证书（支持推送），应用程序启动后，应用程序通过相关代码让 APP 携带设备序列号连接 APNS 服务器进行注册，一旦注册成功，苹果推送服务器会返给我们一个设备令牌 Token，获取到 Token 之后，程序通过接口将 Token 及设备的其他信息提交到我们的前 MDM 服务器，服务器收到信息后，首先查看信息与设备的有效性，一旦合法有效，则完成设备在我们应用的服务器上的注册，其流程如图 3 所示。

5 结束语

通过对理论的研究，本文最终实现了对 iOS 移动设备的管理，经过长时间的测试与使用，该功能各项指标及性能均满足需求和预期研究效果。但消息推送的稳定性还需要进一步提高。

参考文献

[1] 王卫东．企业移动设备安全管理方法与实践 [J]．计算机安全，2011(11)：44-47.

[2] 杭建．移动终端设备管理技术的研究与实现 [D]．西安：西安电子科技大学，2013.

[3] 许丽萍．MDM 引领移动信息化变革 [J]．上海信息化，2013(7)：59-61.

[4] Erica Sadun. The iPhone Develop Cookbook: Building Application with the iPhone SDK[M], USA, 2009.

[5] 肖荣，富杰．基于 push 机制的 MDM 平台研究 [J]．互联网天地，2013(05)：49-54.

作者简介

涂源源（1987-），男，硕士研究生学历。软件工程，北京航空航体大学软件学院。

作者单位

北京航空航天大学软件学院　北京市　100000