Machine Translated by Google

第8章

经济学

信息时代的巨大财富掌握在建立专有架构的公司手中,这些架构被大量固定客户使用。

– 卡尔·夏皮罗和哈尔·瓦里安

这些年来,有两件事我可以肯定:社会对高保证软件的需求不断增长,而市场力量永远不会提供它。

– 博伯特伯爵

法律把偷鹅的男人或女人关起来,却让偷鹅的大坏蛋逍遥法外。

– 传统,17 世纪

8.1 简介

大约在 2000 年左右,我们开始意识到许多安全故障与其说是由于技术错误,不如说是由于错误的激励:如果保护系统的人不是在系统发生故障时遭受痛苦的人,那么您可以预料到麻烦.
事实上,安全机制通常是故意设计来转移责任的,这可能会导致更严重的麻烦。

在成本核算的原始层面上,经济学对工程来说一直很重要;一个好的工程师是在其他人都使用 2000 吨的情况下,可以用 1000 吨的混凝土安全地建造一座桥梁。但是,在具有多个所有者的复杂系统中出现的不当激励使得经济问题对安全工程师来说既重要又微妙。

像互联网这样的真正全球规模的系统产生于数以百万计具有不同利益的独立委托人的行动;我们希望合理的全球

Machine Translated by Google

结果将来自自私的地方行动。我们得到的结果通常是市场均衡,而且通常出奇地稳定。如果不理解这一点,使大型复杂系统更安全或更安全的尝试通常会失败。

在宏观层面上,网络犯罪模式在整个 2010 年代一直非常稳定,尽管技术发生了彻底的变化,手机取代了笔记本电脑,社会转向社交网络,服务器转向云端。

网络不安全有点像空气污染或拥堵,因为将不安全的机器连接到 Internet 的人不会承担其行为的全部后果,而试图正确做事的人却要承受其他人粗心大意的副作用.

一般来说,人们不会改变他们的行为,除非他们有动力去改变。如果他们的行为发生在某种市场中,那么均衡将是在不同方向上推动和拉动的力量相互平衡的地方。但是市场可能会失败;计算机行业从一开始就受到垄断的困扰。其原因现已了解,他们与安全的互动也开始了。

自 2000 年代初以来,安全经济学作为一门学科迅速发展。
它不仅对隐私、错误、垃圾邮件和网络钓鱼等“安全”主题提供了宝贵的见解,而且对系统可靠性的更一般领域也提供了宝贵的见解。例如,程序员和测试人员的最佳平衡是什么? （答案见下文第 8.6.3 节。)它还使我们能够分析许多重要的政策问题 例如网络犯罪的成本和最有效的应对措施。当保护机制被用来限制某人可以对其财产或数据做什么时,竞争政策和消费者权利的问题随之而来 我们需要经济学来分析这些问题。还有公共和私人行动之间的平衡问题:多少保护工作应该留给个人,多少应该由供应商、监管机构或警方承担?每个人都试图推卸责任。

在本章中,我首先描述了我们如何分析经典经济模型中的垄断,信息商品和服务市场有何不同 ,以及网络效应和技术锁定如何使垄断更有可能发生。然后我研究了不对称信息,这是市场力量的另一个来源。其次是博弈论,它使我们能够分析人们是合作还是竞争;和拍卖理论,它让我们了解驱动大部分互联网的广告市场的运作 以及它们是如何失败的。然后,这些基础知识让我们分析信息安全生态系统的关键组成部分,例如软件补丁周期。我们还了解了为什么系统不如应有的可靠:为什么存在太多漏洞以及为什么抓到的网络骗子太少。

8.2 古典经济学

现代经济学是一个涵盖人类行为许多不同方面的广阔领域。到目前为止,它在安全领域得到应用的部分主要来自微观经济学、博弈论和行为经济学。在本节中,我将从直升机之旅开始,了解微观经济学中最相关的思想。我的目标不是提供经济学教程,而是

Machine Translated by Google

了解基本的语言和想法,这样我们就可以继续讨论安全经济学了。

现代学科始于 18 世纪,当时不断增长的贸易改变了世界,导致了工业革命,人们想了解正在发生的事情。1776 年,亚当·斯密的经典著作《国富论》[1788] 提供了初稿:他解释了自由市场中的理性自利如何导致进步。专业化导致生产力的提高,因为人们试图生产其他人认为有价值的东西,以便在竞争激烈的市场中生存。用他的名言来说:“我们的晚餐不是来自屠夫、酿酒师或面包师的仁慈,而是来自他们对自身利益的考虑。”同样的机制从农贸市场或小工厂扩大到国际贸易。

这些想法被 19 世纪的经济学家提炼出来;大卫·里卡多澄清并强化了斯密支持自由贸易的论点,而斯坦·利·杰文斯、莱恩·瓦尔拉斯和卡尔·门格尔则建立了详细的供需模型。 Jevons 和 Menger 的见解之一是,在竞争市场处于均衡状态时,商品的价格是生产的边际成本。当 1870 年煤炭价格为每吨 9 先令时,这并不意味着每个矿井都以这个价格开采煤炭,只是意味着边际生产者 那些勉强维持经营的人 可以以那个价格出售。如果价格下跌,这些矿山就会关闭;如果它上升,甚至更多的边际地雷将被打开。这就是供应对需求变化的反应。 (这也让我们深入了解为什么现在有这么多在线服务是免费的;由于复制信息的边际成本几乎为零,许多在线企业无法出售它而不得不通过其他方式赚钱,例如来自广告。但我们已经超前了。)

到本世纪末,阿尔弗雷德·马歇尔已经将商品、劳动力和资本市场的供求模型组合成一个包罗万象的“经典”模型,在该模型中,在均衡状态下,所有超额利润都将被竞争掉,经济将是有效地运作。到 1948 年,Kenneth Arrow 和 G´erard Debreu 通过证明市场在特定条件下产生有效结果,包括买家和卖家拥有完整的财产权,他们拥有完整的信息,他们是理性的,交易成本可以忽略不计。

对经济学的大部分兴趣来自于这样的情况
不满足其中一个或多个条件。例如,假设交易具有可用产权未捕获的副作用。

经济学家称这些为外部性,它们可以是正的也可以是负的。
正外部性的一个例子是科学研究,一旦发表,每个人都可以从中受益。结果,研究人员无法获得他们工作的全部收益,而我们得到的研究比理想情况要少(经济学家估计我们只进行了理想研究量的四分之一)。负外部性的一个例子是环境污染;如果我烧煤火,我会得到为我的房子供暖的积极影响,但我的邻居会受到气味和灰烬的负面影响,而每个人都会分享二氧化碳排放量增加的负面影响。

Machine Translated by Google

外部性和市场失灵的其他原因对计算机行业,尤其是对安全人员来说,具有真正的重要性,因为它们塑造了我们正在努力解决的许多问题,从行业垄断到不安全的软件。如果一个参与者有足够的权力收取高于市场清算价格的费用,或者没有人有能力解决一个常见问题,那么单靠市场可能无法解决问题。战略是关于获得权力,或防止其他人对你拥有权力;因此,最基本的商业策略是获得市场支配力以获取额外利润,同时尽可能将您的活动成本分摊给其他人。现在让我们更详细地探讨一下。

8.2.1 垄断

作为介绍,让我们考虑一个垄断的教科书案例。假设我们在大学城有一个公寓市场,学生有不同的收入 。我们可能有一个有钱的学生能够每月支付 4000 美元,可能有 300 人愿意每月至少支付 2000 美元,并且(给我们一个整数)至少有 1000 人准备每月至少支付 1000 美元。这给了我们下面图 8.1 所示的需求曲线。

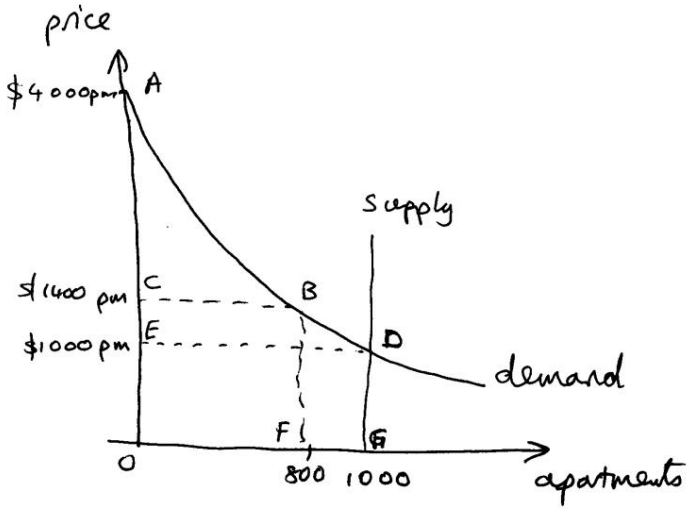

图 8.1:公寓市场

因此,如果有 1000 套公寓被许多相互竞争的房东出租,则市场出清价格将位于需求曲线与垂直供给曲线的交点处,即 1000 美元。但是假设市场被操纵 比如房东建立了一个卡特尔,或者大学让学生通过一个有关联的机构租房。一个垄断地主检查需求曲线,发现如果他只出租 800 套公寓,他每个月可以得到 1400 美元。现在 800 乘以 1400 美元等于每月 1,120,000 美元,这比他从 1000 美元的市场价格每月赚取的百万美元还多。 (经济学家

Machine Translated by Google

会说他的“收益箱”是箱子 CBFO 而不是图 8.1 中的 EDGO。)所以他人为地设定了一个高价,200 套公寓仍然空着。

这显然是低效的,意大利经济学家维尔弗雷多帕累托发明了一种巧妙的方法来将其形式化。帕累托改进是使某些人变得更好 o 而不会使其他人变得更糟 o 的任何变化,如果没有任何可用的帕累托改进,则分配是帕累托有效的。在这里,分配效率不高,因为垄断者可以以较低的价格将一套空置的公寓出租给任何人,从而使他和他们都变得更好 o 。现在帕累托效率是一个相当弱的标准;完美的共产主义(每个人获得相同的收入)和完美的独裁(国王得到很多)都是帕累托效率的。在这两种情况下,你都不能让任何人变得更好 o 而不让其他人变得更糟 o !然而,即使在这种非常弱的意义上,这里描述的简单垄断也不是有效的。

那么垄断者能做什么呢?有一种可能性 如果他可以向每个人收取不同的价格 ,那么他就可以将每个学生的租金准确地设定在他们准备支付的水平。我们称这样的地主为价格歧视垄断者;他向富有的学生收取正好 4000 美元的费用,以此类推,直到他向第 1000 个学生收取正好 1000 美元的费用。同样的学生得到了和以前一样的公寓,但几乎所有的学生都更差 o 。这位富有的学生损失了 3000 美元,这是他准备支付但以前不必支付的钱;经济学家称他存下的这笔钱为盈余。歧视性垄断者设法榨取所有消费者剩余。

自古以来,商人就试图实行价格歧视。伊斯坦布尔的地毯销售商希望您能讨价还价,他正在玩这个游戏,一家航空公司出售头等舱、商务舱和牛排座位也是如此。公司向人们收取不同价格的程度取决于许多因素,主要是它们的市场力量和信息不对称。市场势力是衡量一个商人接近垄断者的程度;在垄断下,商人是价格制定者,而在完全竞争下,他是价格接受者,必须接受市场确定的任何价格。商家自然会尽量避免这种情况。信息不对称可以通过多种方式帮助他们。地毯卖家比路过的游客了解更多有关当地地毯价格的信息,而且游客没有时间在十家不同的商店讨价还价。因此商家可能更愿意讨价还价而不是显示固定价格。航空公司略有不同不同。多亏了比价网站,它的乘客可以很好地了解基本价格,但如果它确实打折来填满座位,它可能能够使用来自广告生态系统的信息来定位其报价。它还可以通过提供偶尔的升级来创建自己的忠诚度生态系统。技术往往使公司更像航空公司,而不像小地毯店;信息不对称与其说是你是否了解平均价格,不如说是系统对你的了解以及它如何锁定你。

垄断可能很复杂。典型的垄断者,比如我们例子中的地主或卡特尔,可能会简单地推高每个人的价格,导致消费者剩余的明显损失。美国的竞争法寻找这种福利损失,这种情况经常发生在卡特尔实施价格歧视的地方。

在 19 世纪后期,铁路运营商向不同的客户收取不同的运费,这取决于他们的利润率、货物的易腐烂程度和其他因素 基本上,根据

Machine Translated by Google

到他们的支付能力。这导致了大规模的不满和铁路监管。
同样,电信公司过去疯狂地实行价格歧视； SMS 过去比语音成本高得多,而语音成本又比数据高得多,尤其是远距离通信。
这导致了 Skype 和 WhatsApp 等服务的出现,这些服务使用数据服务来提供更便宜的通话和消息传递,也导致了一些国家的网络中立监管。这仍然是一个争斗空间,特朗普总统在 FCC 任命的人推翻了许多以前的网络中立裁决。

然而,许多拥有真正市场力量的公司,如谷歌和 Facebook,将他们的产品免费提供给大多数用户,而其他公司,如亚马逊（和沃尔玛）,则为他们的客户降价。这挑战了经济学家和律师过去思考垄断的传统基础,至少在美国是这样。然而,科技领域的垄断力量是毋庸置疑的。我们可能已经从 1970 年代的一个主导者（IBM)发展到 1990 年代的两个（微软和英特尔）,再到现在的少数几个（谷歌、Facebook、亚马逊、微软,也许还有 Netflix）,但每个人都在其领域占据主导地位;尽管 Arm 设法与英特尔竞争,但自 2009 年 Bing（其市场份额正在下滑)以来就没有新的搜索初创公司,而且自 2011 年 Instagram（现为 Facebook 所有)以来也没有大型社交网络。因此,对创新产生了负面影响,而我们如何应对创新的问题正成为一个热门的政治话题。欧盟已多次因违反竞争法对科技专业人士处以罚款。

要了解发生了什么,我们需要更深入地研究信息是如何发生的
信息垄断工作。

8.3 信息经济学

信息和通信行业在许多方面与传统制造业不同,其中最引人注目的是这些市场几代人以来一直非常集中。甚至在计算机出现之前,报纸往往是垄断的,除了在大城市。

铁路和运河之前也发生了同样的事情。当电气制表设备在 19 世纪末出现时,它由 NCR 主导,直到从 NCR 的曼哈顿销售办公室分拆出来的一家名为 IBM 的公司接手。 IBM 在 1960 和 70 年代主导了计算机行业,然后微软出现并在 90 年代占据了领先地位。从那时起,谷歌和 Facebook 开始主宰广告,苹果和谷歌销售手机操作系统,ARM 和英特尔销售 CPU,而许多其他公司主宰着他们自己的专业。为什么会这样?

8.3.1 为什么信息市场不同 erer

回想一下,在竞争均衡中,商品的价格应该是其边际生产成本。但是对于几乎为零的信息!这就是为什么网上有那么多免费学习的原因;零是它的公平价格。如果两个或更多的供应商竞争提供一个操作系统、地图或百科全书,而他们可以免费复制,那么他们将继续无限制地降价。以百科全书为例； 《大英百科全书》过去 32 册售价 1,600 美元;然后微软以 49.95 美元的价格推出了 Encarta,迫使

Machine Translated by Google

制作廉价 CD 版的大英百科全书;现在我们有免费的维基百科 [1718]。一家又一家公司不得不转向一种商业模式,在这种模式下,商品免费赠送,钱来自广告或某个平行市场。并且很难与免费的服务竞争,或者非常便宜以致于很难收回开始所需的资本投资。因此,固定成本高而边际成本低的其他行业往往会集中起来 例如报纸、航空公司和酒店。

其次,通常存在网络外部性,即网络价值的增长超过用户数量的线性增长。电话和电子邮件等网络需要一些时间才能开始,因为一开始只有少数其他爱好者可以交谈,但一旦他们在每个社会群体中超过一定的门槛,每个人都需要加入,网络迅速成为主要溪流。同样的事情在 2000 年代中期再次发生在社交媒体上;最初有 40-50 家初创公司在做社交网络,但一旦 Facebook 开始领先,突然间所有年轻人都必须在那里,因为那是你所有朋友的地方,如果你不在那里,你就会错过机会聚会请柬。这种正反馈是建立网络效应的机制之一。它还可以在汇集两类用户的双边市场中运作。例如,当地方报纸在 19 世纪开始运作时,企业希望在拥有大量读者的报纸上做广告,而读者则希望报纸上有很多小广告,这样他们就可以找到资料 。因此,一旦一份报纸开始运作,它往往会成为当地的垄断企业;竞争对手很难打进来。同样的事情发生在铁路允许农业产业化的时候;Cargill 和 Armour 等强大的公司拥有谷物升降机和肉类包装机,一方面与小农打交道,另一方面与零售业打交道。我们在 1960 年代看到了同样的模式,当时 IBM 大型机主导着计算:公司过去常常为 IBM 开发软件,因为它们可以接触到更多的用户,而许多用户购买 IBM 是因为它有更多的软件。当 PC 出现时,微软出于同样的原因击败了苹果;现在手机正在取代笔记本电脑,我们在 Android 和 iPhone 上看到了类似的模式。另一个赢家是 1990 年代后期的 eBay:大多数想要拍卖物品的人都希望使用最大的拍卖,因为它会吸引更多的竞标者。网络效应也可能是负面的;一旦像 Myspace 这样的网站开始失去客户,负面反馈就会把损失变成溃败。

第三,领先的信息化服务公司享有各种供应方规模经济,从获得无与伦比的用户数据量到运行大量 A/B 测试以了解用户偏好和优化系统性能的能力。这些使先行者能够在服务提供方面创造竞争优势,而在位者则能够捍卫竞争优势。

第四,通常由于互操作性或缺乏互操作性而导致锁定。
一旦软件公司承诺为其产品使用 Windows 或 Oracle 等平台,更改的成本可能很高。这包括技术和人为因素,后者通常占主导地位;更换工具比重新培训程序员更便宜。客户也是如此:如果他们不仅要购买新软件和转换文件,还要重新培训他们的员工,则很难完成销售。这些转换成本阻碍了迁移。互操作性很重要的早期平台包括电话系统、

Machine Translated by Google

电报、主电源甚至铁路。

这四个特征 低边际成本、网络外部性、供应方规模经济和技术锁定 可以导致行业中的主导企业;结合起来,他们更有可能这样做。如果用户希望与其他用户（以及软件等互补产品的供应商)兼容,那么他们自然会从他们希望赢得最大市场份额的供应商处购买。

8.3.2 锁定的价值

由于 Carl Shapiro 和 Hal Varian,有一个有趣的结果:软件公司的价值是其所有客户的总锁定（由于技术和网络效应)[1718]。要了解这可能如何运作,请考虑一家拥有 100 名员工的公司,每名员工都使用 Oce,为此它支付了每份 150 美元。它可以通过转向 LibreOce 等免费程序来节省这 15,000 美元,因此如果安装该产品、重新培训其员工、转换文件等的成本 换句话说,总转换成本 低于 15,000 美元,它会转变。但如果转换成本超过 15,000 美元,那么微软就会提高价格。

作为锁定、定价和价值之间联系的一个例子,考虑一下十年来价格是如何变化的。在本书的第二版中,这个例子的 Oce 成本是 500 美元;从那时起,与 Oce 一样工作的基于云的服务（例如 Google Docs)降低了转换成本 因此微软不得不大幅削减价格。当我在 2019 年开始编写这个版本时,我看到独立的 Oce 以 59.99 美元到 164 英镑的价格出售。自 2013 年以来,微软的回应一直是试图将其客户转移到在线订阅服务 (Oce365),根据他们选择的选项和谈判能力,大学每个席位要花费几十英镑,而谷歌也在努力转移组织从他们的免费服务转向成本大致相同的付费 G Suite 版本。每年为在线服务收取 30 美元的费用比为客户可能使用五年甚至七年的程序收取 60 美元的费用更好。当我在 2020 年修订本章时,我发现我现在可以获得“终身密钥”,其成本约为去年独立产品的两倍。有一种新的锁定形式,即云提供商现在负责管理您的所有数据。

锁定解释了为什么在标准战争和反托拉斯诉讼中付出了如此多的努力。它还有助于解释向云迁移的原因（尽管削减成本是一个更大的驱动因素）。这也是为什么这么多安全机制旨在控制兼容性的原因。在这种情况下,可能的攻击者不是恶意的外部人员,而是设备的所有者,或者试图通过生产兼容产品来挑战现有企业的新公司。这不仅会损害竞争,还会损害创新。过于严格地锁定事物也可能对企业不利,因为创新通常是渐进的,当新公司为他们找到杀手级应用时,产品就会成功 [903]。例如,PC 是 IBM 设计的一种运行电子表格的机器;如果他们只将其锁定到这个应用程序,那么就会失去一个巨大的机会。事实上,IBM PC 比 Apple Mac 更开放这一事实是它成为主导桌面平台的一个因素。 （微软和英特尔后来窃取了 IBM 的

Machine Translated by Google

午餐是一个单独的问题。）

因此,许多国家/地区的法律赋予公司对其竞争对手的产品进行逆向工程以实现兼容性的权利 [1647]。现任者试图建立生态系统,在这个生态系统中,他们的产品比他们的竞争对手更好地协同工作。他们使用云服务和密码学等数字组件来锁定他们的产品,这样即使竞争对手拥有尝试对这些产品进行逆向工程的合法权利,他们也不一定总能在实践中取得成功。现任者还利用他们的生态系统来了解他们的客户,以便更好地锁定他们;而各种数字机制将控制售后市场并强制实施计划内的报废。我将在下面的第 8.6.4 节中更详细地讨论这些更复杂的生态系统策略。

8.3.3 信息不对称

除了垄断和公共物品之外,市场可能失灵的另一种方式是,当一些委托人比其他人知道得更多,或者知道得稍微早一些,或者可以更便宜地发现它。我们讨论了老式地毯商如何比在他店里购物的游客具有信息优势;但是 1970 年一篇关于“柠檬市场”[34] 的著名论文终止了对不对称信息的正式研究,乔治·阿克洛夫 (George Akerlof) 也因此获得了诺贝尔奖。它提出了以下简单而深刻的见解:假设一个城镇有 100 辆二手车待售:50 辆保养良好的汽车每辆价值 2000 美元,50 辆“柠檬”价值 1000 美元。卖家知道哪个是哪个,但买家不知道。二手车的市场价格是多少?

你可能会认为 1500 美元;但按照这个价格,将没有好车出售。所以市场价格将接近1000美元。这就是为什么,如果你买了一辆新车,当你把它从经销商处开走时,价格可能会下降 20%。信息不对称也是劣质安全产品主导某些市场的原因。当用户分不清好坏的时候,还不如买最便宜的。 1990 年代防病毒软件市场兴起时,人们会购买 10 美元的产品,而不是 20 美元的产品。 （现在购买 AV 的理由要少得多,因为恶意软件编写者在发布代码之前会针对所有可用产品测试他们的代码 您应该专注于修补系统。

人们仍然大量购买 AV 是信息不对称的另一个例子。）

可以进一步区分隐藏信息和隐藏动作。例如,沃尔沃以制造安全汽车帮助乘客在事故中幸存而著称,但沃尔沃司机发生事故的次数更多。这是因为知道自己是坏司机的人会购买沃尔沃汽车,这样他们被撞死的可能性就会降低,还是因为沃尔沃汽车的人认为他们更安全并且开得更快?

第一个是隐藏信息案例,也称为逆向选择,第二个是隐藏行为案例,也称为道德风险。这两种效果在安全方面都很重要,并且在特定情况下两者都可以结合使用。 （就司机而言,人们会调整他们的驾驶行为,以将他们的风险敞口保持在他们感到舒服的水平。这也解释了为什么强制性安全带法律往往不能挽救整体生命,只是将死亡人数从车内乘客转移到行人和骑自行车的人 [19]。）

信息不对称解释了现实世界中的许多市场失灵,

Machine Translated by Google

从二手车市场的低价到网络风险保险的高价（知道自己偷工减料的公司可能会购买更多，从而使谨慎的人付出高昂的代价）。在信息安全领域，大多数利益相关者都不愿意说实话，这让情况变得更糟；警察和情报机构以及安全供应商试图大谈这些威胁，而软件供应商、电子商务网站和银行则淡化它们 [111]。

8.3.4 公共物品

正外部性的一个有趣案例是，无论他们是否想要，每个人都获得相同数量的某种商品。典型的例子是空气质量、国防和科学研究。经济学家称这些为公共物品，正式的定义是这些物品是非竞争性的（我用它们并不意味着你用得少）和非排他性的（没有实际的方法可以阻止人们消费它们）。不协调的市场通常无法提供社会最优数量的公共物品。

公共物品可以由政府直接提供，如国防，或通过使用专利和版权法等间接机制，通过给予他们暂时的垄断来鼓励人们生产发明、书籍和音乐。通常，公共物品是由公共和私人行动的某种组合提供的；科学研究是在大学里进行的，这些大学获得一些公共补贴，从学生学费中赚取一些收入，并从工业界获得一些研究合同（可能获得有用发明的专利）。

安全的许多方面都是公共物品。我家屋顶上没有高射炮；防空威胁来自少数行为者，最有效的处理方式是政府行动。那么互联网安全呢？当然有很强的外部性；将不安全的机器连接到 Internet 的人最终会将成本倾销给其他人，因为它们使不良行为者能够建立僵尸网络。自我保护具有公共利益的某些方面，而保险则更多是私人利益。那我们应该怎么办呢？

答案可能取决于我们关注的不良行为者是集中的还是分散的。在第 2.3 节的网络犯罪快速调查中，我们注意到随着恶意软件编写者、垃圾邮件发送者和其他人变得商业化，许多威胁已经整合。到 2007 年，严重的垃圾邮件发送者的数量已经减少到少数，到 2019 年，拒绝服务 (DoS) 攻击也是如此：似乎有一个占主导地位的 DoS 雇佣提供商。

这表明一种更集中的防御策略，即找到坏人并将他们关进监狱。

一些人设想政府会做出更温和的回应，对发现漏洞的研究人员给予奖励，对软件中包含漏洞的公司处以罚款。在某种程度上，这已经通过漏洞赏金计划和漏洞市场发生，而无需政府干预。

但愤世嫉俗者会指出，在现实生活中，漏洞被出售给网络武器制造商，网络武器制造商再将其出售给政府，政府随后将其储存起来 而工业界则为附带损害买单，就像 NotPetya 一样。

那么空气污染或防空是正确的类比吗？这让我们进入游戏

Machine Translated by Google

理论。

8.4 博弈论

博弈论具有现代经济学的一些最基本的见解。
这是关于我们什么时候合作,什么时候战斗。

如果您找不到或无法自己制作,实际上只有两种方法可以获得您想要的东西。您要么制作有用的东西并进行交易;要么或者你用武力、投票箱或其他什么的方式拿走你需要的东西。人类和动物每天都会在各种层面上做出合作与冲突之间的选择。

我们可以用来研究和分析它们的主要工具是博弈论 研究独立决策者之间的合作与冲突问题。博弈论为经济学家、生物学家和政治学家以及计算机科学家提供了一种通用语言,并且是建立跨学科协作的有用工具。我们对策略游戏很感兴趣,我们试图通过抽象掉大部分细节来触及决策的核心。例如,考虑一下学校操场上的“配对硬币”游戏:爱丽丝和鲍勃同时抛硬币,如果硬币不同,爱丽丝得到鲍勃的硬币,如果硬币相同,鲍勃得到爱丽丝的硬币。

我将按照图 7.2 中的方式编写:

		鲍勃	
		H T	
爱丽丝	高	-1,1 1,-1	
	T	1,-1 -1,1	

图 7.2 – 匹配硬币

表中的每个条目首先显示 Alice 的结果,然后显示 Bob 的结果。因此,如果硬币掉落 (H,H),Alice 将损失一分钱,而 Bob 将获得一分钱。这是一个零和游戏的例子:Alice 的收益是 Bob 的损失。

通常我们可以通过写出这样的 payo 矩阵来快速解决游戏。
这是一个示例(图 7.3):

		鲍勃	
		左右	
爱丽丝	前	1,2 0,1	
	底部	2,1 1,0	

图 7.3 – 占优策略均衡

在博弈论中,策略只是一种采用博弈状态和

Machine Translated by Google

输出一个 move1。在这个游戏中,无论 Bob 玩什么,Alice 都更喜欢玩“Bottom”;并且无论爱丽丝玩什么,鲍勃最好玩“左”。每个玩家都有一个占优策略 一个最优选择,不管对方做什么。所以 Alice 的策略应该是一个不变的“Bottom”,而 Bob 的策略应该是一个不变的“Left”。我们称之为占优策略均衡。

另一个例子如图 7.4 所示:

图 7.4 – 纳什均衡

在这里,每个玩家的最佳策略取决于他们认为其他玩家会做什么。当爱丽丝的选择在给定鲍勃的情况下是最优的时,我们说两种策略处于纳什均衡,反之亦然。这里有两个对称的纳什均衡,分别在左上角和右下角。您可以将它们视为局部最优,而占优策略均衡是全局最优。

8.4.1 囚徒困境

我们现在准备研究一个适用于许多情况的著名问题,从国际贸易谈判到狩猎动物之间的合作,再到构成互联网的自治系统是否有效合作以保护其基础设施。兰德公司的科学家于 1950 年在美国和苏联国防开支的背景下首次对其进行了研究;兰德受雇思考核战争中的可能策略。但是他们使用以下简单示例来展示它。

两名囚犯因涉嫌策划抢劫银行而被捕。警察分别采访他们并告诉他们每个人:“如果你们都不承认,你们将因未经许可携带隐蔽枪支而每人被判一年。”如果你们中只有一个人供认,他就会获释,而另一个人将因串谋抢劫而被判 6 年徒刑。如果你们都坦白,你们每人将被判三年。”

囚犯该怎么办?这是他们的 payo 矩阵:

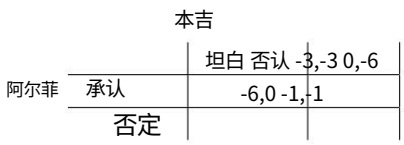

图 7.5 – 囚徒困境

当 Alfie 看着这张桌子时,他会做出如下推理:“如果 Benjy 要坦白,那么我也应该坦白,因为那样我会被判 3 年而不是 6 年;如果他要去1在商业和政治中,战略是通过一系列行动获得权力的手段,例如垄断权力或军

事优势;博弈论的含义是一个稍微简化的版本,使问题更容易处理。

Machine Translated by Google

否认那么我仍然应该承认,因为我会走路而不是做一年”。 Benjy 也会有类似的推理。两人坦白,各判三年。这不仅仅是纳什均衡;这是一个占优策略均衡。无论对方做了什么,每个囚犯都应该坦白。

但是坚持下去,你说,如果他们同意保持沉默,那么他们每人将获得一年的时间,这对他们来说是更好的结果!事实上策略 (deny,deny) 是帕累托有效的,而占优策略均衡则不是。 （这就是拥有“帕累托效率”和“主导策略均衡”等概念比仅仅争论“最佳”更有用的原因之一。）

那么解决方案是什么?好吧,只要游戏只玩一次,而且这是镇上唯一的游戏,就没有解决方案。两名囚犯都会认罪并获刑三年。

您可能认为这很公平,因为这对他们有利。然而,囚徒困境可以用来模拟我们决定是否合作的各种互动:国际贸易、核军备控制、渔业保护、减少二氧化碳排放,以及政治话语的文明程度。甚至肥胖和成瘾等自我控制问题也可以被视为与我们未来的自己合作的失败。在这些应用程序中,我们确实需要合作才能获得好的结果,但单发游戏的结构方式却让它们很难实现。只有当我们能够以某种方式改变游戏本身时,我们才能改变这一点。

有很多可能性:可以有各种各样的法律,从国际贸易条约到黑帮的 omert`a。在实践中,囚徒困境博弈是通过改变规则或环境来改变的,从而将其转变为另一种均衡更有效的博弈。

8.4.2 重复和进化博弈

假设游戏重复进行 假设阿尔菲和本吉是职业罪犯,他们希望一次又一次地与对方打交道。那么当然可以激励他们合作。至少有两种建模方法。

在 1970 年代,Bob Axelrod 开始思考人们如何玩多轮囚徒困境。他设立了一系列竞赛,人们可以提交程序,这些程序在锦标赛中相互反复对弈。他发现总体上最好的策略之一是以牙还牙,这就是你在第一轮合作,在随后的每一轮你对你的对手做他或她在上一轮所做的事情 [147]。人们开始意识到战略演变可以解释很多事情。例如,在存在噪音的情况下,每当一个玩家的合作行为被另一个玩家误读为背叛时,玩家往往会陷入（缺陷,缺陷）。所以在这种情况下,时不时地“原谅”其他玩家是有帮助的。

John Maynard Smith 和 George Price [1251] 开辟了一种平行的方法。他们考虑了如果你有侵略性和温顺的个体混合种群,“鹰派”和“鸽派”,以及鸽派合作的行为,会发生什么;鹰从鸽子那里取食;和鹰派打架,有

Machine Translated by Google

死亡。假设每次互动时食物的价值为 v,而鹰派战斗中每次遭遇的死亡风险为 c。然后 payo 矩阵如图 7.6 所示：

	鹰鸽	
鹰	风险投资 / 2、 风险投资 / 2个	v,0
鸽子	0, v	v / 2,2个 v

图 7.6 – 鹰鸽博弈

在这里,如果 v>c,整个种群都会变成鹰派,因为这是占优策略,但如果 c>v（战斗成本太高）,则存在一个均衡,其中一只鸟是鹰派的概率 p 设置了鹰派payo与鸽子payo相等,即

$$p\frac{\text{风险投资}}{2\text{个}} + (1-p)v = (1-p)\,2\qquad\frac{v}{}$$

由 p = v/c 求解。换句话说,你可以在种群中同时存在攻击性和温顺的个体,攻击性个体的比例将是攻击成本的函数;战斗越危险,好斗的人就越少。当然,成本会随着时间的推移而变化,从进化的角度来看,多样性可能是一件好事,因为当战争爆发时,一个拥有一些硬汉的社会可能会处于优势地位。但一个社会要达到平衡需要几代人的时间。也许我们目前的侵略发生率很高,反映了前国家社会的状况。事实上,人类学家认为部落战争曾经在这样的社会中普遍存在;考古记录表明,在国家出现之前,大约四分之一到三分之一的男人和男孩死于他杀 [1132]。我们只是在文明社会中生活的时间还不够长,无法赶上进化。

这些见解,连同 Bob Axelrod 的模拟方法,使许多人从道德哲学家到对进化博弈论感兴趣的动物行为学生。他们提供了关于合作如何演变的进一步见解。事实证明,许多灵长类动物都有一种内在的公平感,会惩罚被视为作弊的个体 报复的本能是强化社会性的一种机制。公平可以在不同的层面以多种不同的方式运作。例如,如果鸽派能够相互识别并优先互动,那么鸽派可以比鹰派取得更好的成绩,从而为一些社会运动甚至某些宗教如何建立自己提供了一个模型 [1784]。由 eBay 率先推出、现在被 Uber 和 AirBnB 等公司使用的在线声誉系统执行类似的功能:它们通过将交互纳入迭代游戏来帮助鸽派避免鹰派。

当然,以牙还牙背后的基本理念可以追溯到很久以前。旧约有“以眼还眼”,新约有“己所不欲,勿施于人” 后者的表述更容错 它的版本可以在亚里士多德那里找到,在孔子等何处。最近,托马斯·霍布斯 (Thomas Hobbes) 在 17 世纪使用了类似的论点来论证一个国家不需要君权神授

Machine Translated by Google

存在,为十八世纪的革命、共和国和宪法铺平了道路。

自 9/11 以来,人们使用鹰鸽游戏来模拟基要主义者在压力大时接管宗教话语的能力。我的同事和我已经使用进化游戏来模拟叛乱分子如何将自己组织成细胞 [1373]。进化博弈还解释了为什么即使没有秘密交易,类似卡特尔的行为也会出现在行业中。

例如,英国的互联网服务涉及提供本地环路的受监管垄断,以及向家庭销售互联网服务的竞争性零售公司。如果本地环路每月花费 ISP 6 英镑,那么 ISP 为何都收取大约 35 英镑的费用?好吧,如果有人以低于其他人的价格出售,他们都会通过降低自己的价格来报复,惩罚叛逃者。如果有 3 家航空公司经营一条有利可图的航线,而其中一家降低价格以争夺数量,这与您看到的行为完全相同;其他人通常会通过更大幅度地降价来惩罚它并使该路线无利可图。

正如航空公司提供各种优惠、航空里程等来迷惑客户一样,电信提供商也提供他们自己的混淆定价。

相似的结构导致相似的行为。如果公司高管没有真正坐下来同意固定价格（这将是非法的）,这两个行业都可能发生默契勾结。随着定价变得更加算法化,律师和经济学家可能需要了解更多的计算机科学;计算机科学家需要了解博弈论和拍卖论等经济分析工具。

8.5 拍卖理论

拍卖理论对于理解 Internet 服务的工作原理以及可能出现的问题至关重要。许多在线活动的资金来自谷歌和 Facebook 等公司运营的广告拍卖,许多电子商务网站也以拍卖形式运营。

拍卖已经存在了几千年,是出售牲畜、艺术品、矿产权、债券等的标准方式;从公司收购到房屋销售的许多其他交易也都是真正的拍卖。它们是发现独特商品价格的基本方法。游戏玩法、信息不对称、作弊等问题很多
还有一些可靠的理论可以指导

我们。

考虑以下五种传统的拍卖类型。

1. 在英式或升价拍卖中,拍卖师以底价开始,然后提高价格,直到只剩下一名投标人。这是用来出售艺术品和古董的。

2. 在荷兰式或降价拍卖中,拍卖师以高价开始并逐渐降低价格,直到有人出价。这是用来卖花的。

3、首价密封投标拍卖中,每位投标人限投标一次。投标结束后,所有投标都被打开,最高出价获胜。

Machine Translated by Google

这已被用于拍卖电视转播权;它也用于政府合同,以最低出价获胜。

4. 在第二价格密封投标拍卖或 Vickrey 拍卖中,我们也进行密封投标,最高出价者获胜,但该出价者支付第二高出价的价格。这在 eBay 很常见,也是在线广告拍卖的运作方式;它演变为出售稀有邮票,尽管已知最早的用途是诗人歌德在 18 世纪将手稿出售给出版商。

5. 在全额竞拍中,每一轮竞拍者都支付,直到只有一个竞拍者退出。这是几家科技初创公司之间的战争、诉讼或赢家通吃的市场竞赛模式。它还用于慈善筹款。

第一个关键概念是战略对等。荷兰式拍卖和首价密封投标拍卖给出了相同的结果,即出价最高的人以他的保留价 他准备出价的最高价 得到货物。同样,英式拍卖和维克里拍卖给出相同的结果(以出价增量为模)。然而,这两对在战略上并不等同。在荷兰式拍卖中,如果您认为自己的估价比其他人高很多,就应该出低价,而在二价拍卖中,最好如实出价。

第二个关键概念是收入等值。这是一个较弱的概念;重要的不是谁会赢,而是拍卖预计能筹集到多少资金。
这里有趣的结果是收入等价定理,它说在理想条件下,你从任何行为良好的拍卖中获得相同的收入。

这些条件包括风险中性投标人、无串通、帕累托效率(出价最高的人获得货物)和独立估值(投标人之间没有外部性)。在这种情况下,竞标者调整策略,英式、荷兰式和全额拍卖的收益都相同。因此,当您设计拍卖时,您必须关注条件不理想的方式。

有关详细信息和示例,请参阅 Paul Klemperer 的书 [1057]。

而且有很多事情都可能出错。可能存在竞价环,所有买家串通低价拍卖;在这里,最高价拍卖是最好的,因为只需要一个叛逃者就能打破队伍,而不是两个。其次,存在进入检测:在一次英国电视转播权拍卖中,竞标者必须提交大量的节目表,其中涉及与制作公司的交谈,因此业内每个人都知道谁在竞标,而只有一个竞标者的特许经营权获得了花生。第三,存在进入威慑:企业收购中的竞标者通常会宣布他们将出价高于其他任何出价。第四,风险规避:如果你更喜欢 1 美元的特定利润而不是 50% 的机会 2 美元,你会在第一价格拍卖中出价更高。第五,有信号游戏;在美国频谱拍卖中,一些竞标者通过将邮政编码放在投标的最低有效数字中来打破匿名,以表明他们准备争夺哪些区域组合,并阻止竞争对手在那里展开竞购战。然后还有预算限制:如果投标人现金有限,全额拍卖会更有利可图。

广告拍卖是一项大生意,谷歌、Facebook 和亚马逊在 2019 年分别赚取了约 500 亿美元、300 亿美元和 100 亿美元,而该行业的其他公司获得了约 400 亿美元。首创的广告竞价机制

Machine Translated by Google

谷歌是经过调整以优化收入的第二价格拍卖。投标人愿意支付价格bi,平台根据广告的相关性和点击率估计他们的广告质量为ei 。然后它计算“广告评级”为ai = biei。这个想法是,如果我的广告被点击的可能性是您的广告的五倍,那么我 10c 的出价与您 50c 的出价一样好。因此,这是一个二价拍卖,但基于排名ai而不是bi。因此,如果我的广告质量是你的五倍,我出价 10 美分,你出价 40 美分,那么我得到广告并支付 8 美分。可以证明,在合理的假设下,这使平台收入最大化。

不过,有一个陷阱。一旦媒体变得社交化,广告质量就很容易演变成病毒式传播。如果您的广告是很好的点击诱饵并且人们点击了它们,那么您支付的费用就会减少。一个结果是,在 2016 年美国总统大选中,希拉里克林顿为每条广告支付的费用比唐纳德特朗普多得多 [1234]。拍卖理论和实证数据都表明,优化平台收入的驱动力如何可能导致更极端的内容:除了拍卖步骤的病毒式传播效果外,Facebook 的投放算法将广告放在最有可能点击它们的人面前,加强了过滤气泡的效果,这并不是全部归因于用户操作 [40]。有些人认为选举法应该禁止这种“交付优化”;当然,这是在效率和公平之间存在结构性紧张的机制的又一个例子。事实上,在英国,不允许在电视上投放选举广告以及其他一些类别的广告,例如烟草。也许在这些司法管辖区中最干净的解决方案是也禁止他们上网,就像烟草一样。广告定价并不是社交媒体推广极端内容的唯一方式;正如前 Google 员工 Tristan Harris 所解释的那样,该平台的推荐算法也经过优化,以最大限度地延长人们在网站上花费的时间,这意味着不仅滚动提要和关注者,而且会偏向于焦虑和愤怒。更重要的是,由于广告商争夺更“有价值”的人口统计数据,以及由于广告标题或图片的吸引力,广告投放可能会受到性别和种族等因素的影响;这可能是故意的,也可能是偶然的,并且会影响范围广泛的广告,包括就业和住房 [39]。这一切都在经济学和心理学的边界上提出了棘手的政治问题,但拍卖理论等经济工具通常可以用来解决这些问题。

8.6 安全性和可靠性的经济学

经济学家过去常常看到经济与安全之间的简单相互作用:更富裕的国家可以提供更多的军队。但在 1945 年之后,核武器被认为使国家生存与经济实力脱钩,经济学和战略研究领域逐渐分离 [1238]。重新建立连接已留给信息安全领域。

大约在 2000 年左右,我们中的许多人注意到持续的安全故障,这些故障乍一看似乎是不合理的,但一旦我们更仔细地审视了各个参与者面临的动机,我们就开始理解这一点。我观察到银行在信息安全措施方面的奇怪投资模式 [54、55]。

Hal Varian 研究了为什么人们没有像供应商希望的那样在反病毒软件上花那么多钱 [1943]。当我们两人在 2001 年开始讨论这些案例时,我们突然意识到其中有一个有趣且即时的

Machine Translated by Google

这里有一个重要的研究课题,所以我们联系了其他有相似兴趣的人,并为来年组织了一个研讨会。当时我正在写这本书的第一版,发现将许多问题描述为激励问题会使解释更有说服力;所以我将我从这本书的最终编辑中学到的东西提炼成一篇论文“为什么信息安全是困难的 一个经济视角”。这篇论文,加上本书的第一版,引起了人们的讨论 [72]。当他们问世时,9/11 袭击已经发生,人们正在寻找关于安全的新观点。

我们很快发现了许多其他与机构激励相关的安全失败示例,例如医疗主管和管理人员购买的医院系统支持他们的利益但不保护患者隐私。

(后来,我们发现患者安全失败通常有相似的根源。)Jean Camp 一直在撰写关于漏洞市场的文章,两家初创公司已经建立了早期的漏洞市场。网络研究人员开始使用拍卖理论来设计防策略路由协议。国防部一直在考虑未能让供应商向他们出售安全系统,正如您在本章开头的第二个引用中看到的那样。微软正在考虑标准的经济性。 2002 年 6 月在伯克利召开的信息安全经济学研讨会汇集了所有这些想法,该研讨会启动了安全经济学作为一个新的研究领域。开始出现的画面是系统安全失败,因为保护系统的人不是承受失败成本的人。有时,安全机制用于将风险转嫁给其他人,如果您是其他人中的一员,您最好使用不安全的系统。换句话说,安全通常是一种权力关系;在给定系统中控制其含义的负责人经常使用它来促进自己的利益。

这是最初的见解,[78] 中讲述了安全经济学诞生的故事。但是一旦我们开始认真研究这个主题,我们就会发现它的意义远不止于此。

8.6.1 为什么 Windows 如此不安全?

2002 年安全经济学兴起时的热门话题就是这个。为什么 Windows 如此不安全,尽管微软在市场上占据主导地位?编写更好的软件是可能的,在国防和医疗保健等领域,人们付出了巨大的努力来生产可靠的系统。为什么我们看不到商品平台做出类似的努力,特别是因为微软没有真正的竞争对手?

到那时,我们了解了信息经济学的基础知识:高固定成本和低边际成本、网络效应和技术锁定的结合使得平台市场特别有可能由单一供应商主导,如果他们可以赢得争夺市场的竞争。在这样的竞赛中,微软 1990 年代的哲学 “星期二发布并在第 3 版之前把它弄好” 是完全理性的行为。在这样的竞争中,平台供应商不仅要吸引用户,还要吸引互补者 吸引那些决定是为自己的平台还是为别人的平台编写应用程序的软件公司。安全性阻碍了应用程序,而且它往往是一个柠檬市场。所以理性的供应商从事

Machine Translated by Google

争夺平台主导地位将使所有应用程序都可以在他的平台上以 root 用户身份运行2,直到他的位置稳固为止。然后他可能会增加更多的安全性 但会试图以最大限度地锁定客户或吸引数字媒体等新市场的互补者的方式进行设计。

同样的模式也出现在其他平台产品中,从旧的 IBM 大型机操作系统到电话交换机,再到早期的手机 Symbian 操作系统。产品一开始是不安全的,尽管它们会随着时间的推移而改进,但许多新的安全功能对供应商和用户都有好处。而这正是我们在微软产品线中看到的。 DOS 根本没有任何保护,并启动了恶意软件市场； Windows 3 和 Windows 95 很糟糕； Windows 98 只是稍微好一点;安全问题最终惹恼了微软的客户,以至于比尔盖茨最终在 2003 年决定停止开发,直到所有工程师都参加了安全编码课程。随后投资于更好的测试、静态分析工具和定期修补。在 Windows 的更高版本中,可利用漏洞的数量和生命周期继续下降。但是攻击者也变得更好了,Windows 中的保护并不完全是为了用户的利益。正如 Peter Gutmann 所指出的,与保护用户的信用卡号码相比,保护优质视频内容的努力要多得多 [842]。

从消费者的角度来看,锁定市场通常是“讨价还价然后敲诈”。您以 39.95 美元的价格购买了一台不错的新打印机,然后在仅仅几个月后发现您需要两个新的打印机墨盒,每个 19.95 美元,这让您感到厌恶。您想知道是否只购买一台新打印机会不会更好。

从应用程序开发人员的角度来看,基于锁定的标准竞赛市场看起来有点像这样。起初为他们编写代码真的很容易;稍后,一旦你下定决心,就会有更多的障碍需要跳过。从可怜的消费者的角度来看,他们可以被描述为“安全性差,然后是其他人的安全性”。

从安全管理成本到行业共同做出的基础设施决策的外部性,可以看到相同的模式。当竞相建立主导地位时,供应商很想设计产品,以便将大部分安全管理成本转嫁给用户。一个典型的例子是 SSL/TLS 加密。这是在 20 世纪 90 年代中期采用的,当时微软和 Netscape 争夺浏览器市场的主导地位。正如我们在第 5 章中讨论的那样,SSL 让用户自行评估网站提供的证书并决定是否信任它;这导致了各种网络钓鱼和其他攻击。然而,将合规成本转嫁给用户在当时是完全合理的;诸如 SET 之类的竞争协议会让银行承担向每个想在线购买 stu 的客户颁发证书的成本,而这只会花费太多 [524]。世界最终出现了一个不安全的互联网信用卡支付系统,并且大多数利益相关者试图以阻碍更好系统进步的方式将责任转嫁给其他人。

坏事和商品也有网络效应。在 2000 年代,大多数恶意软件编写者都以 Windows 而不是 Mac 或 Linux 为目标,并且

2使编码更容易,并使应用程序开发人员能够窃取用户的其他数据进行销售在二级市场。

Machine Translated by Google

2010 年代,因为有更多的 Windows 机器被感染 导致了一种奇怪的平衡,在这种平衡中,准备为笔记本电脑支付更多费用的人可以获得更安全的笔记本电脑,尽管没有运行那么多软件。当智能手机在 2010 年代席卷全球时,这种模式自我复制;自从 Android 取代 Windows 成为世界上最流行的操作系统以来,我们开始看到许多针对 Android 的不良应用程序,而为 iPhone 支付更多费用的人获得更好的安全性但选择更少。 (在那里,苹果应用商店更严格的政策现在比市场份额更重要。)

8.6.2 管理补丁周期

安全经济学的第二场大辩论是关于如何管理补丁周期。如果你发现了一个漏洞,你是否应该发布它,这可能会迫使供应商对其进行修补,但可能会让人们暴露数月直到他们这样做?或者你应该私下向供应商报告它 如果你告诉其他人,可能会收到一封律师函,威胁要提起昂贵的诉讼,而供应商根本懒得修补它?

这场辩论可以追溯到很久以前。正如我们在序言中指出的那样,维多利亚时代的人苦恼于出版有关开锁的书籍是否对社会负责,并最终得出结论认为是 [1895 年]。最近人们更担心美国陆军简易弹药手册 [1924] 的在线可用性是否有助于恐怖分子;在某些国家/地区,拥有副本是犯罪行为。

安全经济学为讨论此类某些问题提供了理论和定量框架。我们从 2002 年开始使用简单的模型,其中错误是独立的、相同分布的并且是随机发现的;这些具有良好的统计特性,因为攻击者和防御者处于平等地位,并且系统的可靠性仅是初始代码质量和测试它所花费的总时间的函数 [74]。但现实世界真的是这样吗?或者它是否被相关错误或供应商的内部知识所扭曲?这引发了一场大的政策辩论。 Eric Rescorla 认为,软件已经足够接近理想,即删除一个错误对攻击者以后发现另一个错误的可能性几乎没有影响,因此频繁的披露和修补是不必要的开支,除非可能重新发现相同的漏洞 [1596]。 Ashish Arora 和其他人回应的数据显示,公开披露可以让供应商更快地修复漏洞;攻击开始增加,但报告的漏洞随着时间的推移而减少 [133]。 2006 年,Andy Ozment 和 Stuart Schechter 发现核心 OpenBSD 操作系统的独特漏洞的披露率在六年期间有所下降 [1488]。简而言之,在适当的情况下,软件可以更像酒而不是牛奶 它会随着时间的推移而改进。 (可持续性是一个圣杯,我将在第 3 部分中更详细地讨论它。)

几个进一步的制度因素帮助解决了支持负责任的披露的辩论,也称为协调披露,人们向供应商或第三方报告漏洞,这些漏洞在一段时间内保密,直到补丁可用,然后让报告者获得荣誉他们的发现。一个是第一次加密战争结束时的政治解决,其中漏洞将报告给 CERT,CERT 将在漏洞期间与 NSA 共享

Machine Translated by Google

修复过程,我将在后面的 26.2.7.3 节中讨论。这得到了各国政府的支持。第二个是商业漏洞市场的出现,例如由 iDefense 和 TippingPoint 建立的漏洞市场,安全研究人员可以在其中出售漏洞;然后,这些公司会负责任地向供应商披露每个错误,并制定出可以出售给运营防火墙或入侵检测服务的公司的妥协指标。第三,聪明的软件公司开始了他们自己的漏洞赏金计划,这样安全研究人员就可以直接出售他们的漏洞,省去了 CERT 和 iDefense 等中间商。

在 Stuxnet 驱使政府储备漏洞之后,这个市场变得更加尖锐。我们已经看到像 Zerodium 这样的公司的出现,它们购买漏洞并将其出售给国家行为者,以及也出售给国家的网络武器供应商;针对 iPhone 等平台的零日攻击现在可以卖到 100 万美元或更多。这对供应链产生了连锁反应 。

例如,在 2012 年,我们遇到了第一个志愿者故意向开源项目贡献易受攻击代码的案例3,如果它进入广泛使用的平台,无疑是希望获得六位数的报酬。早在 2010 年,Sam Ransbotham 就已经表明,尽管开源软件和专有软件在理想模型中同样安全,但在开源世界中,错误会更快地转化为漏洞利用,因此攻击者更多地瞄准它[1579]。 2014 年,Abdullah Algarni 和 Yashwant Malaiya 调查了漏洞市场并采访了一些多产的研究人员;好奇心和经济激励的结合吸引了许多有能力的年轻人,其中许多来自欠发达国家,一些人负责任地披露,一些人利用漏洞市场来获得金钱和认可,而另一些人则以更多的钱卖给黑帽;有些会向供应商提供漏洞,但如果处理不当,则会将漏洞提供给坏人。供应商以类似的报价作为回应:在 Black Hat 2019 上,Apple 宣布了一项漏洞赏金计划,最高可达 100 万美元,奖励允许在 iOS 上执行零点击远程命令的漏洞。哦,许多 bug 猎人在几年后退休 [38]。不管喜欢与否,运行开源项目的志愿者现在会发现,如果他们的项目取得进展,他们自己就会成为一些有能力、积极进取的对手,即使他们无法与 Apple 的收入相提并论,让尽可能多的研究人员留在原地也是个好主意。

漏洞的生命周期现在不仅涉及漏洞的发现,还可能涉及情报机构或其他黑帽行为者的一些秘密使用;然后是它的重新发现,也许是其他黑帽,但最终是白帽;补丁的运送;然后进一步利用未应用补丁的用户。供应商和他们的客户之间在补丁发布的频率和时间上存在紧张关系,并且在信任问题上与互补者和次级用户之间存在紧张关系。 Linux 中的漏洞不仅影响您实验室的服务器和您孩子的 Raspberry Pi。 Linux 无处不在:空调、智能电视甚至汽车。这就是负责任的披露被重新命名为协调披露的原因。可能有太多的公司使用核心开发人员的平台来信任他们关于即将发布的补丁程序。还有数以千计的漏洞,其中数十个漏洞每年都会出现在犯罪分子使用的漏洞利用工具包中(有些毫无疑问只针对高价值目标使用过一次,因此它们永远不会为防御系统所知)。我们必须研究多个重叠的生态系统

3Webkit,用于手机浏览器

Machine Translated by Google

按 CVE 编号索引的漏洞;被提供给入侵检测系统的妥协指标（IoC）;通过市场、CERT 和 ISAC 直接向供应商披露信息;各种僵尸网络、犯罪团伙和国家行为者;以及各种记录在案的犯罪模式。我们在这些生态系统之间存在部分相关性,但数据通常是嘈杂的。

我将在第三部分中回到所有这些。

8.6.3 攻防结构模型

已故的冲突理论创始人杰克·赫什莱弗 (Jack Hirshleifer) 讲述了 Anar chia 的故事,该岛的防洪设施由各个家庭建造,每个家庭都维护着一段防洪墙。因此,岛上的防洪取决于最薄弱的环节,即最懒惰的家庭。他将此比作一个城市,该城市防御导弹攻击取决于一次最佳防御射击 [906]。最佳射击的另一个例子是中世纪的战争,两支军队的冠军之间可能只有一场战斗。这可能导致不同的政治制度。中世纪的威尼斯是因洪水风险而进行的最薄弱环节防御的最好例子,它拥有强大的中央政府,商人家庭选举总督对洪水防御拥有近乎独裁的权力。在中世纪晚期欧洲的大部分地区,国王或酋长率领自己的军队杀死敌人并夺取土地。最强大的国王建立了最大的帝国,这导致了封建制度优化了人类的数量

武器。

Hal Varian 将该模型扩展到信息系统的可靠性 其中性能可能取决于最薄弱的环节、最大的努力或努力的总和 [1945]。最后一种情况,即努力总和,是现代战争模式:我们纳税,政府雇用士兵。它比最佳射击（大多数人会在英雄后面搭便车)更有效,而最佳射击又比最薄弱环节（每个人都会因最懒惰而变得脆弱)更有效。信息安全是所有三种模式的有趣组合。程序的正确性可能取决于最薄弱的环节（引入漏洞的最粗心的程序员）,而软件漏洞测试可能取决于每个人的努力总和。安全性也可能取决于最大努力 由个人拥护者（例如安全架构师)采取的行动。随着更多代理的添加,系统在努力总和的情况下变得更加可靠,但在最薄弱环节的情况下变得不那么可靠。因此,随着软件公司变得越来越大,他们最终会雇用更多的测试人员和更少（但更有能力)的程序员;到 2000 年代初期,微软发现他们的测试工程师比软件工程师还多。

其他攻击和防御模型包括恶意软件传播的流行病模型,这在计算机病毒通过软盘在机器之间传播时很重要,但现在人们不太感兴趣,因为我们看到的蠕虫攻击相对较少;以及取决于时间的安全游戏模型,特别是 Ron Rivest 及其同事的 FlipIt 游戏 [559];事实上,有一整个会议 (Gamesec) 致力于博弈论和信息安全。

还有社交网络模型。例如,大多数社交网络的连通性归功于数量相对较少的节点,这些节点与其他节点的链接数量相对较多 [1994]。敲除这些节点可以

Machine Translated by Google

快速断开连接;征服者威廉在 1066 年后通过杀死盎格鲁撒克逊贵族并用诺曼人取而代之巩固了英格兰,而斯大林则杀死了较富裕的农民。美国和英国军队在伊拉克战争期间的反叛乱行动中同样以人脉广泛的人为目标（逊尼派地区由此导致的社会崩溃助长了 ISIS 的兴起）。此类模型还表明,叛乱分子形成细胞是对反复斩首攻击的自然且最有效的反应 [1373]。

George Danezis 和我还表明,在防御需要团结的地方,更小和更同质的群体将更有效 [511]。 Rainer B¨ohme 和 Tyler Moore 研究了在没有发生的情况下会发生什么 如果人们使用只会带来私人利益的防御机制,那么最薄弱的环节模型就会成为唾手可得的果实之一。例子包括垃圾邮件发送者,他们只是猜测足够弱的密码来补充他们被破坏的电子邮件帐户的库存,以及针对电子商务网站的无卡欺诈 [276]。

简而言之,任何时代的冲突技术都会对政治产生深刻而微妙的影响,因为它决定了能够生存和繁荣的机构类型。
这些机构反过来塑造了安全格局。泰勒·摩尔 (Tyler Moore)、艾伦·弗里德曼 (Allan Friedman) 和阿里尔·普罗卡西亚 (Ariel Procaccia) 研究了像美国国家安全局这样同时承担防御和进攻任务的国家机构是否会披露漏洞以便修复或储存漏洞;他们的结论是,如果它可以忽略落在他人身上的社会成本,它就会囤积 [1338]。然而,安全生态系统中最大的机构可能不是政府机构,而是占主导地位的公司。

8.6.4 锁定、搭售和 DRM 的经济学

技术锁定是导致主导公司市场的因素之一,软件公司在 30 多年的时间里花费了数十亿美元来建立机制,使他们的客户难以离开,但让他们的竞争对手很容易背叛。 80 年代见证了文件格式大战,公司试图阻止任何其他人访问他们的软件生成的文字处理文件或电子表格。

到 1990 年代,随着 Microsoft 试图将其他操作系统排除在 LAN 之外,这场斗争已经转移到网络兼容性上,直到 SAMBA 创造了与 Apple 的互操作性;在 1993 年的反托拉斯诉讼之后,微软没有使用 Windows 合同来阻止它。对抗性互操作性作为一种对抗网络效应的柔道而出现 [570]。类似的机制被用于控制相邻或互补商品和服务的市场,例如将墨盒与打印机捆绑在一起,以及将音乐和视频锁定到特定机器或机器系列的数字版权管理 (DRM) 系统,通过防止用户简单地将它们复制为文件。在早期的安全经济学论文中,Hal Varian 在 2002 年指出,不受限制地使用它们可能会损害竞争 [1944]。

2003 年,Microsoft、Intel 和其他公司启动了一项“可信计算”计划,将权限管理扩展到其他类型的文件,而 Windows Server 2003 提供了“信息权限管理”(IRM),因此我可以通过电子邮件向您发送一份 Word 文档你只能在屏幕上阅读,不能打印,而且只能到月底。明显存在竞争性滥用的可能性;通过将用户数据的控制权从机器所有者转移到

Machine Translated by Google

它存储给存储它的文件的创建者,锁定的可能性大大增加 [73]。想一想上面 8.3.2 节中的示例,其中一家公司有 100 名员工 ,每人有一台 PC,他们以 150 美元的价格安装了 Oce。

他们支付给微软的 15,000 美元大致相当于转向（比如说)LibreOce 的总成本,包括培训、转换文件等。但是,如果文件的控制权转移到其成千上万的客户手中,并且公司现在必须联系每个客户并请求数字证书才能迁移文件,那么显然转换成本增加了 因此您可以预期成本Oce增加也。 IRM 当时没能发挥作用 :美国公司很快就明白这是一场锁定游戏,欧洲政府反对可信计算计划将小公司排除在外,而微软无法让机制发挥作用与 Vista正常。然而,既然电子邮件已经转移到云端,微软和谷歌都在提供受限的电子邮件服务,这正是 2003 年提出并反对的类型。

另一方面涉及 DRM 和音乐。在 20 世纪 90 年代末和 2000 年代初,好莱坞和音乐界大力游说消费电子设备中的强制 DRM,而我们仍然以各种方式为此付出代价;例如,当您将演示文稿从 VGA 适配器切换到 HDMI 时,您会丢失音频。好莱坞关于未经许可的点对点文件共享将摧毁创意产业的说法始终站不住脚。2004 年的一项研究表明,下载并没有损害音乐行业的整体收入 [1457],而后来的一项研究表明下载者实际上购买了更多的 CD [50]。谷歌首席经济学家 [1946] 在 2005 年如何解释真正的问题:科技行业与音乐之间更紧密的联系将比音乐行业更能帮助科技公司,因为科技更加集中（当时只有三个严肃的音乐平台– 微软、索尼和苹果）。内容产业发展迅速,但到当年年底,音乐出版商抗议苹果公司从在线音乐销售中获得的现金份额过大。

供应链中的权力从音乐巨头转移到平台,因此平台（现在是苹果、谷歌、亚马逊和 Spotify)获得了大部分资金,音乐行业的剩余权力从巨头转移到了附属机构 只是由于航空公司放松管制有利于飞机制造商和低成本航空公司。这是经济分析预测能力的惊人证明。通过与一个不存在的威胁作斗争,唱片业帮助计算机行业吃到了午餐。我将在 24.5 节中更详细地讨论这个问题。

到 2020 年,DRM 已不再是一个问题;从可移动媒体到流媒体服务的转变意味着很少有人再复制音乐或电影;问题是您是否付费订阅以避免广告。同样,转向基于云的服务意味着很少有人会窃取软件。因此,涉及侵犯版权的犯罪急剧下降 [91]。

然而,向云的迁移使锁定成为一个更复杂的问题,在生态系统和单个产品的层面上运行。我们在上面讨论了来自 Google Docs 的竞争如何降低 Oce 的价格,因此微软以转向 Oce365 作为回应;以及该服务或 G-suite 的总拥有成本如何高于独立的生产力产品。那么锁定在哪里呢?那么,如果您选择 Google 生态系统,您可能不仅会使用 Gmail 和 Google Docs,还会使用 Google 日历,

Machine Translated by Google

地图等等。尽管您始终可以下载所有数据,但在不同的平台（例如 Microsoft 或 Apple 的)上重新安装它会很麻烦,所以您可能会咬紧牙关,在免费配额时支付更多存储空间用尽。同样,如果您开始在 IT 公司中使用 Slack 或 Splunk 等工具,您最终将以各种方式自定义它们,这使得迁移变得困难。同样,这并不是什么新鲜事。我所在的大学糟糕的会计系统已经成为 Oracle Financials 的高度定制版本大约 20 年了。现在每个人都在通过诱导客户购买或构建互补资产,甚至外包整个功能来玩锁定游戏。

Salesforce 已经接管了许多公司的销售管理,Palantir 已经锁定了许多美国警察部队,而大型学术出版商正在篡夺大学图书馆的职能。在没有可行竞争的情况下（如第二个案例）,就会出现真正的政策问题。微软锁定公共部门 IT 的深度体现在慕尼黑市为脱离 Linux 并在公共管理中使用 Linux 所做的勇敢尝试:这最终在 15 年、比尔盖茨的几次访问和新的市长 [759]。

卡特尔对整个生态系统的控制并不是什么新鲜事； Joshua Specht 讲述了 Cargill 和 Armour 等大型食品公司如何控制铁路开辟的双边市场、通过购买谷物升降机等基础设施巩固权力、将气候风险转嫁给小农户、组织工会组织者的历史出城,甚至让政客们通过了“ag-gag”法,将动物权利激进主义定义为恐怖主义 [1808]。这在大型 IT 服务公司建立市场力量的方式中有有趣的回响,控制着从广告生态系统到操作系统再到数据中心的一切。事实上,在过去的几十年里,整个全球经济变得更加垄断,而 IT 似乎对行业集中度的增长做出了很大贡献[234]。这不是唯一的因素 其他行业（如国防承包)也有自己的动态,而公用事业等自然垄断的监管者往往会随着时间的推移被游说所俘获。关于护城河的文献越来越多 竞争的结构性障碍,网络效应和技术锁定只是其中的两个例子;其他范围从专利和监管捕获到从数据控制中获得的客户洞察力 [1431]。信息产业的动态使许多现有问题复杂化,并使有效竞争变得更加困难。以哈佛大学的 Lina Khan 为首的竞争法学者多年来一直在争论,美国法律需要从更广泛的角度看待竞争滥用,而不仅仅是消费者剩余（欧洲已经如此）[1044],而芝加哥-卡尔·夏皮罗 (Carl Shapiro) 等学派经济学家谴责反托拉斯民粹主义,并认为补救措施应针对特定的危害,因为反托拉斯法不适合解决大公司掌握的政治权力 [1716]。然而,卡尔承认美国反托拉斯法在过去 40 年中被最高法院过度缩小了范围;消费者福利测试不充分;占主导地位的公司的排他性行为和劳动力市场做法都需要解决,美国需要更好地控制横向合并 [1717]。

多年来,欧洲竞争法一直禁止公司利用在一个市场的支配地位在另一个市场建立市场地位,我们已经看到了一系列针对大型科技公司的判决。至于未来可能的方向,欧盟委员会总司的 2019 年报告

Machine Translated by Google

Jacques Cr´emer、Yves-Alexandre de Montjoye 和 Heike Schweizter 的竞争报告不仅强调了科技巨头的网络外部性和极端规模回报,还强调了由于转向在线,他们控制了越来越多的数据这一事实服务和云计算 [497]。因此,他们具有范围经济:在一项业务中取得成功使得在另一项业务中更容易取得成功。它的结论是,欧盟的竞争法框架基本上是健全的,但需要一些调整:监管机构需要保护市场竞争和市场竞争,例如在占主导地位的平台上,它们有责任不扭曲那里的竞争。在这种环境下,监管机构必须关注多宿主、交换、互操作性、数据可移植性和对售后市场的影响。

搭售备件在欧洲也受到监管,一些行业的特定法律要求供应商让其他公司生产兼容的备件,而在其他行业则要求他们在一段时间内提供备件。

如果您使用安全机制将产品彼此绑定,则可能会出现一些非常具体的策略问题。这与计划报废的法律相关,当供应商限制软件更新可用的时间段时,对于带有数字组件的商品,该法律得到加强。欧盟最近通过一项新的商品销售指令 (2019/771) 对规则进行了升级,该指令从 2022 年 1 月起要求销售带有数字组件(无论是嵌入式软件、云服务还是相关电话应用程序)的商品的公司维护此软件至少在商品售出两年后,如果这是客户的合理预期,则可以延长更长时间(对于汽车和白色家电,这可能意味着十年)。现在我们在汽车和医疗设备等耐用品中有了软件,这样的规定将成为一个更大的问题;我将在本书的最后一章讨论可持续性。

8.6.5 动机不良的警卫

“眼不见为净”,这是一句古老的苏格兰谚语,安全工程举出了很多例子。

- 警方很少对网络犯罪采取行动,因为他们发现阻止人们举报更简单。正如我们在 2.3 节中提到的,这使他们能够声称犯罪率多年来一直在下降,尽管它只是像其他一切一样在网上移动。

- 政府要求银行承担发现洗钱活动的义务,尤其是自9/11 以来。然而,没有哪个银行家真的想知道他的一位客户是黑手党成员。因此,银行游说将降低风险正式化为尽职调查;他们要求制定详细的规定,具体规定开立新账户所需的身份证件形式,以及为识别可疑交易而进行的处理。

- 在欺诈方面,发现罕见的银行欺诈模式意味着支付服务提供商现在应该承担损失,而不是仅仅告诉客户她一定是弄错了或在撒谎。因此,他们倾向于等待并从行业或学术界了解新的欺诈类型,而不是自己进行认真的研究。

Machine Translated by Google

- 点击欺诈是类似的。从僵尸网络中发现“无机点击”模式意味着您不能再为这些点击向广告商收费。你必须做一些工作来减轻最坏的情况,但如果你拥有市场主导地位,那么你越努力打击点击欺诈,就越少

  你赚取的收入。

- 在您自己的代码中查找错误是另一个例子。当然,您必须调整阻止它工作的明显错误,但是攻击者可以利用的更微妙的错误呢?寻找它们的时间越多,修复它们的时间就越多。你总是可以去购买静态分析工具,但是你会发现更多的错误并且你的发布日期会推迟几个月。因此,公司往往只有在客户需要时才这样做,而且只有从项目一开始就这样做才便宜(但在那种情况下,你也可以用 Rust 而不是 C 编写代码)。

还有更微妙的例子,例如说出威胁的真相在政治上是不可接受的。在过去,很难与董事会谈论内部威胁,因为董事们大多更愿意相信他们公司最好的一面;因此,一个典型的安全经理会做出关于“邪恶黑客”的令人不寒而栗的演讲,以便获得建立内部控制的预算。如今,许多公司的安全政策空间已被四大会计师事务所占据,他们对内部控制的共识与他们在治理方面的思想领导力息息相关,愤世嫉俗者可能会说,这是为了他们表面上的客户的福利而优化的,股东,但对于他们真正的客户,首席执行官。高管舞弊很少被发现,除非他们让公司倒闭;这些努力反而变成了烦人和无关紧要的事情,例如每月更改密码和坚持要原始纸质收据。我将在 12.2.2 节详细讨论所有这些。

或者考虑 2.3.6 节中描述的 2009 年英国议会开支丑闻。也许议会的官员们没有更积极地捍卫费用制度,因为在一个以“如果你“没有什么可隐瞒的,你没有什么好害怕的”。该标语的作者,时任内政大臣雅克史密斯,可能没有什么可隐瞒的,但她的丈夫却有:他看色情片并将其计入她的议会费用。 Jacqui 丢了工作,也丢了议会席位。如果官员们知道开支服务器上的信息可能会让内阁部长失去工作,他们可能应该将其列为最高机密并将其保存在保险库中。但是,如何向财政部证明额外成本是合理的呢?在那个愉快的音符上,让我们继续隐私。

8.6.6 隐私经济学

隐私悖论是人们说他们重视隐私,但实际上却并非如此。
如果你在街上拦住行人并询问他们的意见,大约三分之一的人说他们是隐私原教旨主义者,永远不会将他们的个人信息交给营销人员或其他任何人;大约三分之一的人说他们不在乎;大约三分之一的人处于中间状态,表示他们会以务实的方式看待风险和收益

Machine Translated by Google

任何披露。然而,他们的购物行为 无论是线上还是线下 都截然不同 ;绝大多数人很少注意隐私,并且会为了一点好处而泄露最敏感的信息。各种公司都在出售增强隐私的技术,但大多数都在市场上失败了。为什么会这样?

隐私是 2000 年之前经济学家感兴趣的信息安全的一个方面。1978 年,理查德波斯纳将隐私定义为保密 [1536],次年将其扩展为隐居 [1537]。 1980 年,杰克·赫什莱弗 (Jack Hirshleifer) 发表了一篇开创性的论文,他在论文中指出,隐私不是关于退出社会,而是一种组织社会的手段,源于进化的领土行为;对财产的内化尊重支持自治。 1996 年,Hal Varian 从信息市场的角度分析了隐私 [1940]。消费者不想被无关紧要的营销电话打扰,而营销人员不想浪费精力;然而,由于搜索成本、外部因素和其他因素,两者都感到沮丧。瓦里安建议赋予消费者对自己信息的权利,并让合同来解决这些问题。

然而,正如我们所见,信息产业容易出现导致垄断的市场失灵,占主导地位的信息密集型商业模式的扩散需要不同的方法。 Andrew Odlyzko 在 2003 年指出,这些垄断同时增加了价格歧视的激励和机会 [1462]。公司挖掘在线互动以获取揭示个人支付意愿的数据,虽然我们在许多市场上看到的从航空公司收益管理系统到电信价格的差异定价可能在经济上是有效的,但它越来越令人反感。 Peter Swire 认为我们应该衡量隐私入侵的外部性 [1852]。如果一个电话销售员打电话给 100 个潜在客户,向其中三个人推销保险,并惹恼了 80 个,那么传统的经济分析只考虑这三个人和保险公司的利益。但持续的烦恼导致数百万人离开目录,通过答录机屏蔽电话,或者根本没有固定电话。机器人呼叫的长期社会成本可能相当可观。对人们隐私估值的实证研究支持了这一点。

隐私悖论产生了大量文献,并且至少由三个因素构成。首先,有许多不同类型的隐私伤害,从就业、信贷和保险方面的歧视,到表现为付款欺诈的网络犯罪,再到跟踪和非自愿亲密图像等个人犯罪。

其次,我们在 3.2.5 节中讨论的行为因素起着很大的作用。莱斯利·约翰 (Leslie John) 及其同事通过巧妙的实验证明了语境的力量。她以一系列令人尴尬的问题的形式设计了一个“隐私表”;分数是受试者在犹豫之前会回答多少问题。她对三组学生进行了试验:一个在中立大学环境中的对照组,一个隐私处理组,他们得到了他们的数据将被加密的强烈保证,他们的 IP 地址不会被存储,等等;以及一个被带到外部网站的玩家治疗组(howbadareyou.com,带有微笑魔鬼的标志)。你可能认为隐私处理组会披露更多,但实际上他们披露的更少 因为隐私对他们来说很重要。至于游戏玩家群体,他们很高兴

Machine Translated by Google

披露的数量是对照组的两倍 [987]。

第三,业界理解这一点,并竭尽全力降低隐私风险的重要性。隐私政策通常不在首页,但相关用户很容易找到;政策通常以平淡无奇的文字开头,将令人不快的内容留到最后,因此它们不会惊动不经意的浏览者,但警觉的少数人可以很快找到不使用该网站的理由,因此它们也不会阻止其他人用户点击广告。欧洲强制要求的 cookie 警告大多是镇痛剂,尽管一些公司为用户提供了细粒度的控制;如第 3.2.5 节所述,控制的错觉足以让许多人放心。

那么整体效果如何呢?在 2000 年代和 2010 年代初期,有证据表明公众正在逐渐了解我们工程师已经了解的风险;例如,我们可以从选择使用隐私控制来缩小该系统非常开放的默认设置的 Facebook 用户比例稳步上升中看到这一点。

2015 年,也就是斯诺登事件曝光近两年后,皮尤研究中心进行的两项调查显示,美国公众的习得性无助感越来越强烈。 93% 的成年人表示控制谁可以获得有关他们的信息很重要,90% 的人表示控制收集有关他们的信息很重要; 88% 的人表示,未经他们的许可,任何人不得观看或收听他们的内容,这一点很重要。然而,只有 6% 的成年人表示他们“非常有信心”政府机构能够保护他们的记录的私密性和安全性,而另有 25% 的人表示他们“有一定的信心”。电话公司和信用卡公司的数据相似,而广告商、社交媒体和搜索引擎的数据则差得多。然而,很少有受访者做过任何重要的事情,除了偶尔清除浏览器历史记录或拒绝对个人信息的特别不适当的要求 [1204]。

自 1960 年代以来,这些紧张局势一直在加剧,并导致美国和欧洲之间存在显着差异的复杂隐私监管。我将在 26.6 节中更详细地讨论这个问题。

8.6.7 组织和人类行为

组织通常以明显非理性的方式行事。我们经常看到公司甚至政府变得如此自满,以至于他们无法对威胁做出反应,直到危机来临,他们才会感到恐慌。自 1918-19 年西班牙流感以来的一个世纪里,欧洲和北美的卫生服务弹性和大流行防范能力受到侵蚀,这只是众多例子中最突出的一个。再举一个例子,似乎总是有一家电话公司和一家银行成为坏人的目标。低欺诈率会让人们沾沾自喜,直到坏人注意到为止。越来越多的滥用行为被忽视,或者尽可能长时间地归咎于客户。然后它就上了新闻,高管们感到恐慌。大量的钱花了一两年,stu 得到修复,坏人转移到下一个受害者身上。

因此,安全工程师需要预测人类弱点通过组织行为表现出来的方式。

Machine Translated by Google

有大量关于制度经济学的文献可以追溯到 Thorstein Veblen。一位杰出的从业者 Herb Simon 也是一位计算先驱,并在 CMU 创立了计算机科学。在一本关于行政行为的经典著作中,他解释说,管理者所做的决定不仅关乎效率,还关乎组织的忠诚度和权威,以及组织目标与个体员工所面临的激励之间的相互作用;目标层次混乱,价值观和事实混杂在一起[1754]。对这些问题的更现代的分析通常将它们视为微观经济学框架中的委托代理问题;这是会计学教授的典型做法。我们将在后面的 12.2 节中讨论实际会计实践中的失败。另一种方法是公共选择经济学,它应用微观经济学方法研究政治家、公务员和公共部门机构人员的行为。我在第 26.3.3 节总结了公共选择;这些原则在探讨英国公务员行为的电视连续剧“Yes Minister”中得到了很好的阐释。愤世嫉俗者指出,官僚机构似乎以一种将指责的可能性降到最低的方式演变。

我自己的观察是,在银行、大大小小的科技公司以及大学部门工作过,竞争比企业是公有还是私有更重要。大学教授之间竞争激烈;我们的客户不是我们的副校长,而是诺贝尔奖委员会或同等职位。但是,由于大学行政人员在层级结构中工作,风险投资位于顶端,因此他们面临与公务员相同的激励,并表现出许多相同的优势和劣势。与此同时,一些私营公司拥有如此大的市场力量,以至于它们在内部的行为就像政府一样(尽管高层的薪酬要高得多)。

8.6.8 网络犯罪经济学

如果您要保护系统免受攻击,最好了解攻击者是谁、有多少人、来自哪里、他们如何学习工作以及他们的动机如何。这将我们带入了网络犯罪经济学。

在第 2.3 节中,我们概述了网络犯罪生态系统,我们可以使用许多工具来更详细地研究它。在剑桥网络犯罪中心,我们收集和整理执行此操作所需的数据,并将其提供给全球一百多名研究人员。与其他经济学科一样,有一个迭代过程来找出有趣的问题,并收集数据来回答这些问题。提出问题的人不仅是经济学家,还有工程师、心理学家、律师、执法人员,以及越来越多的犯罪学家。

一种研究犯罪的方法是芝加哥学派经济学家的方法,例如加里贝克尔,他在 1968 年从奖惩方面分析了犯罪 [200]。
这种方法提供了许多有价值的见解,但并不是全部。为什么犯罪集中在不良街区?为什么这些社区的一些孩子会成为多产且顽固的罪犯?传统犯罪学家研究这些问题,并找到预防犯罪价值的解释:最严重的罪犯往往遭受多重剥夺、养育不当、滥用药物和酗酒,并陷入犯罪循环。较早的

Machine Translated by Google

他们从十几岁开始,在放弃之前坚持的时间越长。批判犯罪学家指出,法律是由有权势的人制定的,他们通过压迫穷人来维持自己的权力,而且与富裕的白人居住的漂亮郊区相比,糟糕的社区更有可能受到过度监管和污名化。

进一步深入,我们可以查看不良社区、罪犯的心理以及他们采取的犯罪途径。自 1960 年代以来,已有大量研究使用环境设计来抑制犯罪,最初是在低成本住房中,然后是无处不在。例如,庭院比公园好,因为居民更有可能识别和挑战入侵者;许多这些预防情境犯罪的想法都从犯罪学进入系统设计。在 13.2.2 节中,我们将对此进行更详细的讨论。

第二,心理正常的人不喜欢伤害别人;这样做的人往往缺乏同理心,可能是因为童年受虐,或者(更常见的)有最小化策略来为他们的行为辩护。银行劫匪将银行家视为真正的剥削者;士兵将敌人非人化为“gooks”或“terrs”;大多数普通的杀人犯都将他们的罪行视为荣誉问题。

“她欺骗了我”和“他不尊重我”是典型的触发因素;我们在 3.2.4 节中讨论了这些机制。这些机制适用于在线和电子欺诈领域。违法的黑客往往会觉得他们的行为无论如何都是正当的:黑客行动主义者毕竟是政治活动家,而网络骗子则使用各种最小化策略来避免内疚。一些俄罗斯网络骗子认为美国在 1989 年之后把俄罗斯搞砸了,所以他们只是在收回自己的钱(他们在这方面得到了本国政府的态度和政策的支持)。至于那些将欺诈风险转嫁给客户的银行家,他们在内部谈论如果承认安全漏洞,他们将面临“大量的欺诈欺诈风险”。

第三,了解犯罪途径、犯罪团伙的组织和技能扩散很重要。 Steve Levitt 研究了芝加哥犯罪团伙的组织和财务状况,发现街头毒贩的收入低于最低工资 [1151]。他们做好了站在雨中被枪杀的准备,以便有机会进入下一个级别,那里的邻居老板开着一辆宝马和三个女孩。逮捕老板不会有任何不同 ,因为有数十名年轻人会为取代他而战。要得到结果,警察应该瞄准瓶颈,比如进口商的系统管理员。这些想法也有交叉。许多网络罪犯从游戏玩家开始 ,然后在游戏中作弊,然后交易游戏作弊,然后学习如何编写游戏作弊代码,在几年内,更有才华的人成为了恶意软件开发者。因此,一项政策干预是试图阻止孩子们跨越合法和非法游戏作弊之间的界限。正如我在第 3.2.4 节中提到的,英国国家犯罪局购买了 Google 广告,这些广告警告在英国搜索 DDoS 出租服务的人使用此类服务是非法的。 Ben Collier 及其同事使用我们的网络犯罪中心数据表明,与在美国持续增长的情况相比,这阻止了英国 DDoS 攻击的增长 [454]。

我们在第 2.3 节中讨论了网络犯罪的总体成本,指出尽管事实上

Machine Translated by Google

技术已经改变;我们现在更多地通过手机而不是笔记本电脑上网,使用社交网络,并将所有内容保存在云端。现在大多数犯罪都是在网上进行的; 2019 年,我们预计约有 100 万英国家庭遭受入室盗窃或汽车盗窃,而超过 200 万家庭遭受几乎总是在线的欺诈或诈骗。 (到 2020 年,这种差异将更加明显;随着人们在封锁期间呆在家里,入室盗窃率进一步下降。)然而,几乎所有地方的政策反应都滞后。本书多处报道了对特定犯罪的研究。

还通过泄露披露的影响研究了网络犯罪的影响。
Alessandro Acquisti 及其同事研究了报告安全或隐私泄露事件对公司股价的影响 [15];一次违规往往会导致小幅下跌,并在一周左右后消散,但从长远来看,两次违规可能会削弱投资者的信心。违反披露法已将违反可保事件;如果 TJX 丢失了 4700 万条记录并且必须支付 5 美元邮寄给每位客户,这就是索赔;我们将在第 28.2.9 节稍后讨论网络保险。

但总的来说,测量是很棘手的。大多数相关出版物来自有动机谈论损失的组织,从警察机构到反病毒供应商;我们首选的方法是按运作方式和部门计算损失,如第 2.3 节所述。

8.7 总结

许多系统失败是因为激励措施错误,而不是因为某些技术设计错误。因此,安全工程师需要了解基础经济学以及加密、协议、访问控制和心理学的基础知识。安全经济学迅速发展,可以解释许多我们过去认为只是“坏天气”的事情。它不断对各种问题提出引人入胜的新见解,从如何优化补丁周期到人们是否真正关心隐私。

研究问题

到目前为止,已经探索了三个与安全相关的经济学领域,即微观经济学、博弈论和行为经济学。但经济学是一门广泛的学科。它还能给我们什么其他的想法?

在我写的关于安全经济学起源的历史论文中,我建议新的研究生可以遵循以下启发式来选择研究主题。首先,为经济学的其他子领域 X 考虑安全和 X。其次,考虑 Y 对不同应用程序 Y 的安全经济学;已经有一些关于支付、色情、游戏和审查等主题的论文,但这些并不是计算机的唯一用途。第三,在发现金子的地方继续挖掘(例如行为隐私)[78]。从那时起,我将添加以下内容。

第四,数据驱动的研究有很大的空间,现在我们开始了

Machine Translated by Google

为学术界提供大型数据集（通过剑桥网络犯罪中心），许多学生都热衷于发展数据科学技能。一个相关的问题是如何收集更多可能对探索其他领域有用的数据，从个人安全人员的生产力到机构内部的安全工作方式，尤其是政府和医疗保健系统等大型复杂机构。有什么好的方法可以衡量安全文化的质量吗?第五，现在我们开始将软件和在线连接放在汽车和医疗设备等持久安全关键的东西中，我们需要更多地了解安全与安全之间的相互作用，以及我们如何保持这些系统的补丁和运行了几十年。这开启了可靠性和可持续性方面的各种新话题。

目前的安全经济学研究主要发表在信息安全经济学研讨会 (WEIS) 上，该研讨会自 2002 年以来每年举办一次 [76]。除了其中一个研讨会之外，所有研讨会都有实时博客，包括每篇论文的摘要和指向它的链接，您可以在我的博客上找到该链接，也可以直接从我的经济和安全资源页面 http://www.cl 链接。cam.ac.uk/~rja14/econsec.html。

延伸阅读

信息经济学的经典介绍是夏皮罗 (Shapiro) 和瓦里安 (Shapiro) 和瓦里安 (Varian) 的《信息形成规则》(Information Rules)，对于 20 年前 [1718 年] 写的一本书来说，它仍然非常新鲜。这仍然在我们的学生阅读清单上。最新的摘要可能是 Jacques Cr´emer、Yves-Alexandre de Montjoye 和 Heike Schweizter 为欧盟委员会竞争总局提交的 2019 年报告，该报告分析了信息发挥重要作用的市场出了什么问题[497];我还会阅读 Carl Shapiro 2019 年对美国竞争政策状况的评论[1717]。

Tim Wu 的“The Master Switch”从十年前的角度[2049] 总体上讨论了电信和信息产业的垄断。如果您打算在该主题上进行研究并且您的学位不是经济学，您可以阅读标准教科书，例如 Varian [1941] 或 Core Economics 网站。亚当·斯密的经典著作《国家财富的本质与成因探究》仍然值得一看，而迪克·塞勒的《行为不端》讲的是行为经济学的故事。

[78] 讲述了安全经济学的早期故事；有一个早期（2007 年)的调查，我与 Tyler Moore 一起在 [110] 上写了一篇更全面的 2011 年调查，也是与 Tyler 一起在 [111] 上写的。对于隐私经济学，请参阅 Alessandro Acquisti 的在线参考书目，以及他与 George Loewenstein 和 Laura Brandimarte 一起撰写的调查论文 [16]； Spiros Kokolakis [1076] 也对有关隐私悖论的文献进行了调查。然后，要深入研究文献，我会推荐 WEIS 会议论文和实时博客。

许多经济学家研究相关领域。我提到了 Jack Hirshleifer 的冲突理论 [907]；另一个重要的分支是犯罪经济学，它由 Gary Becker [200] 开创，并由 Steve Levitt 和 Stephen Dubner 的“魔鬼经济学”[1151] 普及。迭戈·甘贝塔可能是

Machine Translated by Google

有组织犯罪领域的知名学者;他的“黑社会法典:罪犯如何交流”是经典之作 [742]。最后,关于网络犯罪学的研究社区和文献不断增多,我们剑桥网络犯罪中心的网站可能是一个合理的起点。