第三方支付系统威胁树信息安全评估研究*

李二亮[1,2]

(1. 中央财经大学 信息学院, 北京 100081; 2. 河南工程学院 管理工程学院, 郑州 451191)

摘 要: 在全面分析第三方支付安全事件的基础上,基于威胁树理论构建了第三方支付威胁树风险评估模型,并给出了威胁树的权值计算算法以及最小威胁树修剪算法,最后运用此模型和算法选取典型的第三方支付系统进行了实例评估,对评估结果深入分析的基础上提出了第三方支付系统的安全防范对策建议。结果表明,该评估模型能有效地找到第三方支付系统的威胁路径和风险点,能为第三方支付系统安全的改进和用户选择提供参考。

关键词: 第三方支付系统; 支付流程; 风险评估; 威胁树

中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2014)04-1204-04

doi:10.3969/j.issn.1001-3695.2014.04.059

Assessment of third-party payment security using attack tree

LI Er-liang[1,2]

(1. *School of Information, Central University of Finance & Economics, Beijing* 100081, *China*; 2. *School of Management Engineering, Henan Institute of Engineering, Zhengzhou* 451191, *China*)

Abstract: Based on the analysis of security events occurring to the third-party payment system, this paper proposed a third-party payment attack tree model by using attack tree theory, as well as algorithms about attack tree weights calculation and attack tree pruning. By using the model, it implemend security assessment on typical third-party payment system, also gave security countermeasures on the basis of analysis of the evaluation results. The conclusion shows that the model can effectively find out the threat route and risk point of the third-party payment system, and give a support to the security improvements and users' choosing.

Key words: third-party payment system; payment process; risk assessment; attack tree

0 引言

当前随着我国网络购物的快速发展,网上支付特别是第三方支付日益成为网购首选的支付方式。据 CNNIC 发布的《2012 年中国网络支付安全状况报告》[1] 显示,接近 79.2% 的用户网购时选择了第三方支付账户余额完成支付。同时,从用户视角感知的网上支付的安全度也不断提升,报告显示 69.4% 的用户认为网上支付是比较安全的。然而,针对网购的安全事件不断频发,2012 年 4 月,浮云木马病毒案告破,短短半年时间内,该病毒涉案 30 余起,盗窃金额近 1 000 多万元,是继支付宝大盗后,对第三方支付系统危害最大的木马病毒。

自 1999 年 3 月首都信息股份有限公司推出第三方支付工具首信易支付以来,到 2011 年央行开始对第三方支付行业进行监管,第三方支付行业经历了近十余年的快速发展,支付业务许可证的颁发表明该行业的发展已经到了需要制度化、正规化的阶段,同时第三方支付行业的安全性也引起了政策层面的关注。2012 年 1 月 5 日,中国人民银行发布了《支付机构互联网支付业务管理办法》征求意见稿,其中指出,支付机构开展互联网支付业务采用的信息安全标准、技术标准等应符合中国人民银行关于信息安全和技术标准的有关规定[2]。这一规定对第三方支付企业加强自身的安全建设提出了明确要求。

与国外第三方支付行业发展形成鲜明对比的是,国内第三方支付行业竞争异常激烈,截止 2013 年 1 月已经颁发了 223 张支付许可证,行业发展也形成了鲜明的中国特色。安全关乎网络支付的命脉,也关乎网络购物的发展,当前的网购实践表明,网络支付的安全很大程度上与第三方支付系统的安全息息相关,因此,关注第三方支付系统的安全就是关注网购的安全。而第三方支付的安全除了一般意义上的安全防范,更应当基于当前我国互联网应用的背景,从信息系统安全角度对第三方支付系统进行全面的风险评价并提出有效的防范措施,无疑对网上支付以及网络购物的发展具有十分重要的现实意义。

1 研究综述

当前,众多学者针对电子商务相关的支付系统的安全及风险评估进行了大量研究。典型的研究有,Kim 等人[3] 通过研究表明,系统及支付安全是影响消费者购物价值进而影响网上购物的重要因素之一,因此应该特别关注支付系统的安全因素。Joris 等人[4] 深入分析了当前在线网银系统的风险,提出了满足安全交易需求的支付架构及安全要素,对于分析其他在线支付系统提供了很好的意见参考。Pennathur[5] 研究了互联网时代的银行的风险管理问题,其中在线支付系统是面临风险重要的方面。李良[6] 运用层次分析法针对电子银行进行了系统的

收稿日期: 2013-05-01; **修回日期**: 2013-06-24 **基金项目**: 国家自然科学基金资助项目(71272234);河南省教育厅人文社会科学青年项目(2012-QN-063)

作者简介:李二亮(1978-),男,河南禹州人,讲师,博士研究生,主要研究方向为信息安全、网上支付(13825090@163.com).

信息安全评估,并提出了较完备的安全建议。上述文献对于第三方支付系统的安全研究及评估提供了重要的参考。

当前专门针对第三方支付系统的信息安全风险评估的研究成果较少,只有部分学者在进行研究时内容会涉及到第三方支付系统的信息安全。李敏[7]在基于层次分析法对网络第三方支付风险评估和控制进行研究时,将信息安全作为方案层的指标对风险进行了度量,但该研究主要偏重于信用风险的研究。赵德志[8]基于项目管理视角对第三方支付进行了风险识别,在其识别的风险类别中,技术管理风险是其中之一,并对风险来源进行了细化,但该研究并未深入对第三方支付系统的安全风险进行有效评价。李医群[9]通过选取 2005 年 1 月 1 日—2010 年 12 日 31 日收集到的 228 件第三方支付损失事例,运用极值理论的 POT 模型对在线第三方支付的操作损失进行推算,证明其存在严重厚尾现象,指出我国在线第三方支付市场监管措施还亟待完善,但该研究的目的主要是从效益观点衡量对第三方支付的监管和效率,并未针对收集的安全案例从信息安全的角度进行深入分析。此外,针对网上频发的第三方支付被盗事件,也有学者从微观层面对第三方支付安全进行了深入研究。刘凯[10]以真实的资金诈骗案例,分析了攻击者所采用的攻击技术及其攻击原理以及第三方支付系统客户端存在的安全风险,并提出了技术防范机制来降低系统的安全风险,同时,建议通过用户方、第三方支付商、银行方及监管部门的共同努力,在最大程度上阻止类似的资金诈骗行为。

以上研究对第三方支付市场存在的风险进行了一定的分析,但上述研究仍存在着一定的不足,主要体现在相关研究并未从信息安全的角度深入剖析第三方支付系统所可能存在的脆弱性以及防范重点,也没有对第三方支付进行流程再造提出相关建议,因此对于第三方支付安全事件的发生无法起到实质性的遏制。

信息安全风险评估就是从风险管理角度,运用科学的方法和手段,系统地分析信息系统所面临的威胁及其存在的脆弱性,对安全事件一旦发生可能造成的危害程度进行评估,并提出有针对性的防护对策和整改措施,为防范和化解信息安全风险,将风险控制在可接受的水平,最大限度地保障信息安全提供科学依据[11]。目前已有大量的文献提出了多种风险评估方法,大致可以分为定性、定量以及定性与定量相结合的方法,定性方法主要有:因素分析法、逻辑分析法、历史比较法、德尔斐法;定量的评估方法有:等风险图法、威胁树法、统计学模型等;定性与定量相结合的典型方法是层次分析法[12]。本文将根据第三方支付系统的典型特点选择合适的风险评估方法对第三方支付系统进行评估分析。

2　第三方支付系统安全威胁特征

2.1　第三方支付系统与网银支付系统的区别

同样作为网上支付体系,第三方支付系统与一般网银却存在着较大不同,这些不同之处也是第三方支付系统面临较大威胁的原因之一。与网银的区别主要体现在以下几个方面:

a)第三方支付系统在当前网购中的采用率较高,用户群规模较大,一般会与即时通信工具结合使用,为了交易需要账号信息在互联网上主动公开,这就使得不法份子很容易获取并进行攻击。而网银在网购中也会采用,但账号信息一般不会在网络上主动公开。

b)第三方支付系统几乎所有的业务均通过互联网进行,特别是一些关键环节,如认证、充值等。这样的话,通过互联网带来便利的同时,使得用户在第三方支付系统、网银系统以及购物平台之间的多次页面跳转不可避免,由于环节过多,加之使用的 SSL 安全协议由于美国对密级的限制[4],就使得第三方支付系统很容易遭受外在攻击。

c)第三方支付系统的系统健壮性有待加强,相对于银行网银系统多年的运行经验以及国家相关标准的严格要求,关于第三方支付系统的相关技术安全标准尚未出台,目前只有参考性的标准。

2.2　第三方支付安全事件的特征分析

通过对收集到的大量安全事件的定性分析,第三方支付系统信息安全事件的典型特征有以下几点:a)第三方支付工具一般在网上购物时使用,盗取账户的可支付余额是支付系统面临的最大风险;b)第三方支付系统一般是用户购物议价后使用,而议价的过程有可能需要传递图片、视频等资料,这就给隐藏传播木马程序留下漏洞,从而使一些木马程序如支付宝大盗、浮云木马病毒等实现窜改支付协议中的付款账户和金额,实现更具隐蔽性的盗取;c)第三方支付的转账操作,一般以登录密码和支付密码相结合的方式完成,安全事件的发生一般是该两项密码通过各种手段如钓鱼网站、促销信息、升级提醒等不法手段被盗取;d)第三方支付系统一般提供数字证书来提高系统的安全性,但部分案例显示数字证书可以通过一定手段绕过从而盗取用户资金,此环节可能存在重大安全隐患。

结合上述第三方支付系统的特点和安全事件的特征,即采取各种非法手段盗取账户资金的强目的性,本文拟选择威胁树模型对第三方支付系统进行建模评估,通过威胁树模型能够很好地勾勒出第三方支付系统资金被盗所有可能的路径,在对路径全面分析的基础上,可以有效地决定系统安全防范的重点。

3　基于威胁树的第三方支付系统安全风险评估

威胁树模型从 Schneire[13]在 2000 年提出的攻击树建模方法演化而来,广泛用于信息系统的安全评价中,如甘早斌等人[14]基于威胁树理论提出了一种针对信息系统安全的扩展威胁树模型,使得评估过程更加客观;任丹丹等人[15]基于威胁树提出了一种新的 VANET 位置隐私安全风险评估方法,从而为决策者采取相应的位置隐私保护措施提供了依据。威胁树方法大致可分为两个阶段:a)确定系统的脆弱性,以及枚举脆弱性可能被利用的各种方式,然后进行分析找出最有可能发生的威胁;b)考虑的是如何进行预防,比如是否值得花费时间和资源来改进系统。

3.1　威胁树模型的定义

定义 1　$T=(G,\ \text{type},\text{weight})$是具有一个或多个 AND 或 OR 节点的威胁树,其中:$G(T)$是一个非空有限 AND 或 OR 节点的集合,节点表示攻击者在攻击系统时需要达到的子目标,根节点 root 表示攻击者在成功地攻击一系列子目标后达到的最终目标;type 表示节点的类型,即表示该节点为 AND 或 OR 节点;weight 表示当前节点的攻击权值,该 weight 的取值可随不同的情境和数据意义不同,可以表示为威胁代理攻击所花费

的成本,亦可表示为攻击成功的概率或攻击被抓捕的概率等。

定义 2 AND 节点即串联节点,是指子节点之间是 AND 操作,当且仅当所有子节点均成功实施攻击,才能到达父亲节点。

定义 3 OR 节点即并联节点,是指父节点的所有子节点之间是 OR 操作,当且仅当任一个孩子节点的攻击步骤成功时,即能达到父节点。

3.2 节点权值的计算

定义 4 对于 $\forall q \in V(T)$ 来说,q 节点的攻击权为 w,若 q 有 j 个子节点,每个节点的权值用 $m(i)(1 \leqslant i \leqslant j)$ 表示。

若 q 是 AND 节点,则根据不同的指标,计算函数如表 1 所示。

表 1 AND 节点指标及计算函数

指标	函数
攻击成本	$m(q) = m(1) + m(2) + \cdots + m(j)$
成功概率	$m(q) = m(1) \times m(2) \times \cdots \times m(j)$
被抓获的概率	$m(q) = 1 - (1 - m(1) \times (1 - m(2)) \times \cdots \times (1 - m(j))$

若 q 是 OR 节点,则计算函数如表 2 所示。

表 2 OR 节点指标及计算函数

指标	函数
攻击成本	$m(q) = m(1) + m(2) + \cdots + m(j)$
成功概率	$m(q) = 1 - (1 - m(1)) \times (1 - m(2)) \times \cdots \times (1 - m(j))$
被抓获的概率	$m(q) = \min\{m(1), m(2), \cdots, m(j)\}$

3.3 基于威胁树的第三方支付风险评估算法

算法 1 威胁树节点值计算算法

输入:威胁树的根指针。

输出:计算威胁树的各节点权值。

/ * 该算法采取非递归后根遍历序列的方式计算节点的权值,空树时为“零”,威胁树采取子女兄弟二叉链表的方式存储,节点数据采取结构体 u 表示,其中 n_n 表示节点名,n_type 表示节点类型,以 0 表示 OR 节点,1 表示为 AND 节点,3 表示叶子节点,n_w 表示节点权值,视情况可以更改算法求解条件即可,当前算法以较为复杂的概率计算为例如

a)输入威胁树的根指针 p。

b)初始化堆栈 st,创建 AND 权重计算变量 mulp 和 OR 权重变量 sump,并初始赋值为 1;创建当前指针 t。

c) t 非空或 st 非空执行循环操作。

d)t 非空,t、mulp、sump 入栈,mulp 和 sump 值重新赋值为 1,访问当前节点的第一个孩子节点。

e)t 为空,st 出栈操作,并判断当前节点类型。如果是叶子节点,则计算 mulp 和 sump 值,t 指向当前节点的下一个兄弟节点;当前节点为 AND 节点,mulp 赋值给当前节点,并以当前节点为基准重新计算 mulp 和 sump 值,然后访问下一个兄弟节点;当前节点为 OR 节点,则将 sump 赋值为当前节点的权值,并以当前节点为基准重新计算 mulp 和 sump 值,然后访问下一个兄弟节点。

f)执行循环操作步骤 c) ~ e)直到遍历访问所有的节点。具体算法如下 :

```
1  PostOrder(TreeNode * p = root)
2  { TreeNode * t = p ;
3    Stack st; mulp = sump = 1;
4    while(t || st. empty())
5     {if(t)
6       {st. Push(t, mulp, sump);
7        mulp = sump = 1;
8        t = t→firstchild;}
9     else{ e = st. pop();t = e. t;
10       if(t→u. n_type = =3)
11          {mulp = e. mulp * t→u. n_w;
12           sump = e. sump * (1 - t→u. n_w);
13           t = t→nextsibling; }
14       else if(t→u. n_type = =1)
15          {t - >u. n_w = mulp;
16           mulp = e. mulp * t→u. n_w;
17           sump = e. sump * (1 - t→u. n_w);
18           t = t→nextsibling;}
19       else
20          {t→u. n_w = 1 - sump;
21           mulp = e. mulp * t→u. n_w;
22           sump = e. sump * (1 - t→u. n_w)
23           t = t→nextsibling; }}
24  }}
```

算法 2 威胁树的修剪算法

输入:威胁树的根指针和剪树条件值。

输出:第三方支付系统的最小威胁树。

/ * 该算法采取非递归先根遍历的方式访问威胁树的各节点,依据条件对威胁树进行剪除,得到最小威胁树 * /

a) 输入威胁树的根指针 p 和剪树条件值 w。

b)初始化堆栈和条件值 w_1。

c)首先访问根节点,小于条件值则直接赋 NULL,修剪结束,否则访问第一个子节点。

d)当指针不为空或堆栈为不空执行循环操作;当前节点权值小于条件值则执行出栈操作,删除当前节点,访问下一个兄弟节点;否则执行入栈操作,访问当前节点的第一个子节点;直到遍历所有的节点。具体算法如下:

```
1  PreOrder(TreeNode * p = root, w)
2  {TreeNode * t = p ; w1 = w
3     Stack st;
4     if t→u. n_w < w1 {p = NULL; return;}
5     else {st. Push(t);t = t→firstchild;}
6     while(t || st. empty())
7     {if(t)
8        {if(t→u. n_w < w1)
9           {e = st. pop();
10          e→firstchild = t→nextsibling;
11          t = t→nextsibling;}
12       else
13          {st. Push(t); t = t→firstchild;}
14    }}}
```

3.4 基于威胁树的第三方支付系统评价实例

通过对第三方支付系统业务流程分析以及综合安全事件的情况,生成了以下第三方支付系统的威胁树模型,如图 1 所示。

针对不同的第三方支付系统,其面临的风险会有所不同,例如与购物平台关联性较强的支付系统面临的风险更大。以下选择当前主流第三方支付快钱和支付宝进行实例评估。

本评估的数据(表 3),通过邀请笔者在读博士学校的五位相关业务专家打分获得,五位专家中包括两名博士生导师,两

名教授和一名副教授,均长期从事电子商务或网络支付安全方面的研究。打分的标准是,威胁代理的攻击支付系统成功的概率,具体如下。

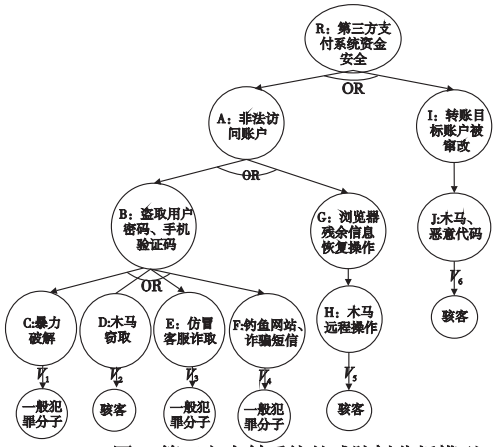

图1　第三方支付系统的威胁树分析模型

表 3　支付宝和快钱的三轮专家打分加权结果

支付工具	V_1	V_2	V_3	V_4	V_5	V_6
快钱	0.012	0.626	0.094	0.42	0.074	0.188
支付宝	0.078	0.566	0.27	0.376	0.076	0.284

通过 Turbo C 运行权值计算程序进行威胁树权值运算并输出威胁树,如图 2、3 所示。图 2、3 中以“〈〉”表示该节点为 OR 节点,从属于同一父节点的兄弟节点之间以“|”分隔,下同。

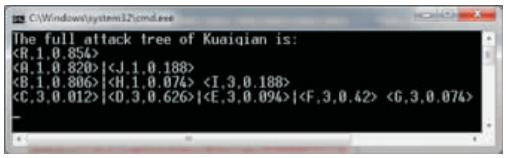

图2　快钱的完整权值威胁树

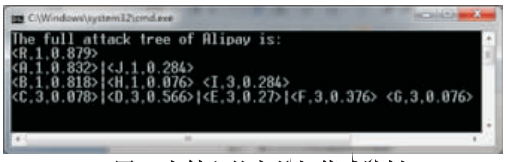

图3　支付宝的完整权值威胁树

按成功概率小于 0.1 的条件下运行修剪程序对两支付系统的威胁树进行修剪,生成了各自的最小威胁树,结果如图 4 和 5 所示。

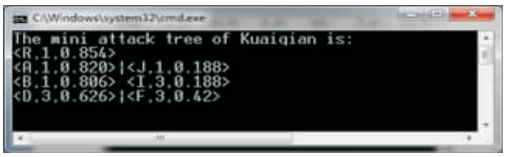

图4　快钱的最小威胁树

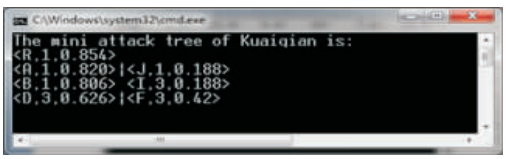

图5　支付宝最小威胁树

3.5　第三方支付平台的风险分析及风险管理

通过图 4、5 显示的两个不同第三方支付系统的最小威胁树可以看出,各种威胁对不同第三方支付系统所带来的风险是不同的,对各自机密性、完整性和可用性的影响以及具体攻击路径也存在不同,具体如表 4 所示。从表中可以看出。木马盗取、钓鱼网站、诈骗短信对不同的第三方支付平台来说,都是威胁最大的三种方式;而对于支付宝来说,由于交易的需要,支付宝的账号在互联网上很容易查到,并且也很容易在网上被不法分子或骇客使用特定的木马病毒攻击,因此应该引起特别关注。而造成这种原因的最大问题在于支付流程设计环节,由于充值、转账等操作需要在不同页面之间跳转,这种跳转很容易被骇客利用病毒木马窜改支付协议中的相关数据,而这是用户很难进行防范的。

表 4　第三方支付工具的攻击路径分析

支付工具	系统特性	攻击路径	具体影响
支付宝	机密性	〈A〈B〈D〉〉〉→R 〈A〈B〈E〉〉〉→R 〈A〈B〈F〉〉〉→R	非法窃取支付密码等信息
	完整性	〈J〈I〉〉→R	窜改支付过程中的金额和付款目标账户
	可用性	支付账号和密码被窃取后,密码被非法重置将使原用户无法登录系统	合法用户无法正常使用账户
快钱	机密性	〈A〈B〈D〉〉〉→R 〈A〈B〈F〉〉〉→R	非法窃取支付密码等信息
	完整性	〈J〈I〉〉→R	窜改支付过程中的金额和付款目标账户
	可用性	支付账号和密码被窃取后,密码被非法重置将使原用户无法登录系统	合法用户无法正常使用账户

结合上述两个具体第三方支付工具的可行威胁树,提出以下若干风险管理建议:

a)加强用户操作的主体性认证,增加实时性主体认证手段,如手机短信、动态口令等手段,特别是改变账户关键操作仅依靠密码进行的流程,从而增强安全性;从上述两个最小威胁树中,木马窃取以及钓鱼网站、诈骗短信是最主要的盗取方式,骇客在盗取用户的关键信息即可完成对资金的盗取,多数支付系统虽提供了数字证书服务 + 支付密码的操作方式,但有案例显示数字证书在用户不知情的情况下仍然存在被盗取的情况。目前一些主流的第三方支付工具,仅在安装数字证书、快捷支付等情况下才使用手机验证码,因此建议在转账、更换手机、提现等关键操作时,额外增加实时身份验证手段。

b)针对数字证书用户,应加强对数字证书申请、取消环节的管理,进行必要的身份认证;并且建议增加对账户登录、异地操作的实时提醒,尽可能地避免非法登录的操作,提高账户的安全性,而此种服务目前多数第三方支付工具尚未提供。

c)再造支付流程,由于美国软件出口对 SSL 协议的限制,致使当前我国使用的 SSL 协议级密较低,协议数据很容易被窜改,建议为用户提供安全的快捷支付功能,尽量减少页面间的跳转操作,并且应当与银行加强合作,推出针对非快捷支付用户的专用网关,并且在转账、充值等操作过程中,之前能通过一定的方式如短信提醒等确认转账目标账户的真实身份。而目前各个银行推出的网关均为默认网关接口,并且在操作过程中没有进行必要的账户验证和提醒。

d)加强对用户的安全防骗教育,提醒用户识别常用的诈骗手段,如图 1 所示的防冒客服以及诈骗短信等手段。

(下转第 1211 页)

捕获 n_1 的签名和哈希值,进而同样伪造路径 S-n_1-A-D,破坏路由发现过程。

类型Ⅵ单个内部攻击者,即 Dolev-Yao 攻击,不限制攻击者的接收传输能力,攻击者 A 无须了解网络拓扑结构,就可以接收网络中传输的任何消息。如果前两种单个内部攻击者(类型Ⅱ、Ⅳ)情形没有发现攻击,Dolev-Yao 攻击模型将作为最后安全协议评估保障。第Ⅱ、Ⅳ类攻击的安全协议评估依靠网络拓扑,为了保障此类型攻击在安全协议评估过程能被发现,评估过程需要反复地去改变网络拓扑结构,以便发现任何可能存在的攻击情形。第Ⅵ类攻击,自适应攻击模型提供了 Dolev-Yao 攻击者强度,可以在任何网络拓扑的情形下,评估攻击者攻击强度和破坏协议的最小攻击强度。

4　结束语

随着 WSN 技术的发展,其路由发现过程中安全性评估问题备受关注,本文首先分析了典型的 WSN 路由发现攻击,然后介绍了规范化 Dolev-Yao 威胁模型,并在对其进行改进的基础上,建立面向 WSN 安全路由协议的自适应威胁模型。该模型对路由协议的评估不是基于某种安全假设前提,而是采用自适应方式确定何种强度的攻击可以使路由发现协议失效。

参考文献:

[1] KASHIF K, MADJID M, DAVID L J. Security in wireless sensor networks[M]//PETER S, MARK S. Handbook of Information and Communication Security. Berlin: Springer, 2010: 513-552.

[2] 周雁, 王福豹, 黄亮. 无线传感器执行器网络综述[J]. 计算机科学, 2012, 39(10): 21-25.

[3] STAVROU E, PITSILLIDES A. A survey on secure multipath routing protocols in WSNs[J]. Computer Networks Journal, 2010, 54(13): 2215-2238.

[4] SINGH S K, SINGH M P, SINGH D K. Routing protocols in wireless sensor networks: a survey[J]. International Journal of Computer Science and Engineering Survey, 2010, 1(2): 63-83.

[5] XIAO Zheng-hong, CHEN Zhi-gang. A secure routing protocol with intrusion detection for clustering wireless sensor networks[C]// Proc of International Forum on Information Technology and Applications. Washington DC: IEEE Press, 2010: 230-233.

[6] WESTHOFF D, GIRAO J, SARMA A. Security solutions for wireless sensor networks[J]. NEC Journal of Advanced Technology, 2006, 1(3): 106-111.

[7] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Trans on Information Theory, 1983, 29(2): 198-208.

[8] NEWSOME J, SHI E, SONG D. The sybil attack in sensor networks: analysis & defenses[C]//Proc of the 3rd International Symposium on Information Processing in Sensor Networks. New York: IEEE Press, 2004: 259-268.

[9] 董晓梅,杨洁. 一种无线传感器网络中的虫洞攻击检测算法[J]. 东北大学学报, 2012, 33(9): 1253-1256.

[10] 李宗海, 柳少军, 王燕,等. 无线传感器网络中的虫洞攻击防护机制[J]. 计算机工程与应用, 2012, 48(27): 94-98.

[11] HU Y A, ADRIAN P. A secure on-demand routing protocol for Ad hoc networks[J]. Wireless Networks, 2005, 11(2): 21-38.

[12] SEBASTIAN N. Specification and security analysis of mobile Ad hoc networks[D]. London: University of London, 2006.

[13] LEVENTE B, ISTVAN V. Towards provable security for Ad hoc routing protocols[C]//Proc of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. New York: ACM Press, 2004: 94-105.

(上接第 1207 页)

4　结束语

本文基于威胁树理论构建了第三方支付系统的威胁树模型,给出了第三方支付系统威胁树权值计算及最小威胁树修剪算法,并运用该模型选择当前主流的第三方支付平台进行的实例评估,基于评估提出了针对性的安全建议和对策,从而为用户识别和选择第三方支付工具提供了一定的参考依据。本例评估过程中数据的获取采取了专家打分法,存在着一定的主观性,这是以后研究中需要不断改进的。

参考文献:

[1] 中国网络支付安全状况报告[R]. 北京:中国互联网络研究中心, 2012.

[2] 《支付机构互联网支付业务管理办法》征求意见稿[R]. 北京:中国人民银行,2012.

[3] KIM C S, GALLIERS R D, SHIN N, *et al*. Factors influencing Internet shopping value and customer repurchase intention [J]. Electronic Commerce Research and Applications, 2012, 11(4):374-387.

[4] JORIS C, VALENTIN D, DANNY D C,*et al*. On the security of today's online electronic banking systems [J]. Computers & Security, 2002, 21(3):253-265.

[5] PENNATHUR A K. "Clicks and bricks" e-Risk management for banks in the age of the Internet [J]. Journal of Banking & Finance, 2001, 25(11):2103-2123.

[6] 李良. 中国电子银行风险评估研究[D]. 大连:大连理工大学, 2010.

[7] 李敏. 网络第三方支付风险评价与控制研究[D]. 大连:东北财经大学,2007.

[8] 赵德志. 第三方支付公司的发展与风险研究[D]. 北京:北京邮电大学,2007.

[9] 李医群. 在线第三方支付市场交易效率与风险度量研究[D]. 上海:东华大学,2011.

[10] 刘凯. 第三方支付系统客户端的安全风险及防范机制[J]. 北京信息科技大学学报,2011,26(1):30-35.

[11] GB/T 20984—2007,信息安全技术信息安全风险评估规范[S]. 2007.

[12] 冯登国,张阳,张玉清. 信息安全风险评估综述[J]. 通信学报, 2004,25(7):12-20.

[13] SCHNEIER B. "Attack trees",secrets and lies [M]. New York:Wiley, 2000:318-333.

[14] 甘早斌,吴平,路松峰,等. 基于扩展攻击树的信息系统安全风险评估[J]. 计算机应用研究,2007,24(11):153-156.

[15] 任丹丹,杜素果. 一种基于攻击树的 VANET 位置隐私安全风险评估的新方法[J]. 计算机应用研究,2011,28(2):728-732.