移动互联网安全研究

贾心恺　中国人民解放军驻上海沪东中华造船（集团）有限公司军事代表室
顾庆峰　海军驻广州地区通信军事代表室

【摘　要】文章以移动互联网网络结构为基础，分析了移动互联网各个层次的安全威胁，从而给出了移动互联网安全框架和解决方案，最后设计了移动互联网安全防护系统。

【关键词】移动互联网　应用安全　安全管理　基础支撑　安全防护系统

1　移动互联网概述

移动互联网是移动网络与互联网融合的产物，并且随着两者融合的扩大和深入，能够为用户提供更具移动特性的、更深入到人们生产生活的网络与服务体系。移动互联网以手机、个人数字助理（PDA）、便携式计算机、专用移动互联网终端等作为终端，以移动通信网络（包括2G、3G、4G等）或无线局域网（WiFi）、无线城域网（WiMAX）作为接入手段，直接或通过无线应用协议（WAP）访问互联网并使用互联网业务。移动互联网网络结构如图1所示：

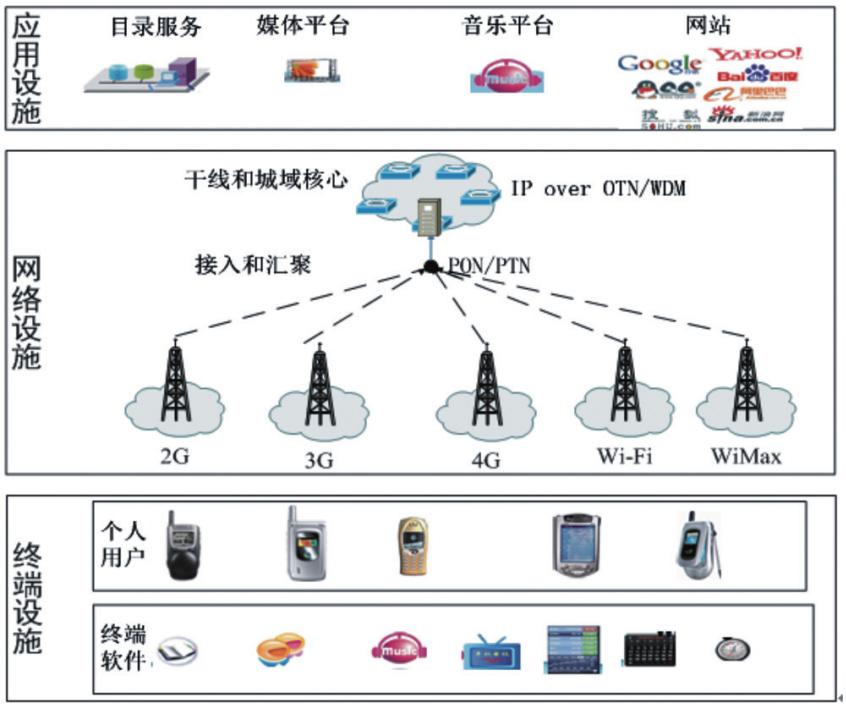

图1　移动互联网网络结构

收稿日期：2011-05-12

责任编辑：左永君　zuoyongjun@mbcom.cn

移动互联网安全威胁存在于各个层面[1-2]，包括终端安全威胁、网络安全威胁和业务安全威胁。智能终端的出现带来了潜在的威胁，如信息非法篡改和非法访问，通过操作系统修改终端信息，利用病毒和恶意代码进行系统破坏。数据通过无线信道在空中传输，容易被截获或非法篡改。非法的终端可能以假冒的身份进入无线通信网络，进行各种破坏活动；合法身份的终端在进入网络后，也可能越权访问各种互联网资源。业务层面的安全威胁包括非法访问业务、非法访问数据、拒绝服务攻击、垃圾信息的泛滥和不良信息的传播等。

2 移动互联网安全框架

根据上节的分析，将移动互联网安全分为应用安全、网络安全和终端安全三个层次。移动互联网安全框架如图2所示，其中安全管理负责对所有安全设备进行统一管理和控制，基础支撑为各种安全技术手段提供密码管理、证书管理和授权管理服务。

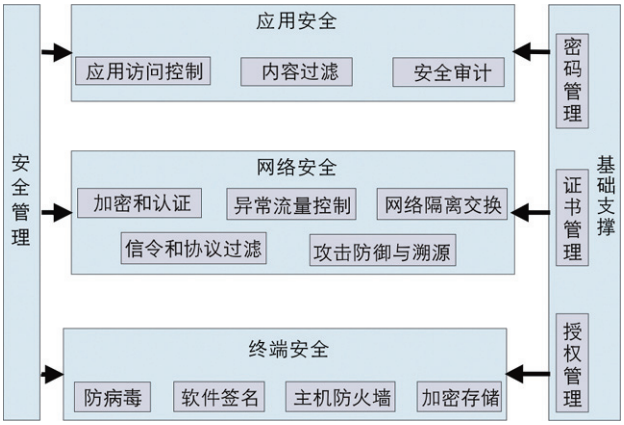

图2　移动互联网安全框架

2.1 应用安全

移动互联网业务可以来自互联网、移动网以及移动网与互联网结合所得的创新业务，包括移动浏览、移动Web2.0、移动搜索、移动地图、移动音频、移动视频、移动广告、移动Mashup等业务。应用安全主要采用如下措施保证移动互联网业务的安全[3]：

（1）应用访问控制

由于互联网上资源众多，资源的种类和信息量日益增加，使用环境也越来越复杂，必须有严格的安全认证手段，以防止对手控制资源的非法访问和非授权访问。应用访问控制为应用系统提供统一的基于身份令牌和数字证书的身份认证机制、基于属性证书的访问权限控制，保护受控制的信息不被非法和越权访问，并对事后的追踪提供可靠的依据。应用访问控制采用安全隧道技术，在应用的客户端和服务器之间建立一个安全隧道，并且隔离客户端和服务器之间的直接连接，所有的访问都必须通过安全隧道，没有经过安全隧道的访问请求一律丢弃。

（2）内容过滤

Web内容过滤：内容过滤基于分类库的URL进行访问控制，对色情、反动等多种负面网站按类别进行选择控制；对Web网页关键字和Java、JavaScript、ActiveX等移动代码过滤；以黑名单/白名单、通配符、正则表达式的方式进行网址过滤。反垃圾邮件：对收发邮件的地址、附件名、附件内容、主体、正文内容、收发邮件人姓名等关键字匹配过滤；对中转垃圾邮件进行识别和过滤；具备反垃圾邮件功能，在线查询垃圾邮件服务器，阻断垃圾邮件源。

（3）安全审计

安全审计一般包含两类审计策略：系统审计策略控制哪些事件应该作为系统相关的活动被记录，包括主体鉴别、改变特权以及管理安全策略的事件（如修改访问控制数据）等；应用审计策略控制应用程序应该审计哪些事件。

2.2 网络安全

移动互联网网络主要分两部分，接入网及IP承载网/互联网。接入网采用移动通信网时涉及基站（BTS）、基站控制器（BSC）、无线网络控制器（RNC）、移动交换中心（MSC）、媒体网关（MGW）、服务通用分组无线业务支持节点（SGSN）、网关通用分组无线业务支持节点（GGSN）等设备以及相关链路，采用WiFi时涉及接入（AP）设备。IP承载网/互联网主要涉及路由器、交换机、接入服务器等设备以及相关链路[4]。

（1）加密和认证

加密和认证体系可以参考WPKI认证体系[5]。WPKI（WAP Public Key Infrastructure）借鉴PKI标准的主要思想，并针对WAP安全规范和移动互联网的特别环境做了必要的改动。WAP安全规范包括WAP传输层安全规范WTLS、WAP应用层安全规范、WIM规范和WAP证书管理规范。

数据加密。移动终端和服务器初次通信时，它们通过WTLS握手协议商定一组会话状态的密码参数，包括协议版本号、选择密码算法、可选择的相互鉴别，使用公开密钥加密技术生成共享密钥。在应用数据阶段中，所生成的共享密钥（预主密钥）将首先被转换成主密钥，主密钥再被转换成加密密钥和MAC密钥，加密密钥为客户机和服务器所共有，使用它对传输数据进行对称加密，保证了机密性，并提高了加密速度。移动终端的弱计算力将影响加密算法的选择和实现。由于移动终端CPU的处理能力有限，所以椭圆曲线算法（ECC）特别适用于移动互联网公钥体系。

身份认证。在进行安全握手时，服务器的证书会通过无线网络传到移动终端。对无线网络而言，定义一种缩微证书格式是很有必要的，这既能减轻传输负载，也可以减轻移动终端的处理负载。WTLS证书是X.509证书的缩微格式，适用于无线网络环境。电子商务应用需要一种证书取消机制，在无线网络环境下，可以采用短时效证书来实现证书取消。对内容服务器或WAP网关依旧采用长时效信用验证，但同有线网络不同的是，在时效期间，不是自始至终用一对密钥。证书颁发机构每天都向内容服务器或WAP网关颁发新的证书，如果证书颁发机构决定取消对服务器的信用，就不再颁发证书。

（2）异常流量控制

异常流量控制对协议、地址、服务端口、包长等进行流量统计，基于地址特征进行会话数统计，基于策略进行流量管理和Diffserv服务等级设置，还可以进行最大/最小/优先带宽控制和DSCP服务级别设置，以及上下行双向流量控制。

（3）网络隔离交换

网络隔离交换能够实现两个互联网络的安全隔离，并只允许指定的数据包在两个网络之间进行交换。通过设置两个独立的网络处理单元，每个网络处理单元对应一个连接的网络，各网络处理单元间具有惟一的隔离数据通道；两个网络处理单元在物理上是两个独立的实体，二者通过隔离通道实现数据交换，任何一个网络处理单元都不能控制另一个网络处理单元的运行；各处理单元之间交换的对象不是IP数据报文，而是经专用内部协议封装的应用层数据报文，任意原始IP数据报文不可能通过该通道实现数据交换。

（4）攻击防御与溯源

攻击防御能检测并抵抗DDoS/DoS攻击，积极防御syn flood、ping flood、arp flood、udpflood、teardrop、sweep、land-base、ping of death、smurf、winnuke、ipspoofing、sroute、queso、sf_scan、null_scan等（D）DoS攻击；基于内置事件库对各种攻击行为进行实时检测；在发现攻击行为后能追溯攻击源，便于事后跟踪和监察。

（5）信令和协议过滤

移动通信网由基站、核心网设备等功能单元组成，能够提供移动电话业务；固定电话网由端局、汇接局等主要功能单元组成，能够提供固定电话业务；移动通信网环境和固定电话网通过七号信令实现网络互联和业务互联。信令和协议过滤能防御针对七号信令和各种通信协议的攻击，在安全管理系统的管控下完成信令和协议安全防护功能。

2.3 终端安全

（1）防病毒

移动互联网终端多属智能设备，通常具备操作系统，应当对常见的病毒如木马、钓鱼和针对操作系统、应用程序漏洞的攻击具备一定的防范能力[4]。防病毒支持HTTP、FTP、POP3、SMTP、IMAP协议的病毒防护；可过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒；能对Blaster、Nachi、Nimda、Redcode、Sasser、Slapper、Sqlexp、Zotob等主流蠕虫病毒进行过滤和拦截；对灰色软件、间谍软件及其变

责任编辑：左永君 zuoyongjun@mbcom.cn

种进行阻断。

（2）软件签名

通过签名手段对软件进行完整性保护，防止软件被非法篡改。一旦检测到应用程序被非法篡改，可以向安全管理设备报警。

（3）主机防火墙

通过在智能终端上进行主机防火墙的控制，可以通过白名单/黑名单对呼入呼出号码进行控制，对进出终端的数据包进行基于五元组等特征的控制。

（4）加密存储

移动互联网终端的信息自身安全主要是指存储在终端中的用户隐私信息和个人信息（包括通信录、通话记录、收发的短信/彩信、IMEI号、SIM卡内信息、用户文档、图片、照片在内）不被非法获取。重要信息加密存储在终端上，防止被非法窃取，并且加解密是低延迟的，对用户透明。

2.4 安全管理

安全管理设备能够对全网安全态势进行统一监控，在统一的界面下完成对所有安全设备的统一管理，实时反映全网的安全状况，能够对产生的安全态势数据进行汇聚、过滤、标准化、优先级排序和关联分析处理，提高安全事件的应急响应处置能力，还能实现各类安全设备的联防联动，有效抵挡复杂的攻击行为。

2.5 基础支撑

基础支撑包括密钥管理、证书管理和授权管理，证书、密钥及授权管理系统支持单机模式和级联模式。级联模式分为一级中心和二级中心，一级中心包含所有二级中心的密钥数据，二级中心只含有自己的密钥数据。证书密钥及授权管理系统为涉密信息系统提供互联互通密码配置，以及公钥证书和对称密钥的管理。

3 安全防护系统设计

为了将移动互联网安全框架细化，并验证移动互联网安全技术手段，设计移动互联网安全防护系统如图3所示。这需要研制终端安全软件、信令和协议过滤设备、内容过滤系统、网络密码机、网络隔离交换设备、异常流量监控设备、攻击检测和溯源系统、应用访问控制设备、安全管理设备、密码管理系统、证书管理系统和授权管理系统，并将这些设备和系统进行集成联试，形成一个有机整体的安全防护体系。

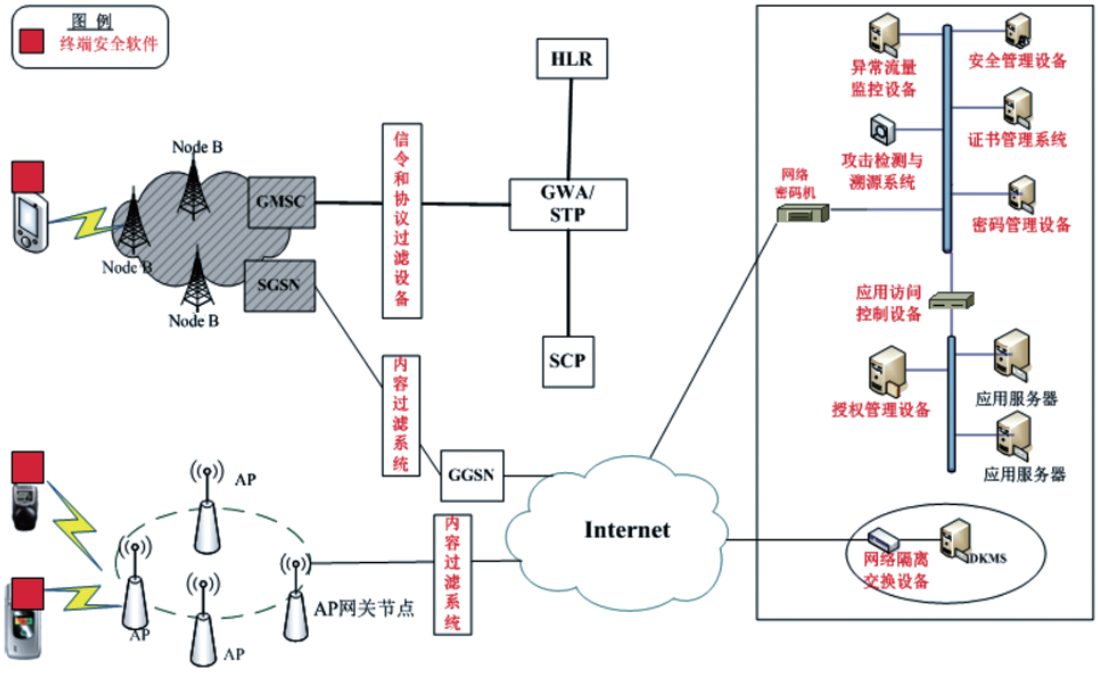

图3　安全防护系统设计

4 总结

本文在移动互联网网络结构的基础上，分析移动互联网各个层次的安全威胁，并给出了移动互联网安全框架和解决方案：从应用安全、网络安全和终端安全三个层面进行安全防护，通过安全管理对所有安全设备进行统一管理和实现安全设备间的联防联动，通过基础支撑为三个层面的安全防护手段提供密码、证书和权限服务。也给出了移动互联网安全防护系统的设计。对移动互联网安全防护系统功能、性能和关键技术的验证是下一步的工作。

参考文献

[1]蒋晓琳,黄红艳. 移动互联网安全问题分析[J]. 电信网技术,2009(10).
[2]杨剑锋. 移动互联网安全威胁探析[J]. 电信网技术,2009(3).
[3]魏亮,伍国锐. 移动互联网安全探讨[J]. 现代电信科技,2009(4).
[4]王永斌. 移动互联网安全探析[J]. 通信世界,2008(47).
[5]谢胜落,张佩辰. 移动互联网安全加密技术[J]. 网络安全技术与应用,2001(4). ★

【作者简介】

贾心恺：现任中国人民解放军驻上海沪东中华造船（集团）有限公司军事代表室高级工程师，技术七级，主要从事舰船的通信系统、反潜系统、导航系统和电子战系统等武备电子专业的研究。

顾庆峰：本科毕业于海军电子工程学院，现任职于海军驻广州地区通信军事代表室，主要从事无线电通信工程的管理。

R&S DVMS数字电视监测系统已全面支持对DVB-T2网络的监测

R&S DVMS紧凑型数字电视监测系统新增了两个选件，使其成为目前市场上唯一在单台设备上实现DVB-T2网络监测的解决方案。网络运营商无需增加其它设备，就可以通过T2-MI接口监测DVB-T2发射机及其信号回路。此外，R&S DVMS还支持对单频网和射频频谱（带肩测量）的监测。

DVB-T2作为DVB-T的升级版标准，目前已开始应用。在欧洲，已建立了第一个DVB-T2网络，它提供了DVB-T2的所有优势，如：提高了30%的传输容量，高清节目的传输，覆盖能力更强等等。为了对DVB-T2网络进行全面的监测，罗德与施瓦茨公司发布了用于R&S DVMS数字电视监测系统上的两个DVB-T2选件。

通过R&S DVMS-B54 DVB-T2选件接收模块，网络运营商可以测量和解调DVB-T2信号。使用R&S DVMS-K3选件，就可以通过R&S DVMS上的ASI和IP接口对T2-MI信号进行监测和分析。对于IP接口，R&S DVMS可以支持电口和光口，这样就可以适应网络中不同接口类型的需要。此外，用于带肩和单频网测量的DVB-T选件也可以支持DVB-T2的相关测量。

R&S DVMS仅有1U高度，是目前市场上可同时监测多种数字电视信号的最为紧凑型的设备。它可以监测射频、IP和传输流层的所有相关错误，为网络运营商提供了一个全面的监测解决方案。R&S DVMS系列有两个型号：R&S DVMS4可以同时监测一个发射站内多达4台发射机的射频信号，R&S DVMS1则适用于只需进行一路射频或传输流监测的发射站。R&S DVMS系列具有高度的灵活性，可以有效满足用户的特定需求，同时又有极佳的性价比。

R&S DVMS-B54 DVB-T2选件目前已可以订购，R&S DVMS-K3选件（T2-MI监测）将于2011年6月发布。

责任编辑：左永君 zuoyongjun@mbcom.cn