

社交金融的信息安全风险分析与防范

朱建明¹, 高博^{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, 河南 郑州 451191)

摘要: 当前我国金融业正在进行深化改革, 在“互联网+”的背景下互联网金融发展迅速, 尤其是随着移动互联网和互联网社交化的快速发展, 社交金融的发展已经成为趋势。但同时, 依托于移动互联网和社交网络的社交金融也面临着由移动互联网和社交网络所带来的信息安全风险。介绍了社交金融面临的信息安全风险, 通过建立社交金融信息安全博弈模型, 分析并指出了要制订正确的防御策略和采取有效的防御措施来应对社交金融信息安全风险, 从而促进我国社交金融健康快速的发展。

关键词: 社交金融; 信息安全风险; 博弈论; 社交网络

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00034

Social financial information security risk analysis and prevention

ZHU Jian-ming¹, GAO Bo^{1,2}

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

Abstract: The finance is reforming deeply in the country now, and the internet finance develops quickly under the background of “internet+”. Especially with the rapid development of mobile internet and internet socialization, the social finance has become a trend. But at the same time, it faces information security risk brought by the social network and the mobile internet that are the bases of social finance. The social financial potential information security risks were introduced. By modeling a social finance security game, that the correct defense strategy and adopt effective defense measures should be developed was analyzed and pointed out to cope with the social finance information security risks, so as to promote the healthy and quick development of social finance in our country.

Key words: social finance, information security risk, game theory, social network

1 引言

近年来, 随着云计算、大数据、移动互联网、社交网络等新技术的不断发展, 新技术被广泛地应用到金融业, 互联网与金融业在客户管理、风险控制、渠道建设等方面进行了广泛的融合和创

新。金融业可以拓展互联网服务功能的广度与深度^[1], 互联网也可以帮助金融业创新产品和服务, 满足日益增长的不同金融需求。以 P2P、众筹、第三方支付、大数据金融等为代表的新兴互联网金融产业的高速发展, 引发了金融市场交易模式和交易观念上的一场深层次的历史变革, 正成为

收稿日期: 2016-03-02; 修回日期: 2016-03-05。通信作者: 朱建明, zjm@cufe.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61272398); 北京市哲学社会科学重点基金资助项目 (No.14JGA001)

Foundation Items: The National Natural Science Foundation of China (No.61272398), The Key Project of Philosophy and Social Science of Beijing (No.14JGA001)

一股潜力巨大的金融发展创新力量^[2]。

根据 2016 年 1 月中国互联网信息中心发布的第 37 次《中国互联网络发展状况统计报告》显示,截至 2015 年 12 月,中国网民规模达 6.88 亿人,全年共计新增网民 3 951 万人。互联网普及率为 50.3%,较 2014 年年底提升了 2.4 个百分点。中国手机网民规模达 6.2 亿人,较 2014 年年底增加了 6 303 万人。网民中使用手机上网人群占比由 2014 年的 85.8% 提升至 90.1%。截至 2015 年 12 月,网上支付用户规模达 4.16 亿人,增长率为 36.8%。其中手机网上支付用户规模达 3.58 亿人,增长率为 64.5%。

随着移动互联网和互联网社交化的快速发展,社交金融的发展已经成为趋势。社交金融是指使用者借助社交网络在社交信任的基础上建立用户之间的金融关系,开展相关金融服务,实现普惠金融。在社交金融中投融资都不需要通过银行或 P2P 等中介机构,借款人可通过社交信用快速、低成本地获得资金;出资人可以获得收益并加强与借款人之间的社交关系。供需双方信息基本对称,交易成本比较低,可以相对比较容易地进行风险控制,并且降低了风险控制成本。

2 社交金融发展概述

社交金融概念起源于美国 SoFi (social finance) 公司,SoFi 最初由斯坦福大学的 4 个校友创办,旨在面向斯坦福大学学生和毕业生提供贷款,最初的资金由斯坦福校友众筹而来。SoFi 与金融机构的不同之处是它强调的是贷款人和学生之间的校友关系,是一家以校友为纽带的 P2P 借贷平台。借助 SoFi,大学生既可以增加现有贷款限额,也可以申请新的贷款,最低利率约为 5.9%,而美国政府贷款最低利率为 6.8%。SoFi 的放款人通常是各个学校的校友,他们希望至少能够获得 5% 的回报率。此外,SoFi 也在积极地推广线下活动,借助校友的力量组建起大量的线下群体,增强用户粘性。它为每一个高校构建了一个社交网络,帮助投资及借款的校友双方建立联系。对于在校学生而言,这些线下活动可以有效地帮助在校学生寻找社会资源,构建人脉,甚至可以帮助他们找到心仪的工作。SoFi 是社交金融的第一次实践,取得了比较好的成效。在

这以后,Facebook 和 Twitter 等美国著名社交网络都推出了自己的社交金融。

最近两年国家也有越来越多的互联网企业和金融企业进入社交金融领域,如平安集团的壹钱包、团贷网旗下的你我金融、靠谱鸟都是社交金融平台。其中靠谱鸟成立于 2014 年,被认为是中国最早探索社交金融的平台,主要为北京大学、清华大学等高校的校友提供校友圈理财投资以及 P2P 网络借贷平台。熟信、赢贝、友借友还、米啊、借点儿、朋友范等软件平台也在积极开拓社交金融市场。2015 年 7 月,支付宝软件平台添加了由蚂蚁小贷提供的借条服务,意味着阿里巴巴旗下的蚂蚁金融也进入了社交金融领域。微信红包是微信于 2014 年 1 月 27 日推出的一款应用,功能上可以实现发红包、查收发记录和提现。微信红包与 2015 年春节联欢晚会进行互动,2015 年除夕当日微信红包收发总量达 10.1 亿次,使得数以亿计的微信用户切实地体验到了社交金融带来的收益和娱乐的双赢。

由此可见,社交金融发展迅速,社交金融可以增加借款人的失信成本,对 P2P 平台的风险控制起到一定的提升作用,也是互联网金融创新的一种表现形式,社交金融的发展必将进一步促进国家金融业的改革和发展。

3 社交金融面临的信息安全风险

社交金融依托于移动互联网和社交网络,因此也面临着由移动互联网和社交网络所带来的信息安全风险。社交金融主要面临的信息安全风险是移动互联网恶意程序、网络钓鱼、个人隐私泄露和盗窃。

2015 年,国家互联网应急中心通过测发现的移动互联网恶意程序已超过 145 万件,较 2014 年增长 52%,2015 年具有恶意扣费、信息窃取等高危恶意行为的恶意程序快速增长,已严重影响到我国网民的财产安全和个人信息安全。根据 360 互联网安全中心发布的《2015 年中国手机安全状况报告》显示,2015 年,360 手机卫士共为全国手机用户拦截各类钓鱼网站攻击 48 亿次,占 360 各类终端安全产品拦截钓鱼网站总量 (379.3 亿次) 的 12.6%。无论是拦截的总攻击次数还是

拦截量在总拦截量中的占比,均创历史新高。从全年整体情况来看,钓鱼网站对手机端的攻击次数越来越多,占比也越来越大,但这一趋势在过去几年中并不太明显。

3.1 移动互联网恶意程序

在互联网上有许多可以下载的应用程序,其中大多数有比较多的安全问题。在网站下载恶意应用程序最大的担忧是被欺诈。基于移动应用程序的威胁可分为以下2种^[3]。

1) 木马程序。木马程序是指在没有经过用户授权的情况下收集用户个人隐私数据。木马程序窃取的数据通常包括用户的位置、通讯录、私人照片、电子邮件地址、浏览器浏览历史记录、电话通讯记录等,被盗的信息可能用于假冒身份或金融诈骗^[4]。

2) 恶意软件。恶意软件是指在未经用户授权同意的情况下将恶意软件安装在用户的移动设备上,它会造成用户资费消耗和恶意扣费,并向用户通讯录中的联系人发送恶意信息,让攻击者完全控制移动设备^[5]。

3.2 网络钓鱼

正如网络钓鱼这个名字表明的一样,网络钓鱼就是为窃取敏感信息的媒介伪装一个合法的来源^[6]。例如,黑客假装银行并发送信息要求用户进行身份验证并登录银行,但是用户可能会被重定向到一个网站,而该网站的外观与真实银行网站的外观非常相似,黑客获取用户输入的银行登录凭证信息。高水平黑客会利用社会工程学等攻击技术和浏览器/服务器模式缺陷(例如XSS即跨站脚本攻击),让他的钓鱼网站设计看起来更为合理。

由于互联网用户在日常生活中广泛地使用Twitter、Facebook、LinkedIn、微博、微信和QQ等社交网络软件,因此它们具有很好的商业价值而被广泛地接受,企业防火墙基本上是不会阻止这一类软件使用的。用户基本上没有经过信息安全教育,这些社交网络软件本身又开放应用程序编程接口(API, application programming interface)并且隐私设置不够完善,因此黑客喜欢选择社交网络作为他们收集用户个人信息和发起攻击的地方。通常黑客会利用社交网络在上面发送比较吸引用户的网络钓鱼恶意消息,用户一不小心查看

这些信息之后就会进入钓鱼网站成为受害者。

3.3 个人隐私泄露和盗窃

社交网络中最敏感的问题就是用户隐私问题,社交网络从一诞生起就与这个问题相伴相生,随着大数据时代的到来,隐私问题显得越来越重要。在社交金融中,一方面要为用户提供更加精准良好的金融服务,另一方面也要注重对用户隐私的保护,社交金融只有在满足用户金融需求的同时又能满足用户的安全需求,才能健康持续地发展。

根据六度分离理论,一个人和任何一个陌生人之间所间隔的人不会超过5个,也就是说最多通过5个人就能够认识任何一个陌生人。因此,通过社交网络,一个人可以联系认识很多的陌生人,虽然说更多的联系和接触并不一定是坏事,但是这些人到底谁有权查看用户的个人信息?社交网站提供一定程度的访问控制,但是很多人并没有将这些访问控制配置正确,因此可能所有人都具有一样的访问权限,人们并不知道根据六度分离理论通过社交网络认识的那个陌生人是不是就是黑客。

由于有些用户的信息安全意识不足,他们在社交网络中使用的都是真实信息,包括名字、生日、教育背景以及家乡等信息,这样是非常不安全的,很容易被黑客利用进行攻击。在社交网络中有些用户选择性地透露自己的信息,但是恶意攻击者也会利用社交网站的高级搜索功能和交叉引用用户信息的方法来窃取用户的个人信息。

4 社交金融信息安全博弈模型

依托于社交网络的社交金融面临着社交网络所带来的信息安全风险,通过社交网络建立起金融联系的用户往往并不是毫无相关的陌生人,彼此之间都有一定程度的信任。社交金融网络中的用户由于彼此之间有一定程度的信任,用户对社交金融网络中其他用户发送和共享的信息、链接和内容一般不会产生怀疑,就会查看这些信息和内容,这样其他用户就会被恶意程序感染和受到攻击。当社交金融网络中有一个用户的手机感染恶意程序、受到钓鱼网站攻击或者个人隐私被盗和泄露时会快速感染和攻击用户所在社交金融网络中的其他用户,造成用户的金融财产损失,因

此社交金融比传统金融和互联网领域面临更严峻的信息安全风险和威胁。

近年来, 博弈论被广泛地应用于信息安全领域, 安全博弈为建模分析攻击者和防御者之间的相互作用提供了一个定量的框架, 安全博弈及其均衡解可以作为正式决策、算法发展以及预测攻击行为的基础。本文利用博弈论建立一个社交金融信息安全博弈模型, 社交金融网络攻击是社交金融网络的恶意攻击者和社交金融网络的所有者或管理者之间的战略博弈。该博弈建立在社交金融网络复杂和相互联系的系统之上, 在这个系统中攻击者主要通过恶意程序、网络钓鱼和窃取个人隐私等方式对社交金融系统进行攻击, 防御者采取安全网关、入侵检测系统等防御措施进行防御。

4.1 建立安全博弈模型

定义一个社交金融信息安全博弈模型, 在这个博弈当中, 有 2 个参与者, 即防御者用 P^D 表示, 攻击者用 P^A 表示。防御者通过采取多种安全技术措施保护社交金融网络中的金融信息资产和数据的安全, 防止相关信息资产和数据被外部或者内部的攻击者进行攻击, 该博弈是一个非合作的静态博弈。攻击者 P^A 会在他所发现的社交金融网络用户集合 $S = s_1, s_2, \dots, s_n$ 中选择一个用户作为攻击目标进行攻击, 而防御者则会采用不同级别的防御措施对攻击进行防御^[7]。当攻击者攻击用户 s_i , 防御者采用基本防御策略进行防御时, 他的效用记为 $U_a^j(s_i)$; 当攻击者攻击用户 s_i , 防御者采用最优防御策略进行防御时, 他的效用记为 $U_a^b(s_i)$; 如果攻击者没有发起攻击, 则防御者的效用为 0。类似地, 可以将攻击者的基本攻击效用和最优攻击效用表示为 $U_a^j(s_i)$ 和 $U_a^b(s_i)$, 进一步对于攻击目标用户 s_i , 将防御者 P^D 的效用变化值记为 $\Delta U_a(s_i)$, 将攻击者 P^A 的效用变化值记为 $\Delta U_a(s_i)$, 当防御者采用防御措施对攻击目标进行防御时, $\Delta U_a(s_i) > 0$, 而且 $\Delta U_a(s_i) > 0$ 。定义 $p^A = [p_1, \dots, p_n]$ 为攻击者攻击社交金融网络中相应攻击行为的概率分布, 其中 p_i 为攻击者 P^A 攻击网络用户 s_i 的概率; $q^D = [q_1, \dots, q_n]$ 为防御者相应防御行为的概率分布, 其中 q_i 为防御者 P^D 防御网络用户 s_i 遭受攻击的概率。定义 A 为攻击者 P^A 攻击社交金融网络中 n 个用户的一个攻击混合策略,

定义 D 为防御者 P^D 防御社交金融网络中 n 个用户的一个防御混合策略。

4.2 安全博弈模型分析

根据上面的定义, 可以定义社交金融网络信息安全博弈模型中攻击者 P^A 和防御者 P^D 的效用函数分别为

$$U_d(D, A) = \sum_{i=1}^n p_i [q_i U_a^b(s_i) + (1 - q_i) U_a^j(s_i)] \quad (1)$$

$$U_a(D, A) = \sum_{i=1}^n p_i [q_i U_a^b(s_i) + (1 - q_i) U_a^j(s_i)] \quad (2)$$

如果参与博弈的防御者和攻击者都是理性的, 那么他们会同时达到纳什均衡 (Nash equilibrium)。

若防御者 P^D 和攻击者 P^A 所采用的防御混合策略 D^* 和攻击混合策略 A^* 满足以下条件, 则混合策略 D^* 和 A^* 构成一个纳什均衡的混合策略, 即

$$U_a(D, A^*) \geq U_a(D, A), \forall A \quad (3)$$

$$U_d(D^*, A) \geq U_d(D, A), \forall D \quad (4)$$

在这个社交金融网络安全博弈模型当中可能存在多个纳什均衡, 然而因为并不知道攻击者的具体攻击行为, 所以并不是所有防御者的纳什均衡防御策略效果都是一样的, 在社交金融信息安全博弈中更关注的是防御策略而不是攻击策略, 最关注的是能够使防御者效用函数达到最大的纳什均衡。

在一个真实的社交金融网络攻击中, 攻击者和防御者都会有自己的选择和标准来评估一个攻击的经济效益, 所以社交金融网络安全博弈不一定是零和博弈。网络安全博弈中防御者的纳什均衡防御策略是一个最小最大策略, 并且它最小最大化了攻击者的效用^[7]。这里设定社交金融网络零和博弈为 $\bar{G}$, 非零和博弈为 G , 设定攻击者 P^A 在社交金融网络零和博弈 $\bar{G}$ 中攻击任何一个用户的基本攻击效用、最优攻击效用与在非零和博弈 G 中的基本攻击效用、最优攻击效用是一样的, 则

$$\bar{U}_a^j(s_i) = U_a^j(s_i), \forall s_i \in S, \bar{U}_a^b(s_i) = U_a^b(s_i), \forall s_i \in S \quad (5)$$

由于 $\bar{G}$ 为零和博弈, 所以 $U_a^j(s_i) = -U_a^j(s_i)$, 并且 $U_a^b(s_i) = -U_a^b(s_i)$ 。

下面定义一个函数 μ , 该函数是一个将零和博弈 $\bar{G}$ 中攻击一个目标用户的攻击概率映射到非零和博弈 G 中攻击一个目标用户的攻击概率^[7], 即

$$\mu(p_i) = \bar{p}_i = \lambda p_i \frac{\Delta U_d(s_i)}{\Delta U_a(s_i)}, \forall s_i \in S \quad (6)$$

其中, $\mu(p_i)$ 是非零和博弈 G 中攻击目标 s_i 的攻击概率, 因此 $\mu(p^A) = p^A$ 。

当 D^* 和 $\mu(A^*)$ 是零和博弈 $\bar{G}$ 中的一个纳什均衡时, 对应的 D^* 和 A^* 也是非零和博弈 G 中的一个纳什均衡, 下面证明这个结论。 D^* 和 $\mu(A^*)$ 是零和博弈 $\bar{G}$ 中的一个纳什均衡, 也就是说

$$U_a^{\bar{G}}(D, \bar{A}^*) - U_a^{\bar{G}}(D, \bar{A}) \geq 0, \forall \bar{A}$$

而 D^* 和 A^* 也是非零和博弈 G 中的一个纳什均衡, 意味着

$$U_a^G(D, A^*) - U_a^G(D, A) \geq 0, \forall A$$

根据式(6), 有 $p_i = \bar{p}_i \frac{1}{\lambda} \frac{\Delta U_a(s_i)}{\Delta U_d(s_i)}$, 已知 $\Delta U_a(s_i)$, $\Delta U_d(s_i), \lambda \geq 0$, 由式(1)和式(2), 有

$$\begin{aligned} & U_a^G(D, A^*) - U_a^G(D, A) \geq 0 \\ \Leftrightarrow & \sum_{i=1}^n p_i^* [q_i U_a^b(s_i) + (1-q_i) U_a^j(s_i)] - \\ & \sum_{i=1}^n p_i [q_i U_a^b(s_i) + (1-q_i) U_a^j(s_i)] \geq 0 \\ \Leftrightarrow & \sum_{i=1}^n (p_i^* - p_i) [q_i U_a^b(s_i) + (1-q_i) U_a^j(s_i)] \geq 0 \\ \Leftrightarrow & \sum_{i=1}^n \frac{1}{\lambda} \frac{\Delta U_a(s_i)}{\Delta U_d(s_i)} (\bar{p}_i^* - \bar{p}_i) [q_i U_a^b(s_i) + (1-q_i) U_a^j(s_i)] \geq 0 \\ \Leftrightarrow & \sum_{i=1}^n (\bar{p}_i^* - \bar{p}_i) [q_i U_a^b(s_i) + (1-q_i) U_a^j(s_i)] \geq 0 \\ \Leftrightarrow & U_a^{\bar{G}}(D, \bar{A}^*) - U_a^{\bar{G}}(D, \bar{A}) \geq 0 \end{aligned}$$

同理可以证明

$$\begin{aligned} & U_d^{\bar{G}}(D^*, \bar{A}) - U_d^{\bar{G}}(D, \bar{A}) \geq 0 \\ \Leftrightarrow & U_d^G(D^*, A) - U_d^G(D, A) \geq 0, \forall D \end{aligned}$$

可以得出 D^* 和 A^* 也是非零和博弈 G 中的一个纳什均衡, D^* 和 $\mu(A^*)$ 是零和博弈 $\bar{G}$ 中的一个纳什均衡, 无论是零和博弈还是非零和博弈, D^* 都是防御者 P^D 纳什均衡防御策略独立于攻击者的攻击策略, 因此社交金融网络的防御者要把主要精力放在制定防御策略上, 而不是过多关注攻击者的攻击策略。

5 社交金融信息安全风险的防范措施

这两年社交金融发展迅速, 促进了实体经

济发展, 方便了居民日常生活, 满足了投资需求, 推动了普惠金融的发展^[8]。由上面的对社交金融信息安全博弈模型的分析可以知道要把主要精力放在制订防御策略和采取防御措施来提高社交金融的安全上。针对社交金融面临的信息安全风险, 需要采取多种措施来进行防范, 这样才能够更好地推动我国社交金融健康快速的发展。

5.1 强化安全防御技术

针对移动互联网恶意程序造成的信息安全风险, 在强化防御技术上需要移动应用程序商店、移动设备操作系统生产商、应用程序提供商一起合作建立一个安全的移动服务生态系统。移动应用程序商店例如苹果商店、安卓应用商店应该提供安全的移动应用程序商, 移动应用程序商店应该加强对商店中应用程序的功能、数据安全和隐私的测试。若发现恶意应用程序应该及时删除, 直到该软件经过测试没有安全威胁以后才允许进入应用程序商店。移动设备操作系统生产商应该及时更新操作系统, 确保用户隐私和数据的安全性。应用程序提供商在一个安全的移动服务生态系统中起到了很重要的作用, 开发人员可以利用应用程序的漏洞直接访问用户的移动设备, 窃取用户有价值的业务或者个人数据, 因此对开发人员应该有一定的控制和限制机制^[9]。

针对网络钓鱼造成的信息安全风险, 用户应该了解网络钓鱼带来的严重后果, 用户不仅应该对可疑的 URL 网址信息和短消息非常敏感, 而且还要重视安全软件对钓鱼网站的警告消息, 最重要的是用户应该审查他们的社交网络应用程序中的隐私安全设置是不是有问题。

针对个人隐私泄露和盗窃造成的信息安全风险, 用户应该对于自己的个人信息针对不同的人给予不同的查看权限, 可以将社交网络中的联系人定义为不同的组, 每个组设置不同的权限^[10]。在社交网络中应该对用户发送和查看信息的范围进行限制, 这样可以有效地防止恶意信息的自动传播^[11]。因为大部分信息不是通过社交网络中用户个人原始配置文件泄露的, 而是从旁观者的评论中泄露的, 所以用户应该有权审查和管理评论^[12]。

5.2 完善法律制度, 提高监管能效

对社交金融进行监管的同时应该坚持鼓励

金融创新、保障金融稳定、维护市场公平竞争, 人民银行和中国银行监督管理委员会等监管机构要完善相关法律法规制度, 增强政策和制度的可执行性, 加强与第三方支付机构和金融机构的沟通, 提高监管效能。在对社交金融进行监管时, 要适当转变监管理念, 不能拘泥于传统的金融监管思路, 阻碍金融创新, 同时也要明确监管主体与保证监管措施的严厉性。社交金融作为新生事物, 其在发展过程中可能出现各种各样的问题, 因此更应该对监管机制加以完善, 做到未雨绸缪。

5.3 加强宣传教育, 增强用户安全意识

要通过各种媒介加强信息安全的宣传教育, 增强用户的安全意识, 养成良好的网络和软件使用习惯, 从而消除部分安全隐患。手机安全的主要问题之一在于部分智能手机用户尤其是使用安卓操作系统的用户没有安装有效的手机安全软件, 用户安全意识严重不足。要加强宣传教育, 培养良好的安全习惯, 从正规的应用商店下载安全的移动应用程序, 及时更新操作系统和升级应用程序, 安装有效的手机安全软件。发现有要求输入银行卡号和输入支付账号的邮件、短信等信息不要轻易点击地址链接, 保护自己的资金安全, 防止被骗。

6 结束语

社交金融作为互联网金融的一种新的表现形式, 其能够利用社交网络成本低、效率高、覆盖广等优势优化金融市场资源配置, 提高金融服务质量。在鼓励其不断创新的同时, 也要对其面临的信息安全风险制定相应的防范和监管措施。只要制订正确的防御策略和采取有效的防御措施, 社交金融面临的信息安全风险是完全可以控制的, 要保持对社交金融信息安全风险的高度警惕, 也要时刻关注相关信息安全技术的最新发展情况, 及时掌握和应用最新的信息安全技术, 从而有效地规避社交金融带来的信息安全风险, 更好地促进社交金融持续、健康、稳定的发展, 进一步促进我国金融业深化改革和健康发展。

参考文献:

- [1] SHAHROKHI E. Finance: status, innovations, resources and future challenges[J]. Managerial Finance, 2008(6):365-398.
- [2] 谢平, 邹传伟. 互联网金融模式研究[J]. 金融研究, 2012(12):

11-22.

- XIE P, ZOU C W. Research on internet financial model[J]. Journal of Financial Research, 2012(12):11-22.
- [3] SUJITHRA M, PADMAVATHI G. Mobile devices security: a survey on mobile device threats, vulnerabilities and their defensive mechanism[J]. International Journal of Computer Applications, 2012(14):24-29.
- [4] Lookout, "what is a mobile threat"[EB/OL]. <https://www.lookout.com/resources/know-your-mobile/what-is-a-mobilethreat>.
- [5] DAGON D, MARTIN T, STARNER T. Mobile phones as computing devices: the viruses are coming[J]. IEEE Pervasive Computing, 2004, 3(4):11-15.
- [6] WEBSTER M. Phishing[EB/OL]. <http://www.merriam-webster.com/dictionary/phishing>.
- [7] KORZHYK D, YIN Z, KIEKINTVELD C, et al. Stackelberg vs. Nash in security games: an extended investigation of interchangeability, equivalence and uniqueness[J]. Journal of Artificial Intelligence Research, 2011, 41(2):297-327.
- [8] 刘鑫. 我国互联网金融的发展情况及模式浅析[J]. 当代经济, 2014(24):4-5.
- LUI X. The development and pattern analyses of internet financial situation in our country[J]. Contemporary Economics, 2014(24): 4-5.
- [9] JANG J J, NEPAL S. A survey of emerging threats in cyber security[J]. Journal of Computer and System Sciences, 2014,80(5): 973-993.
- [10] WOLFR D, WILLAERT K, PIERSON J. Managing privacy boundaries together: exploring individual and group privacy management strategies in facebook[J]. Computers in Human Behavior, 2014(35): 444-454.
- [11] FENG Y, XIE W. Teens' concern for privacy when using social networking sites: an analysis of socialization agents and relationships with privacy protecting behaviors[J]. Computers in Human Behavior, 2014(33): 153-162.
- [12] ANDERSON J, STAJANO F. Must social networking conflict with privacy[J]. IEEE Security and Privacy, 2013,11(3):51-60.

作者简介:



朱建明(1965-), 男, 山西太原人, 中央财经大学信息学院教授、博士生导师, 主要研究方向为信息安全、电子商务安全。



高博(1981-), 男, 河南郑州人, 中央财经大学信息学院博士生, 河南工程学院管理工程学院讲师, 主要研究方向为电子商务、管理信息系统。