



移动互联网核心安全需求及防护研究^{*}

许方恒, 陈 暄, 沈才樑, 杜焕强

(浙江工业职业技术学院信息工程学院 绍兴 312000)

摘 要:近年来,移动互联网在技术、业务和用户需求的驱动下得到了快速发展。然而,我国移动互联网发展在总体上仍然处于产业的初步形成阶段,产业形态、格局还不是非常清晰。在移动互联网发展的基础上,纵观新形势下网络存在的安全问题,重点介绍了移动互联网网络受到的威胁,并提出了移动互联网安全防护思路和相关建议。

关键词:移动互联网;核心安全需求;安全防护思路

doi: 10.3969/j.issn.1000-0801.2013.11.013

Research of Mobile Internet Core Security Requirement and Protection

Xu Fangheng, Chen Xuan, Shen Cailiang, Du Huanqiang

(Department of Information Engineering, Zhejiang Industry Polytechnic College, Shaoxing 312000, China)

Abstract: Driven by the technology, service and user demand, the mobile internet has enjoyed rapid development in recent years. However, the mobile internet industry of China is still at the initial stage with its form and pattern remains unclear. Based on the development of mobile internet, an overview of the network security problems at current stage was presented, the threats facing mobile internet network were introduced and the relevant ideas and proposals on the security protection were raised.

Key words: mobile internet, core security requirement, security protection idea

1 新形势下的网络安全威胁

纵观 2011 年、2012 年,数据信息泄露事件愈演愈烈。

2011 年,CSDN、天涯、新浪等一批著名网站数据库连续外泄,涉及用户数量巨大。

2012 年 1 月,亚马逊旗下美国电子商务网站 Zappos 2 400 万用户的电子邮件和密码等信息被窃取。

2012 年 7 月,京东、雅虎、Linkedin 和安卓论坛累计超过 800 万用户信息泄露。

2012 年 10 月,媒体报道:有黑客组织声称破解了联邦

调查局(FBI)主管的笔记本电脑,获得了 1 200 万苹果 iOS 用户 UDID、用户名、设备名称、设备类型、苹果推送通知服务记录、电话号码、地址等重要内容。

2012 年 1 月至 8 月的数据与 2011 年同期对比:2012 年发生数据泄露事件数量较 2011 年略有下降;2012 年每发生一次数据泄露事件,造成平均 640 169 个身份被盗,这一数字与 2011 年相比,降幅超过一半;零售业与电信业是身份被盗数量的重灾区,信息技术和计算机软件次之;2012 年的被盗身份数量的中位数数据比 2011 年上升了 41%,这说明了黑客的攻击变得更有针对性和选择性。

^{*} 国家自然科学基金资助项目(No.61173124),浙江省科技厅科技计划基金资助项目(No.2012R30067),绍兴市科技局重点科技项目(No.2010ADJ1034)



2 移动互联网网络安全威胁

网上银行、手机程序、应用软件等遭受的威胁愈演愈烈。CNCERT 监测显示, 捕获移动互联网恶意程序增加较快, 针对网银的钓鱼网站域名不断增加。据 Gartner 权威统计, 目前 75% 的黑客攻击发生在 Web 应用层, 近期层出不穷的安全事件均源于 Web 应用层防护不到位所致, 应用系统漏洞的根源还是来自程序开发者对网页程序的编制和检测。只要网络设防或监管稍有不严, 攻击者就会利用一切可乘之机对互联网的任意角落发起各类攻击, 如非法窃听、用户身份仿冒、服务滥用、破坏数据和信令完整性、非授权定位。

图 1 为移动互联网技术体系示意。从图 1 可知, 移动互联网的内容安全涉及两个层面: 一是信息传输内容安全, 也就是加解密; 另外一个不是不良信息的核查。移动智能终端是最容易受到威胁, 同时也是受到安全威胁最严重的。

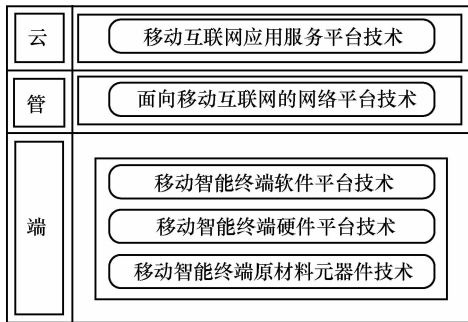


图 1 移动互联网技术体系

移动智能终端受到的安全威胁分为资费损失、隐私窃取、功能损坏等类别。

- 资费损失类。恶意代码数量剧增, 相对其他各种危害类型的恶意代码占比不断上升。智能终端恶意软

件植入方式包括伪装成正常软件通过分发网站植入、固件植入、系统漏洞植入、已安装恶意软件后台下载、诱骗下载、捆绑植入、手工植入。

- 隐私窃取。隐私窃取成为互联网和移动智能终端的重灾区, iOS、Android 都被曝发生过私自上传用户私密信息、搜集用户行为的事件。
- 功能损坏类。近年出现的变种“骷髅头”病毒不仅会对移动终端操作造成危害, 还附加了恶意吸费软件。

3 新形势下的安全需求

3.1 现状剖析

信息泄露事件频发的关键在于现有信息系统未能有效地解决身份可信及数据保护问题。信息泄露主要由以下问题引起:

- 身份可信问题没能解决;
- 特权人员难以管理;
- 安全事件难以定位;
- 数据泄密问题严重。

目前, 安全风险重点已从可用性转移至信息资产损失, 从统计数据来看, 企业服务器端的防护将成为整个安全链条上的薄弱环节。基于口令的用户认证机制难以抵抗穷搜索和字典攻击。安全投入不足导致大规模用户信息资产损失事件集中爆发。无线应用固有的安全隐患和相应程序自身的漏洞预计将给计算能力有限的无线终端带来更大的安全威胁。

3.2 移动互联网安全需求

图 2 从国家、运营商、企业用户、个人用户等的安全需求角度出发, 全面反映了移动互联网安全的重要意义。

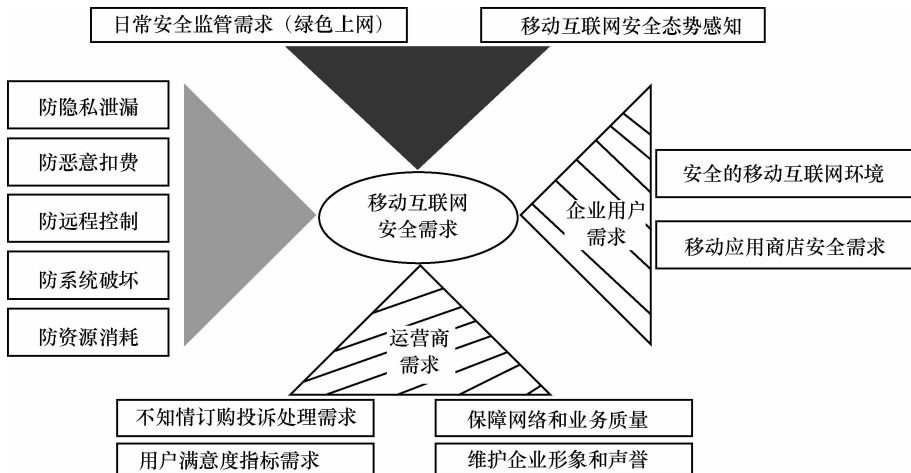


图 2 移动互联网安全需求

3.3 核心安全需求

可信、开放、体系化服务是移动互联网、云计算、大数据发展的必备要件。

云计算的出现使得传统的网络边界不复存在,信息的所有权和管理权分离,信息资产的非授权访问成为云计算系统的首要安全问题。云计算多租户环境、虚拟技术、动态性、数据迁移等综合因素导致数据安全和隐私保护面临更大挑战。

国外科技、媒体和电信行业的公司普遍认为,企业员工移动设备中存储的数据将会给企业带来最大的信息安全风险。移动终端存储的隐私信息及蕴含的经济利益使其成为黑客首要的攻击目标。网络违法犯罪行为的趋利化特征明显。

大数据集中凸现大容量、高价值、多样性、频繁周转的业务特征。数据防泄露、身份与访问管理是安全需求焦点。

依靠传统孤立地采用一种安全产品或技术,部署在局部范围内来识别和发现网络中的安全事件已经非常困难或有失准确性。共享安全信息数据,基于统一的安全体系结构整合单点产品实现安全保障成为必然。

安全将从硬件交付、软件交付向运营化服务过渡,依托产品+服务,提供 7x24 h 的运营化服务才能更无缝地契合用户的安全需求。

4 移动互联网安全防护思路

4.1 减少我国移动恶意应用的数量和危害

减少我国恶意应用的数量,必须加强以下几方面的力度。

(1)加强移动应用商店的安全审核机制

关于移动商店的安全审核机制可参见表 1。

(2)应用商店的安全审核要严格

实行开发者中心账户验证机制,无论是公司账户或个人、学生账户均需身份证;实行软件审查机制,5~7 天进行人工审核;建立应用商店下载机制,采用 DRM 技术和加壳混淆技术,下载时需手机实时与服务器多次通信交换设备密钥。

(3)确定可疑行为的危害程度

大量存在的可疑行为急需确定其危害程度,尤其是多个可疑行为组合后的危害程度。

(4)需要权威第三方来执行

应用商店安全审核需要权威第三方来执行。

4.2 监控移动互联网恶意程序

(1)移动互联网恶意程序的分类

移动互联网恶意程序主要分为恶意扣费、远程控制、

表 1 移动应用商店的安全审核机制

移动商店	注册是否需要上传身份证		是否有开发者身份审核		是否有应用杀毒扫描		垃圾广告应用是否通过	
	公布	测试	公布	测试	公布	测试	公布	测试
91 手机资源商城	是	是	是	否	是	是	是	否
中关村在线市场	是	是	是	是	是	是	是	是
优亿市场	是	是	是	是	是	是	是	是
腾讯应用中心	是	是	是	是	是	是	是	否
360 应用中心	是	否	是	否	是	是	是	否
安卓网	是	是	是	是	否	是	否	是
机锋市场	是	是	否	否	是	是	是	是
木蚂蚁应用市场	是	是	是	是	是	是	是	是
Appchina 应用汇	否	否	否	否	是	是	是	否
N 多网	否	否	否	否	是	是	是	是
安卓市场	否	否	否	否	是	是	是	是
网易应用中心	否	否	否	否	是	是	是	否
百度应用中心	否	否	否	否	是	是	是	否
搜狐应用中心	否	否	否	否	是	是	否	否
豌豆荚	否	是	否	否	否	否	否	是
中国移动 MM 商店	是	否	是	否	是	是	否	否
中国联通 WO 商店	是	是	是	是	是	是	是	否
中国电信天翼商城	是	是	是	是	是	是	是	否
联想乐商城	是	是	是	否	是	是	是	是
小米应用商城	是	是	是	否	是	否	是	否



隐私窃取、恶意传播、资费消耗、系统破坏、诱骗欺诈、流氓行为等。TOP 活跃恶意程序见表 2。

从表 2 所列 TOP 活跃恶意程序可以看出:不同地域的流行病毒种类不尽相同;同一类病毒在不同地域的流行程度不同;恶意扣费、隐私窃取类病毒在流行病毒中所占比例最大。恶意程序造成用户隐私信息泄露,如窃取通讯录、通话记录、短信内容、定位信息、账户信息等。为用户正常使用造成不便,如破坏手机系统或部分功能、恶意删除用户软件、耗尽电池而使手机无法使用等。

4.3 移动互联网恶意程序安全防护方案

在移动通信核心网,移动互联网恶意程序安全防护方案与通信管道结合,建设面向互联网的安全监测与处置系统,

并辅以终端安全杀毒软件,可有效解决传统方案面临的难点问题。移动互联网恶意程序安全防护方案如图 3 所示。

移动互联网恶意程序安全防护方案实现功能如下。

终端侧计算能力制约了防护手段,解决终端侧防护技术的制约,移动智能终端的安全防护技术刚起步,智能终端有限的计算能力和宽带无线网络有限的空口资源制约了移动互联网安全防护措施的有效性,急需建立全程全网的移动互联网网络安全监测、预警及处置体系,实现云、管、端一体化联动。

管道侧实现恶意行为和软件的实时监测和阻截,安全云实现恶意行为和软件的集中研判和处置,移动终端实现终端恶意程序的确认和清除。

表 2 TOP 活跃恶意程序(2013 年 2 月数据)

区域	序号	病毒名称(中文)	病毒名称(英文)	属性主分类	感染用户数
A 区域	1	伪视频病毒变种	Video.B	恶意扣费	4 271
	2	疯狂短信	Smswish.A	隐私窃取	3 763
	3	泄密超短裙病毒变种	skirtup.b	隐私窃取	3 387
	4	XVCI 病毒变种	XVCLB	隐私窃取	3 119
	5	系统设置吸费王	Smart.A	资费消耗	2 998
	6	JazzMusic 病毒	JazzMusic.A	隐私窃取	2 792
	7	FakeS60App 病毒	FakeS60App.a	恶意扣费	2 395
	8	伪 OVI 客户端病毒	OVIClient.A	隐私窃取	2 336
	9	毒媒手机木马	dumusicplay.b	远程控制	2 204
	10	伪视频病毒	Video.A	隐私窃取	2 194
B 区域	1	伪视频病毒变种	Video.B	恶意扣费	5 719
	2	AknMimeUpdateSrv 病毒	AknMimeUpdateSrv.A	隐私窃取	3 879
	3	疯狂短信	Smswish.A	隐私窃取	3 746
	4	InstallGuide 病毒	InstallGuideDy.A	系统破坏	3 523
	5	伪云视频病毒	Cloudvideo.A	系统破坏	3 149
	6	Videoff 木马	Videoff.A	隐私窃取	2 929
	7	AppServer 病毒	AppServer.B	隐私窃取	2 477
	8	伪安全监测中心病毒	20063FE4.A	隐私窃取	2 441
	9	伪彩信病毒	OviPerform.A	隐私窃取	2 321
	10	JazzMusic 病毒	JazzMusic.A	隐私窃取	2 236

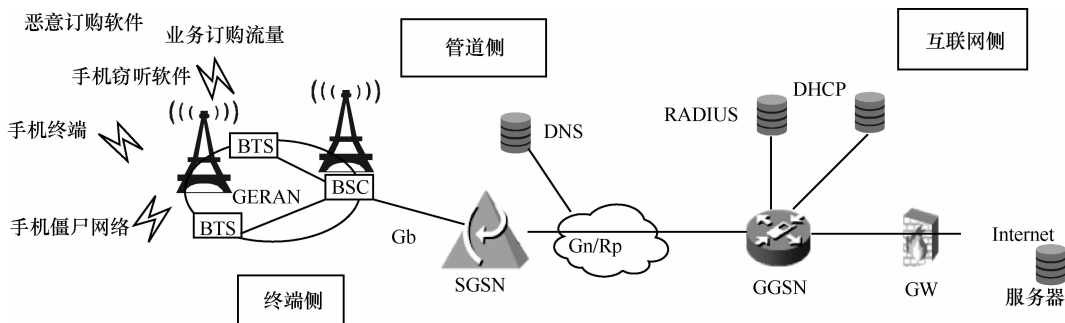


图 3 移动互联网恶意程序安全防护方案

移动互联网云安全防护平台如图 4 所示。

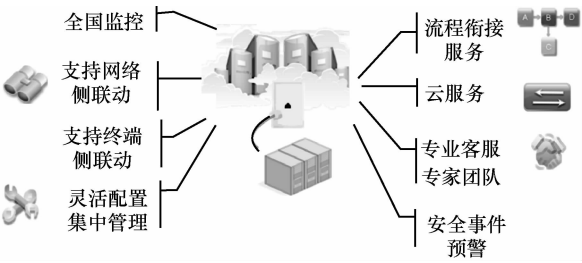


图 4 移动互联网云安全防护平台

5 结束语

近年来,移动互联网在技术、业务和用户需求的驱动下得到了快速发展。然而,我国移动互联网发展在总体上仍然处于产业的初步形成阶段,数据信息泄露事件愈演愈烈,网上银行、手机程序、应用软件所涉及的移动互联网网络安全遭受的威胁愈演愈烈。移动互联网安全对于国家、运营商、企业用户、个人用户具有重要意义。

当前复杂、多样、频发的大规模信息安全事件,暴露了现网应用系统的脆弱性,特别是缺乏完整、开放、安全身份互信机制,应用系统安全风险重点已从可用性转移至信息资产损失。

移动互联网、云计算、大数据已逐步进入规模化发展阶段,信息安全重心已从边界防护转向数据保护。身份互信、数据防护已成为移动互联网、云计算、大数据发展的核心基

础安全需求。

产业链相关各方应携手合作,基于可信应用安全架构,适应市场发展需求,构建移动互联网云安全防护平台,携手共同建设可信应用生态体系,以期更好地服务客户,促进产业繁荣发展。

[作者简介]



许方恒,男,浙江工业职业技术学院信息工程学院讲师,主要研究方向为数据库与信息系统、信息安全、网络通信。

陈暄,男,浙江工业职业技术学院信息工程学院讲师、系统分析师、信息系统项目管理师,主要研究方向为计算机体系结构、软件方法学、算法设计。

沈才樑,男,浙江工业职业技术学院信息工程学院教授,主要研究方向为虚拟现实、系统仿真、计算机网络。

杜焕强,男,浙江工业职业技术学院信息工程学院讲师,主要研究方向为信息安全、计算机网络。

(收稿日期:2013-08-30)



·简讯·

2013 年 9 月通信业主要指标完成情况 (二)

指标名称	单位	本月末到达	比上年末净增	本月净增
固定电话用户合计	万户	27 040.2	-775.1	-93.6
公用电话用户	万部	2 260.3	-86.8	-5.8
城市电话用户	万户	18 613.3	-280.1	-37.2
住宅电话用户	万户	10 604.9	-408.3	-41.6
农村电话用户	万户	8 427.0	-494.9	-56.4
住宅电话用户	万户	6 816.2	-499.6	-54.1
移动电话用户合计	万户	120 655.3	9 439.8	1 093.7
其中:3G 用户	万户	36 759.8	13 479.4	1 630.8
互联网拨号用户	万户	560.8	-9.0	-0.4
互联网宽带接入用户	万户	18 580.7	1 595.4	170.1
其中:xDSL 用户	万户	11 087.5	-377.4	-63.3
移动互联网用户	万户	81 953.6	5 517.2	-825.7
固定电话普及率	部/百人	20.0		
移动电话普及率	部/百人	89.2		

注:(1)收入增长率按可比口径计算。(2)固定长途电话通话时长和移动电话通话时长均包含相应的 IP 电话通话时长。(3)通话时长各项指标均为去话通话时长。

(来源:工业和信息化部运行监测协调局)