

信息安全视角下的软件供应链 厂商开发策略选择研究

孙 丹, 朱逸飞

江苏大学管理学院, 江苏 镇江

收稿日期: 2024年4月22日; 录用日期: 2024年5月15日; 发布日期: 2024年11月26日

摘 要

信息安全已成为软件产品的基础, 引起了软件厂商和软件用户的广泛关注。本文以信息安全视角为切入点, 研究软件供应链厂商的开发策略选择。通过构建对称信息安全环境下的软件供应链厂商开发策略选择博弈模型, 得到了不同情形下的软件厂商的相应开发策略。研究发现: (1) 在两家软件厂商都开发闭源软件时, 较高的产品间替代率会使得两家软件厂商的软件产品提高并影响软件厂商信息安全投入水平, 影响消费者的需求, 并进一步增加他们在竞争市场中的利润。(2) 若开源开发策略的回报较高, 即使信息安全问题较为严重, 软件厂商仍更有可能选择开源的开发模式。(3) 同构开发模式下闭源软件厂商的利润高于异构开发模式下闭源厂商的利润。

关键词

信息安全, 软件供应链, 软件厂商, 开发策略选择, 博弈论

Research on Vendor Development Strategy Selection of Software Supply Chain from the Perspective of Information Security

Dan Sun, Yifei Zhu

School of Management, Jiangsu University, Zhenjiang Jiangsu

Received: Apr. 22nd, 2024; accepted: May 15th, 2024; published: Nov. 26th, 2024

Abstract

Information security has become the foundation of software products, which has attracted the wide

attention of software manufacturers and software users. This paper studies the development strategy choice of software supply chain manufacturers from the perspective of information security. By constructing a game model of software supply chain vendor development strategy selection under symmetric information security environment, the corresponding development strategies of software vendors under different situations are obtained. The results show that: (1) When both software vendors develop closed-source software, the higher inter-product substitution rate will improve the software products of the two software vendors, affect the information security investment level of software vendors, affect the demand of consumers, and further increase their profits in the competitive market. (2) If the return of open source development strategy is higher, even if the information security problem is more serious, software manufacturers are more likely to choose open source development mode. (3) The profit of closed-source software vendors in homogeneous development mode is higher than that of closed-source software vendors in heterogeneous development mode.

Keywords

Information Security, Software Supply Chain, Software Vendors, Development Strategy Selection, Game Theory

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在传统的软件行业中, 软件厂商通常采用闭源开发策略, 将封闭源代码的软件产品销售给个人和组织, 用户无法获取源代码、修改或分发。然而, 开源软件的出现改变了这种商业模式和开发策略。开源软件是指源代码对公众开放, 允许用户在许可范围内自由使用、改进、修复漏洞并免费二次分发。这种模式下, 软件厂商不直接通过软件销售获利, 而是通过提供补充和增值服务赚取收益。在过去十多年, 开源软件如火狐浏览器、Linux 系统、安卓平台等取得巨大成功。在这样的环境下, 不少软件厂商也改变开发策略, 尝试开发开源软件或将原有闭源软件转变为开源软件。以曾经成功的动画与应用程序创造软件 Adobe Flash 为例, Adobe Flash 在过去曾占有很大一部分市场, 但由于其开发协议和技术由 Adobe 公司闭源独占, 且安全性能堪忧, 并且随着 HTML5 的出现和普及, Adobe Flash 逐渐失去市场份额, 谷歌和苹果也不再支持该软件。相对地, 开源的 HTML5 虽然存在缺陷, 但不断发展且更受用户欢迎。

然而, 软件市场的蓬勃发展同时伴随着频繁的信息泄露事件, 日益严重的用户信息安全担忧将最终影响软件厂商的开发策略。软件厂商存在开源和闭源两种截然不同的开发方式, 它们也影响着利润获取的途径。在这样的背景下, 软件厂商面临着如何在考虑信息安全问题的情况下选择开发策略, 在保证软件产品信息安全的同时, 实现利润最大化。因此, 本文在考虑黑客入侵等信息安全因素的基础上, 构建了两家厂商在信息安全威胁环境下的古诺双寡头博弈模型, 研究软件厂商在不同情形下的开发策略选择。

2. 相关研究

开源软件是指开放源代码的软件包, 其定义表明源代码可供大众使用, 且该软件包的使用、修改和发布没有任何限制, 专有软件和开源软件的区别主要是源代码是否公布[1]。在开源软件出现后, 许多学者是从经济学角度通过对比开源软件和专有软件来分析开源软件的经济效益。开源软件的获取和使用并不收费, 软件厂商则是通过一系列的衍生产品和服务来获取收益。Bandyopadhyay [2]等认为开源和闭

源对软件质量没有直接影响, 没有证据表明开源软件质量一定劣于专有软件, 软件质量更多地取决于外部因素, 如程序员结构和协作、激励、市场结构以及内生变量等。Lakhani 等[3]研究表明公益性开源软件并不总是会激励专有软件公司提高软件质量, 反而价格为零的开源软件可能会降低价格竞争, 使得专有软件利润更高, 消费者剩余更差。在软件市场中, 垄断和竞争环境下开源软件和闭源软件的问题被反复讨论。在垄断环境下, Economides 和 Katsamakas [4]分析了专有技术平台针对平台用户和提供与该平台互补的应用程序的公司的最优双边定价策略。Caulkins 等人[5]研究了在将软件开源之前保持软件专有的最佳时间。Haruvy 等人[6]研究了在考虑产品质量、网络规模和雇佣策略的情况下, 企业在开放和封闭资源之间选择最优商业模式。Augus 等研究了当开源软件发布后, 在此开源软件基础上进行开发更新的贡献者做出战略性努力时, 创立者在开源和闭源软件之间的关系[7]。Sen 发现, 在竞争市场中, 包括开源软件和开源软件的商业版本, 闭源软件公司在低网络外部性的存在下会更好[8]。Kumar 等[9]讨论了两家生产商业软件和开源软件的企业之间的竞争, 发现企业努力之间的搭便车行为可以产生高质量的产品, 甚至增加消费者剩余和企业利润。Casadesus-Masanell 和 Ghemawa 研究了一种动态混合双寡头垄断的竞争博弈模型, 即利润最大化的闭源软件产品(如 Windows)与开源软件(如 Linux)以零价格相互作用[10]。网络外部性对于软件市场也有很大影响, Cheng 等研究了正网络外部性对开源和开源企业之间竞争的影响。他们在网络外部性中发现, 对于封闭源代码的公司来说, 与其竞争对手兼容是不可取的, 但是对于开放源代码的公司来说, 这是可取的[11]。Kort 和 Zaccour 的研究讨论了两家竞争公司商业模式战略选择问题[12]。他们发现, 当软件产品市场竞争更激烈、互补产品市场竞争较弱、互补产品质量较高时, 两家公司都会选择开放源代码。目前相关文献关于软件厂商开发策略的研究主要集中在开源软件的出现如何影响闭源软件, 当前的研究更倾向于在考虑消费者偏好或 R&D 等经济因素下对软件厂商开发策略的影响。但是对于软件厂商在开发软件产品上的策略选择研究中, 较少考虑信息安全问题。本文将考虑在信息安全视角下, 讨论软件厂商的开发策略选择问题。

3. 模型构建与分析

3.1. 模型假设

本文假设市场上存在两个提供同类软件产品的厂商 1 和厂商 2, 在进行开发策略选择时, 可分为两个阶段。第一阶段, 软件厂商 1 和软件厂商 2 选择软件研发的方式, 第二阶段, 软件厂商 1 和软件厂商 2 决定软件产品及其衍生品和服务的价格和信息安全投入水平, 开源厂商的主要收入来自开源软件的衍生产品和服务的销售。当他们选择一个闭源的开发模式时, 他们会对软件产品收费, 而当他们制定一个开源的开发模式时, 他们会将价格设为 0。免费加收费模式是软件市场上的一种常见形式, 软件厂商往往通过向用户提供一个开源免费版本来吸引用户购买其功能更多更强大的收费版本, 或者通过向用户提供增值服务来获取利润。类似的, 安卓平台是一个完全开源的平台, 而 IOS 则是封闭源代码的。博弈在 2 个同质的参与方之间展开, 即软件厂商 1 和软件厂商 2 面临的外在威胁、脆弱性 V 、预期损失 L 和投资效率 k 相等。博弈同时在进行。软件厂商 1 和软件厂商 2 在考虑对方软件产品价格 p 的情况下, 最大化自身利润。

假设 1: 两家竞争的软件厂商提供的软件产品互为替代品。当没有安全威胁时, 假设软件厂商 1 的需求函数在自我效应和交叉价格效应中是线性的:

$$q_i = 1 - p_i + \lambda p_j$$

q_i 是软件厂商 1 的软件产品数量, p_i 是软件厂商 1 的软件产品价格, p_j 为软件厂商 2 的软件产品价格 ($i, j = 1, 2; j \neq i$) (Gal-Orand Ghose) [13]。软件厂商 1 的初始需求为 1, 表示当软件产品价格为 0 时的截

距。参数 λ 是两家软件厂商软件产品的替代率, 用来衡量两家软件厂商之间的竞争强度。由于软件厂商 1 的价格对其需求的影响大于软件厂商 2 的价格, 所以参数 λ 满足 $\lambda \in [0, 1]$ 。随着 λ 的增大, 两家软件厂商的软件产品成为彼此的更好的替代品, 竞争变得更加激烈。而在 $\lambda = 0$ 时表示两家软件厂商的软件产品是独立的, $\lambda = 1$ 表示两家软件厂商的软件产品是完全替代品, 完全同质。对于替代率 λ 的现实解释。举例来说, IOS 和安卓这两种手机操作系统在许多方面存在不同, 如它们的状态栏、返回密钥、类型的多样性、文件读取权限、应用程序市场规则和虚拟商品的版税规则, 这就产生了一定的替代性, 此处用 λ 表示两家软件厂商间产品的替代率。

假设 2: 当软件供应链存在外部安全威胁时, 考虑软件安全对每个软件厂商的影响。假设信息系统被直接成功入侵的概率为 $g = \frac{v}{ks+1}$, 其中 v 表示软件固有的网络脆弱性, s 表示软件厂商的信息安全投入, k 表示信息安全投入效率, k 越大则表示两家软件厂商在信息安全方面的投入效率越高, 反之则越低。当两家软件厂商的软件产品都存在安全威胁时, 安装此类软件产品的用户数量为 $q_i + q_j$ 。随机攻击是指利用使用软件的软件产品存在漏洞的用户发起的随机攻击, 如蠕虫攻击, 攻击强度为 $g > 0$ 。然后, 蠕虫成功渗透用户网络的概率为 $g(q_i + q_j)$ 。这里, 假设 $g(q_i + q_j)$ 足够小, 位于 0 和 1 之间。由于用户网络的相互依赖性, 用户在黑客攻击下存活概率为 $(1-g)(q_i + q_j)$ [14]。黑客攻击是通过一种软件产品或两种软件产品共享的安全漏洞渗透到用户网络。另一方面, 黑客攻击可以通过社交网络或用户之间的业务关系传播, 例如上游供应商和下游零售商的供应链, 通过电子数据交换连接(Hausken 2006) [15], $(1-g)(q_i + q_j)L$ 可以看作软件厂商进行信息安全投入带来的收益, 两家软件厂商会面临相同的入侵概率。

假设 3: 两家公司可以战略性地选择两种类型的开发模式: 一种是封闭源代码模式, 即公司通过出售软件产品实现利润最大化, 另一种是开源模式, 公司免费提供软件产品, 并从互补或增值服务中获益。作为一种信息商品, 软件产品具有较高的固定成本和可忽略的可变成本, 软件厂商的信息安全投入可作为固定成本计入软件开发中, 排除固定成本不会改变主要结果, 因此在不丧失一般性的情况下, 本文假设软件产品的成本为零。如果软件厂商 1 选择封闭源代码的开发模式, 其利润(收入)函数的形式为:

$$\begin{aligned}\pi_i &= p_i q_i + (1-g)(q_i + q_j) \\ \pi_i &= p_i(1-p_i + p_j \lambda) + L \left(1 - \frac{v}{1+ks}\right) (2-p_i - p_j + p_i \lambda + p_j \lambda)\end{aligned}\quad (1)$$

如果软件厂商 1 选择开源的开发模式, 用户可以访问和提高软件产品的质量并因此吸引 α 倍的额外的用户, 这样软件厂商 1 的需求量是:

$$q_i(\alpha+1) = q_i + \alpha q_i$$

此时软件厂商 1 的利润函数为:

$$\begin{aligned}\pi_i &= b(\alpha+1)(1-p_i + p_j \lambda) + L \left(1 - \frac{v}{1+ks}\right) (2-p_i - p_j + p_i \lambda + p_j \lambda) \\ \pi_i &= b(\alpha+1)(1+p_j \lambda) + L \left(1 - \frac{v}{1+ks}\right) (2-p_j + p_j \lambda)\end{aligned}\quad (2)$$

具体参数设置如表 1 所示。

3.2. 不同情形下软件厂商利润最大化模型分析

情形 1: 当软件供应链处于同构开发模式, 且两家软件厂商都选择研发开源软件时, 即 $p_i = p_j = 0$, $s_i = s_j = s$ 。

Table 1. Parameter setting
表 1. 参数设置

符号	含义
$q_i, q_i \in [0,1]$	软件厂商 1 的产品需求量
$p_i, p_i > 0$	软件厂商 1 的产品价格
$s_i, s_i > 0$	软件厂商 1 的安全投入
$\lambda, \lambda \in [0,1]$	两家软件厂商间的产品替代率
$g, g \in [0,1]$	软件被黑客攻击的概率
$\alpha, \alpha > 0$	开源软件用户的创新幅度
$v, v \in (0,1)$	软件产品固有的漏洞系数
$L, L > 0$	以金钱计量的被攻破后遭受的损失
$k, k > 0$	信息安全投入效率

需求函数为:

$$q_i = q_i (\alpha + 1)$$

利润函数为:

$$\pi^{oo} = b(\alpha + 1)q_i + Lg(q_i + q_j)$$

其中, 需满足 $1 - \frac{v}{ks+1} > 0$, $s > \frac{v-1}{k}$, 由于 $v \in (0,1)$ 且 $s_i > 0$, 所以一定满足 $s_i > \frac{v-1}{k}$, 此时选择开源开发模式的软件厂商均衡利润为:

$$\pi^{oo} = b(\alpha + 1) + 2 \frac{Lv}{ks+1} \tag{3}$$

情形 2: 当两家软件厂商都选择研发闭源软件。

两家利润函数为:

$$\pi^{cc} = p_i (1 - p_i + p_j \lambda) + L \left(1 - \frac{v}{1+ks} \right) (2 - p_i - p_j + p_i \lambda + p_j \lambda) \tag{4}$$

此时对 π^{cc} 求关于 p_i 的偏导, 令其等于 0, 可得

$$\frac{\partial \pi^{cc}}{\partial p_i} = 1 - 2p_i + L \left(1 - \frac{v}{ks+1} \right) (-1 + \lambda) + p_j \lambda = 0$$

在纳什均衡下, 由于 2 个软件厂商是同质的, 根据对称性, 必有 $p_i = p_j = p$, $s_i = s_j = s$, 带入式(4)可得软件厂商此时最优价格 p 为

$$p = \frac{-1 + L - ks + kLs - Lv - L\lambda - kLs\lambda + Lv\lambda}{(1+ks)(-2+\lambda)} \tag{5}$$

此时选择闭源开发模式的软件厂商的均衡利润为:

$$\pi^{cc} = \frac{(1+ks - (-3+\lambda)L[1+ks-v])(1+ks + (-1+\lambda)^2 L[1+ks-v])}{(1+ks)^2 (-2+\lambda)^2} \tag{6}$$

对 π^{CC} 求二阶偏导, 均衡价格的二阶条件满足 $\frac{\partial^2 \pi^{CC}}{\partial^2 p} = -2 < 0$, 所以

$\pi^{CC} = \frac{(1+ks - (-3+\lambda)L[1+ks-v])(1+ks + (-1+\lambda)^2 L[1+ks-v])}{(1+ks)^2 (-2+\lambda)^2}$ 是两家软件厂商都选择开发闭源软件时的最优利润。

命题 1: 当 $\pi^{OO} > \pi^{CC}$ 时, 所有软件厂商都会选择开源开发模式, 当 $\pi^{OO} < \pi^{CC}$ 时, 所有软件厂商都会选择闭源开发模式。

$$\begin{aligned} b(\alpha+1) + 2\frac{Lv}{ks+1} &> \frac{(1+ks - (-3+\lambda)L[1+ks-v])(1+ks + (-1+\lambda)^2 L[1+ks-v])}{(1+ks)^2 (-2+\lambda)^2} \\ b(\alpha+1) &> -\frac{2Lv}{1+ks} + \frac{(1+ks - (-3+\lambda)L[1+ks-v])(1+ks + (-1+\lambda)^2 L[1+ks-v])}{(1+ks)^2 (-2+\lambda)^2} \end{aligned} \quad (7)$$

情形 3: 两家软件厂商选择异构开发模式, 即软件厂商 1 选择开发闭源软件, 软件厂商 2 选择开发开源软件。

此时软件厂商 2 将软件产品的价格 p_j 设为 0, 软件厂商 1 的利润函数为:

$$\pi_i^{CO} = p_i(1-p_i) + L\left(1 - \frac{v}{ks+1}\right)(2-p_i + p_i\lambda) \quad (8)$$

$$\pi_j^{CO} = b(\alpha+1)(1+\lambda p_i) + \left(1 - \frac{v}{1+ks}\right)(2+\lambda p_i - p_i)L \quad (9)$$

下面求软件厂商 1 的最优价格, 对 π_i^{CO} 求关于 p_i 的偏导, 令其等于零, 可得软件厂商 1 的最优价格 p_i ,

$$\begin{aligned} \frac{\partial \pi_i^{CO}}{\partial p_i} &= 1 - 2p_i + L\left(1 - \frac{v}{ks+1}\right)(-1+\lambda) = 0 \\ p_i &= \frac{1+ks - L - ksL + Lv + ksL\lambda - Lv\lambda}{2(1+ks)} \end{aligned} \quad (10)$$

将式(10)代入式(8)和式(9)可得软件厂商 1 和 2 的最优利润:

$$\pi_i^{CO} = \frac{(1+ks)^2 + L^2(1+2ks-sk-v)(1+sk-v)(-1+\lambda)^2}{4(1+ks)^2} + \frac{+2L(1+sk)(1+ks-v)(3+\lambda)}{4(1+ks)^2} \quad (11)$$

$$\begin{aligned} \pi_j^{CO} &= \frac{L(1+ks-v)(-L(1+ks-v)(-1+\lambda) + (1+ks)(3+\lambda))}{2(1+ks)(1+ks)} \\ &+ b[1+\alpha] \frac{2+\lambda + L(-1+v)\lambda + ks(2+\lambda-L\lambda)}{2+2ks} \end{aligned} \quad (12)$$

当 $\pi_j^{CO} > \pi^{OO}$ 时:

$$\begin{aligned} \pi_i^{CO} &= \frac{(1+ks)^2 + L^2(1+2ks-sk-v)(1+sk-v)(-1+\lambda)^2 + 2L(1+sk)(1+ks-v)(3+\lambda)}{4(1+ks)^2} \\ &> b(\alpha+1) + 2L\left(1 - \frac{v}{1+ks}\right) \end{aligned}$$

$$b(\alpha+1) < \frac{(1+ks)^2 + L^2(1+ks-v)^2(-1+\lambda)^2 + 2L(1+ks)(1+ks-v)(3+\lambda)}{8(1+ks)^2 \left(L - \frac{Lv}{1+ks} \right)} = T_2(\lambda, s) \quad (13)$$

当 $\pi_j^{CO} > \pi^{CC}$ 时,

$$\begin{aligned} \pi_j^{CO} &= \frac{L(1+ks-v)(-L(1+ks-v)(-1+\lambda) + (1+ks)(3+\lambda))}{2(1+ks)(1+ks)} \\ &\quad + b[1+\alpha] \frac{2+\lambda+L(-1+v)\lambda+ks(2+\lambda-L\lambda)}{2+2ks} \\ &> \frac{(1+ks-(-3+\lambda)L[1+ks-v])(1+ks+(-1+\lambda)^2 L[1+ks-v])}{(1+ks)^2(-2+\lambda)^2} \end{aligned} \quad (14)$$

$$\begin{aligned} b(\alpha+1) &> \frac{(2+2ks) \left(\frac{2(1+ks-L(1+ks-v)(-3+\lambda))(1+ks+L(1+ks-v)(-1+\lambda)^2)}{(-2+\lambda)^2} \right)}{2(1+ks)^2(2+\lambda+L(-1+v)\lambda+ks(2+\lambda-L\lambda))} \\ &\quad - \frac{(2+2ks)L(1+ks-v)(-L(1+ks-v)(-1+\lambda) + (1+ks)(3+\lambda))}{2(1+ks)^2(2+\lambda+L(-1+v)\lambda+ks(2+\lambda-L\lambda))} = T_1(\lambda, s) \end{aligned} \quad (15)$$

结论 1: 在两家软件厂商都开发闭源软件时, 高产品替代率(λ)会使得这些公司的软件产品价格很高, 因为每家软件厂商的产品都相似, 两家软件厂商也没有意愿降价, 此时, 软件厂商的竞争会导致软件厂商信息安全投入水平(s)的提高, 影响消费者的需求, 并进一步增加他们在竞争市场中的利润, 这也与 Gao 的研究结果相似[16]。

命题 2: 两家软件厂商选择开发模式的策略如图 1 所示。存在两种情况如下: (1) 如果 $T_1(\lambda, s) < T_2(\lambda, s)$, 当 $b(\alpha+1) < T_1(\lambda, s)$ 时, 平衡为 (C, C) , 即两家软件都会选择开发闭源软件; 当 $T_1(\lambda, s) < b(\alpha+1) < T_2(\lambda, s)$ 时, 平衡为 (C, O) , 即一家软件厂商会选择开发开源软件, 一家软件厂商选择开发闭源软件; 当 $b(\alpha+1) > T_2(\lambda, s)$ 时, 平衡为 (O, O) , 即两家软件厂商都会选择开发开源软件。(2) 如果 $T_1(\lambda, s) > T_2(\lambda, s)$, 当 $b(\alpha+1) < T_2(\lambda, s)$ 时, 平衡为 (C, C) ; 当 $T_2(\lambda, s) < b(\alpha+1) < T_1(\lambda, s)$ 时, 平衡为 (C, C) 和 (O, O) , 两家

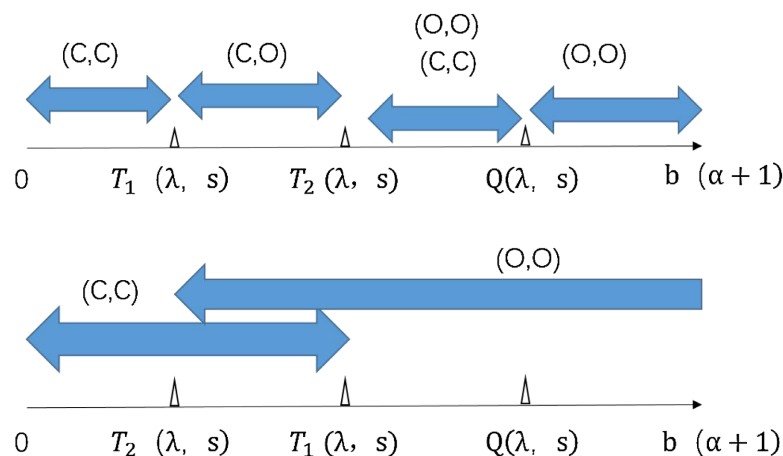


Figure 1. Optimal development strategies of software vendors under symmetric information security environment

图 1. 对称信息安全环境下软件厂商的最优开发策略

软件厂商可以选择都开发闭源软件,也可以选择都开发开源软件;当 $b(\alpha+1)>Q(\lambda,s)$ 时,平衡为 (O,O) 。

命题 3: 当 $\max\{T_1(\lambda,s),T_2(\lambda,s)\}<b(\alpha+1)<Q(\lambda,s)$, 存在 (C,C) 是为帕累托最优下的开发模式。

当 $\max\{T_1(\lambda,s),T_2(\lambda,s)\}<b(\alpha+1)<Q(\lambda,s)$ 时, 选择开发开源软件的回报仍然相对较高, 软件厂商可以选择开源模式, 然而, 开源会导致大量的软件复用和组件依赖, 加剧安全威胁, 由于 $b(\alpha+1)$ 不够高, 软件厂商选择开发开源软件并进行信息安全投入后的收益并不理想, 如前所述, 许多国家和地区都在推广开源的商业模式, 但越来越多的软件供应链安全事件表明, 开源开发模式可能会伤害软件厂商, 除非开源的回报 $b(\alpha+1)$ 的返回超过了 $Q(\lambda,s)$, 在这种情况下, 软件厂商才会选择开发开源软件, 两家软件厂商进行信息安全投入的意愿会较低, 因为即使进行较高的信息安全投入开源的回报也不会提升多少, 但开源的高回报会弥补安全威胁带来的损失。否则即使存在有两种均衡的开发策略 (C,C) 和 (O,O) , 软件厂商也会选择均衡 (C,C) 来开发封闭源的软件产品以尽可能降低安全威胁来保证他们的利益。

结论 2: 在对称的信息安全环境中, 信息安全投入 (s) 相同, 产品替代率 (λ) 趋近于 1 的情况下, 同构开发模式下闭源软件厂商的利润高于异构开发模式下闭源厂商的利润, 这是由于均衡为 (C,O) 时软件厂商选择开源时软件产品的价格都为 0, 吸引了比原有市场上更多的用户, 从而导致了 (C,O) 均衡下选择闭源开发策略的软件厂商利润的降低。

结论 3: 当参数 λ 和 s 都较低时, 开源的回报非常低, 两家软件厂商都不会选择开源。对于两个完全对称的公司, 当异构开发模型 (C,O) 处于均衡状态时, 开发开源软件带来的回报 $b(\alpha+1)$ 不是很低, 而且对软件厂商有些吸引力, 但是两家软件厂商都不可能选择开源, 因为开源会导致大量的安全问题, 选择开发闭源软件更为稳妥。当整体利润相似, s 较高时, 软件厂商更有可能选择开源的开发模式, 因为能带来更多的用户和创新, 此时软件被黑客入侵的概率也较低, 软件厂商更有可能选择开源开发模式。

4. 仿真分析

为了更好地展示对上述命题和结论, 现进行数值模拟仿真, 赋值 $v=0.3$, $k=0.5$, $L=1.5$, $\lambda\in[0,1]$, $s\in[0,10]$, 假定 $s_i=s_j=s$, 观察 λ 的变化对软件厂商利润和开源回报的影响, 具体灵敏度分析如表 2 所示。

Table 2. Influence of software product substitution rate on profit of software manufacturers

表 2. 软件产品替代率对软件厂商利润的影响

λ	π^{CC}	π_i^{CC}	$Q(\lambda,s)$	$T_1(\lambda,s)$	$T_2(\lambda,s)$
0	2.74	2.57	2.29	0.019	0.019
0.2	2.56	2.55	2.11	-0.13	0.0001
0.4	2.45	2.56	2.01	-0.21	0.0139
0.6	2.49	2.61	2.04	-0.14	0.060
0.8	2.78	2.69	2.33	0.21	0.139
1	3.55	2.8	3.1	1.16	0.25

由表 2 可以看出, 当 $\lambda>0.6$ 时两家软件厂商产品替代率变高会导致 (C,C) 和 (C,O) 均衡下软件厂商选择闭源开发策略时利润的提高, 同时也提高了选择开源开发策略的影响因素 - 开源的回报的下限。证明了命题 1。

5. 均衡策略分析

由图 2 和图 3 不难看出, $Q(\lambda,s)>T_1(\lambda,s)$ 和 $T_2(\lambda,s)$ 恒存在, 两个对称软件厂商的异构开发模式可

能处于均衡, 即一家软件厂商选择开发闭源软件, 一家软件厂商选择开发开源软件。

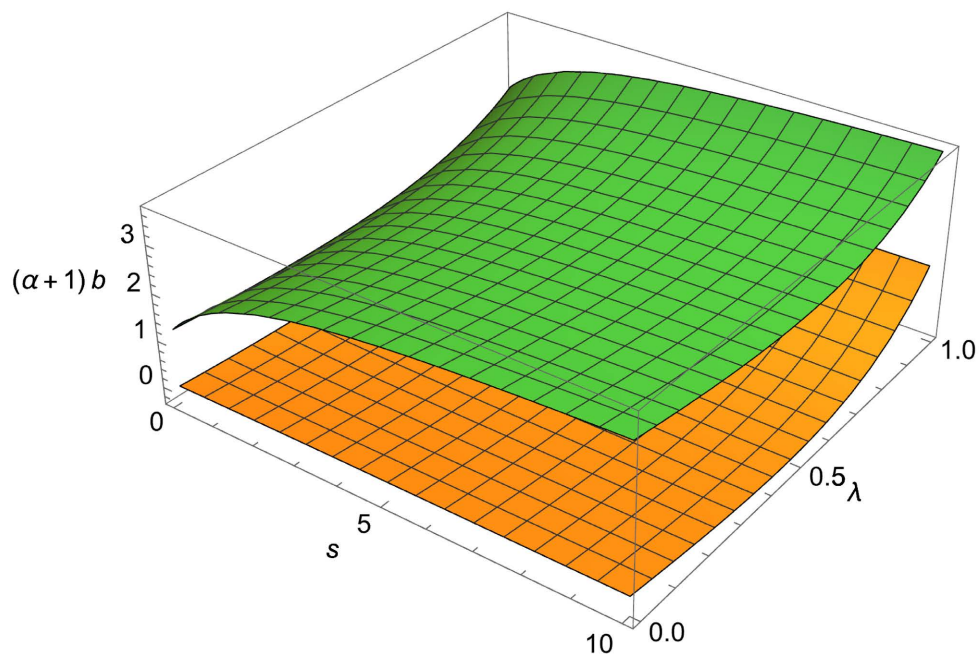


Figure 2. Comparison between $Q(\lambda, s)$ and $T_1(\lambda, s)$

图 2. $Q(\lambda, s)$ 与 $T_1(\lambda, s)$ 比较图

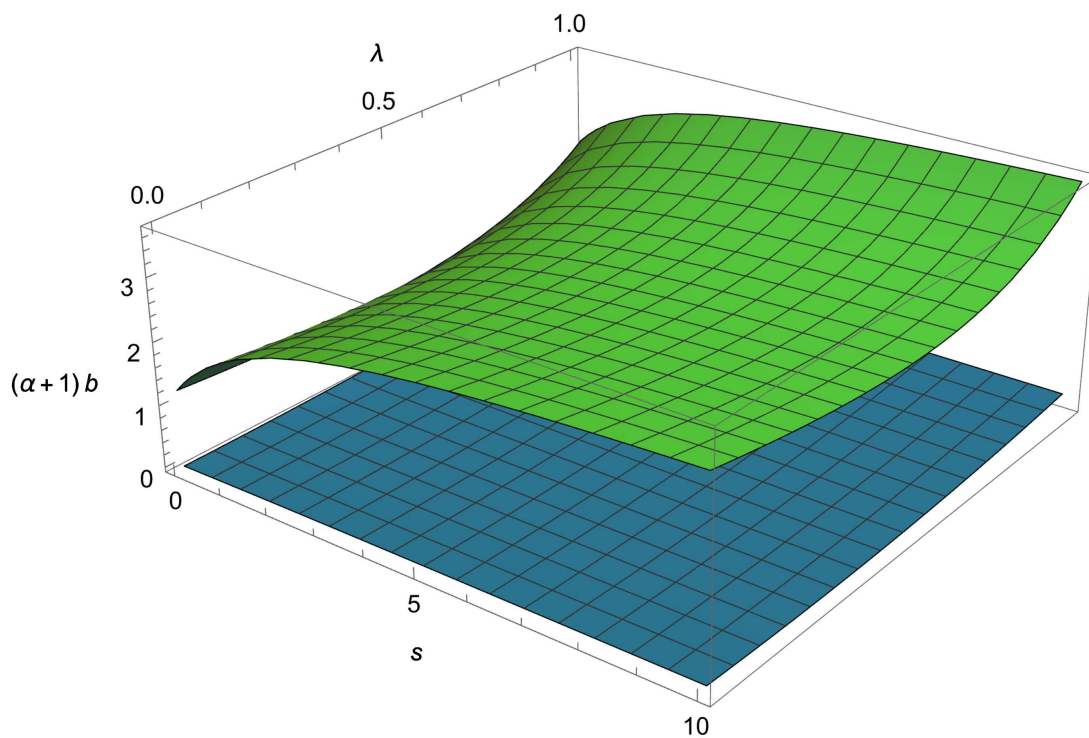


Figure 3. Comparison between $Q(\lambda, s)$ and $T_2(\lambda, s)$

图 3. $Q(\lambda, s)$ 与 $T_2(\lambda, s)$ 比较图

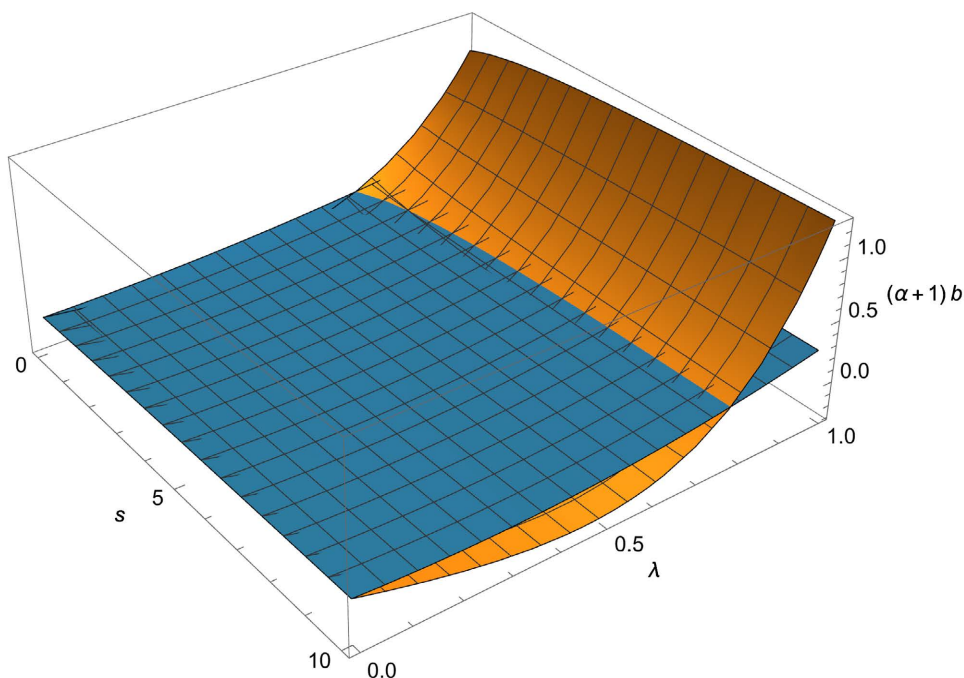


Figure 4. Comparison between $T_1(\lambda, s)$ and $T_2(\lambda, s)$

图 4. $T_1(\lambda, s)$ 和 $T_2(\lambda, s)$ 比较图

由图 4 可以看出, 命题 2 两种情况均存在, 如果 $T_1(\lambda, s) > T_2(\lambda, s)$, 当 $b(\alpha+1) < T_2(\lambda, s)$ 时, 平衡为 (C, C) ; 当 $T_2(\lambda, s) < b(\alpha+1) < T_1(\lambda, s)$ 时, 平衡为 (C, C) 和 (O, O) , 两家软件厂商可以选择都开发闭源软件, 也可以选择都开发开源软件; 当 $b(\alpha+1) > Q(\lambda, s)$ 时, 平衡为 (O, O) 。

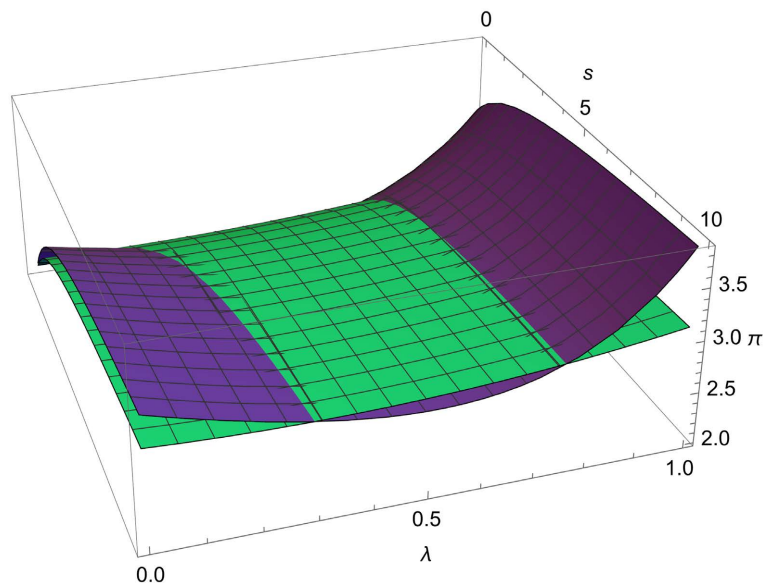


Figure 5. Comparison of profits of software vendors when the development strategy equilibrium is (C, C) and (O, O) respectively

图 5. 开发策略均衡分别为 (C, C) 和 (O, O) 时软件厂商的利润比较

从图 5 可以看出, 在两家软件厂商产品替代率 λ 较高时, (C,C) 均衡下软件厂商开发闭源软件的利润较高, 这是因为在 (C,O) 开发模式下, 选择开发开源软件的软件厂商的用户数量高于闭源软件厂商, 证明了结论 2。这就启示了软件厂商要审视自身技术水平及竞争对手的水平, 在都选择闭源开发模式的情况下考虑通过降价和提升信息安全投入等方法吸引消费者。若竞争对手选择不同的开发策略, 则需要努力提升自身技术水平, 拉开软件产品质量上的差距, 降低 λ , 来获取更高收益。

6. 结语

本文探讨了两家对称竞争的软件企业在选择开源或封闭源开发模式时的考量, 聚焦了软件产品的安全威胁及信息安全投入这一核心议题。通过数学建模与仿真分析, 从信息安全管理角度出发得到了以下管理建议:

(1) 从软件供应链角度出发, 首先要加强对软件供应链各个环节的信息安全相关知识培训, 提高软件供应链整体的安全水平, 降低固有的漏洞脆弱性, 然后建立软件供应链的溯源制度, 在信息安全事件发生后快速定位和处理, 降低黑客成功入侵带来的损失。

(2) 从软件厂商角度出发, 如果选择开发闭源软件, 就要努力提高技术水平, 做出更有差异化和独特功能的软件, 并尽可能压低软件产品售价, 占领更多市场获得更高的利润, 如果选择开发开源软件, 就要通过建立开源社区, 搭建开源项目, 尽可能地利用开源软件的特性, 提高创新幅度吸引更多用户, 提高开源开发模式的回报无论选择哪种开发策略, 软件厂商都要重视信息安全问题, 合理进行信息安全投入, 降低黑客成功入侵软件的概率, 保障软件产品的安全。

7. 展望

(1) 开源软件的特性使得其安全漏洞和威胁可能在不同厂商间传播, 这种“关联风险”为信息安全带来了新的挑战。在未来的研究中, 可以深入探讨开源软件厂商之间在信息安全方面的相互依赖性。

(2) 本文将黑客作为外部客观因素, 未来可以进一步考虑黑客的策略行为, 如针对性攻击, 黑客收益等, 并推广到软件厂商数量更多时的情况。

参考文献

- [1] Bretthauer, D. (2001) Open Source Software in Libraries. *Library Hi Tech News*, **18**. <https://doi.org/10.1108/lhtm.2001.23918eaf.002>
- [2] Bandyopadhyay, T., Jacob, V.S. and Raghunathan, S. (2005) Information Security Investment Strategies in Supply Chain Firms: Inter-Play between Breach Propagation, Shared Information Assets and Chain Topology. *11th Americas Conference on Information Systems, AMCIS 2005*, Omaha, 11-14 August 2005.
- [3] Lakhani, K.R. and von Hippel, E. (2004) How Open Source Software Works: “Free” User-to-User Assistance. In: Herstatt, C. and Sander, J.G., Eds., *Produktentwicklung mit virtuellen Communities*, Gabler Verlag, 303-339. https://doi.org/10.1007/978-3-322-84540-5_13
- [4] Economides, N. and Katsamakas, E. (2006) Two-Sided Competition of Proprietary vs. Open Source Technology Platforms and the Implications for the Software Industry. *Management Science*, **52**, 1057-1071. <https://doi.org/10.1287/mnsc.1060.0549>
- [5] Caulkins, J.P., Feichtinger, G., Grass, D., Hartl, R.F., Kort, P.M. and Seidl, A. (2013) When to Make Proprietary Software Open Source. *Journal of Economic Dynamics and Control*, **37**, 1182-1194. <https://doi.org/10.1016/j.jedc.2013.02.009>
- [6] Haruvy, E., Sethi, S.P. and Zhou, J. (2008) Open Source Development with a Commercial Complementary Product or Service. *Production and Operations Management*, **17**, 29-43. <https://doi.org/10.3401/poms.1070.0004>
- [7] August, T., Shin, H. and Tunca, T.I. (2013) Licensing and Competition for Services in Open Source Software. *Information Systems Research*, **24**, 1068-1086. <https://doi.org/10.1287/isre.2013.0486>
- [8] Sen, R., Verma, A. and Heim, G.R. (2020) Impact of Cyberattacks by Malicious Hackers on the Competition in Software

-
- Markets. *Journal of Management Information Systems*, **37**, 191-216. <https://doi.org/10.1080/07421222.2019.1705511>
- [9] Kumar, V., Gordon, B.R. and Srinivasan, K. (2011) Competitive Strategy for Open Source Software. *Marketing Science*, **30**, 1066-1078. <https://doi.org/10.1287/mksc.1110.0669>
- [10] Casadesus-Masanell, R. and Ghemawat, P. (2006) Dynamic Mixed Duopoly: A Model Motivated by Linux vs. Windows. *Management Science*, **52**, 1072-1084. <https://doi.org/10.1287/mnsc.1060.0548>
- [11] Cheng, H.K., Liu, Y. and Tang, Q. (2011) The Impact of Network Externalities on the Competition between Open Source and Proprietary Software. *Journal of Management Information Systems*, **27**, 201-230. <https://doi.org/10.2753/mis0742-1222270407>
- [12] Kort, P.M. and Zaccour, G. (2011) When Should a Firm Open Its Source Code: A Strategic Analysis. *Production and Operations Management*, **20**, 877-888. <https://doi.org/10.1111/j.1937-5956.2011.01233.x>
- [13] Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research*, **16**, 186-208. <https://doi.org/10.1287/isre.1050.0053>
- [14] Gao, X. (2020) Open Source or Closed Source? A Competitive Analysis with Software Security. *Decision Analysis*, **17**, 56-73. <https://doi.org/10.1287/deca.2019.0390>
- [15] Hausken, K. (2006) Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, **8**, 338-349. <https://doi.org/10.1007/s10796-006-9011-6>
- [16] Gao, X. and Zhong, W. (2015) Economic Incentives in Security Information Sharing: The Effects of Market Structures. *Information Technology and Management*, **17**, 361-377. <https://doi.org/10.1007/s10799-015-0253-1>