

移动办公终端信息安全技术研究

董晶晶^{1,2}, 霍珊珊^{1,2}, 袁 泉^{1,2}, 孙 琪^{1,2}, 刘艺翔^{1,2}

(1. 中国电子科技集团公司第十五研究所 北京 100083;

2. 信息产业信息安全测评中心, 北京 100083)

摘要:随着移动互联网的快速发展和移动智能终端的广泛应用,移动智能终端在人们社会、经济生活中的重要性日益凸显,同时移动智能终端也逐渐进入企业办公领域,越来越多的办公应用会运行在移动终端上,越来越多的员工也会通过移动终端来处理日常工作事宜,从而实现移动办公,提高工作效率。移动办公终端作为实现移动办公的重要组成部分,由于接入的开放性、灵活性和终端的多样性,其安全问题一直备受关注。首先对移动办公终端面临的安全问题进行分类,分析不同类别安全问题及其可能的应对策略,在此基础上,对比分析基于沙箱防护和双系统两种移动办公终端安全技术,并验证了两种移动办公终端技术的特点和安全性。

关键词:移动办公;沙箱;双系统;信息安全

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2018)01-0155-04

doi:10.3969/j.issn.1673-629X.2018.01.033

Research on Information Security Technology of Mobile Office Terminal

DONG Jing-jing^{1,2}, HUO Shan-shan^{1,2}, YUAN Quan^{1,2}, SUN Qi^{1,2}, LIU Yi-xiang^{1,2}

(1. No. 15 Research Institute of China Electronics Technology Group, Beijing 100083, China;

2. Information Technology & Security Test Evaluation Center, Beijing 100083, China)

Abstract: With the rapid development of mobile Internet and the extensive application of mobile intelligent terminal, mobile intelligent terminal has played an important role in people's social and economic life. In the meantime, it has gradually entered the field of business office, where more and more applications will be running, and more and more staffs will handle the daily work, so as to realize mobile office and improve work efficiency. As an important part of mobile office system, mobile office terminal has been concerned in security because of its openness and flexibility of accessing and diversity of terminals. Firstly, we classify the security problems of mobile office terminal, and then analyze them with different categories and their possible strategies. On the basis, two mobile office terminal security technology like sandbox-based and dual system are compared, and their characteristics and security are verified.

Key words: mobile office; sandbox; dual system; information security

0 引言

随着移动互联网技术的飞速发展,移动智能终端设备的功能越来越强大,移动智能终端在人们的工作和生活中扮演着越来越重要的角色。移动智能终端为企事业单位提供了更为丰富的办公渠道、提高了工作效率,同时,也为企事业单位保护和维持系统安全、数据安全带来了更大的挑战。移动智能终端接入办公网络,要考虑的安全包括移动终端安全^[1-4]、通信网络安全、移动接入区安全三部分。接入部分的安全使用传

统的安全技术手段就可以解决,如部署边界防护设备等,而对于移动终端安全和通信网络安全,不是简单部署一套移动办公终端管理系统对终端进行监测和管理就能解决的,移动办公终端自身的安全性更加值得关注。

文中首先对移动办公终端面临的安全问题进行分类,分析不同类别的安全问题及其可能的应对策略,然后对比分析基于沙箱防护和双系统两种移动办公终端安全技术,并验证两种技术方案的有效性,最后对研究

收稿日期:2017-02-25

修回日期:2017-06-27

网络出版时间:2017-10-19

基金项目:国家质量基础的共性技术研究与应用重点专项(2016YFF0204003)

作者简介:董晶晶(1983-),男,工程师,硕士,CCF会员(19850M),从事信息安全产品及软件系统检测、标准与技术规范制定、信息安全咨询培训等方面的工作。

网络出版地址: <http://cnki.net/kcms/detail/61.1450.TP.20171019.1626.068.html>

成果进行总结展望。

1 移动办公终端安全问题及应对策略

1.1 非法移动终端接入

由于移动办公场景的多样性、灵活性以及无线接入的开放性,导致内部的重要数据资源处于一种完全暴露的状态。如果在用户接入时,不能对接入终端合法性进行有效鉴别,将导致非法移动终端通过伪装身份后,接入内部网络访问内部重要资源,导致信息泄露。使用不易伪造的终端设备及严谨的终端管理和认证方式,确保接入终端的合法身份,最大程度防止非法接入。

1.2 移动终端恶意程序侵入

移动设备随时随地联网的特性,如果对其安全防护不够,很容易遭受恶意程序的攻击。目前,针对移动终端恶意程序大肆传播,在终端设备后台执行静默安装,不仅能够窃取终端设备隐私、敏感数据甚至能够进行远程控制,造成内部重要信息资源和数据被窃的安全风险。对移动终端应用程序进行严格的管理和监控,实现应用的合法安装和运行,避免引入恶意程序。

1.3 移动终端企业数据和个人数据混合存储

移动终端设备企业内部数据和个人数据不加以区分存放,而且通常是明文存储,容易导致数据丢失和被盜,轻易被非法使用,造成内部数据泄露。移动终端连接内部网络时,实现内部数据与其他数据隔离存放,并且进行加密存储,避免数据外泄。

1.4 移动终端不安全连接

移动办公终端访问内部网络资源时,数据在无加密的传输通道或以明文方式进行传输时,使得数据容易被窃听或篡改。同时,由于无线网络的开放性和恶意接入点的存在,更是增加了移动办公终端接入的安全问题,给内部数据的保护带来了隐患。因此,一方面需要对移动终端连接无线网络进行严格管理;另一方面,移动办公终端连接内部网络时,强制执行安全连接和加密传输,最大限度地避免传输数据泄露。

1.5 移动终端丢失泄密

移动终端设备体积较小,携带方便,在便捷的同时也容易丢失或被盜,非法获取者可能获取终端中存储的敏感数据,甚至利用终端设备保存的信息冒充使用者身份访问内部系统和数据,造成内部数据被窃和泄露。在移动办公终端丢失或处于不可信状态时,终端自身应具有安全保护措施,确保其存储的敏感信息不被非法获取,其合法身份信息不被非法使用。

2 移动办公终端安全技术研究

针对上述移动办公终端可能面临的安全隐患,为

了解决存在的安全问题,提出了两种应对技术。

2.1 基于沙箱防护的移动办公终端安全技术

沙箱^[5]是在移动终端设备系统层面运行并创建的虚拟环境,包括主屏幕、任务栏、应用程序及小组件,能够实现与外部(用户个人使用空间)应用程序及数据隔离的一种技术。沙箱通过在终端上创建安全的虚拟运行环境,将自身运行与终端本地的运行严格区分开,进行安全隔离,从而实现专门地处理内部应用程序和数据,称为“工作空间”。工作空间中通常运行着内部的一些应用程序,如内网电子邮件、内网应用、浏览器,下载和存储着内网的一些数据,而且对数据进行加密存储。沙箱外部运行个人使用的应用程序,称为“个人空间”,个人空间中的应用程序不能访问工作空间中的任何数据;工作空间中的应用程序通常也不能与个人空间中的应用程序交互或访问外部资源,但是在移动终端管控系统(MDM)授权的情况下,能够获得个人空间中数据的只读权限。

基于沙箱防护技术使得一台移动终端既可作为个人使用又可以为工作使用。通过系统层面的独立运行实现隔离,保证工作空间中的应用和数据不脱离防护沙箱的保护,减少数据泄露的风险。

2.2 基于双系统的移动办公终端安全技术

双系统移动办公终端是在一个终端上实现两个操作系统^[6-8],一个为安全系统(工作系统),一个为生活系统(个人系统),两个系统同时运行,互相隔离,兼顾工作使用和个人使用。双系统移动终端技术^[9]利用 Linux Namespaces 机制提供的基于容器的虚拟化技术,实现资源的隔离。工作系统和生活系统分别有各自独立的文件系统、应用和数据,工作系统通常安装内网的工作应用,生活系统安装个人应用,两个系统拥有各自独立的数据存储区,实现应用和数据的隔离。在工作系统内,通常还可以根据用户需求,从硬件驱动层进行限制(包括禁用工作系统的 USB 口、蓝牙和 SD 卡等),防止数据泄露。

双系统移动办公终端接收移动终端管控系统(MDM)推送的安全控制策略,实现工作系统和生活系统使用各自独立的安全策略管控,有效避免工作应用和个人应用的混淆使用,减少内部数据外泄风险。

3 移动办公终端安全技术实验

3.1 实验环境

通过实验来验证基于沙箱防护和基于双系统两种移动办公终端安全技术的特点和安全性。实验中分别使用各自支持的移动终端管控系统(MDM)实现安全策略的推送。

基于沙箱防护移动办公终端的实验环境如图 1 所

示。通过运营商提供的网络接入互联网,在访问工作内网时,需要使用 VPN 进行安全连接^[10-12]。其中,用于接收 MDM 服务器推送策略的 MDM 客户端安装在沙箱防护的外部区域“个人空间”中。

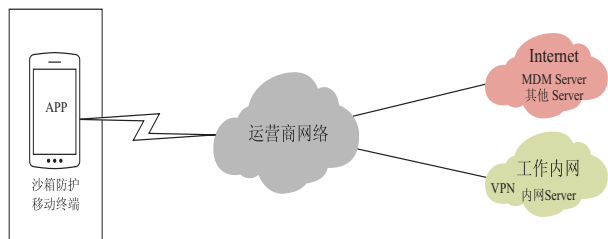


图1 沙箱防护移动办公终端实验环境

基于双系统移动办公终端实验环境如图2所示。通过运营商提供的公用 APN 接入互联网,提供的专用 APN 接入工作内网。其中,用于接收 MDM 服务器推送策略的 MDM 客户端安装在“工作系统”中。

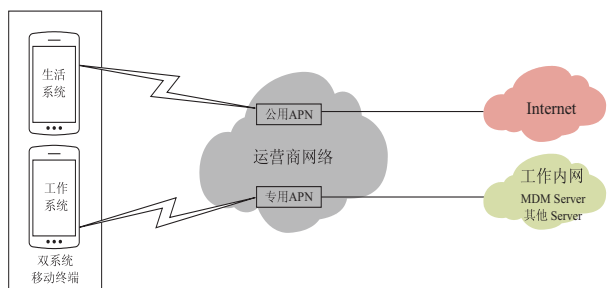


图2 双系统移动办公终端实验环境

3.2 实验过程

实验过程中,对基于沙箱防护和基于双系统两种移动办公终端安全技术提供的的安全机制分别进行了验证,包括数据隔离、应用隔离、外设控制、网络安全连接、用户鉴别认证等。

3.2.1 基于沙箱防护移动办公终端安全机制验证

(1) 数据隔离。

①通过个人空间内的应用程序访问工作空间内的数据,如:尝试通过个人空间的文件浏览类应用或社交应用访问工作空间的文档文件或图片文件等;

②通过工作空间的应用程序访问个人空间的数据,如:尝试通过工作空间的相册应用或邮件应用访问个人空间的文档文件或图片文件等;

③在 MDM 服务器上推送允许数据移动策略前,尝试将工作空间的数据移动到个人空间,尝试将个人空间的数据移动到工作空间;

④在 MDM 服务器上推送允许数据移动策略后,尝试将工作空间的数据移动到个人空间,尝试将个人空间的数据移动到工作空间。

(2) 应用隔离。

①尝试将工作空间应用程序的链接或内容分享到个人空间的程序中,验证工作空间和个人空间的

应用程序是否隔离运行^[13-14],互不影响;

②在工作空间和个人空间分别安装、卸载不同的应用,验证个人空间和工作空间的应用是否互不影响。

(3) 外设控制。

①在 MDM 服务器上推送截屏功能、摄像头功能禁止策略前,验证是否可以正常使用工作空间的截屏和摄像头的功能;

②在 MDM 服务器上推送截屏功能、摄像头功能禁止策略后,验证工作空间的截屏和摄像头功能是否能正常使用。

(4) 网络安全连接。

①在工作空间配置 VPN,并且尝试与工作内网进行连接;

②连接成功后,检查是否能够正常进行工作内网应用访问。

(5) 用户鉴别认证。

①在进入工作空间时,验证是否只有输入正确的用户鉴别信息才能成功;

②在输入鉴别信息不正确时,进行多次尝试,检查工作空间是否采取相应的锁定策略,避免进一步尝试操作。

3.2.2 基于双系统移动办公终端安全机制验证

(1) 数据隔离。

①在工作系统中产生相应数据,如执行新建文档、录制视频、保存通讯录等操作,切换到生活系统,尝试访问工作系统中的相关内容;

②在生活系统中产生相应数据,如执行新建文档、录制视频、保存通讯录等操作,切换到工作系统,尝试访问生活系统中的相关内容。

(2) 应用隔离。

①在两个系统中分别安装、卸载不同的应用,验证两个系统中的应用是否互不影响;

②在两个系统中分别运行相同的应用,使用不同账户分别进行登录,确认两个系统中相同应用的运行互不影响。

(3) 外设控制。

①分析对外设使用进行控制的相关功能,如摄像头、USB 接口、Wifi 等,验证对外设的使用是否符合 MDM 服务器设置的策略;

②修改 MDM 策略后,验证对外设的使用是否符合修改后的策略。

(4) 网络安全连接。

①在生活系统中配置公用 APN,在工作系统中配置专用 APN,检查两个系统是否能够分别接入网络;

②接入成功后,尝试在生活系统中访问互联网和工作内网,工作系统中访问互联网和工作内网,确认是

否只有生活系统能够访问互联网,只有工作系统能够访问工作内网;

③验证两个系统是否能通过更改 APN 实现两个系统的交叉访问。

(5) 用户鉴别认证。

①在进入工作系统时,验证是否只有输入正确的用户鉴别信息才能进入;

②在输入鉴别信息不正确时,进行多次尝试,检查工作系统是否采取相应的锁定策略,避免进一步尝试操作。

3.3 实验结果

对基于沙箱防护和基于双系统两种移动办公终端安全技术提供的的安全机制验证结果进行记录,如表 1 所示。

表 1 实验结果比较

结果	基于沙箱防护 移动办公终端	基于双系统移动 办公终端
数据隔离	沙箱实现数据隔离,并在 MDM 策略允许情况下,实现个人空间和工作空间数据的移动	双系统独立运行实现数据隔离
应用隔离	个人空间和工作空间应用隔离运行,互不影响	生活系统和工作系统应用隔离运行,互不影响
外设控制	工作空间中截屏、摄像头等功能使用受 MDM 策略控制	生活系统使用摄像头、USB 接口、Wifi 等受 MDM 策略控制,工作系统严格限制对外设使用
网络安全连接	终端通过公用 APN (Wifi、无线通信网络) 接入互联网,工作空间通过 VPN 实现与工作内网连接	生活系统通过公用 APN (Wifi、无线通信网络) 接入互联网,工作系统通过专用 APN 接入工作内网
用户鉴别认证	进入工作空间需要身份鉴别(如口令、指纹等),提供鉴别失败处理功能	进入工作系统需要身份鉴别(如口令、指纹等),提供鉴别失败处理功能
终端定制	需要定制终端	需要定制终端

由表 1 可以看出,两种移动办公终端技术均能实现数据隔离、应用隔离、外设控制、网络安全连接和用户鉴别认证等安全功能,同时,两种技术均需要在不同程度上对移动办公终端从硬件层面进行必要的定制,使其支持沙箱防护或双系统运行,需要依靠 MDM 提供的移动终端管理功能,实现移动终端设备的有效管理和监控。

4 结束语

针对基于沙箱防护和双系统两种移动办公终端安全技术的研究,已经取得了一定的成果,对外发布了两项技术检测规范:《ISCCC-TR-046-2015 移动终端安全域加固产品安全技术要求》和《ISCCC-TR-051-2016 双系统移动终端安全技术要求》,希望对相关技术的发展、产品研发设计以及产品检测评估起到一定的指导作用。

参考文献:

[1] 袁志坚,王春平,陈 融,等. Android 平台安全威胁及其应对策略[J]. 计算机技术与发展,2013,23(9):110-113.

[2] 宋 杰,党李成,郭振朝,等. Android OS 手机平台的安全机制分析和应用研究[J]. 计算机技术与发展,2010,20(6):152-155.

[3] 张玉清,王 凯,杨 欢,等. Android 安全综述[J]. 计算机研究与发展,2014,51(7):1385-1396.

[4] 朱佳伟,喻梁文,关 志,等. Android 权限机制安全研究综述[J]. 计算机应用研究,2015,32(10):2881-2885.

[5] 李 彬. 基于 Android 沙箱的软件行为分析系统的设计与实现[D]. 北京:北京邮电大学,2013.

[6] 蒋绍林,王金双,张 涛,等. Android 安全研究综述[J]. 计算机应用与软件,2012,29(10):205-210.

[7] 朱筱赟,胡爱群,邢月秀,等. 基于 Android 平台的移动办公安全方案综述[J]. 信息安全,2015(1):76-83.

[8] 钱海龙. 移动终端应用安全加固关键技术研究[D]. 北京:北京邮电大学,2014.

[9] BOSE A, HU X, KANG G S, et al. Behavioral detection of malware on mobile handsets [C]//International conference on mobile systems, applications, and services. [s. l.]: [s. n.], 2008:225-238.

[10] 董 钟. 面向移动办公的安全接入方法的研究与实现[D]. 北京:北京邮电大学,2015.

[11] 张 滨,赵 刚,袁 捷. 移动终端安全关键技术与应用分析[M]. 北京:人民邮电出版社,2015.

[12] 张京京,闫晓蔚,蔡建顺,等. 基于 Android 系统的手机隐私安全的研究与实现[J]. 信息安全,2012(5):59-63.

[13] KANTOLA D, CHIN E, HE W, et al. Reducing attack surfaces for intra-application communication in android [C]//ACM workshop on security and privacy in smartphones and mobile devices. [s. l.]: ACM, 2012:69-80.

[14] ENCK W, OCTEAU D, MCDANIEL P, et al. A study of android application security [C]//USENIX conference on security. [s. l.]: USENIX Association, 2011:21.