·移动互联与通信技术·　　文章编号：1000-3428(2018)05-0078-05　　文献标志码：A　　中图分类号：TP309

基于图的可扩展移动应用安全评估模型

陈　璐[1]，刘　行[2]，陈　牧[1]，李尼格[1]，戴造建[1]

（1. 全球能源互联网研究院有限公司 信息网络安全国网重点实验室，南京 210003；
2. 南京南瑞信息通信科技有限公司，南京 210003）

摘　要：目前针对移动应用的安全评估方法多数关于漏洞收集和恶意样本行为的关联挖掘，难以应对移动应用快速增多的现状。为此，将安全漏洞和攻击威胁作为节点，基于攻击图的方式构建移动应用安全威胁评估模型。使移动应用的安全漏洞和攻击威胁基于关联性相互连接，在评估移动应用的安全威胁时量化漏洞风险值并考虑其关联性对评估结果的影响。实验结果表明，该模型能够提高移动应用安全威胁评估的准确性，并且适用于大规模移动应用模型的构建，具有良好的可扩展性。

关键词：移动应用；评估模型；安全漏洞；攻击威胁；风险值

中文引用格式：陈　璐，刘　行，陈　牧，等. 基于图的可扩展移动应用安全评估模型[J]. 计算机工程，2018，44(5)：78-82.

英文引用格式：CHEN Lu，LIU Xing，CHEN Mu，et al. Scalable Security Evaluation Model of Mobile Application Based on Graph[J]. Computer Engineering，2018，44(5)：78-82.

Scalable Security Evaluation Model of Mobile Application Based on Graph

CHEN Lu[1]，LIU Xing[2]，CHEN Mu[1]，LI Nige[1]，DAI Zaojian[1]

（1. State Grid Key Laboratory of Information and Network Security，
Global Energy Interconnection Research Institute Co.，Ltd.，Nanjing 210003，China；
2. Nanjing NARI Information Communication Technology Co.，Ltd.，Nanjing 210003，China）

【Abstract】At present，the evaluation methods of mobile application mostly focus on the association mining of the vulnerability collection and malicious sample behaviors，which is difficult to cope with the rapid increase in mobile applications. Aiming at this problem，based on the attack graph，this paper takes security loopholes and attack threats as node and establishes a mobile application security threat assessment model. It makes the mobile application vulnerabilities and attack threats interconnected based on the relevance. At the same time，it considers the quantification of the vulnerability risk value and the impact of the relevancy on the assessment results when evaluating the security threats of mobile application. Experimental results show that this model can improve the accuracy of mobile application security threat assessment，and can be used for large-scale mobile application model building with good scalability.

【Key words】mobile application；evaluation model；security vulnerability；attack threat；risk value

DOI：10.19678/j.issn.1000-3428.0046075

0　概述

移动通信和移动互联网技术的飞速发展使移动智能设备在社会各领域被广泛应用。GSMA 报告显示 2014 年底全球共有 36 亿移动用户，其中智能手机用户达到了 26 亿，我国的智能手机用户则在 2014 年6 月底超过了 5.27 亿[1]，智能手机已超越个人电脑成为主流网络工具。而根据中国互联网协会、国家互联网应急中心联合发布的《中国移动互联网发展状况及其安全报告(2016)》资料显示，2015 年中国境内活跃的手机网民数量达 7.8 亿人，活跃的智能手机联网终端达 11.3 亿部[2]。与此同时，移动智能设备所具有的功能扩展性和平台开放性带来了数以百万计的移动应用程序，这些移动应用给人们提供了诸如 MP4、网络相机、电子书等多样化的服务。

然而，上述移动应用在给人们带来便利的同时，也带来了各种安全问题，病毒、木马与恶意软件等攻击技术和威胁方式给移动智能设备应用程序与用户

基金项目：国家电网公司科技项目“电力移动应用信息安全防护关键技术研究”(SGRIXTKJ[2016]183 号)。

作者简介：陈　璐(1984—)，女，工程师、硕士，主研方向为移动通信、信息安全、移动应用安全；刘　行、陈　牧，工程师、硕士；李尼格、戴造建，高级工程师。

收稿日期：2017-02-23　　**修回日期：**2017-05-23　**E-mail：**chenluchina@aliyun.com

信息安全造成重大威胁[3]。由于移动应用开放的应用市场中存在层次不齐的应用商店以及相对宽松的应用审核机制,导致恶意软件泛滥,安全威胁与日俱增。同时,通过正规渠道下载的移动应用也存在二次打包、漏洞利用、恶意行为等不安全因素,这些不安全的移动应用会对移动终端用户造成巨大的安全风险和资产损失[4-6]。根据安天发布的《2016 移动安全年报》显示,移动互联网在 2016 年仍面临恶意应用的持续威胁,新增威胁继续涌现,威胁手段持续进化,攻击者加强仿冒、社工欺诈、勒索手段、权限冒用、开源组件恶意利用等攻击手段的使用。同时存量威胁依然泛滥,电信诈骗拦截马、扣费、流氓、色情等威胁仍在持续演化和进化,整个移动威胁面临全面迁徙和规模化增长以及爆发。因此,针对移动应用进行分析和安全保护具有重要意义[7]。

目前,研究人员提出了一些面向移动应用的安全评估方法[8-9],但其中多数集中在对漏洞收集、恶意样本行为等的关联挖掘研究,面对快速增大的移动应用规模安全评估能力较差[10]。针对该问题,本文构建一种基于图的可扩展移动应用安全评估模型,以期提高评估准确性。

1　相关研究

文献[11]针对移动应用的安全评估模型构建问题,分析了风险评估的 3 个要素:威胁行为,资产,脆弱性,同时建立一种新的智能终端系统安全风险评估模型。该模型基于 AHP 算法和安全评估的各要素,将整个移动应用系统分为不同的风险等级。

文献[12]针对智能终端的风险评估提出了一种需要裁剪的方法。该方法步骤如下:1)明确终端资产和威胁;2)通过分析危害程度确定威胁值;3)采用具体算法计算出风险评估值。

文献[13]通过对计算机网络攻击效果指标体系的研究,将其应用到移动终端评估中,建立层次化的移动终端攻击效果评估的指标体系,采用模糊层次分析法和多专家决策得出恶意软件的整体攻击效果评价。

文献[14]提出了一种基于图的移动终端系统安全评估方法。该方法借鉴攻击图方法,通过威胁图节点来构建安全威胁模型,其中节点分为威胁节点和缺陷或漏洞节点两类。该方法通过量化节点来对待测终端进行评估。

上述模型和方法在进行移动应用的安全评估时,只是针对特定的或者较小规模的移动应用进行安全威胁建模或评估[15]。然而,现有的移动应用通常是大规模存在的,针对移动应用的安全模型应该具有很好的扩展性[16]。同时移动智能系统存在的一些漏洞、安全机制具有一定的关联性,只有考虑到这些关联性,移动应用的安全评估才能更准确。

本文在借鉴上述研究成果的基础上,构建一种安全评估模型。该模型以安全漏洞和攻击威胁为节点,并以各个节点间的关联性相互连接,同时也考虑对漏洞风险值的量化和它们之间的关联性。

2　基于图的移动应用安全评估模型

2.1　移动应用安全评估模型分析

当前针对移动应用的攻击主要利用系统存在的安全漏洞获取用户权限。在该过程中,攻击者通过系统存在的漏洞,不断地利用恶意代码、病毒等实现权限的提升,获取用户的特定资源。

造成移动应用安全威胁的要素包括系统遭受的恶意代码、病毒等网络攻击,以及移动应用和系统固有的安全机制脆弱性、安全漏洞、策略漏洞等,本文称这两种要素为攻击威胁和安全漏洞。攻击者利用安全漏洞或者发动网络攻击获取用户权限。

攻击手段的发展,使得现有的攻击方法已经不局限于单一的攻击手段,而是采用多种攻击手段的组合攻击。因此,不同的网络攻击和安全漏洞之间存在一定的关联性。

根据上述分析,移动应用安全评估模型应是一个以安全漏洞和攻击威胁为节点的模型,其中各个节点之间存在特定的关联性,且模型各个节点通过这种关联性相互连接,具有可扩展性。

2.2　移动应用安全评估模型

根据 2.1 节的分析构建移动应用安全评估模型。该模型定义如下:

定义 1　模型 $G=(V,E,P,\beta,R)$ 为具有一个或者多个 AND-OR 节点的有向无圈图。

$V=\{V_i \mid i=1,2,\cdots,N_i\}$ 为威胁节点集合,包括攻击威胁和安全漏洞 2 种要素,它是一个非空有限的 AND-OR 节点集合。

$E=\{E_i \cup E_j\}$ 为关联各类节点的有向边集合。以 $e_{ij}=<V_i,V_j>$ 表示从节点 V_i 指向其子节点 V_j 的一条有向边,攻击者通过安全漏洞 V_i 获取权限后,沿着边 e_{ij} 向 V_j 发动攻击。一般地,记 $Pre(V_i)$ 为节点 V_i 的父节点集合,$Con(V_i)$ 为节点 V_i 的子节点集合。

$P=\{P_1 \cup P_2\}$。P_1 为安全漏洞的先验概率,即节点之间实现单步攻击的概率;P_2 为节点 V_i 在其父节点满足条件下的条件概率。由于只有 V_i 的父节点 $Pre(V_i)$ 满足条件时 V_j 才能发生,因此 $P_2=(V_i \mid Pre(V_i))$ 满足条件:

$$\{P_2:Pre(V_i),V_i\}\rightarrow[0,1] \tag{1}$$

β 为模型各节点的联合概率分布集合,表示攻击者成功利用该漏洞的难易程度。对任意节点变量 V_i:

$$\beta(V_i)\geqslant 0 \tag{2}$$

$R=\{\text{AND},\text{OR}\}$ 为节点之间关联关系的集合。AND 节点指的是节点 V_i 的所有父节点 $Pre(V_i)$ 之间

是 AND 关系,即 $Pre(V_i)$集合中的所有节点同时满足条件时,才能引发节点 V_i。图 1 是父节点$Pre(V_i)$之间是 AND 关系的示意图,只有 V_j和 V_k同时满足条件时才能引发节点 V_i。OR 节点指的是节点 V_i的所有父节点 $Pre(V_i)$是 OR 关系,即 $Pre(V_i)$集合中的任一节点满足条件时,就能引发节点 V_i。图 2 是父节点 $Pre(V_i)$之间是 OR 关系的示意图,只要 V_j 或者 V_k任一节点满足条件就能引发节点 V_i。

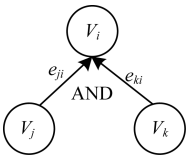


图 1 AND 关系节点

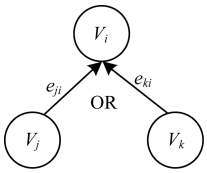


图 2 OR 关系节点

定义 2 对于一个模型 G,如果到达某个威胁节点所经历的所有节点和边组成的一组有序节点序列 $l=\{V_0,e_{01},V_1,e_{12},\cdots,V_i,e_{ij},V_j,\cdots,V_n\}$,使得对节点序列中任意 2 个相邻节点总有 $<V_i,V_j>\in E,(0<i<n,0<j<n)$,则称节点序列 l 为一条攻击路径。

3 移动应用安全威胁评估

3.1 威胁节点评估标准的量化

移动应用面临的攻击方法和安全漏洞是多样的,如何对这些攻击方法和安全漏洞进行量化,是准确评估安全威胁的前提和保障。文献[11-12]、移动终端信息安全技术要求(YD/T 1699-2007)等对移动应用的安全漏洞和攻击威胁进行量化,具体见表 1 和表 2。

表 1 安全漏洞的量化

安全漏洞描述	概率
公开报告过此攻击,未给出实现方法	0.1
公开报告过此攻击,简要提及实现方法	0.3
无攻击实现源码但有具体的实现方法	0.5
有可用的攻击实现源码和详细的实现方法	0.7
无需攻击工具,有详细的攻击实现方法	0.9
上述判断的中间值	0.2,0.4,0.6,0.8

表 2 攻击威胁的量化

风险级别	风险值范围
很低	[0.0,0.1]
低	(0.1,0.3]
中等	(0.3,0.5]
高	(0.5,0.7]
很高	(0.7,0.9]

考虑到安全漏洞之间的关联性,攻击者通过安全漏洞获取权限的可能性不仅和安全漏洞自身有关,也和攻击者利用该漏洞时所拥有的权限有关。因此,表 1 中安全漏洞的概率仅作为威胁节点的先验概率,即 P_1。

3.2 威胁节点概率的计算

攻击者通过安全漏洞获取权限的可能性和安全漏洞自身以及攻击者利用该漏洞时所拥有的权限有关。因此,威胁节点概率,即模型各节点的联合概率分布 β 取决于先验概率 P_1 和条件概率 P_2。本文对其给出如下定义:

定义 3 对模型 G 中的任意节点 V_i,其有 s 个父节点,即 $Pre(V_i)=\{V_1,V_2,\cdots,V_s\}$,则:

$$\beta(V_i)=P(V_i,V_1,V_2,\cdots,V_s)=P_1(V_i)\cdot P_2(V_i|V_1,V_2,\cdots,V_s) \tag{3}$$

定义 4 在模型 G 中,对于任意节点 V_i,其有 s 个父节点,即 $Pre(V_i)=\{V_1,V_2,\cdots,V_s\}$,则节点 V_i 发生的条件概率 $P_2(V_i|V_1,V_2,\cdots,V_s)$为:

1)如果 V_i 为起始节点,定义为 V_0,则:

$$P_2(V_i|V_1,V_2,\cdots,V_s)=1.0 \tag{4}$$

2)如果 $Pre(V_i)$中节点关系 $R=$AND,则:

$$P_2(V_i|V_1,V_2,\cdots,V_s)=\frac{1}{s}\sum_{j=1}^{s}\beta(V_j) \tag{5}$$

3)如果 $Pre(V_i)$中节点关系 $R=$OR,则:

$$P_2(V_i|V_1,V_2,\cdots,V_s)=\max\{\beta(V_j)|j=1,2,\cdots,s\} \tag{6}$$

4)如果 $Pre(V_i)$中节点关系既非 $R=$OR,又非 $R=$AND,则:

$$P_2(V_i|V_1,V_2,\cdots,V_s)=P_2(V_i|Pre(V_i))=\beta(Pre(V_i)) \tag{7}$$

定义 5 分析考虑威胁节点关联关系条件下威胁节点条件概率的数学模型。初始状态下,攻击者已经获取了利用初始威胁节点的权限。因此,初始的威胁节点条件概率为 1.0。对于初始威胁节点以外的节点,当节点 V_i的父节点间关系为 AND 时,表示攻击者必须成功地利用节点 V_i 得所有父节点漏洞才能获取节点 V_i的权限。因此,所有到达节点 V_i的父节点的概率是相同的。当节点 V_i的父节点间关系为 OR 时,表示攻击者只需成功地利用节点 V_i的具有最大威胁概率的父节点代表的漏洞,就能获取节点 V_i 的权限。此时,父节点中威胁概率的最大节点就会是攻击者所选择的威胁节点。当节点 v_i 的父节点间关系为非 AND 节点和非 OR 节点,实际上表示 V_i 的父节点只有一个,因此,父节点的威胁节点概率就是节点 V_i的条件概率。

3.3 安全威胁评估算法

本文设计移动应用的安全威胁评估算法 STNPA,依据移动应用安全评估模型 G 和各节点先验概率 P_1计算安全威胁节点概率 β。在任何一个时刻该评估算法都能评估那些未被利用的安全漏洞,并检测该时刻最可能的攻击路径(攻击者会选择那些具有最大节点概率的威胁节点作为下一个攻击目标),最后返回沿该路径欲到达的下一个攻击目标的

威胁节点概率β,其对应的安全风险量化值就是当前时刻的安全风险级别。β 计算方法见定义 4。STNPA 算法具体描述如下:

算法　安全威胁节点概率算法 STNPA

输入　模型 G,节点先验概率 P_1

输出　安全威胁节点概率 β

IF　节点 v 是初始节点　THEN　$\{P_2(v)=1.0\}$

RETURN $\beta(v)=P_1(v)\cdot P_2(v)$//初始节点安全//威胁节点概率

END IF

IF　节点 v 的父节点 Pre(v)中节点关系 R = AND THEN

v 发生的条件概率为 $P_2(V_i|V_1,V_2,\cdots,V_s)=\frac{1}{s}\sum_{j=1}^{s}\beta(V_j)$

RETURN $\beta(v)=P_1(v)\cdot\frac{1}{s}\sum_{j=1}^{s}\beta(V_j)$

END IF

IF　节点 v 的父节点 Pre(v)中节点关系为 OR　THEN

v 发生的条件概率为 $P_2(V_i|V_1,V_2,\cdots,V_s)=\max\{\beta(V_j)|j=1,2,\cdots,s\}$

RETURN $\beta(v)=P_1(v)\cdot\max\{\beta(V_j)|j=1,2,\cdots,s\}$

END IF

ELSE　节点 v 的父节点 Pre(v)中节点关系既非 R = OR,又非 R = AND,THEN v 发生的条件概率为 $P_2(V_i|V_1,V_2,\cdots,V_s)=\beta(Pre(V_i))$

RETURN $\beta(v)=P_1(v)\cdot\beta(Pre(v_i))$

4　实验与结果分析

为验证本文评估模型的有效性,实验选取 Android 系统存在的 9 个相关安全机制和安全漏洞作为节点,具体信息如表 3 所示。根据对待测终端和这些节点的分析,建立的安全评估模型 G,并为每个节点进行先验概率赋值,如图 3 所示。

表 3　选取的安全威胁节点

节点	名称	描述	概率
V_1	套接字漏洞	标准规定的中间值情况	0.8
V_2	权限提升	标准规定的中间值情况	0.8
V_3	机密性机制	有现成可用的攻击工具和详细的攻击方法	0.7
V_4	软件管理	有现成可用的攻击工具和详细的攻击方法	0.7
V_5	完整性机制	标准规定的中间值情况	0.6
V_6	访问控制机制	无现成可用攻击工具但有具体的攻击方法	0.5
V_7	SMS 短信安全漏洞	无现成可用攻击工具但有具体的攻击方法	0.5
V_8	系统审计机制	公开报告过此安全漏洞,简要提及攻击方法	0.3
V_9	CVE-2011-3901	公开报告过此安全漏洞,简要提及攻击方法	0.3

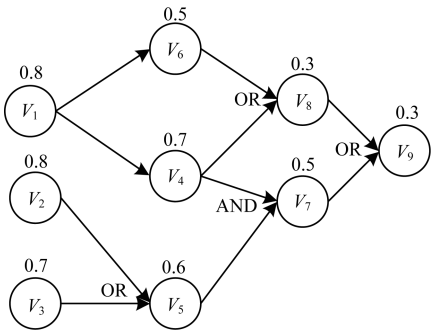


图 3　安全威胁评估模型构建示意图

依据表 3、图 3 以及 STNPA 算法所得到的各安全威胁节点评估值如图 4 所示。其中,β_1 表示未考虑各节点间关联关系情况下的安全威胁节点评估值,β_2 表示考虑各节点间关联关系情况下的安全威胁节点评估值。

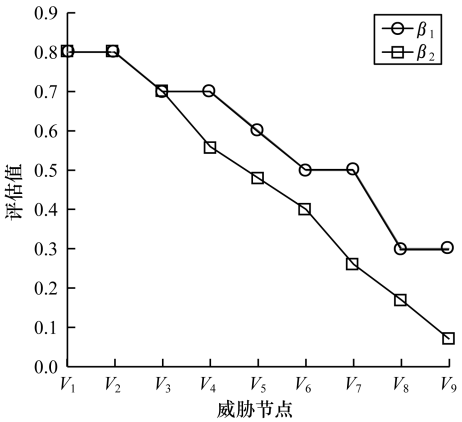


图 4　安全威胁节点评估值对比

对比 β_1 和 β_2 曲线可知,从节点 V_4 开始,β_2 曲线上的各个节点的评估值均低于 β_1 曲线各对应节点的值,其原因是攻击者通过多种路径获取目标节点权限时,考虑到成本、获取更多的节点权限等因素,其攻击难度会增大。以节点 V_4 和 V_5 为例,攻击者需要同时获取这两个节点的权限才能到达目标节点,从而降低了成功获取节点权限的可能性。考虑到实际的攻击,攻击者往往通过多种攻击途径获取目标权限,因此,本文构建的评估模型能够更准确地评估移动应用的安全威胁。

此外,节点间关联关系也影响移动应用安全威胁评估攻击路径的预判,具体分析如图 5 所示。

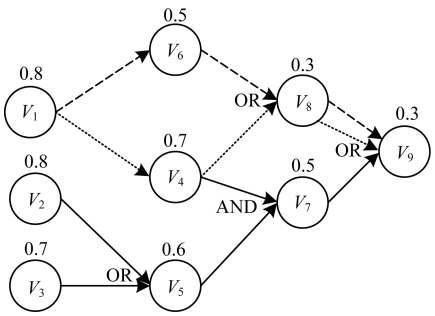


图 5　攻击路径预判示意图

攻击路径是移动应用安全威胁评估的一个重要组成部分。在选择攻击路径时,攻击者倾向于选择最易获取节点权限的路径到达目标节点。攻击路径用 l 表示,其中 V_i 表示第 i 个节点,e_{ij} 表示节点 V_i 到节点 V_j 的有向路径。图 5 中,在不考虑节点间关联关系情况下,路径 $l_1=\{V_1,e_{14},V_4,e_{47},V_7,e_{79},V_9\}$ 为攻击者最可能选择的攻击路径。实际上,攻击者除了倾向于选择最易获取节点权限的路径,还会综合考虑成本、到达目标可行性等多种因素。在实际攻击中,由于攻击者必须同时成功的利用节点 V_4 和 V_5 才能到达节点 V_7,因此在不考虑节点间管理关系时,l_1 将成为理论上可达而实际上不可能到达目标节点 V_9 的路径,降低了路径预判的正确率。在图 5 中,将 AND 和 OR 等节点间关联关系作为影响因素评估移动应用安全时,由于攻击者通过节点 V_7 到达目标节点 V_9 需要同时成功利用节点 V_4 和 V_5,会降低成功的可能性,而且在对比 V_4 和 V_6 节点时,节点 V_4 具有更高的成功可能性,因而最终会放弃路径 $l_2=\{V_1,e_{16},V_6,e_{68},V_8,e_{89},V_9\}$(图 5 中虚线路径),而选择路径 $l_3=\{V_1,e_{14},V_4,e_{48},V_8,e_{89},V_9\}$(图 5 中点线路径)到达目标节点,从而达到消除类似于 l_1 的路径,提高预判准确性的目的。

5 结束语

在评估移动应用安全时,对现有移动应用安全漏洞风险值的量化限于衡量漏洞自身被利用的难易程度,不能用作评估移动应用安全威胁的唯一要素。同时,攻击者利用安全漏洞发动攻击时,不同安全漏洞存在一定的关联性,这种关联性影响着对移动应用安全的评估。因此,本文在构建移动应用安全评估模型时充分考虑了上述 2 个问题,从而提高了评估的准确性,而且模型基于节点间关系,能够用于大规模移动应用模型的构建,具有良好的可扩展性。

虽然本文移动安全评估模型考虑了安全漏洞、攻击威胁以及相互之间的关联性,但仍存在一定程度误报。因此,下一步将在攻击路径预判的基础上进行有针对性的渗透测试,从而提高评估的准确性。

参考文献

[1] 中国互联网络信息中心. 第 34 次中国互联网络发展状况统计报告[EB/OL]. (2014-07-21)[2017-01-12]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201407/P020140721507223212132.pdf.

[2] 中国互联网协会,国家互联网应急中心. 中国移动互联网发展状况及其安全报告(2016)[Z]. 2016.

[3] 张玉清,王 凯,杨 欢,等. Android 安全综述[J]. 计算机研究与发展,2014,51(7):1385-1396.

[4] CHAN P P F,HUI L C K,YIU S M. Droidchecker:analyzing Android applications for capability leak[C]// Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York,USA:ACM Press,2012:125-136.

[5] 王菲飞. 基于 Android 平台的手机恶意代码检测与防护技术研究[D]. 北京:北京交通大学,2012.

[6] SHABTAI A,FLEDEL Y,ELOVICI Y. Securing Android-powered mobile devices using SELinux[J]. IEEE Security and Privacy,2010,8(3):36-44.

[7] 岳 倩. 移动互联网 APP 应用安全评估模型[J]. 沈阳航空航天大学学报,2016,33(5):68-73.

[8] 陈建民. 面向移动应用安全评估的多属性专家决策模型及应用研究[D]. 北京:北京工业大学,2014.

[9] 张 健,舒 心,杜振华,等. 一种评估恶意代码危害性方法的研究[J]. 信息网络安全,2009,39(10):7-9.

[10] 李向东,夏 冰,郑秋生. Android 应用软件安全测评方法研究[J]. 信息安全与通信保密,2014(9):133-135.

[11] 唐 杰,逯全芳,文 红,等. 基于 AHP 移动终端系统的安全风险评估[J]. 信息安全与技术,2013,4(3):13-16.

[12] THEOHARIDOU M,MYLONAS A,GRITZALIS D. A risk assessment method for smartphones[J]. IFIP Advances in Information and Communication Technology,2012,376:443-456.

[13] 李 佳,郑康锋,崔 旭. 一种基于模糊层次分析的智能手机攻击效果评估方法[C]//第十三届中国科学技术协会年会-中国智慧城市论坛论文集. 北京:中国科学技术协会,2011:103-107.

[14] 唐 杰,逯全芳,文 红. 基于图的移动终端系统安全评估[J]. 信息安全与通信保密,2013(5):72-75.

[15] CHIN E,FELT A P,GREENWOOD K,et al. Analyzing inter-application communication in Android [C]// Proceedings of the 9th International Conference on Mobile Systems,Applications,and Services. New York,USA:ACM Press,2011:239-250.

[16] 李铮山,林 干,范文浩,等. Android 的应用程序安全评估系统设计[J]. 软件,2013,33(12):287-291.

编辑 金胡考