电力系统移动应用安全测试技术研究

郭　静，姜海涛，王梓莹
（国网电力系统人工智能联合实验室（国网江苏省电力有限公司电力科学研究院），江苏 南京 211103）

摘　要：文中首先阐述了移动业务在电力系统的发展现状、部署特点和应用情况，分析了其客户端、服务端、数据传输、管理端等层面面临的安全风险。接着特别针对移动客户端安全特性，从应用安全防护角度出发提出了安全机制检测方法，并从检测手段和检测要点两方面详细描述了检测方法。最后，综合静态分析、渗透测试、安全机制检测的思想，进行了测试案例分析。文中所提出的测试方案和测试方法，能够全面有效地检测移动应用可能存在的安全风险，为上线前安全测评与加固提供了技术指导。

关键词：电力移动应用；风险分析；安全测试
中图分类号：TP399.0　　**文献标志码：**A　　**文章编号：**2096-3203(2018)04-0102-07

0　引言

移动应用因其使用便捷、个性化等特点，快速渗透到电力行业后，极大转变了电力领域的服务模式，提升了用户体验。

电力行业因其自身特性，对移动应用安全性、私密性、稳定性的要求越来越严格。然而，移动应用开发具有开放性和灵活性，其安全测试技术研究又尚在起步阶段，因此给电力行业带来了更多的安全隐患。近年来，移动安全事件频发，某安全网站曝出电力移动应用 2 个高危敏感信息泄露漏洞，相关人员迅速修补漏洞并更新版本，未造成严重后果和不良社会影响。2016 年，电 e 宝、掌上电力相继被曝疑似大量客户信息流出，造成了较大的社会影响。移动应用安全形势严峻，安全漏洞和安全隐患严重威胁着每个电力用户利益和企业数据安全。

关于移动应用，目前国内外已经做了很多基于应用的安全研究。文献[1—2]设计了一种基于应用程序请求的权限来检测应用是否为恶意应用软件的系统，该系统在应用安装时读取应用程序申请的权限，并与一组已知的视为可疑危险行为的规则进行比较，如果检测应用存在危险权限组合则推迟应用权限申请的认证，从而提供在应用安装的过程中给予用户警示的功能。但是现有的移动应用功能越来越强，仅通过权限区分应用的安全性，缺乏强有力的说服力。2015 年美国国家标准技术研究院发布新版指南，新版指南审查移动应用程序的安全性，为机构提供其所需的移动应用相关安全和隐私风险评估信息，包括内部开发的程序以及在移动应用市场中下载的程序。新版指南也有助于研发人员了解软件开发周期中安全漏洞的类型。该指南提供了应用程序开发安全性要求的审查过程实施计划和注意事项，并介绍了应用程序类型的漏洞和相关测试方法，还提供了机构可以使用的应用程序实例。

以上研究都是针对普通移动应用，因此文中基于电力移动应用的发展现状，分析其面临的各项安全风险，针对现有移动应用测试方法的不足提出安全机制测试方法，并结合传统测试方法，制定全面的安全测试方案，确保移动应用安全稳定运行。

收稿日期：2018-03-20；修回日期：2018-04-28

1　电力移动应用安全风险分析

移动应用在电力行业起步晚，但发展迅猛。近年来，迅速与生产、营销、金融支付、调度、办公等领域密切融合，已经为企业级用户所接受。其类型主要包括独立安装的移动应用以及在微信平台上进行二次开发的移动业务。然而，与市面上的移动应用略有区别，电力移动应用不仅服务于广大电力用户，更为内部生产做支撑服务。

1.1　架构分析

电力信息安全防护体系始终围绕安全分区、网络专用、横向隔离、纵向认证的基本原则。企业内网的建立，各分区之间的安全隔离与逻辑隔离都为信息安全提供了坚实的保障基础。图 1 为电力移动应用建设的基本框架。

电力移动应用部署基本原则遵循分区分域，安全接入。客户端与服务分区部署，并采用防火墙等设备实现逻辑隔离。后台管理端及数据库与外网服务之间采用符合标准的隔离装置，实现物理隔

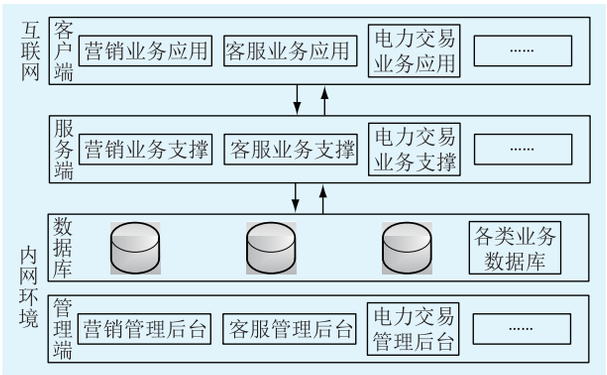

图 1　电力移动应用基本框架

Fig.1　Architecture diagram of mobile application in power system

离。各分区的具体组成模块如下:

(1) 客户端。部署在互联网,安装具体应用。客户端是连接用户与服务的桥梁,用户通过客户端应用可对营销、客服、电力交易等业务模块进行访问与操作,客户端将各种请求发送给服务端。

(2) 服务端。部署在信息外网,提供后台服务接口。服务端接收客户端提供的各种请求并进行处理反馈,同时可与信息内网数据库进行交互,交互过程设置了安全措施。

(3) 数据库。部署在信息内网,存储各类应用相关数据。

(4) 管理端。部署在信息内网,为移动应用的信息发布和统计提供相关的后台管理及服务。

1.2　安全威胁

根据结构框图,简单把 4 个模块划分为"客户端-传输-管理端",分析移动应用可能面临的安全威胁,此处管理端包含了数据库及管理后台应用。

1.2.1　客户端安全

(1) 物理威胁。客户端终端包括智能手机、平板设备等智能设备。设备具有灵活便携的特点,容易被非法盗取。设备遗失后,如果应用数据及登录信息等未及时销毁,可能造成用户个人信息泄露甚至经济损失。

(2) 操作系统威胁。目前,Android 和 iOS 操作系统占据了市场主流[2-5]。为保护用户的数据、应用程序和设备的安全,两个系统设置了相对全面的安全机制。但目前,root 和越狱越演越烈,root 或越狱后的设备,能够完美绕过安全机制。尽管设备生产厂家采取了设备锁定等一系列措施,但收效甚微,而且很多用户因为自身需求也会主动选择 root 设备[6]。

(3) 病毒木马和恶意代码。病毒木马和恶意代码一直困扰着用户,攻击者借助开源技术方案带来的技术积累制作攻击武器,通过病毒传播、短信攻击、网关攻击等造成用户损失。2016 年度,Android 平台约 10 台设备中就有 1 台染毒,设备感染率达 10%。

(4) 应用威胁。移动应用是连接用户与业务的桥梁,通过智能设备与用户直接交互,并通过通信链路传输业务请求到后端服务器。以移动应用为入口,进行漏洞挖掘及业务安全分析,可逐步渗透到服务端、管理端。根据漏洞来源,应用威胁主要可分为以下三大类:

① 传统 web 漏洞[7-8]。移动应用通常采用客户端/服务器(clients/server, C/S)或者 C/S 和浏览器/服务器(browser/server, B/S)相结合的开发架构,其开发技术渐渐和 web 开发技术融合在一起。所以,常见的 web 应用相关漏洞在手机前段都有可能存在。开放式 web 应用程序安全项目组织(open web application security project organization, OWASP) top 10 详述了 web 开发面对的 10 大安全漏洞,包括结构化查询语言(structured query language,SQL)注入,跨站脚本攻击漏洞,跨站请求伪造(cross-site request forgery, CSRF)等等。这些漏洞可能会造成机密信息被窃取、网络服务被中断、破坏等后果。但由于大部分 APP 不是采用直接嵌入网页的模式,而是使用应用程序编程接口(application programming interface,API)返回数据,导致扫描器爬虫无法大量获取链接,因此该类漏洞利用率比较低。

② 应用自身安全机制问题。不安全的数据存储,不安全的身份验证,过多的授权,未进行源代码保护等引发的逆向工程攻击。逆向工程[9]通过对核心二进制代码以及业务逻辑的分析研究,确定应用源代码、库文件、算法和其他资产。常用的分析方法包括包分析,协议分析,代码注入,组件攻击等等,能够造成拒绝服务、运行崩溃、数据监听、源代码泄露等后果。

③ 业务设计不合理引发的安全漏洞。应用中涉及到的第三方引用(服务、支付、地图等)不当也会造成安全风险。如访问第三方应用后原页面被替换或者覆盖,内部员工使用不加密的二维码作为认证信息,通过拍照获取或者重构二维码易引起内部信息泄露和越权访问。

1.2.2　传输安全

APP 网络传输安全指数据从客户端到数据库中间过程的安全。传输安全本质上是信任问题。攻击者通过证书伪造、数字签名伪造等手段伪装成

为信任的对象，进行数据窃取或篡改，这就是所谓的中间人攻击方式。此外，移动通信数据传输采用无线网络接入服务器、客户端，也可通过 wifi 钓鱼或基站伪装等方式，对用户信息进行监听和分析。攻击者盗取数据包后，可进行数据篡改或以此用户信息为跳板获取更多后台机密信息。

1.2.3 管理端安全

应用管理后台通常使用 web 技术开发，提供方便快捷的管理页面，由系统管理员个人使用，承担了更多的管理职能。后台能够进行信息发布，数据增删改查等关键操作。一旦发生攻击事件，能够造成大范围用户影响，是攻击者的终极目标。

（1）应用系统威胁：关于 web 系统常见风险同“应用威胁”分析。

（2）内部威胁：电力系统依赖物理隔离的保护，内网用户在系统管理及使用上存在不合理行为容易造成弱口令利用，攻击者登录系统更改应用配置信息，使业务应用不能访问；发布恶意公告，造成恶劣社会影响。规范用户行为管理的同时，重视安全策略制定，加强机密数据的存储和传输安全，建立良好的数据恢复系统，建立用户操作审计机制都可以解决这类问题。

（3）环境威胁：环境安全主要包括网络层、主机层、应用层、数据层的安全。主要有网络设备、操作系统、数据库、中间件、应用服务器等多类设备及系统的安全配置问题；主机感染的病毒、木马以及恶意代码问题。这些问题均会成为攻击的可利用漏洞，如利用系统漏洞远程获取访问权限或管理权限，从而控制整个系统。

2 常规安全测试方法

为应对移动用快速发展带来的安全问题，充分保护电力用户隐私及内部生产数据，已建设的生产应用通常以展示功能为主，其他关键操作性的设置较少，以此来减少安全风险。随着应用与业务的紧密融合，很难再使用这种方法来限制用户操做行为。面对越来越多的攻击方式和攻击数量，应用必须从根本上规范安全机制，加强系统上线前安全测试，提升移动应用安全性、健壮性。

常见安全测试方法主要检测电力应用面对的技术方面的威胁，通常运用代码审计和渗透测试方法确保各类应用安全，同时采取安全配置核查，病毒木马查杀等检测手段确保部署环境安全。

（1）代码审计[10-11]。代码审计属于静态测试方法[12]，是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析。目前比较流行的检测标准是 OWASP 安全标准，对跨站脚本攻击（cross site scripting，XSS）、文件上传、各类注入漏洞等主流攻击漏洞进行代码级检测。常用的代码审计方法是软件扫描，该方法误报率较高，因此必须请专业人员对代码报告进行审计，确定真实威胁。

（2）渗透测试[13-16]。渗透测试属于动态测试方法，通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的。目前，针对 web 应用系统，已经有各种自动化测试工具为测试者提供帮助和参考。对于移动应用来说，还没有权威的自动化测试工具，因此测试效果主要依赖测试人员的个人能力。

（3）安全配置核查。安全配置核查[17]主要是对系统部署环境各要素的综合检查。目前常见的配置核查涵盖了操作系统、网络设备、数据库、中间件等多类设备及系统的安全配置检查，其发现的问题包括未安装补丁、错误的安全配置、各类弱口令等。企业可以根据自身需求，定制一套安全配置核查标准，称之为安全基线。常用的安全配置核查手段是人工检查和设备检测。

（4）病毒木马查杀。病毒木马查杀主要是防止系统服务器、数据库等关键设备被病毒木马入侵。主要手段是安装主流防病毒木马软件，使用最新病毒库进行查杀。同时，针对顽固病毒，在不影响业务的情况下，采取端口、服务禁用的应急手段防止进一步侵害。病毒木马检测手段日趋成熟，但一些紧急情况和潜在漏洞仍然具备很大威胁性，如近期肆虐的勒索病毒，因此病毒木马检测属于常规型检测。

以上方法在移动应用安全检测中仍然适用，能够有效检测到后台应用、部署环境存在的安全漏洞，但一方面移动应用和 web 应用存在架构及开发、应用模式上的差异性，另一方面以上针对应用软件的检测方法主要从攻击者角度出发，面对层出不穷的攻击方式和攻击方法有些力不从心。因此，亟需一套针对性强且能够实现主动防御的完整的移动应用测试方案。

3 一种基于安全机制的测试方法

针对常规安全测试方法的不足，文中提出了基于安全机制移动应用测评方法。该测评方法针对电力移动应用开发可规划、规范性强的特点，结合

等级保护测评思想整体测评分析移动客户端应用的安全性。主要通过规范化要求,减小或部分消除各种安全威胁给信息系统带来的安全风险,最终确保信息系统安全防护能力达到保障业务安全可靠的水平。

安全机制检测主要覆盖用户鉴别、数据传输、数据存储、输入健壮性、异常管理、源代码保护、包分析、组件安全、API 使用、权限机制等几大方面,能够针对性测试目前流行的反编译、二次打包、组件暴露劫持、中间人攻击等主流移动应用威胁。

3.1　用户身份鉴别机制

检测客户端用户身份鉴别机制和客户端身份鉴别机制。用户身份鉴别应用场景较多,关键场景有用户登录场景,关键操作场景等。其检测点有:

(1) 用户身份鉴别方式。检测移动应用使用的身份鉴别方式。移动应用应设置相应的身份鉴别方式,如口令、验证码等,更安全的方式是采用验证码、生物特征识别(如指纹等)相结合的方式来作为用户的唯一身份标识。

(2) 鉴别失败处理机制。检测移动应用对多次登录身份验证失败的处理机制。对于多次登录失败的用户,应当做锁定处理,杜绝恶意尝试的暴力破解行为。

(3) 登录防暴力破解机制。检测移动应用对失败登录请求的处理机制。对于恶意发送的登录失败请求,服务器端应当拒绝处理,以免处理大量无效请求时占用资源,引起系统崩溃。

(4) 用户登录失败提示。用户登录失败时谨慎提示,以免暴露更多用户口令信息,降低攻击者保利破解难度。

(5) 客户端与服务器端身份鉴别。客户端与服务器通信时一般采用安全套接层(secure sockets layer, SSL)安全协议,SSL 存在单向认证和双向认证两种方式。单向认证过程中只需要服务器将自己的证书,以及同证书相关的信息发送给客户浏览器。双向认证则是需要服务端与客户端提供身份认证,只能是服务端允许的客户能去访问,安全性相对而言要高一些。使用这种方法,攻击者无法轻易模拟客户端进行欺骗通信,有效阻止了中间人攻击。

(6) 用户口令设置机制。检测用户口令复杂度、用户口令重复次数及用户口令对特殊符号输入的处理。

(7) 用户身份信息泄露等。检测用户鉴别信息是否存在过期、泄露等情况。如短信验证码是否可以长期使用,验证码内是否含有口令或其他身份信息等。

3.2　卸载升级

(1) 检测软件卸载是否清除完全,是否有数据残留。主要是针对客户端进行的检测,软件卸载后应全部删除自身文件,尤其是容易被转移的外设中不应留存敏感信息。

(2) 检测软件升级功能的正确性和安全性:检测软件升级方式,如果是通过链接方式推送升级,尝试替换升级信息,检测升级过程中是否进行了完整性校验。

3.3　数据通信机制

(1) 检测客户端在与服务端软件通信过程中数据加密机制:对于通信过程中传输的敏感数据,如口令、支付信息、用户隐私信息及其他涉密数据应采取加密方式传输,加密算法应采用密级较高、密钥长度合适的算法。

(2) 检测数据传输过程中是否使用安全套接层/传输层安全(secure sockets layer / transport layer security , SSL/TLS)、网际协议安全(internet protocol security, IPSec)等安全通信协议:通信过程中应采用安全通信协议,对通信网络连接进行加密。

(3) 检测客户端与服务端软件通信过程中是否进行完整性校验机制:通信过程中应采用完整性算法对敏感数据进行保护,如 MD5、SHA1 等。可尝试修改传输数据,看服务端是否能够识别。

(4) 检测软件是否可以建立非法会话:检测会话标识是否容易被盗用,尝试退出登录后发送相同会话请求,服务器应不能正常响应。

(5) 检测软件是否具备会话超时机制:会话建立后,应当有会话连接时间设定,超过会话连接时间应关闭会话。

3.4　数据存储机制

(1) 检测软件记录的隐私信息是否加密处理:客户端是否明文存储敏感信息,应用配置信息、敏感报错信息、关键代码等。敏感信息应采用密级较高、密钥长度合适的算法。

(2) 检测数据存储位置是否安全:应用敏感数据应存储在应用本身目录下,尤其是可移动外设中应尽量不存放应用信息。

3.5　输入健壮性测试

(1) 检测软件是否对错误的操作或者输入进行处理:尝试输入特殊字符、超长内容及不同类型的数据,检测软件对用户输入的限制。如果引发程序异常,对报错信息进行分析,不应含有敏感信息。

（2）检测隐私数据输入时是否明文显示：在输入口令，支付密码、身份私密信息等用户个人隐私时，应当对关键信息进行隐蔽处理。在输入这些隐私信息时，尽量使用加密键盘。

3.6 API 误用

检测软件是否存在已知漏洞的 API。通过调用各类问题 API，测试应用在不同版本的系统上是否能够激活该漏洞。

3.7 调试功能

检测软件是否开启调试功能及备份功能，这两个功能常常被攻击者利用。

3.8 组件安全

（1）检测是否存在不必要的暴露组件：查看暴露组件情况，如存在必须暴露的组件，应进行权限声明，避免组件被恶意程序利用或攻击。

（2）检测 Activity、BroadcastRecevier、Service、Content Provider 组件是否会被权限攻击或劫持：Activity 组件被劫持无法避免，劫持后应用应给用户提示当前应用已进入后台运行。使用工具进行组件模拟攻击，查看是否会引起程序异常，是否存在组件权限攻击或者被监听。

3.9 权限机制

（1）检测软件是否存在权限滥用问题。查看 manifest 文件，分析 system 级别权限和级别 root 权限使用情况。应用依照最小化权限原则进行设置。

（2）检测用户操作权限管理。确定已通过验证用户的访问和操作权限。防止错误的授权或弱授权导致应用程序信息和用户敏感信息被非法访问或篡改。① 纵向越权：一个低权限的用户访问高权限用户的资源或功能。② 横向越权：用户尝试访问与其同级权限用户的资源或功能。

3.10 软件防篡改

（1）检测软件是否能被反编译：对 Android 安装包（Android package，apk）进行反编译，查看是否能正常分析得到的源码。Android 应用应对源代码进行加壳或混淆处理，以免信息泄露。

（2）检测软件的本地库文件是否加密：解压 apk 包，提取 dex 文件并使用工具转换，查看得到的代码能否正常分析。

（3）检测软件是否够重打包：反编译 apk 安装包后，对源码进行修改，重新打包签名，查看 APP 是否能够正常运行。应用应对 apk 包完整性进行校验，避免重打包现象。

以上安全机制检测根据 APP 常见缺陷总结，能够有效评估应用安全性。

4 案例分析

结合传统的的安全检测方法和安全机制检测方法，可分别涵盖了移动终端安全、客户端应用安全、通信和传输安全、服务端安全几个方面来进行检测。检测整体框图如图 2。

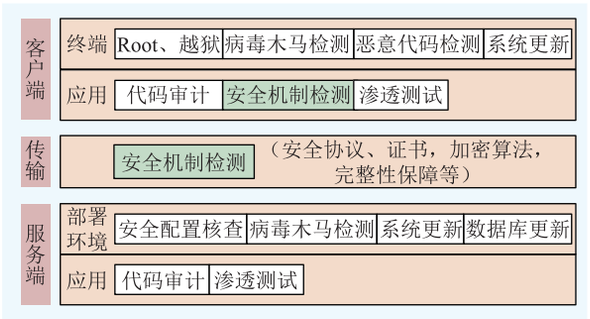

图 2 移动应用安全测试方法

Fig.2 Mobile application security testing scheme.

本方法基于电力系统行业特点，考虑了可能发生威胁的各个模块，利用安全机制检测实现安全威胁主动防御，并综合已有的代码审计、渗透测试、配置核查、病毒木马查杀等多种技术手段，提供移动应用全面的安全保障。本方案可通用于各类电力移动应用，为上线前安全测试提供理论基础和具体实现。

挑选 3 个移动应用 A、B、C，在硬件条件同等的情况下（包括客户端硬件及服务端硬件），使用该方案进行测试。其中 A 系统为独立开发，B 系统和 C 系统集成在同一平台内开发。检测发现 A 应用安全机制问题 11 项，其他安全问题 2 项；B 应用安全问题 6 项，其他安全问题 1 项；C 应用安全机制问题 5 项，其他安全问题 1 项。测试结果如表 1 和表 2 所示。通过测试结果可以看出，就服务端而言，管理后台采用 Web 技术开发，通过代码测试和渗透测试 A、B、C 均测试出少量低危漏洞。究其原因，web 安全近年来越来越受到重视，开发人员安全意识上升，安全防护技术越来越成熟，很大程度降低了管理后台的技术漏洞。

APP 的主要安全问题集中在客户端。使用基于安全机制的测试方法能够测试出更多的安全漏洞。就客户端而言，A 系统存在较多漏洞。因用户鉴别机制不完善，可进行登录信息猜测；因为传输机制不完善，可通过抓包获取到用户敏感信息，且可以对截取的数据包进行修改；本地存储敏感信息可进行源代码反编译；存在高级别权限，超出本身应用范围。B 系统和 C 系统安全机制相对完善，因为开发时以同一平台为基础，安全问题趋于一致。

表 1　3APP 客户端测试结果比较

Tab. 1　Test result comparison between 3 APPs clients

测试方法	类别	A	B	C
安全机制测试	用户身份鉴别	无账户锁定机制	账户锁定时间不足	账户锁定时间不足
		未采用多重身份鉴别机制	未采用多重身份鉴别机制	未采用多重身份鉴别机制
		用户登录失败提示暴露信息		
		用户验证码复杂度不足		
	数据通信机制	未设置会话超时时间	未设置会话超时时间	未设置会话超时时间
		未进行数据传输完整性校验		
		未进行数据传输加密		
	数据存储机制	本地存储敏感文件,可反编译为系统源代码		
	输入健壮性	输入隐私数据可全部明文显示,未进行部分屏蔽	未对输入数据类型进行限制	
	组件安全	存在暴露的组件	存在暴露的组件	存在暴露的组件
	权限管理	存在高级别权限申请(打电话)	存在高级别权限申请	存在高级别权限申请
渗透测试	端口检测		存在无关的服务和端口	存在无关的服务和端口
	传输可靠性检测	明文传输敏感信息		
	数据可重放检测	数据可实现修改重放		

表 2　3APP 服务端测试结果比较

Tab.2　Test result comparison between 3 APPs severs

测试方法	A	B	C
代码审计	Excessive session timeout(low)	Leftover debug code(low)	Leftover debug code(low)
	System information leak(low)	System information leak(low)	System information leak(low)
渗透测试	应用程序错误(低)	发现电子邮件地址模式(低)	发现电子邮件地址模式(低)
	发现电子邮件地址模式(低)	Html 注释敏感信息泄露(低)	Html 注释敏感信息泄露(低)
	缺少跨站脚本编制防御(低)	缺少跨站脚本编制防御(低)	缺少跨站脚本编制防御(低)
	查询中接受的主体参数(低)	检测到隐藏目录(低)	检测到隐藏目录(低)

电力系统逐步采用基于平台统一开发的模式,将各类应用保护起来,解决了开发团队水平参差不齐的问题,提高了整体安全水平。但与此同时,统一平台的安全必须通过严格测试。

4　结语

文中针对常规安全测试方法能够适应电力移动应用测试的不足和电力移动应用开发可规划、规范性强的特点,结合等级保护测评思想整体测评分析移动客户端应用的安全性,提出了基于安全机制的测试方法,从根本上规范安全机制,加强系统上线前安全测试,从而提升了移动应用安全性和健壮性。同时,该移动安全测试方案适用于电力移动应用的安全测试,为电力移动应用上线前安全测评与加固提供了技术指导。

参考文献:

[1] ZHOU W, ZHOU Y, JIANG X, et al. Detecting repackaged smartphone application in third-party android marketplaces [C]// Proceedings of the second ACM conference ondata and application security and privacy.ACM,2012:317-326.

[2] ENCK W, GILBERT P, CHUN B G, et al. TaintDroid: an information flow tracking system for real-time privacy monitoring on smartphones [J]. Communications of the ACM, 2014, 57(3):99-106.

[3] 徐小天,王　刚,陈　威. 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.
XU Xiaotian, WANG Gang, CHEN Wei, et al. Research of vulnerability and security of mobile platform applications [J]. North China Electric Power, 2016(10): 59-63.

[4] NIKOLAY E. Android 安全架构深究[M]. 电子工业出版社,2016:11-18.
NIKOLAY E. Anatomy of the android security architecture[M]. Electronic Industry Press,2016:11-18.

[5] 杨正军, 潘　娟. 移动应用软件安全威胁及其检测技术[J]. 互联网天地, 2013,11:1-4.
YANG Zhengjun, PAN Juan. Security threats of mobile application software and its detection technologies[J]. China Internet, 2013, 11: 1-4.

[6] 徐君锋, 吴世忠, 张　利. Android 软件安全攻防对抗技术及发展[J]. 北京理工大学学报, 2017, 37(2):163-167.
XU Junfeng, WU Shizhong, ZHANG Li. Survey on attack and defense technologies of Android software security[J]. Transactions of Beijing Institute of Technology, 2017, 37(2): 163-167.

[7] 陈　昊. 灰盒代码审计在 Web 安全检测中的应用研究与实现[D]. 北京:北京邮电大学, 2011.
CHEN Hao. Gray box code audit in web safety inspection application research and implementation[D]. Beijing: Beijing University of Posts and Telecommunications, 2011.

[8] 王　丹, 赵文兵, 丁治明. Web 应用常见注入式安全漏洞检

测关键技术综述[J]. 北京工业大学学报,2016,42(12):1822-1832.
WANG Dan, ZHAO Wenbing, DING Zhiming. Review of detection for injection vulnerability of web applications [J]. Journal of Beijing university of technology, 2016, 42(12): 1822-1832.

[9] 严 炜. 基于iOS平台的应用软件安全检测关键技术的研究与实现[D]. 北京:北京邮电大学, 2014.
YAN Wei. Research and implementation of key techniques of application security evaluation based on iOS platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2014.

[10] ZHENG M, SUN M S, JONHAN C S. DroidTrace: a ptrace based Android dynamica analysis system with forward execution capability[C]// Proceedings of 2014 International Wireless Communications and Mobile Computing Conference. Cyprus: 2014: 128-133.

[11] JING Y, AHN G J, ZHAO Z, et al. Toward automated risk assessment and mitigation of mobile applications[J]. IEEE Transctions on Dependable and Secure Computing, 2015(5): 571-584.

[12] BAGHERI H, SAEGHI A, GARCIS J, et al. Covert: com-positional analysis of Android inter-app permission leakage[J]. IEEE Transactions on Software Engineering, 2015, 41(9): 866-886.

[13] YANG Zhemin, YANG Min. LeakMiner: detect information leakage on android with static taint analysis[C]//Proceedings of 3rd World Congress on Software Engineering. Hong Kong, China: 2012: 101-104.

[14] HALFOND W G J, CHOUDHARY S R, ORSO A. Penetration testing with improved input vector identification[C]// Proceedings of the 2nd International Conference on Software Testing, Verification and Validation. Piscataway: IEEE, 2009: 346-355.

[15] HALFOND W G J, CHOUDHARY S R, ORSO A. Improving penetration testing through static and dynamic analysis[C]// Proceedings of the Seconde IEEE International Conference on Software Testing, Verification and Validation. West Sussex: John Wiley and Sons Ltd, 2011:195-214.

[16] MARTIN M, LAM M S. Automatic generation of XSS and SQL injection attacks with goal-directed model checking[C]// Proceedings of the 17th Conference on Security Symposium. San Jose: USENIX Association, 2008: 31-43.

[17] 车翔飞. 信息系统上线前安全评测方案的研究[J]. 软件工程, 2015(11):15-17.
CHE Xiangfei. Study on the security evaluation scheme before the information system go online[J]. Software Engineer, 2015(11): 15-17.

作者简介:


郭 静

郭 静(1985—),女,硕士,工程师,从事信息安全工作(E-mail: guojing5126@163.com);

姜海涛(1985—),男,博士研究生,研究方向为信息安全(E-mail: jianghaitao1@js.sgcc.com.cn);

王梓莹(1991—),女,硕士,工程师,从事信息安全工作。

Research on Security Testing Technology of Mobile Application in Power System

GUO Jing, JIANG Haitao, WANG Ziying
(State Grid Power System Artificial Intelligence Joint Laboratory(State Grid Jiangsu Electric Power Co., Ltd. Research Institute), Nanjing 211103, China)

Abstract: This paper first describes the development and characteristics of mobile application in power system, and analyzes the security risks faced by clients, servers, data transmission and management. Then, aiming at the security characteristics of mobile clients, a security mechanism detection method is put forward from the perspective of application security protection, and the detection method is described in detail from two aspects of detection means and detection points. Finally, comprehensive static analysis and penetration test method, the APP security test was carried out. The test scheme and test method proposed in this paper can find the security risk in mobile application comprehensively and efficiently. It provides technical guidance for pre-line safety evaluation.

Key words: power system; security test; security mechanism

(编辑 方 晶)