移动应用安全需求分析与安全保护工程

移动应用安全威胁与需求分析
Android系统安全与保护机制
IOS系统安全与保护机制
移动应用安全保护机制与技术方案
移动应用安全综合应用案例分析

文老师软考教育

移动应用安全威胁与需求分析

文老师软考教育

◆移动应用系统组成：包括三个部分：一是移动应用，简称App；二是通信网络，包括无线网络、移动通信网络及互联网；三是应用服务端，由相关的服务器构成，负责处理来自App的相关信息或数据。

◆移动应用安全分析：移动应用的安全威胁主要有以下类型。

1．移动操作系统平台安全威胁。移动应用的安全性依赖于移动操作系统。目前，市场上主要的移动操作系统是苹果公司的iOS操作系统与Google公司开源的Android操作系统。根据CVE公开漏洞信息，移动操作系统都不同程度地存在漏洞。

2．无线网络攻击。攻击者利用移动应用程序依赖的无线网络通信环境或网络服务的安全隐患，实施通信内容监听、假冒基站、网络域名欺诈、网络钓鱼等攻击活动。WiFi“钓鱼”是移动应用安全威胁常见的形式，攻击者通过一台可控的路由器发射无线信号，可以监控连接到该路由器的智能设备，分析智能设备与服务器通信的数据包，修改服务器返回的网页，甚至还可以伪装成受害者与服务器通信。

3．恶意代码。针对智能手机的恶意代码行为呈上升趋势，常见的恶意行为有流氓行为、资费消耗、恶意扣费、隐私窃取、远程控制、诱骗欺诈、系统破坏、恶意传播等。

4．移动应用代码逆向工程。攻击者通过对移动应用程序的二进制代码进行反编译分析，获取移动应用源代码的关键算法思路或窃取敏感数据。

5．移动应用程序非法篡改。攻击者利用安全工具，非法篡改移动应用程序，实现恶意的攻击，窃取用户信息。

Android系统安全与保护机制

◆ Android系统组成概要：Android是一个开源的移动终端操作系统，其系统结构分成Linux内核层（Linux Kenel）、系统运行库层（Libraries和Android Runtime）、应用程序框架层(Application Framework)和应用程序层(Applications)。
◆ Android系统的各层都面临着不同程度的安全威胁。其中，Android系统的基础层安全威胁来自Linux内核攻击，目前，Linux内核漏洞时有出现，内核漏洞常常导致攻击者能够获得系统最高权限，严重危及Android整体系统的安全。Android系统成为恶意代码利用的重点目标，常见的形式有APK重打包(repackaging)、更新攻击、诱惑下载、提权攻击、远程控制、恶意付费、敏感信息搜集。

◆ Android系统安全机制：为保护Android系统及应用终端平台安全，Android系统在内核层、系统运行库层、应用程序框架层以及应用程序层等各个层面采取了相应的安全措施，以尽可能地保护移动用户数据、应用程序和设备安全。
1．应用程序层：权限声明机制。为操作权限和对象之间设定了一些限制，只有把权限和对象进行绑定，才可以有权操作对象。当然，权限声明机制还制定了不同级别不同的认证方式的制度。应用程序层的权限包括normal权限、dangerous权限、signature权限、signatureOrSystem权限。normal权限不会给用户带来实质性的伤害；dangerous权限可能会给用户带来潜在威胁，如读取用户位置信息，读取电话簿等，对于此类安全威胁，目前大多数手机会在用户安装应用时提醒用户；signature权限表示具有同一签名的应用才能访问；signatureOrSystem权限主要由设备商使用。

Android系统安全与保护机制

文老师软考教育

2．应用程序框架层：应用程序签名机制。Android将应用程序打包成.APK文件，应用程序签名机制规定对APK文件进行数字签名，用来标识相应应用程序的开发者和应用程序之间存在信任关系。所有安装到Android系统中的应用程序都必须拥有一个数字证书，此数字证书用于标识应用程序的作者和应用程序之间的信任关系。

3．系统运行层：沙箱机制、SSL。
◆沙箱隔离机制使应用程序和其相应运行的Dalvik虚拟机都运行在独立的Linux进程空间，不与其他应用程序交叉，实现完全隔离。
◆ Android支持使用SSL/TSL协议对网络数据进行传输加密，以防止敏感数据泄露。

4．内核层：文件系统安全、地址空间布局随机化、SELinux。
◆ Android系统的内核层采用分区和Linux ACL权限控制机制。Linux ACL权限控制机制是指每个文件的访问控制权限都由其拥有者、所属的组、读写执行三个方面共同控制。文件在创建时被赋予了不同的应用程序ID，只有拥有相同应用程序ID或被设置为全局可读写才能够被其他应用程序所访问。每个应用均具有自己的用户ID，有自己的私有文件目录。在系统运行时，最外层的安全保护由Linux提供，其中system.img所在的分区是只读的，data.img所在的分区是可读写的，用于存放用户的数据。
◆除了Linux常见的安全措施外，Android后续版本不断增强抗攻击安全机制，在Android 2.3版本之后增加了基于硬件的NX (No eXecute)支持，不允许在堆栈中执行代码。在Android 4.0之后，增加了“地址空间布局随机化(ASLR)”功能，防止内存相关的攻击。

IOS系统安全与保护机制

◆ iOS系统组成概要：苹果公司建立以iOS平台为核心的封闭的生态系统。iOS的系统架构分为四个层次：核心操作系统层(Core OS Layer)、核心服务层(Core Services Layer)、媒体层(Media Layer)和可触摸层(Cocoa Touch Layer)。
◆可触摸层。为应用程序开发提供了各种常用的框架并且大部分框架与界面有关，负责用户在iOS设备上的触摸交互操作。
◆媒体层。提供应用中视听方面的技术。
◆核心服务层。提供给应用所需要的基础的系统服务，如账户、数据存储、网络连接、地理位置、运动框架等。
◆核心操作系统层。提供本地认证、安全、外部访问、系统等服务。

◆ iOS系统安全机制：iOS平台的安全架构可以分为硬件、固件、软件。
◆硬件、固件层由设备密钥、设备组密钥、苹果根认证、加密引擎、内核组成。
◆软件层则由文件系统、操作系统分区、用户分区、应用沙盒及数据保护类构成。

◆苹果基于这一整体安全架构，集成了多种安全机制，保护iOS平台的安全性，主要安全机制如下。
1．安全启动链。iOS平台的安全依赖于启动链的安全，为防止黑客攻击启动过程，iOS启动过程使用的组件要求完整性验证，确保信任传递可控。iOS启动过程如下。

IOS系统安全与保护机制

文老师软考教育

◆打开iOS设备后，其应用处理器会立即执行只读内存（也称为引导ROM）中的代码。这些不可更改的代码是在制造芯片时设置好的，为隐式受信任代码。引导ROM代码包含苹果根CA公钥，该公钥用于验证底层引导加载程序(LLB)是否经过苹果签名，以决定是否允许其加载。引导路径从引导ROM出来之后分叉为两条执行路径：一条是普通引导；另一条则是设备固件更新模式，这个模式用于更新iOS镜像。

2．数据保护。针对移动设备因丢失或被窃取导致的泄露数据的风险，提供了数据保护API。API让应用开发者尽可能简单地对文件和keychain项中存储的敏感用户数据施以足够的保护。

3．数据的加密与保护机制。而iOS内所有用户数据都是强制加密的。苹果的AES加解密引擎都是硬件级的，位于存储与系统之间的DMA内，所有进出存储的数据都要经过硬件的加密与解密，这样提供了较高的效率与性能。除此之外，iOS提供了名为File Data Protection的数据保护方法。所有文件在加密时使用的key都是不同的，这些key被称作Profile Key，存储于Metafile内。

4．地址空间布局随机化。利用ASLR技术，确保iOS的二进制文件、库文件、动态链接文件、栈和堆内存地址的位置是随机分布的，从而增强抗攻击能力。
5．代码签名。为防止应用攻击，iOS系统要求所有可执行程序必须使用苹果公司发放的证书签名。
6．沙箱机制。通过沙箱机制，可以限制进程的恶意行为。

移动应用安全保护机制与技术方案

◆移动应用App安全风险：移动应用App是指运行在智能设备终端的客户端程序，其作用是接收和响应移动用户的服务请求，是移动服务界面窗口。由于移动应用App安装在用户的智能设备上（通常为智能手机），很容易遭受到反编译、调试、篡改、数据窃取等安全威胁。

◆移动应用App安全加固：为保护移动应用App的安全性，通常采用：

1．防反编译。对移动应用程序文件进行加密处理，防止攻击者通过静态的反编译工具，获取到应用的源代码。除了加密措施之外，还可以对移动应用程序进行代码混淆，增加破解者阅读代码的难度。常见的混淆方法有名字混淆、控制混淆、计算混淆等。

2．防调试。为防止应用程序动态调试，应用程序设置调试检测功能，以触发反调试安全保护措施，如清理用户数据、报告程序所在设备的情况、禁止使用某些功能甚至直接退出运行。

3．防篡改。通过数字签名和多重校验的防护手段，验证移动应用程序的完整性，防范移动应用程序APK被二次打包以及盗版。

4．防窃取。对移动应用相关的本地数据文件、网络通信等进行加密，防止数据被窃取。

移动应用安全保护机制与技术方案

文老师软考教育

◆移动应用App安全检测：常见的移动应用App网络安全检测内容如下：

◆身份认证机制检测；通信会话安全机制检测；敏感信息保护机制检测；日志安全策略检测；交易流程安全机制检测；服务端鉴权机制检测；访问控制机制检测；数据防篡改能力检测；防SQL注入能力检测；防钓鱼安全能力检测；App安全漏洞检测。

◆为保护个人信息安全，规范App的应用，国家有关部门已发布了《信息安全技术移动互联网应用程序(App)收集个人信息基本规范（草案）》。其中，针对Android 6.0及以上的可收集个人信息的权限，给出了服务类型的最小必要权限参考范围，具体要求是：

地图导航：位置权限、存储权限；　　网络约车：位置权限、拨打电话权限；
即时通信：存储权限；　　博客论坛：存储权限；
网络支付：存储权限；　　新闻资讯：无；　　网上购物：无；
短视频：存储权限；　　快递配送：无；
餐饮外卖：位置权限、拨打电话权限；　　交通票务：无；
婚恋相亲：存储权限；　　求职招聘：存储权限；
金融借贷：存储权限；　　房屋租售：存储权限；
二手车交易：存储权限；　　运动健身：位置权限、传感器权限；
问诊挂号：存储权限；　　网页浏览器：无；　　输入法：无；
安全管理：存储权限、获取应用账户、读取电话状态权限、短信权限。

移动应用安全综合应用案例分析

◆金融移动安全： 移动金融引发大量黑客攻击活动，常见的安全风险有木马控制用户手机、钓鱼App捕获用户账户信息、窃取转移用户资金等。围绕金融类App的安全防护，安全保护方案内容如下。
1. 实施移动App安全开发管理。针对金融业务安全性需求提供咨询服务，帮助客户了解潜在安全风险、优化业务设计。在App设计时，考虑应用安全问题。开展移动安全编程培训，培养安全意识。App增加安全防护功能，提供安全软键盘、防界面劫持、短信保护、清场等安全SDK和组件。对移动应用源代码进行安全性检查及风险排查，减少App代码安全漏洞，及早发现金融业务安全风险。

2．移动App网络通信内容安全加密保护。针对移动App应用通信协议进行加密保护。
3．移动App安全如固。对App进行安全加固，如dex加密、smali流程混淆、so文件加密、关键函数加密、增加反调试和反编译功能。
4．移动App安全测评。对移动应用进行渗透性测试服务，挖掘移动应用的安全漏洞，避免安全风险。

5．移动App安全监测。
◆钓鱼监测及响应。对App的仿冒、钓鱼应用进行钓鱼监测及响应，快速联系渠道下架仿冒、钓鱼应用App，避免安全影响。
◆ App漏洞监测及响应。监测移动设备、移动应用、服务器等新增、突发漏洞，及时规避漏洞风险。
◆盗版监测及响应。监测App应用分发渠道上出现的盗版应用，随时进行盗版下架处理。
◆移动威胁安全态势感知。捕获针对App的攻击行为，提供可视化数据分析平台及实时安全防控技术。

移动应用安全综合应用案例分析

文老师软考教育

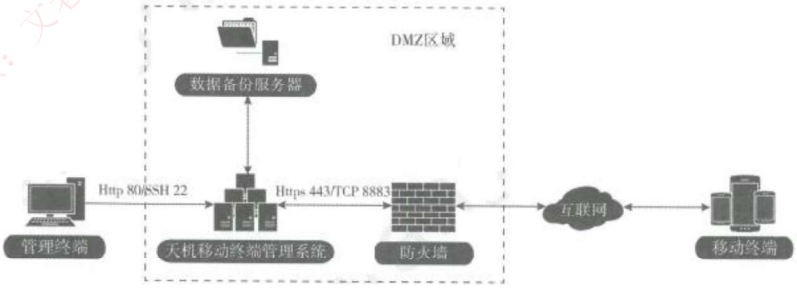
运营商移动安全：运营商移动应用安全主要面临的安全威胁如下：
◆账号、密码窃取。
◆漏洞利用。黑客及非法利益团体，通过系统漏洞侵入运营商服务器。
◆恶意代码。将病毒、木马、逻辑炸弹、恶意扣费等恶意代码捆绑在移动应用上。
◆数据窃取。利用非法手段窃取、盗用运营商用户重要数据。
◆恶意刷量、刷单。伪造大量虚假身份／盗用真实用户身份进行自动化大批量的刷单、刷量。
◆拒绝服务攻击。非法用户利用拒绝服务手段攻击系统。
◆计费SDK破解。通过反编译、破解等手段，屏蔽、破解运营商的移动应用计费SDK。
◆钓鱼攻击。通过仿冒正版的钓鱼移动应用程序，截获、捕捉用户输入数据，非法入侵用户互联网账户系统。
◆社工库诈骗。通过盗版、高仿应用收集用户信息，以及泄露的其他社工库，对用户实施诈骗。

针对运营商移动应用安全问题，安全保护方案如下：
◆加固运营商App，以及通过运营商应用市场推广的所有第三方App。
◆对提交到运营商应用市场的第三方App提供病毒、木马、恶意代码查杀服务。
◆对运营商的计费SDK提供基于防调、防改、防破解的加固保护服务。
◆对运营商的通信协议、证书进行加密。
◆提供基于移动应用的威胁态势感知服务，实时预警接入网络的异常流量、入侵攻击、风险App等。

移动应用安全综合应用案例分析

移动办公安全：移动办公主要面临以下风险：
◆设备丢失。操控丢失设备接入企业内网，窃取企业机密数据，破坏后台系统。
◆信息泄露。存储在本地设备中的敏感数据丢失或被窃取，导致信息泄露。
◆恶意攻击。植入恶意程序，对组织机构服务器进行入侵攻击。
◆共享访问。员工分享设备、账号密码，泄露组织机构机密信息。
◆WiFi监听。接入钓鱼热点，通信数据被劫持监听。

◆针对移动办公安全问题，网络安全厂商提出移动设备安全接入、移动设备安全管理、移动恶意代码防范、移动App安全加固等技术方案。以360移动终端安全管理系统方案为例，其方案描述如下。
◆ 360天机移动终端安全管理系统包括安全管理平台和移动客户端两个部分，通过管理平台对装有移动客户端的终端进行安全管理，提供对终端外设管理、配置推送、系统参数调整等服务，同时结合管理员可控的安全策略机制，实现更全面的安全管控特性。



谢谢！