基于AHP法的移动支付安全风险评估

单美静

(华东政法大学信息科学与技术系 上海 201620)

摘 要 大数据时代影响移动支付发展的重要因素就是安全。总结了移动支付相对于互联网支付而存在的个性和疑难安全问题,通过德尔菲法构建了安全评估指标结构。运用层次分析法计算各指标的权重,在设计的指标体系中找出风险节点,最终得到整个系统的安全值。该方法将层次分析法引入移动支付指标系统信息安全度计算。实验表明,该评估指标结构以及安全度计算能为移动支付提供有效的安全量化评估。

关键词 移动支付,层次分析法,安全评估

中图法分类号 TP391 **文献标识码** A

Analytic Hierarchy Process-based Assessment Method on Mobile Payment Security

SHAN Mei-jing

(Department of Information Science and Technology, East China University of Political Science and Law, Shanghai 201620, China)

Abstract In big data ages, the security is the greatest concern of mobile payment. Compared with the Internet payment, mobile payment has many personal and difficult problems. A security assessement indexes system was built up through Delphi method, and the weight of each index was calculated with analytic hierarchy process, then the top risk node and security value of the whole system were gotten. According to the designed index system, fuzzy comprehensive analysis method was introduced to the security evaluation of mobile payment. The experiment illustrates this index system can effectively quantify and assess the security level of mobile payment.

Keywords Mobile payment, Analytic hierarchy process, Security assessment

1 引言

2014年是移动支付发展最迅猛的一年。智能终端的普及极大程度地提升了移动支付的使用率。2014年的移动支付大战始于打车补贴、春节微信抢红包、年底的双十一和双十二使全民购物狂欢达到高潮。iResearch艾瑞咨询的统计数据显示,2014Q3中国第三方移动支付市场交易额达14332.7亿元,环比上涨7.8%,第三方移动支付交易规模企稳。

移动支付井喷式发展的同时,风险形势更为严峻。安全仍旧是普遍使用移动支付的最大障碍。与PC端支付不同,移动支付有着个性化的安全特点,包括多终端可接入、移动设备易丢失和借用、移动设备常用性、与传统线下欺诈相结合、便捷性和安全性相结合等。移动支付带给大众便捷体验的同时,也对信息和财产安全工作带来较大挑战。移动支付产业链中每一个环节的安全隐患、移动支付可能存在的安全风险,目前都是工业界和学术界的研究热点。。

移动支付过程的安全性除了使用定性的方法来进行分析之外,为了使安全风险可控,可通过风险隐患的安全度来度量,科学地分析支付数据和个人信息在保密性、完整性等方面所面临的威胁,找到安全隐患的环节并加以量化分析,从而在安全风险的预防、减少、转移、分散、控制和化解方面有的放矢,为切实提高移动支付的安全水平提供重要依据。

风险评估的常用方法。从国内外研究现状来看,目前的定量风险评估方法可分为两类:一是基于概率统计的风险量化方法;二是基于专家知识的风险量化方法。对于信息安全风险评估方法,重点研究信息系统风险分析和量化评估方法,对信息系统风险的评估不仅需要考虑独立的子系统的风险,还要考虑子系统之间相互作用造成的风险。

中国银联发布的《2014移动互联网支付安全调查报告》中提出,未来需要加大移动支付的风险防控研究。实际上,目前已有一些关于移动支付风险的研究[1-7]。这些文献中对移动支付风险创建了物元模型,提出了风险评估参考目标或者风险因素,给出了一些安全策略或者安全解决方案。然而,对于移动支付是否真正安全,风险防控中的评估环节是非常重要的,但目前针对移动支付风险评估的量化研究工作还不多见。文献[8]在贝叶斯网络基础上提出移动支付的量化风险评估模型。本文利用层次分析法建立了移动支付安全风险评估模型,实现了对移动支付安全隐患的系统定性和定量分析,并通过德尔菲法以专家评估意见为依据,分析了各个因素对总体风险的影响,提出了一种针对移动支付漏洞的量化评估方法。按照分层思想将移动支付安全隐患分为因素层、特性层和目标层。从安全保障的脆弱性、安全保障的威胁、移动通信网的缺陷和监管政策不足等方面造成的漏洞进行专家评定,并通过计算各因素的权重值来评价对总体目标的影响。

本文受教育部人文社会科学项目:大数据背景下移动支付的信息安全问题和法律制度研究(14YJCZH020),国家社会科学重大基金项目:涉信息网络违法犯罪行为法律规制研究(14ZDB147),国家社会科学项目:移动智能终端犯罪问题及法律监管策略研究(13CFX049)资助。

单美静(1979—),女,博士,讲师,主要研究方向为新型网络犯罪与信息安全。

实验结果表明，基于德尔菲法和层次分析法的移动支付安全评估方法能对漏洞的严重程度进行有效量化和评估。

2 大数据背景下移动支付的信息安全风险

2.1 安全威胁选择的准则与评判指标

360互联网安全中心发布的《2014年第一期中国移动支付安全报告》和腾讯移动安全实验室发布的《2014年第一期手机支付安全报告》显示，移动支付面临的主要安全威胁包括以下3方面。

1)移动终端的电子商务App染毒最多

随着移动支付的进一步普及，智能移动终端对支付类App下载量猛增，其中电商、第三方支付和团购是恶意病毒代码植入的重灾区，感染病毒软件款数位居所有购物支付类App的前3位。

2)超六成手机支付病毒会联网

对截获的手机支付类病毒进行了详细分析，其中最大的特征是表现为静默联网、删除短信、发送短信、读短信、开机自启动。其中，“静默联网”会导致手机用户资费消耗，同时病毒还会通过联网功能将用户手机上的隐私信息包括手机网银、支付相关账号和密码等内容上传至指定位置，导致用户隐私泄露和财产安全问题。

3)二维码成支付病毒传播关键渠道

了解手机支付病毒的传播渠道，对于用户防范病毒至关重要。报告显示，手机支付类病毒除了通过二次打包到手机网购、支付等5大类应用并散布在一些电子市场、手机论坛传播外，二维码已经成为手机支付病毒传播的关键渠道。

总结发现，移动支付的生态链以及所依托的移动终端，与互联网支付相比有以下个性化和疑难问题：

1)移动终端的开放性，扩大了系统攻击面。

2)移动终端的计算能力相对较弱，限制了高强度非对称加密算法的使用。

3)移动终端硬件扩展性不足，限制了对U盾和数字证书的广泛使用。

4) 移动终端的软件功能有所简化，其浏览器不能像电脑浏览器一样支持控件，如密码控件。

5)移动终端的网络速度大大低于电脑的上网速度，特别是基于GPRS和CDMA等2G或者2.5G的通信，限制了应用的使用。

因此，需要针对移动支付建立安全风险指标体系，围绕交易中的五大关键要素——人、账户、卡、设备和交易，来进行后台大数据系统的数据分析。通过层次分析法来计算每个节点的安全值，找到风险最大的节点，然后有的放矢地打击非法行为。

2.2 大数据时代移动支付的安全机制

移动支付方式包括短信支付、扫码支付、指纹支付、声波支付等，产生多种结构化与非结构化的移动支付数据。

针对这些复杂形式数据的大数据分析技术为移动支付提供了快速发展的契机，又给移动支付过程中的隐私保护以及数据安全提出了新的攻关课题。

移动支付安全机制是传统的信息安全技术在大数据时代移动互联网下的新发展，通过发展新的安全技术、修改原有的安全解决方案或提出新的解决方案，为大数据时代移动安全支付提供安全技术保障。

3 层次分析法

层次分析法(Analytic Hierarchy Process，AHP)[9]是美国运筹家学T. L. Saaty教授提出的一种多准则层次化权重决策方法。它的基本层次有目标层、准则层和指标层。基本原理是首先将要决策的问题看作是受多个因素影响的大系统，这些相互关联、相互制约的因素可以按照它们之间的隶属关系排成从高到低的若干层次；然后利用数学方法对各因素逐层排序；最后对排序结果进行分析，辅助进行决策。

AHP算法的基本步骤如下：

1)建立层次结构：明确所研究问题的目标、分层准则和所有可能的影响因素。

2)构造判断矩阵：对于同一层次的各元素，以相邻上一层支配元素为准则，使用德尔菲法两两比较因素间的相对重要性，具体原则参照表1；得出相对权重比值，构造出判断矩阵C。

表1 Satty 9级评价体系

标度	含义	说明
1	元素B_i与B_j同等重要	·标度值还可以取2,4,6,8,表示相对重要性介于左侧相邻两情况之间 ·标度值还可以取上述数值的倒数，即若因素B_i与B_j相与得b_{ij}，则因素B_i比B_j相比得$b_{ji}=1/b_{ij}$
3	元素B_i比B_j稍微重要	
5	元素B_i比B_j明显重要	
7	元素B_i比B_j强烈重要	
9	元素B_i比B_j极端重要	

这里，b_{ij}表示对于上层因素A_k而言，下层因素B_i和B_j相对重要性的数值。一般地，C为$n\times n$的方阵，具有如下性质：

$$\forall i,j\in \mathrm{N}\triangleq\{1,2,\cdots,n\},\text{有}\begin{cases}b_{ij}>0\\ b_{ii}=1\\ b_{ji}=1/b_{ij}\end{cases}\tag{1}$$

3)一致性检验：对于上一步构造的判断矩阵，需要检验其一致性，以保证后续做出的排序和决策是可靠的。判断$B=(b_{ij})_{n\times n}$的一致性是指满足条件$b_{ik}b_{kj}=b_{ij}(i,j,k=1,2,\cdots,n)$，它反映了两两比较判断之间是协调一致、不矛盾的。由于实际问题的复杂性和不确定性，特别是涉及的因素较多时，构造的判断矩阵可能不完全满足上述一致性。为此，Satty教授提出了判断矩阵只要满足“满意一致性”，就可以进入下一步操作。

具体的“满意一致性”计算方法：对每一个判断矩阵求其最大特征根λ_{max}及一致性指标：

$$CI=\frac{(\lambda_{max}-n)}{(n-1)}\tag{2}$$

再计算一致性比例

$$CR=CI/RI\tag{3}$$

其中，RI是平均随机一致性指标，它与n有关，如表2所列。当$CR\leqslant 0.1$时，认为判断矩阵具有“满意一致性”，是可以接受的；否则需要对判断矩阵进行适当的修正。

表2 平均随机一致性指标值

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

4)层次单排序：根据判断矩阵，计算下层各因素对上层因

素的影响性排序(权重),称为层次单排序。设当前层对应的判断矩阵为 $B=(b_{ij})_{n\times n}$,有多种方法进行单层次排序。这里选用特征根法,即计算判断矩阵 B 的特征根和特征向量,将最大特征根 λ_{max} 对应的特征向量进行归一化后作为排序权重,即层次单排序的结果。

5)层次总排序与决策:将层次单排序结果进行合成,以得到各层元素特别是最底层元素对总目标的影响权重,这称为层次总排序。其计算过程如下:假定上层有 m 个元素 A_1,A_2,…,A_m,已得到该层次的总排序权重为 a_1,a_2,…,a_m;下层有 n 个元素 B_1,B_2,…,B_n,且 B_1,B_2,…,B_m 对 A_j($j=1,2,\cdots,m$)的单排序权重为 c_{1j},c_{2j},c_{nj}(当下层元素 B_i 与上层元素 A_i 无关时,取 $c_{ij}=0$),则下层元素 B_1,B_2,…,B_n 对于总目标的总排序权重向量 $b=(b_1,b_2,\cdots,b_m)$ 按以下方法计算:$b_i=\sum_{j=1}^{m}a_jc_{ij}$($i=1,2,\cdots,n$)。

表 3 给出总排序权重的递推计算方法,其核心是以单排序权重向量为例,兼顾上层的总排序权重进行横向求和。

表 3 层次总排序的递推计算方法

层次	A_1	A_2	…	A_m	B 层总排序权重
	a_1	a_2	…	a_m	
B_1	c_{11}	c_{12}	…	c_{1m}	$b_1=a_1c_{11}+a_2c_{12}+\cdots+a_1c_{1m}$
B_2	c_{21}	c_{22}	…	c_{2m}	$b_1=a_1c_{21}+a_2c_{22}+\cdots+a_mc_{2m}$
⋮	⋮	⋮		⋮	⋮
B_n	c_{n1}	c_{n2}	…	c_{nm}	$b_n=a_1c_{n1}+a_2c_{n2}+\cdots+a_mc_{nm}$

4 实例分析

4.1 建立移动支付安全风险递阶层次结构

Step1 通过对移动支付的安全隐患要素进行识别,建立了移动支付的风险递阶层次结构模型,其中设 A_i,B_j($i=1,2,3,4$;$j=1,2,\cdots,12$)分别表示准则层以及指标层各因素,具体如图 1 所示。

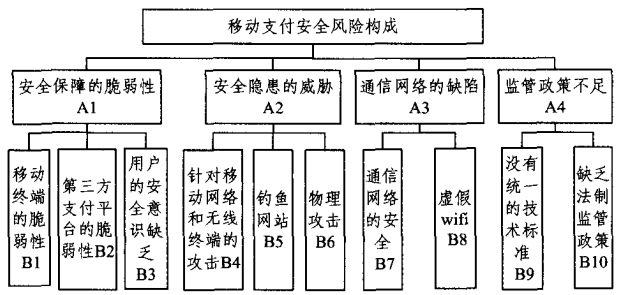

图 1 移动支付风险层次模型

Step2 综合 3 位专家的评判,根据模糊德尔菲法构造层次判断矩阵 C 并验证一致性。$C=\begin{pmatrix}1&2&3&5\\1/2&1&1&1\\1/3&1&1&3\\1/5&1&1/3&1\end{pmatrix}$,其最大特征根 $\lambda_{max}=4.166$,代入式(2)以及式(3),得到 $CR=0.0622<0.1$,说明所构造的判断矩阵满足"满意一致性"。

Step3 层次单排序。求判断矩阵 C 的最大特征根对应的特征向量,对其归一化后即可得准则层元素 A_1,A_2,A_3,A_4 相对于总目标的权重向量 $u=(0.4886,0.1834,0.2129,0.1152)$。

类似地,计算指标层各元素相对于准则层元素的权重向量,得到如下结果:

1)将指标 B_1,B_2,B_3 进行两两比较,得到判断矩阵 $D_1=\begin{pmatrix}1&2&5\\1/2&1&3\\1/5&1/3&1\end{pmatrix}$,其最大特征根 $\lambda_{max}=3.0037$,代入式(2)以及式(3),得到 $CR=0.0036<0.1$,说明所构造的判断矩阵满足"满意一致性"。

指标 B_1,B_2,B_3 相对于准则 A_1 的权重向量为 $v_1=(0.5813,0.3092,0.1096)$。

2)将指标 B_4,B_5,B_6 进行两两比较,得到判断矩阵 $D_2=\begin{pmatrix}1&2&1\\1/2&1&1\\1&1&1\end{pmatrix}$,其最大特征根 $\lambda_{max}=3.0537$,代入式(2)以及式(3),得到 $CR=0.0516<0.1$,说明所构造判断矩阵满足"满意一致性"。

指标 B_4,B_5,B_6 相对于准则 A_2 的权重向量为 $v_2=(0.4111,0.2611,0.3278)$。

3)将指标 B_7,B_8 进行比较,得到判断矩阵 $D_3=\begin{pmatrix}1&1\\1&1\end{pmatrix}$,其最大特征根 $\lambda_{max}=2$,代入式(2)以及式(3),得到 $CR=0<0.1$,说明所构造的判断矩阵满足"满意一致性"。

指标 B_7,B_8 相对于准则 A_3 的权重向量 $v_3=(0.5,0.5)$。

4)将指标 B_9,B_{10} 进行比较,得到判断矩阵 $D_4=\begin{pmatrix}1&1\\1&1\end{pmatrix}$,其最大特征根 $\lambda_{max}=2$,代入式(2)以及式(3),得到 $CR=0<0.1$,说明所构造的判断矩阵满足"满意一致性"。

指标 B_9,B_{10} 相对于准则 A_4 的权重向量 $v_4=(0.5,0.5)$。

Step4 层次总排序,如表 4 所列。

表 4 移动支付安全隐患层次总排序

B	A_1	A_2	A_3	A_4	权重	排序
B_1	0.5813				0.2840	1
B_2	0.3092				0.1510	2
B_3	0.1096				0.0535	8
B_4		0.4111			0.0754	6
B_5		0.2611			0.0479	9
B_6		0.3278			0.0601	7
B_7			0.5		0.1064	3
B_8			0.5		0.1064	4
B_9				0.5	0.0768	5
B_{10}				0.5	0.0384	10

4.2 结果分析

通过上述分析和计算表明,对移动支付安全隐患影响较大的因素是移动终端的脆弱性和第三方支付平台的脆弱性。因此,在保障移动支付信息安全和隐私保护方面,应加强移动终端的硬件和应用安全研究,对于第三方支付平台的安全保障也必须加大力度。同时随着接入移动互联网的终端设备的增加,移动互联网业务频繁发生,wifi 的安全也需要认真对待。而对于权重较小的政策监管措施的研究,应根据成本和效益相结合的原则来考虑。

结束语 本文在移动支付安全隐患分析中,将层次分析法引入,采用了德尔菲法与层次分析法相结合的方法来计算可能度,对移动支付的各安全隐患指标因素进行权重计算,解决了基于群组决策和多指标集中人为判断的模糊性问题,为科学研究和决策提供了理论依据;创新性地进行了移动支付的风险防控研究,为进一步全面升级防控体系、规范开展移动支付产品创新、打造安全支付生态环境提供了思路。

参 考 文 献

[1] Zhang Jun-cai, Zhao Jin-hui, Qian Xun. Risk assessment of mobile payment system security based on extension theory[C]// Proceedings of 2012 International Conference on Computer Science and Service System. 2012:880-883

[2] 戴宏. 移动支付系统安全风险评估[D]. 北京:北京交通大学, 2010

[3] 李峰. 移动支付安全研究[D]. 济南:山东大学, 2008

[4] Sun Wang-quan. The risk analysis and safety strategy on remote mobile payment[C]// Proceedings of 2012 IEEE Symposium on Digital Object Identifier. 2012:400-402

[5] 卫红春, 马丁. 基于改进的 3-D Secure 协议的移动支付安全解决方案[J]. 计算机应用与软件, 2011, 28(4):189-192

[6] 许峰, 崔隽, 黄皓. 基于 J2ME 的移动支付安全方案研究[J]. 计算机科学, 2008, 35(10):94-121

[7] 黄晓芳, 周亚建, 赖欣等. 基于第三方的安全移动支付方案[J]. 计算机工程, 2010, 36(18):158-162

[8] 张旋, 林逸风, 白川, 等. 基于贝叶斯网络的移动支付风险评估模型[J]. 计算机工程与应用, 2014, 50(5):60-64

[9] Saaty T L. The Analytic Hierarchy Process[M]. USA: McGraw Hill, 1980

(上接第 347 页)

(3)实施运行时监控,防止 TCB 被旁路。攻击者无法通过软件攻击的方式探测到安全服务子系统的存在,因此无法将其旁路。因此,攻击者虽然可以利用目标计算子系统的内核漏洞,旁路掉核心层的安全机制,但是无法旁路安全服务子系统实施的运行时监控。对运行系统的实时监控,可以及时检测出恶意程序的存在,并采取相应措施防止恶意行为的扩散。

(4)系统被破坏时可以进行可信恢复。安全服务子系统中将系统关键资源进行了备份储存,一旦检测出其中某个资源被破坏,可以及时将被破坏的资源进行替换,提高了系统的可用性和健壮性。

4 系统受攻击实例

在本节中,通过一类典型的攻击实例来分析说明在保证 TCB 的不可旁路和不可篡改方面,本文提出的体系结构比传统的体系结构有明显的优势。

传统的体系结构中,内核通常共享地址空间,任何一个模块都可以直接访问其他模块的功能,并修改其数据,甚至内核关键数据结构,因此可以轻易地旁路和篡改系统的安全机制。系统攻击一般通过篡改系统关键数据结构并插入恶意代码来改变系统正常的运行控制流,以获取更高的权限实施攻击。比较典型的如内核级 Rootkit,以劫持系统调用、拦截中断、模块注入等攻击手段,可以绕过传统的参考监视器来窃取重要数据。本文设计的体系结构中,由于安全服务子系统占用的是一块独立的物理内存,攻击者无法访问到这一块物理地址空间。下面以 Knark 等为样本,测试系统的防攻击能力。

图 2 给出了系统调用表的部分动态度量结果,从图中可知,独立监视器可以监测出 Knark 对系统调用表的修改状态。独立监视器也可以对中断向量表、内核内存映像等其余的关键数据结构进行动态度量,并能根据动态度量的结果与策略库中的策略进行及时处理,有效保障了 TCS 系统安全。

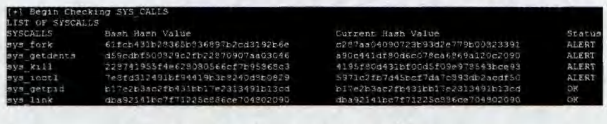

图 2 系统调用表度量结果

结束语 构建高安全级信息系统的首要前提,就是设计一个高安全的体系结构。针对目前基于 TPM/TCM 的可信计算架构和基于 VMM 的虚拟化架构存在被旁路和被篡改的威胁,本文提出了一个基于独立核心安全组件的高安全体系结构 HAICC。该体系结构通过硬件层实现了安全功能与计算功能的强隔离,将系统划分为独占不同物理资源的安全服务子系统和目标计算子系统。实施核心安全机制的安全服务子系统近似于一个主动控制、资源独立、密闭的物理设备,实施对整个计算系统的主动度量、实时监控、安全关键数据恢复。系统安全性分析及攻击实例表明,HAICC 体系结构有效缓解了核心安全组件被篡改和被旁路的风险,有效保障了系统安全机制的完整有效。

参 考 文 献

[1] Peinado M, Chen Y, England P, et al. NGSCB: A trusted open system[M]// Information Security and Privacy. Springer Berlin Heidelberg, 2004:86-97

[2] Sailer R, Zhang X, Jaeger T. Design and Implementation of a TCG-based Integrity Measurement Architecture[C]// Proceedings of 13th Usenix Security Symposium. San Diego, California, 2004:223-238

[3] Pfitzmann B, Riordan J, Stuble C, et al. The PERSEUS system architecture: RZ 3335[R]. 2001

[4] Sailer R, Valdez E, Jaeger T, et al. sHype: Secure hypervisor approach to trusted virtualized systems: RC23511[R]. 2005

[5] McDermott J, Freitas L. A formal security policy for xenon [C]// Proceedings of the 6th ACM workshop on Formal methods in security engineering. ACM, 2008:43-52

[6] Coker G. Xen security modules(xsm)[C]// Xen Summit. 2006: 1-33

[7] Kivity A, Kamay Y, Laor D, et al. Kvm: the Linux virtual machine monitor[C]// Proceedings of the Linux Symposium. 2007: 225-230

[8] 项国富, 金海, 邹德清, 等. 基于虚拟化的安全监控[J]. 软件学报, 2012, 23(8):2173-2187