文章编号：1005-8451（2017）12-0049-06

企业移动互联网应用安全保障体系构建方案

王伟萌[1]，刘承亮[1]，朱韦桥[1]，林　珊[2]
（1.中国铁道科学研究院　电子计算技术研究所，北京　100081；
2.国网北京市电力公司　信息通信分公司，北京　100031）

摘　要：针对企业内部使用的移动互联网应用安全性问题，提出了一种适用于企业的移动互联网应用安全保障体系，作为企业移动互联网应用安全设计、开发、维护及测试的依据。通过研究移动互联网应用渗透测试技术，以获悉企业移动应用易暴露的漏洞。同时参照信息系统安全等级保护大纲内容，规划企业移动互联网应用安全保障体系，从技术安全和管理安全两个方面完善体系内容。所构建的移动互联网应用安全保障体系满足内容全面性与平台普适性需求，为形成企业移动互联网应用安全防护技术要求、检测判断准则打下基础。论文最后针对企业移动互联网应用平台化发展及其所涉及的安全问题进行了研究，这对于完善企业移动互联网应用安全保障体系具有重要的意义。

关键词：移动应用；信息安全；安全保障体系；移动平台应用安全
中图分类号：U29：TP393 **文献标识码：**A

Construction scheme of enterprise mobile Internet application security assurance system

WANG Weimeng[1], LIU Chengliang[1], ZHU Weiqiao[1], LIN Shan[2]
(1. Institute of Computing Technologies, China Academy of Railway Sciences , Beijing　100081, China;
2. Information & Telecommunication Branch, State Grid Beijing Electric Power Company, Beijing　100031, China)

Abstract: In order to improve the enterprise mobile Internet application security, a security assurance system for enterprise mobile Internet applications was proposed, which was taken as safety design, development, maintenance and test basis. This paper studied on mobile Internet application penetration testing technology to learn of enterprise mobile applications easily exposed vulnerabilities, and planed the enterprise mobile Internet application security assurance system through the outline content of classified protection of information system. The assurance system completed from the viewpoint of technology safety and management safety. The mobile Internet application security assurance system constructed in this article satisfied the requirements of content integrity and platform universality, meanwhile it was laid the foundation for the formation of enterprise mobile Internet application security protection technology, detecting and judging criteria. At the end, this paper paid attention to enterprise mobile Internet application platform development and platform security problems involved. It brought an important meaning for improving the enterprise mobile application security assurance system.

Keywords: mobile application; information security; security assurance system; mobile platform application security

随着移动互联网技术的迅速发展，移动互联网应用软件在企业得到了广泛应用。企业移动互联网应用在功能上不断扩展、业务层出不穷的同时，也面临着各种安全威胁，如企业机密信息被盗、员工信息泄露、交易内容篡改等，应用软件的安全面临着严峻挑战。构建企业移动互联网应用安全保障体系的目的在于正确指导企业移动互联网应用的设计、开发、维护及测试。目前，在移动互联网应用安全保障体系建设方面，专家学者试图不断完善体系内容，但已发表可供参考的文献不是很多。常玲[1]等人针对敏感数据暴露、鉴权机制缺陷、代码保护不足、公共组件漏洞、应用配置错误，移动应用的5个典型安全漏洞制定检查方法，但仅关注的是Android平台应用安全，并且涉及的内容不全面，无法形成体系。陈希[2]等人收集了众多移动应用漏洞点，并将这些内容归纳为了程序安全、数据安全、通信安全、业务安全4个方面，构建了较完整的移动应用安全保

收稿日期：2017-07-27
基金项目：中国铁道科学研究院重大课题（17TKT020）。
作者简介：王伟萌，研究实习员；刘承亮，高级工程师。

障体系。但该体系内容也仅仅针对 Android 应用，无法覆盖市面上全部主流系统下的应用。Himanshu D[3] 等人于 2014 年针对移动互联网应用技术安全提出了完整的安全体系，提供了移动应用安全风险和主要的安全防护手段等内容，但近年来随着漏洞不断更新，该体系已经不能保证现有移动应用安全。同时，上述成果也均未考虑移动应用安全管理层面的问题。本文针对上述移动互联网应用安全保障体系结构不完整、平台适用性差等问题，结合企业级移动互联网应用相关特征，从技术安全和管理安全两方面构建普适性的企业移动互联网应用安全保障体系，尽力实现安全保障体系的全面性、适用性。同时本文希望将移动互联网应用安全保障体系建设内容引申到企业移动平台应用软件上，面对平台应用会遇到的问题漏洞，探索安全保障体系内容的扩展。

1 企业移动互联网应用安全研究基础

1.1 移动智能终端安全管理体系

YD/T 2407-2013《移动终端安全能力技术要求》[4] 与 YD/T 2408-2013《移动终端安全能力测试方法》[5] 作为构建企业移动互联网应用安全保障体系的主要依据，其框架如图 1 所示。

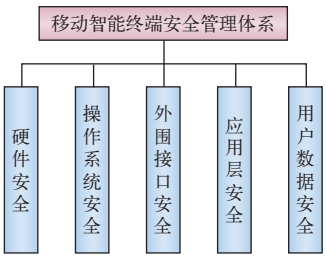

图1 移动智能终端安全能力框架

移动智能终端安全管理体系中应用层安全要求与用户数据保护安全要求提供了安全保障体系中应用安全与数据安全有关安全风险和安全防护手段的内容参考，包括终端设备权限控制、认证机制安全、密码保护、敏感数据授权使用、数据存储、数据销毁等。

1.2 移动互联网应用渗透测试技术

移动互联网应用渗透测试包括逆向审计、流量分析、数据取证、动态分析等流程。各流程实施中将客户端测试与网络测试分成两个测试领域，如图 2 所示。客户端测试划分为基于主机与基于云。基于主机是指运行在智能终端上的测试分类。而涉及复杂运算需移到远端服务器的测试分类为基于云测试。实施中又细分基于签名或基于异常两类测试技术[6]。在基于签名测试技术中，通过判断漏洞签名来识别移动互联网应用漏洞。而基于异常测试技术则是为正常安全移动互联网应用建模，判断被测试应用与正常模型是否相符。

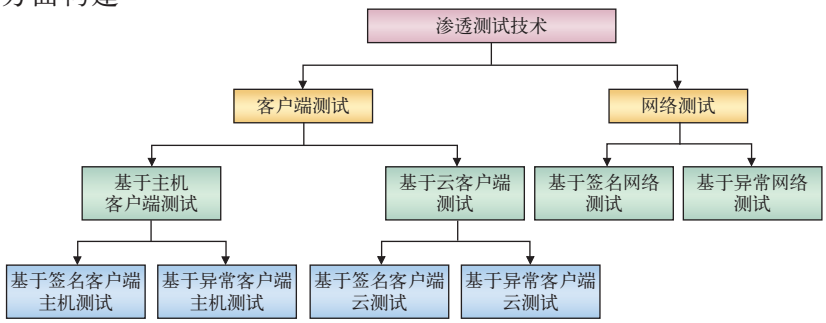

图2 移动互联网应用渗透测试分类

1.2.1 应用程序逆向源代码审计

应用程序如同一个数据和资源的归档文件，只不过是将可读源代码转换成不可读字节代码。利用 Apktool、dex2jar、jd-gui 等 Android 逆向工具及 class-dump 等 iOS 逆向工具逆向应用程序，还原源代码[7]。再对源代码进行静态分析。通过词语分析、语法分析、控制流等静态分析技术对源代码进行审计，查找应用程序中代码漏洞。

1.2.2 移动终端网络流量分析

移动终端网络流量分析的目的在于查找应用程序在网络数据中泄露的敏感信息。利用该技术检测应用程序是否通过不安全的网络协议执行身份验证和会话管理等操作。流量分析的方式分为被动和主动两种。被动分析是使用 Wireshark 等网络分析器分析捕获到的所有网络数据包，从中查找漏洞和安全问题；主动分析是通过设置代理，将应用 / 设备生成和接收的所有网络流量经由代理，拦截正在进行的网络通信，实时分析和评估流量内容。

1.2.3 移动终端数据取证

数据取证是指使用逻辑采集和物理采集等取证方法从移动终端中提取和分析数据。逻辑采集是通

过与设备交互从文件系统提取数据；物理采集是对整个物理存储介质进行逐位拷贝。数据取证便于分析敏感信息本地存储情况、应用程序数据库中敏感信息加密情况等。

1.2.4 动态分析方法

动态分析方法可实现在应用程序运行过程中检测程序的行为，从中查找存在的相关安全问题，动态分析法因其可对移动终端应用程序层和操作系统层进行全面监测[8]，所以成为渗透测试的重要补充。动态分析法可用于监测移动程序运行权限等信息。

2 企业移动互联网应用安全

企业移动互联网应用安全重点应关注3个方向：应用和数据安全、网络和通信安全以及移动应用运维管理安全。将应用和数据安全与网络和通信安全作为技术安全，将移动应用运维管理安全作为管理安全。因此，移动互联网安全问题不仅体现在软件技术漏洞，更包括了管理方面的安全问题。通过对部分企业级移动应用进行渗透测试，从测试结果信息中总结出企业在技术安全方面除关注如下常见的软件技术漏洞外，还应该注重用户身份确定及用户访问权限限制方面的安全[9]。管理安全则应涉及设计、开发、发布、维护全套移动应用产品流程。以这些漏洞问题为突破口，构建安全保障体系。

2.1 移动互联网应用仿冒

本漏洞通过对移动应用进行反编译为可读文件，从而实现软件破解、内购破解、软件逻辑修改、插入恶意代码、插入广告等破坏性操作。该问题所产生的仿冒移动应用，可能导致信息泄露或直接间接的经济损失。

2.2 敏感信息泄露

敏感信息泄露漏洞如下：

（1）常规漏洞：移动应用中最易暴露的漏洞，包括代码注入、XSS跨站脚本攻击、暴力破解等，易被攻击者利用窃取信息。

（2）不安全的通信协议：使用HTTP、FTP等不安全协议，由于这些协议存在明文传输数据、缺少访问控制等缺陷，将会导致数据泄露问题。

（3）不安全的第三方SDK或代码：未进行安全性校验的第三方SDK或代码会带来未知的安全风险，可能存在恶意操作。

（4）不安全数据存储：移动应用数据存储在本地未使用可靠的加密措施对敏感数据进行保护，数据只采用弱加密的方式，或采用不加密的方式，这便降低攻击者对数据的破解难度。

（5）不安全数据使用：使用弱口令导致数据泄露。

（6）网络钓鱼：利用经过伪装的不安全网络链接搜集信息。

（7）应用程序访问：移动应用向终端操作系统申请系统权限从而获取信息。

（8）Log日志文件：日志中往往存在传输的数据等敏感信息，导致信息暴露。

（9）不安全配置文件：允许程序被调试、允许程序备份、全局可读文件等可导致信息泄露。

2.3 会话安全问题

软件与后台服务器之间的会话被窃听、篡改、伪造，会话被录制后重放，中间人攻击，会话无法自动终止，均为严重的安全问题，会致使信息泄露。

3 企业移动互联网应用安全保障体系结构

企业移动互联网应用安全保障体系结构如图3所示。

3.1 技术安全

3.1.1 物理安全

及时更新移动应用后端服务器版本，保障服务器安全。

3.1.2 通信安全

（1）通信协议：移动应用与服务器之间利用TLS或IPSEC等协议建立安全的信息传输通道。移动应用与服务器在建立连接前，移动应用采用证书校验技术验证服务器身份。

（2）会话安全：保障移动应用与服务器之间的会话不可被窃听、篡改、伪造、重放[10]。设定会话超时时间，当会话空闲时长超出设定时间时自动终止会话。用户注销/登出后，确保会话终止的同时应注销会话凭证，清除会话信息。限制会话并发连接数，避免恶意创建多并发会话消耗系统资源。

3.1.3 设备安全

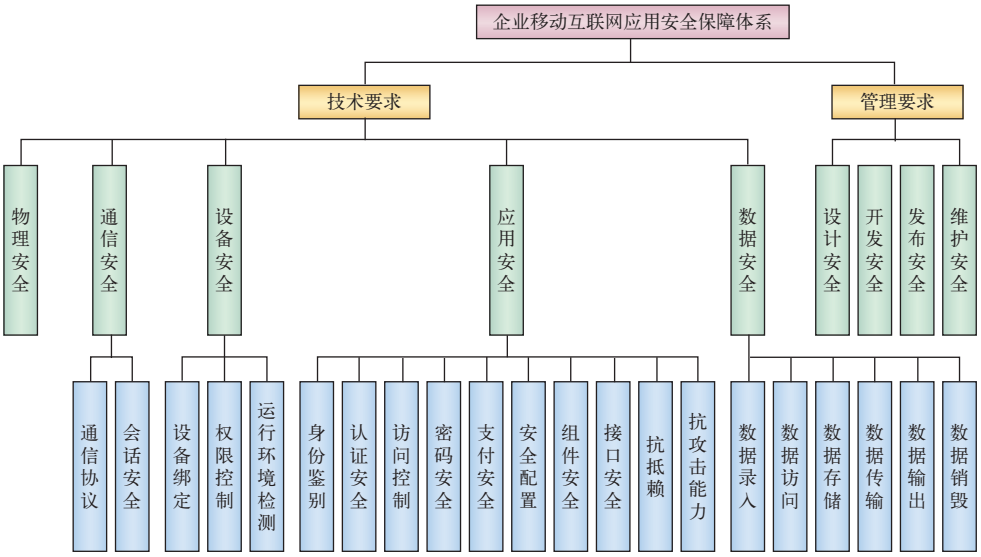

图3 企业移动互联网应用安全保障体系结构

（1）设备绑定：绑定设备的唯一标识来判断用户身份。

（2）权限控制：移动应用向移动终端操作系统申请权限遵循最小权限原则。

（3）运行环境检测：检测到移动应用的运行环境处于ROOT或越狱等非安全环境时，发出安全警告[11]。

3.1.4 应用安全

（1）身份鉴别[12]：使用双因子认证、多因子认证等方式进行身份鉴别。用户鉴别信息修改，移动应用应进行二次鉴权。身份鉴别失败，移动应用应设置结束会话等相关处理功能，同时提供通用的鉴别失败提示信息。

（2）认证安全：应用程序与服务器通过证书进行通信验证，要保证证书的合法性和一致性。更换移动设备后，需重新进行认证。登录认证结束后进行缓存清除工作。

（3）访问控制[13]：移动应用要设立用户对业务功能、数据等对象访问权限的限制。限制同一个账号同时在多个设备成功登录。禁止利用第三方应用作为入口，进行不安全跳转，访问移动应用。

（4）密码安全：保证用户设置的密码达到一定的密码复杂强度。使用官方开发SDK中自带算法库，若使用第三方算法库也需验证其安全性。

（5）支付安全[14-15]：支付交易通信过程中采用密码技术，以确保交易数据完整性与机密性。交易方身份认证密码和支付密码不允许明文显示，采取技术措施防止密码盗取。交易前对远程支付系统进行身份认证。

（6）安全配置：移动应用关闭应用调试、数据备份等相关功能。

（7）组件安全：尽量避免系统组件暴露，对于需要暴露的组件应进行代码检测。避免使用有漏洞的开源第三方应用组件及代码。

（8）接口安全：防止其他应用对移动应用软件接口进行非授权调用。移动应用对传入的URI进行校验与安全处理。

（9）抗抵赖：通过绑定用户名、密码、手机号等信息来判断用户身份。

（10）抗攻击能力：移动应用应具备抵御静态分析、动态调试、进程注入等操作的能力。使用代码加壳、代码混淆、检测调试器等手段对移动应用程序进行安全保护。

3.1.5 数据安全

（1）数据录入：移动应用在获取数据时需对输入数据进行有效性校验。保护用户输入的敏感信息不被其他程序盗取及篡改。移动应用应注意保护内存中的敏感信息，同时移动应用的临时文件中不该出现敏感信息。保证输入敏感信息数据无法被终端其他应用篡改。

（2）数据访问：移动应用需采取措施确保敏感数据仅能被授权用户或授权应用组件访问。对于移动应用，不应访问移动终端中非业务必须的文件和数据。

（3）数据存储：保护内存数据安全和内部存储文件的安全。移动应用不应在本地存储用户敏感信息。设置敏感信息的最大保存时间，超时自动删除。敏感信息存储时应进行加密或不可逆变换，安装包或本地文件系统需保证无法通过逆向工程恢复完整密钥明文。移动应用配置文件中不应明文存储敏感信息。不应在日志中记录敏感信息。

（4）数据传输：确保通信过程进行安全认证。移动应用与服务器鉴别接收到的数据，防止数据伪造。敏感信息在传输前应经过加密，在本地程序组件间或通过公共网络传输时，采取加密措施确保其保密性与完整性。

（5）数据输出：移动应用在显示敏感信息时，宜屏蔽部分内容。移动应用密码框禁止明文显示密码。调试日志不暴露敏感信息。系统运行时不输出包含敏感数据的调试信息。屏蔽系统技术错误信息与服务器报错信息。移动应用应对后台任务列表中的预览界面采取模糊处理或其他防护措施。

（6）数据销毁：移动应用退出时，清除非业务功能运行所必须留存的业务数据。移动应用卸载后，文件系统中不残留信息。

3.2 管理安全

3.2.1 设计安全

移动应用设计应遵循安全、可靠、易用、可维护和可扩展等原则。若存在用户信息发布功能，设计时对发布内容进行监测。

3.2.2 开发安全

移动应用开发过程中遵守严格的开发流程和编码安全规范，进行完整的测试，建立并维护开发文档。移动应用开发完成后，同步完成产品手册、用户手册等，需进行安全测试，保证安全测试使用的数据是经过混淆后的脱敏数据。

3.2.3 发布安全

规范上线发布流程。提供安全可靠的移动应用下载、发布、升级渠道。保证用户所下载的移动终端应用程序来源于所信任的机构。移动应用在安装前，应有明确的风险提示，上线发布前，删除所有用于调试的代码。

3.2.4 维护安全

制定科学、合理的管理策略和执行条例，建立并维护移动应用设计、开发、维护过程中文档。记录用户日志信息。

4 平台化及移动平台应用软件安全威胁与保护

企业移动互联网应用现已趋于平台化发展[16-17]。互联网融入企业业务的方方面面后，涉及到多个集成点、多个移动互联网应用以及多种移动设备支撑的问题。进行平台化发展，有利于加快业务的部署，降低总成本消耗，优化企业应用重复存在的推送服务、用户认证与权限管理、离线访问与同步、多平台支持等服务流程。

企业移动平台开发面临计算模式、开发模式、平台环境、开发环境以及生态环境5方面的威胁[18]，具体体现在：（1）计算模式：业务逻辑前端化，将更多的隐私数据暴露在移动端；（2）开发模式：移动应用开发使用Web页面技术，由此引入传统的Web应用安全风险；（3）平台环境：由于存在了多个移动应用共享终端的存储、计算、界面、输入等资源问题，致使平台所在的终端环境变得复杂；（4）开发环境：移动应用内部广泛使用第三方组件及代码，来自多个商业利益体的产品运行在一个程序中，导致开发环境混乱；（5）生态环境：缺乏强有力手段保障移动应用的发布，平台应用商城管理易混乱，同时易造成重打包现象。

制定移动应用平台安全防护体系应关注：（1）终端安全：限制平台环境。针对用户使用过程的操作系统权限、应用安装和使用情况进行全方位检测[19]；（2）数据安全：保护落地终端的数据，可以试图避免采用通用文件存储结构[20]，以及对核心数据进行签名；（3）通信安全：保障终端与服务器通信会话过程中的安全，数据传输加密；（4）应用安全：管控第三方组件与代码以及对APP加固，加固可利用签名加壳或代码混淆技术避免二次打包、资源文件被窃取、植入恶意代码等漏洞。同时考虑Web安全风险，修复公开漏洞；（5）管理安全：管控发布混乱现象。因此现有移动互联网安全保障体系中，以设备安全为重点还需增加相关内容。

5 结束语

当今移动互联网时代，企业移动互联网应用数量呈现出爆炸式增长趋势。但企业使用移动互联网应用得到便利的同时如果安全上出现问题，则会造成更大的损失。因此，研究企业移动互联网应用安全，建立安全保障体系有着重要意义。研究结果对其他类别移动互联网应用的安全性提高也能起到重要作用。

参考文献：

[1] 常　玲，赵　蓓，薛　姗，等．移动应用安全防护技术研究 [J]. 电信工程技术与标准化，2016，29（9）：86-91.

[2] 陈　希，刘颖卿，叶　芳．构筑移动应用安全评测体系 [J]. 电信工程技术与标准化，2015，28（12）：11-16.

[3] Himanshu D，Chris C，David T. Mobile Application Security [M]. Bharath Padmanabhan , 2012.

[4] 中华人民共和国工业和信息化部．移动智能终端安全能力技术要求：YD/T 2407-2013 [S]. 北京：中华人民共和国工业和信息化部，2013.

[5] 中华人民共和国工业和信息化部．移动智能终端安全能力测试方法：YD/T 2408-2013[S]. 北京：中华人民共和国工业和信息化部，2013.

[6] He Daojing，Sammy C，Mohsen G. Mobile application security: malware threats and defenses[J].Wireless Communications IEEE，2015, 22(1): 138-144.

[7] Aditya Gupta. Learning Pentesting for Android Devices[M]. packet publishing, 2014.

[8] 费　会．移动应用安全检测系统的设计与实现 [D]. 北京：北京邮电大学，2015.

[9] FreeBuf 研究院．2017 年度移动 App 安全漏洞与数据泄露现状报告 [R]. 北京：FreeBuf 研究院，2017.

[10] 上海市信息安全测评认证中心．移动互联网应用软件安全通用技术规范（试行）[Z]. 上海：上海市信息安全测评认证中心，2016.

[11] Lin Yingdar, Huang Chunying, Matthew W, et al. Mobile Application Security[J]. Computer, 2014, 47(13): 21-23.

[12] 中华人民共和国公安部．信息系统安全等级保护基本要求：GB/T 22239-2008[S]. 北京：中华人民共和国公安部，2008.

[13] 蒋笑冰．铁路移动办公系统安全防护方案的研究 [J]. 铁路计算机应用，2015，24（9）：22-26.

[14] 中国人民银行．中国金融移动支付客户端技术规范：JR/T 0092-2012 [S]. 北京：中国人民银行，2012.

[15] 中国人民银行．中国金融移动支付应用安全规范：JR/T 0095-2012 [S]. 北京：中国人民银行，2012.

[16] 邹　煜．企业级移动应用平台建设与安全保障体系探析 [J]. 网络空间安全，2016，7（6）：80-82.

[17] 李　彬，田　毅．企业移动应用平台展望 [J]. 信息通信，2015（1）：254-255.

[18] ISC2016 移动安全论坛开讲聚焦移动端隐私泄露新风险 [EB/OL]. [2016-08-01.]huanqiu.com/hot/2016-08/9333967.html.

[19] 刘孝男，任　望，安绍旺，等．企业级移动应用平台安全保障体系研究 [J]. 中国信息安全，2015（7）：90-93.

[20] 徐小天，王　刚，陈　威，等．移动平台应用安全风险与防护方法研究 [J]. 华北电力技术，2016（10）：59-63.

责任编辑　陈　蓉

（上接 P44）

方式解决冲突，并在工程实践中取得了良好的效果，对于提高车站调度效率以及降低操作人员劳动强度具有现实意义。下一步的工作将在现有功能基础上，进行机车交路对车站作业影响等问题的研究。

参考文献：

[1] T.Crainic, J.Ferland and J.Rousseav. A tactical planning model for rail Freight transportation[J]. Tans.Sci., 1984(18): 165-183.

[2] M.A.Turquist, M. S. Dadkin. Queuing models of classification and Connection delay in rail yard[J]. Trans. Sci. , 1982(16): 207-230.

[3] 彭其渊，赵　军．技术站列车解编顺序的调整方法 [J]. 西南交通大学学报，2009（3）.

[4] 李文权，王　炜，杜　文，等．铁路技术站调机运用模型及算法 [J]. 系统工程学报，2000，15（1）：38-43.

[5] 徐　杰，杜　文，常均乾，等．基于遗传算法的区段站到发线运用优化安排 [J]. 中国铁道科学，2003（2）.

[6] 张雪松，马　亮．基于约束规划的编组站阶段作业计划优化研究 [J]. 铁路计算机应用，2012, 21（9）：1-3.

[7] 杨文冠，张雪松．编组计划服务模型的研究 [J]. 铁路计算机应用，2015, 24（4）：9-11.

[8] 中华人民共和国铁道部．列车运行图编制管理规则：铁运 [2008]206 号 [S]. 北京：中华人民共和国铁道部，2008.

责任编辑　陈　蓉