文章编号: 2096-1618(2017)03-0239-08
稿件来源:科学网
网　　址: http://blog.sciencenet.cn/blog-453322-1007253.html
发表时间:2016-10-07

安全通论(18)

——网络安全经济学(1):攻防一体

杨义先,　钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:谁都知道:早在200多年前,亚当·斯密就在其《国富论》中指出,当自由市场经济充分竞争时,总有一只"看不见的手",牵引着竞争各方,最终达成互利。谁也都知道,在网络空间中,黑客与红客的竞争对抗非常激烈,而且,还会越来越激烈;换句话说,黑客与红客已经处于充分竞争状态了。但是,至今谁也没想到,在网络空间的黑客和红客对抗中,也有一只"看不见的手",它能最终安抚红黑双方,让他们心平气和地休战(当然,也可以说是为下一场、更惨烈的对抗战做准备)。本文将在攻防一体的情况下,描绘这只"看不见的手"的数学本质,以及这只手到底是怎么安抚黑客和红客的,此外,还再一次从另一角度证实了网络安全的"三状态"观念(我们曾用《博弈论》证明过)。关于攻防分离的情况,将在《安全通论》(19)中论述。

doi:10.16836/j.cnki.jcuit.2017.03.002

0　引言

根据热力学第二定律,热水中的快分子与凉水中的慢分子相遇时,它们将发生激烈碰撞(充分竞争),这时,将有一只"看不见的手",来安抚这些水分子,让它们的速度最终趋同,使碰撞不再激烈,从而水温达成一致。

根据达尔文进化论,当各种生物充分竞争时,将有一只"看不见的手",出面"劝架",将生物们"彼此分离",从而演化出不同的物种(然后,物种们再展开下一轮,或许更激烈的竞争)。

根据耗散结构理论,当一个远离平衡态的非线性开放系统,不断与外界"抢夺"物质和能量时,若这种激烈的竞争使系统内某参量变化,达到一定阈值时,就会出现一只"看不见的手",它通过涨落,让系统发生突变,由原来"打架"时的混沌无序状态,转变为一种在时间、空间或功能上的有序状态。

根据协同学理论,在复杂开放系统中,受外来能量或物质的"侵扰",系统中的大量"子系统"将相互"打架",于是,就会出现一只"看不见的手",使系统在临界点发生质变,产生协同效应,使系统从无序变为有序,从混沌中产生某种稳定结构。

根据超循环理论,分子们通过疯狂的"自我复制"来彼此竞争,积累信息。当这种信息积累,达到单元容量上限时,就会出现一只"看不见的手",它把"自复制和选择上稳定的单元"结合成更高的组织形式,以便下一步再产生选择上稳定的行为。于是,无机分子逐渐形成简单的有机分子,原核生物逐渐发展为真核生物,单细胞生物逐渐发展为多细胞生物,简单低级的生物逐渐发展为高级复杂的生物。

根据日常经验,当你冥思苦想,思考某个难题时,你的脑细胞异常活跃(彼此激烈竞争),各种思维猛烈碰撞,于是,那只"看不见的手"很可能就会突然出现,并送上灵感,让你顿悟,引你进入"柳暗花明又一村"。

其实,那只"看不见的手"的真正成名之作,是充分竞争的市场经济。

早在二百多年前,亚当·斯密就在其《国富论》中说:"每个人都试图应用他的资本,来使其生产品得到最大的价值。一般来说,他并不企图增进公共福利,也不清楚增进的公共福利有多少,他所追求的仅仅是他个人的安乐,个人的利益,但当他这样做的时候,就会有一双看不见的手引导他去达到另一个目标,而这个目标绝不是他所追求的东西。由于追逐他个人的利益,他经常促进了社会利益,其效果比他真正想促进社会效益时所得到的效果为大。"不过,必须指出的是,只有在充分竞争的"市场经济"中,才会出现这只"看不见的手",而在缺乏竞争的"计划经济"中,这只"手"就永远也不会出现,当然也就更看不见了。

总之,各领域成果都好像在异口同声地说:哪里有充分竞争,哪里就会出现那只"看不见的手"!

但是,事情远非如此简单! 其实,这只"看不见的手"绝对神出鬼没,不但你很难抓住它,很难搞清它的

结构,甚至连它的大概功能也都很难描述。比如,为了搞清亚当·斯密的那只“看不见的手”,全世界的经济学家们,前赴后继探索了上百年,好容易才在 1972 年和 1983 年等多个诺贝尔奖和其它成果的支撑下,取得了突破,建立了微观经济学的“一般均衡理论”。

既然网络空间安全中,红客和黑客也处于激烈的竞争状态,因此,从定性角度,并不难猜测其中也存在“看不见的手”,但关键是要把这只“手”画出来。因此,下面就借助经济学的“一般均衡理论”成果,来探索那只“看不见的手”的数学实质(当然,网络空间对抗中,各种各样的“看得见的手”实在太多了,比如,安全保障的软硬件设备、断网封堵的行政命令等都是典型代表)。

为此,首先在攻防一体的假设下,建立红客和黑客竞争对抗的“经济学”模型。

1 攻防一体的“经济学”模型

为什么要建立“经济学”模型呢?

原因之一,经济才可数字化(比如,政治、军事等就很难数字化),从而,为后续的量化研究奠定基础;而只有量化研究,才能深入本质,才更具说服力。当然,本文并不考虑如何把政府、军事事件等数字化的问题,只假定已经数字化了。

原因之二,虽然表面上,红客与黑客攻防竞争的目的各不相同;但是,这些千差万别的目的背后,其实都隐藏着一个真正的、相同的最终目的:经济利益。正可谓“天下熙熙,皆为利来;天下攘攘,皆为利往。”当然,这里的经济利益,可能是直接的,也可能是间接的;可能是显性的,也可能是隐性的;可能是当前的,也可能是未来的;可能是战术的,也可能是战略的。比如,今天的攻防活动,可能是为了明天的经济利益;甲地的攻防活动,可能是为了乙地的经济利益;对张三的攻防活动,可能是针对李四的经济利益等。当然,本文不考虑任何间接目的,只锁定经济利益,把所有的攻防活动都看成现时、显性的经济指标。

原因之三,可以借用经济学数百年来的众多成果,特别是微观经济学的“一般均衡理论”。当然,本文只是抛了块砖,其实利用经济学来研究网络攻防,还有大量的工作要做,还有一个大而富的金矿要挖。只可惜,过去“网络空间安全”与“经济学”这两门学科相距太远,很少有人能在它们之间“跨界”,笔者更是经济学的文盲。但愿有某些经济学家,能够进入网络空间安全领域来掏金;也希望安全专家们能够多学一点(微观)经济学。真心盼望,“网络空间安全”与“经济学”能够早日“天涯若比邻”。

为什么要假定攻防一体呢?主要理由就是:简单且不失真。所谓攻防一体,即,每一个人(用户)都既是红客,又是黑客;他既要保护自己的信息系统,又要想攻击别人的系统。(攻防分离,即专职红客和专职黑客的情况,将在《安全通论》(19)中论述)。于是,就没必要刻意区分谁是红客,谁是黑客了,而统一都把他们看成用户。现实生活中,确实也是这样。因为,一方面,如今做黑客的“门槛”越来越低,只要愿意,人人都可以当黑客了;另一方面,黑客正在(其实已经)产业化,只要肯“出血”,任何人都可以雇佣专职黑客,或者直接“购买”黑客服务,从而,使自己实质上成为黑客。当然,每个人本来天生就可当红客(虽然水平可能很差),绝对愿意保护自己的信息系统,比如,为自己的系统配备安全保障设施,或直接“购买”红客服务等。当然,本文中的“人”,既可以是自然个人,也可以是目标一致的任何群体,比如,法人机构、团队等利益共同体等。下面,有时也用“用户”来表示“人”。

用 H 表示所有可能用户的集合,它当然是一个有限集,虽然人数(用 $\#H$ 来表示)可能很多。对每个用户 $h \in H$ 来说,他又可能拥有多个规模不同、价值不同、安全度不同的信息系统,比如,他有自己的网银帐号、社交帐号、电子邮件系统、个人电脑、办公自动化系统、甚至还有大型的网络应用信息系统等。这里的“系统”采用了贝塔朗菲(一般系统论创始人)的定义,即,系统是相互联系、相互作用的诸元素的综合体;或者,更形象地说,系统是能够完成一种或者几种功能的多个部分按照一定的秩序组合在一起的结构。所以,信息系统的个数非常多,但是,始终是有限的。

为了公平起见(因为,每个人的攻防水平各不相同),再假定:每个用户都不亲自动手从事攻防活动,而是雇佣一批能力完全相同的、不带感情色彩的机器黑客(红客)来帮忙。这个假定是合理可行的,因为,如果某人的攻防水平特别高,那么他可以将其能力“出售”给机器黑客(红客),并收取其应有的报酬;而对那些攻防水平差的人,他就没有这部分收入了,所以,其公平性是有保障的。

当然,机器黑客得根据被攻击系统的安全程度,来公平地向用户收取雇佣费,而且对这些用户是“童叟无欺”,即,收费不会因人而异;此外,机器黑客还很仁慈,它允许用户毁约,即,当它受雇将某个信息系统攻破后,在向雇主收取佣金时,如果雇主觉得要价太高了,那么,它可以降价,甚至雇主想给多少就给多少,绝不讨价还价;但是,如果雇主出价低于攻击成本,那么机器黑客将把该系统原样归还给原来的主人;如果雇主出价高于攻击成本,那么机器黑客交付给雇主的也只是一个“装有被攻破系统的、且定时才能打开的信

封”。但是,请注意,如果雇主甲给钱较少,若另一雇主乙却想以高一点的价来购买“甲刚刚获得的信封”时,机器黑客会毫不犹豫地重新攻破雇主甲,把这个信息系统装入另一个“定时才能打开的信封中”,卖给雇主乙;如此往复,直到所有用户不再有攻击意愿为止。还要假定,机器黑客很老实,只有受雇后,它才对目标系统发动攻击,而且自己从不主动攻击,更不会获取除佣金之外的其它收入。

每个人的网上资金(网下资金,比如,不动产等,不在此处的考虑之列)被分割成三个部分:一部分,称为建设费,用于建设自己的信息系统,当然包括购买防火墙等和支付给红客的安全保护费等;一部分,称为攻击费,用于雇佣机器黑客,攻破自己想要的、别人的目标信息系统;一部分,称为业务费,用于自己的各信息系统中网络业务的正常开销,比如,存放在“支付宝”中的散银、存放在微信红包中的钢鏰儿等。

对专业红客来说,他的大部分网上资金,都分配给了建设费,意在构筑牢不可破的安全防线。对专业黑客来说,他的大部分网上资金,都分配给了攻击费,意在攻破别人更多的系统,获取更多的黑产收入;对没有攻击意愿的普通用户来说,其攻击费预算可能为零,即,他们不发动攻击,只雇佣红客来保护自己的信息系统。对一般人来说,可能建设费、攻击费和业务费都各分配了一些;至于到底如何分配,纯粹根据个人意愿而定。此外,业务费是分散存放的,不参与攻防活动,但是,一旦某个信息系统被攻破了,那么,在“定时打开的信封”被启封后,该系统中存放的所有经费,就归其新主人了;当然,万一存放的经费为零,那么就活该新主人倒霉;万一存放的经费巨大,那么新主人就发财了。

好了,现在攻防一体的模型场景就清楚了:每个用户都从机器红客那里买得一批钱袋子,然后,将自己的业务费分装在这些钱袋子里;接着,在身上挂着自己的钱袋子,同时冲入竞技场中;然后,彼此(雇佣黑客)抢夺其它人身上的钱袋子,当然,自己身上的钱袋子也会被别人抢走;等到大家都“抢累了”(即,再也没有抢夺意愿了,这便是那只“看不见的手”的神奇功效,它能安抚大家,停止对抗)后,同时打开自己(抢来或守住)的钱袋子,于是,本轮攻防就结束了。

当然,大家清理完本轮战果后,还将进入下一轮类似的、可能更惨烈的抢夺战。上轮中,如果某人彻底破产了,那他可以自愿退出下一轮对抗(其实,除非弃网,否则只要留在网上,就不可能真正退出下一轮竞争;因为,你不抢别人,别人可以抢你嘛,除非你的钱袋子太不起眼,没人看得上);如果某人发财了,那他可能在下轮竞争中,分配更多的资金给攻击费,从而,成为更凶的黑客;某些人也可能吸取教训,将更多的资金投入建设费,使自己的信息系统更难被机器黑客攻破(于是,机器黑客向雇主收取的佣金就会更高;愿意出此价的人就更少,主人的信息系统就更安全)。下一轮攻防也可能出现一些极端情况,比如,大家都不再分配资金给攻击费了,于是,黑客就消失了;大家都不再分配业务费了,于是,竞争就演变成纯粹的“斗气”了,因为,所有钱袋子都是空的,抢不抢都没啥意思了,就算钱袋子丢了,也不心痛了。

在两轮对抗之间的这段时期,便是大家相安无事的和平期,这应该归功于那只“看不见的手”。

由于机器黑客和机器红客是“一家人”(现实中也是这样的,因为,从技术角度看,红客和黑客也基本上可以是同一帮人;能当黑客就能当红客,反之亦然),所以,在冲进竞技场之前,每个用户对挂在自己身上的所有钱袋子的攻破成本是知道的,它就是其它用户想要(雇佣机器黑客)将其抢走的最低价。但是,每个用户并不知道其它用户身上钱袋子的攻破成本。

设用户集 H 中,所有用户的钱袋子总数为 N(分别编号为 $1,2,\cdots,N$),它当然是一个有限整数,虽然非常巨大。用户 h 身上的钱袋子状况,可以用一个 N 维 2 进制向量 $x=(x_1,x_2,\cdots,x_N)$ 来表示,其中,若 $x_i=1$,则表示此刻第 i 个钱袋子仍然挂在用户 h 的身上;否则,若 $x_i=0$,则表示第 i 个钱袋子在别人身上。设用户 $h\in H$ 给自己预留的攻击费为 r^h,它也是一个 N 维向量,其第 i 个分量的值,表示预算给第 i 个钱袋子的攻击费(如果该分量小于别人身上某个钱袋子的攻击成本价,那么,这个用户就甭想得到别人的这个钱袋子,因此,这笔预算就白花了)。当然,r^h 各分量之和,不该小于该用户 h 冲入竞技场之前,其身上悬挂的所有钱袋子的攻破成本价之和,否则,他就是去“送死”,连自己的“老本”都保不住。

由于用户很多,又由于机器黑客并不讨价还价(只是低于攻破系统的成本价时,就罢工而已),所以,任何用户都没有实力来确定攻破每个钱袋子的佣金价格,而只能被动地接受竞争佣金价格。设某个时刻,攻破第 i 个钱袋子的佣金价格为 p_i,$i=1,2,\cdots,N$,于是,N 维向量 $p=(p_1,p_2,\cdots,p_N)$ 就表示此刻所有钱袋子的攻破佣金价格,当然,这个价格是会随着各用户给机器黑客出价的变化而变化。

在竞技场上,假设每个用户 $h\in H$ 都是理性的,这至少意味着如下两方面:

第一,在佣金向量为 p 时,用户 h 想争取抢到的钱袋子向量 x,一定会满足不等式 $p.\ x=\sum_{i=1}^{N}p_ix_i\leqslant r^h$,即,他的攻击费用预算 r^h 永远不会被突破(此文中,如果 x 和 y 是两个 N 维向量,那么,记号 $x\leqslant y$ 就表示 x

的每个足标,都不超过向量 y 的相应足标)。今后称满足这个预算限制的钱袋子向量 x 为可行向量。形象地说,对交不起佣金的"抢劫计划",用户是不会奢望的。用户 h 的所有可行向量的集合记为 X^h,它显然是空间 R_+^N 中的一个子空间,这里 R_+^N 表示足标全为非负的 N 维向量的集合。

第二,进入竞技场后,每个用户 h 并不会胡乱"抢劫",他们都有自己的"抢钱袋子"偏好 $\angle_h$,这里"$\angle_h$"是 N 维实数空间 R^N 上的一个弱序关系(即,对任何的 N 维向量 x,y,z 都成立如下两条性质:1)自反性,$x\angle_h x$;和 2)传递性,若 $y\angle_h x$ 同时 $z\angle_h y$,那么就有 $z\angle_h x$)。换句话说,如果 x 和 y 都可行的钱袋子向量,但是,它们的偏好关系如果满足 $y\angle_h x$(即,用户 h 更偏好于 x),那么,用户 h 愿意用身上的钱袋子 y 去换取 x。形象地说,如果用户只能从"西瓜"和"芝麻"中选一个的话,他会理性地选择更喜欢的西瓜,而丢掉芝麻;当然,如果允许两者都可同时拥有时,他也决不会客气,因为,他要合理地追求自己的利益最大化。另外还有,1)如果同时满足 $y\angle_h x$ 和 $x\angle_h y$(即,从用户 h 的偏好角度看,y 和 x 并没有哪个占优势,此时也称"x 与 y 无差异",记为 $x\backsim_h y$),那么,他就不会用现有的 x 去换取 y,因为,他没能从中获得额外的利益嘛。2)如果 $y\angle_h x$ 成立,但是不成立 $x\angle_h y$(即,从偏好角度看,x 严格优于 y,记为 $x>_h y$),那么,他就一定会用 x 去换取 y。

关于用户的偏好 $\angle$,我们还可以做如下几个合理的假设:

假设 1(弱单调性 T_1):总有某个可行向量(比如,冲进竞技场之前,h 自己身上的钱袋子向量)是自己看重的,并且,所有钱袋子(无论是自己的还是别人的)都是无害的。准确地说,如果 x 和 y 是用户 h 的两个可行向量,而且 $x>>_h y$(即,在 N 维实向量 x 和 y 中,x 的每个足标,都严格大于 y 的对应足标),那么,就有 $x>_h y$,即,用户 h 严格偏好于 x。

假设 2(连续性 T_2):对每个用户 h 的任意给定的可行向量 x^0,由所有偏好优于 x^0 的可行向量的集合 $A^h(x^0)=\{x:x$ 是 h 的可行向量,并且 $x^0\angle_h x\}$ 是闭集;同时,由所有偏好劣于 x^0 的可行向量的集合 $G^h(x^0)=\{x:x$ 是 h 的可行向量,并且 $x\angle_h x^0\}$ 也是闭集。这里"闭集"是集合论的基本术语,意指包含自身边界的集合。

上面的假设 T_2,虽然看起来有点抽象,它其实暗含了人类的"贪婪性"(即,"上下通吃,能吃的都要吃"),因此也是合理的。具体说来,从任何一个可行向量 x 出发,考虑用户 h 的可行向量集内的一个线段,从优于 x 的一端开始,最终行进到劣于 x 的点(可行向量);该线段必定也包含了与 x 无差异的某点。也就是说,当从优于 x 的点,行进到劣于 x 的点时,必然要触及到无差异点。这便是为什么称该假设为"连续性假设"的原因。

假设 3(严格凸性 T_3):令 $y\angle_h x$(当然,也包含了 $x\backsim_h y$ 的可能性),且 $x\neq y$,$0<a<1$,那么,成立 $ax+(1-a)y>_h y$,即 $ax+(1-a)y$ 严格优于 y。

该假设的数学含义表明"可行向量集内,无差异曲线是严格弯曲的,其内部不存在平坦段";其经济学含义是:不存在完全可替代的"钱袋子向量",这也是日常生活常识。

好了,模型和假设就是这些了。下面开始寻找那只"看不见的手"了。

2 寻找"看不见的手"

每个用户在冲进竞技场之前,身上都挂着自己的钱袋子,而且还有一笔攻击费,这些东西称为他的"初始资源禀赋"。根据日常经验,为在竞技场上增进自身利益,用户们最好自发地组成一个个联盟:在联盟内,即使大家仍然相互抢夺钱袋子,但是,大家却都能获益,即,每个人身上保留的"钱袋子向量"都朝着自己更加偏好的方向发展。若当前联盟不能给某个用户带来偏好度更高的"钱袋子向量",那么,他就可以退出,并加入另一个能给自己带来利益的联盟(当然,也可能是由自己一个人组成的独善其身的联盟)。如此循环,直到所有联盟都最终被融合成一个联盟为止,即,每个用户都再也不能从"抢夺"别人的钱袋子中,获得偏好性更优的"钱袋子向量"了,于是,大家便理性地停止"抢夺",心满意足地结束本轮攻防对抗。下面就来严格证明,确实有一只"看不见的手"能够牵引大家,进入这种休战状态。

定义 1(阻碍):一个联盟,其实就是用户集 H 的任何一个子集。因此,每个用户自己,也可以构成一个单成员联盟。若存在某个联盟 S,及其可行向量集 $\{y^h:h\in S\}$(以下称为"配置")满足如下三个条件,则称某配置 $\{x^h:h\in H\}$ 的建立将会受到阻碍:

条件 1,$\sum_{h\in S}y^h\leqslant\sum_{h\in S}r^h$(这里的不等式意指在向量的各个坐标分量上都成立。提醒:r^h 表示用户 h 的预算攻击费);

条件 2,对所有的 $h\in S$,有 $x^h\angle_h y^h$;

条件 3,对某些 $g\in S$,有 $y^g>_g x^g$,即,按照用户 g 的偏好,他的钱袋子向量 y^g 严格优于钱袋子向量 x^g。

该定义 1 中,"阻碍"的基本思想是:若仅利用联盟 S 内的可得钱袋子资源,则 S 中的某成员(比如那

个 g)就能够获得一个新的“钱袋子向量”(y^g),其偏好程度严格优于他原来的“钱袋子向量”(x^g)(经济学上,称为 g 取得了一个“帕累托改进”),那么,联盟 S 将阻碍配置$\{x^h:h\in H\}$的建立。当联盟 S 考虑实施阻碍时,它只根据自己的资源和偏好来做出决策,而不关心联盟外用户($H\backslash S$)的境况。

定义 2(核):配置核,简称“核”,是指任何联盟 S 都无法阻碍的可行配置所构成的集合。

根据该定义 2,与核相对应的配置具有如下性质:

其 1,核中的所有配置都必须满足个人理性原则,即若$\{x^h:h\in H\}$是一个核配置,则对所有的 $h\in H$,都必有:x^h优于他冲进竞技场之前的钱袋子向量。若没有此性质,则该核将被一个单成员联盟所阻碍,因为他的当前“钱袋子向量”比初始状态还差,此时的核配置违背了个人理性。

其 2,核中的任何配置都不可能再取得“帕累托改进”,也称为是帕累托有效的。若$\{x^h:h\in H\}$不是帕累托有效的,则由所有用户构成的联盟 H 仅需对配置进行再分配,就可增进其成员的偏好满意水平。也就是说,若$\{x^h:h\in H\}$是一个核配置,则对所有其他的可行配置 y^h 来说,对所有的 $h\in H$,有 $y^h\angle_h x^h$或者对某些 $h\in H$,有 $x^h>_h y^h$。所有其他的可行配置 y^h都必须满足这一性质,否则,核配置将被由所有用户构成的联盟 $S=H$ 所阻碍。

该性质的等价解读是:如果用户的“钱袋子向量”处于核配置状态,那么,所有用户就都达到了自己的最理想状况(因为,其偏好不可能再获得改进,即,达到了帕累托有效状况),因此,理性将提醒大家:可以休战了。但是,核配置状态能否达到呢? 因此,下面就来证明:核配置状态是能够达到的。为此,引入如下竞争性均衡定义。

定义 3　若以下条件得到满足,则对每个 $h\in H$,$p\in R_+^N$,$x^h\in R_+^N$,就构成了一个竞争性均衡(回忆提醒:这里 $p=(p_1,p_2,\cdots,p_N)$,其中 p_i是机器黑客攻破第 i 个钱袋子的佣金价格;而 R_+^N是各分量都非负的 N 维向量集合):

(1)对每个 $h\in H$,均有 $p.\ x^h\leqslant p.\ r^h$;

(2)对所有的 $y\in R_+^N$,有 $y\angle_h x^h$,且满足条件 $p.\ y\leqslant p.\ r^h$;

(3)$\sum_{h\in H}x^h\leqslant\sum_{h\in H}r^h$(不等式在各个坐标分量上均成立),若存在满足不等式严格成立的坐标分量 $k=1,2,\cdots,N$,则有 $p_k=0$。

从定义 3 开始,此文中运算符号“.”表示两个向量的“点积”运算。

定理 1(竞争性均衡含在核中):若用户偏好∠满足弱单调性(T_1)和连续性(T_2),并令 $p,x^h,h\in H$ 是一个竞争性均衡,则配置$\{x^h,h\in H\}$包含在核中。

证明　用反证法。假设定理的命题是错的,则存在一个阻碍原始配置建立的联盟 S 和某个更优配置 $y^h,h\in S$。于是由联盟的可行性,我们有:$\sum_{h\in S}y^h\leqslant\sum_{h\in S}r^h$;而且,对所有的 $h\in S$,有 $x^h\angle_h y^h$;对某些 $g\in S$,有 $y^g>_g x^g$。

但是,由于 x^h是一个竞争性均衡配置。也就是说,对所有的 $h\in H$,$p.\ x^h=p.\ r^h$,且对所有使得 $p.\ y\leqslant p.\ r^h$ 满足的 $y\in R_+^N$,都成立 $y\angle_h x^h$。

注意到$\sum_{h\in S}p.\ x^h=\sum_{h\in S}p.\ r^h$,因而,对所有的 $h\in S$,有 $p.\ y^h\geqslant p.\ r^h$。这就是说,x^h代表了用户 h 在佣金预算约束下,最希望得到的“钱袋子向量”。在满足单调性假定(T_1)的偏好 $\angle h$ 下,y^h至少与 x^h一样好,因此,y^h所需的佣金成本不低于 x^h。更进一步地,对 g,我们必定有 $p.\ y^g>p.\ r^g$。因而有:$\sum_{h\in S}p.\ y^h>\sum_{h\in S}p.\ r^h$(注意,这是一个严格不等式)。然而,由联盟的可行性得知,我们必定还有:

$$\sum_{h\in S}y^h\leqslant\sum_{h\in S}r^h$$

因为 $p\geqslant 0$,$p\neq 0$,故有 $\sum_{h\in S}p.\ y^h\leqslant\sum_{h\in S}p.\ r^h$。配置$\{y^h,h\in S\}$在资源总量上小于或等于初始资源禀赋,但与此同时,以佣金价格 p 衡量时,又比初始资源禀赋的价值高,这就出现了矛盾。该矛盾使定理的原命题得证,证毕。

在微观经济学中,已经证明了竞争性均衡的存在性(比如,文献[20]中的定理 7.1,定理 11.1 和定理 17.7 等),因此,由此处的定理 1 就知,核配置集是非空的,换句话说,H 中的所有用户都能获得自己偏好度最高的钱袋子向量。即,正是那只“看不见的手”,将用户们一步步地牵引到各自最偏好的钱袋子向量。

其实,如果对偏好再加一些限制,那么,上述定理 1 的逆也是成立的,即,核中的配置,也达到竞争性均衡。为此,虽然用户集 H 已经很大了,但是,我们还要通过复制手段,将其变得更大,从而挖掘出更深刻的结果。

我们将讨论一个由用户集 H(后面称为原始用户集),复制 Q 倍后所得到的更大型的用户集,并将其标记为 QH。这里 Q 是一个正整数($Q=1,2\cdots,n$)。原始用户集里,用户 $h\in H$ 的初始攻击费禀赋为 r^h,偏好为 $\angle_h$。用户集被复制 Q 倍后,用户数也增加为原来的 Q 倍;并且,其中有 Q 个用户的偏好和初始攻击费禀赋分别为$\angle_1$和 r^1,有 Q 个用户的偏好和初始攻击费禀赋分别为$\angle_i$和 r^i,$i=1,2,\cdots,\#H$(初始用户集 H 中的元素个数,或初始用户数)。于是,原来的每个用户 $h\in H$,被扩展成了一类用户。在复制用户集 QH 中,有 Q

个 h 类的用户。请注意,H 的竞争性均衡佣金价格,仍然是复制用户集 QH 中的均衡佣金价格。在原来 H 中,用户 h 的竞争性均衡配置 x^h,则是复制用户集 QH 中,处于竞争性均衡时,所有 h 类用户的均衡配置。复制用户集 QH 中,以类型和序号来标记各用户。这样,对所有的 $h\in H, q=1,2,\cdots,Q$,标记为 h,q 的用户,表示 h 类用户中的第 q 个用户。

定理 2(核中成员的平等性):若偏好满足 T_1,T_2,T_3,令 $\{x^{h,q},h\in H,q=1,2,\cdots,Q\}$ 是复制用户集 QH 中的核,则对每个 h,$x^{h,q}$,对所有的 q 都是相同的,也就是说,对每个 $h\in H,q\neq g$,有 $x^{h,q}=x^{h,g}$。

证明 由于核配置必须是可行的,所以有:$\sum_{h\in H}\sum_{q=1}^{Q}x^{h,q}\leqslant\sum_{h\in H}\sum_{q=1}^{Q}r^h$ 或等价地说,有:

$$\sum_{h\in H}\sum_{q=1}^{Q}x^{h,q}\leqslant Q\sum_{h\in H}r^h$$

下面用反证法。假若该定理是错的。考虑 h 类用户,则有 $x^{h,q}\neq x^{h,g}$。注意到,对 h 类用户来说,他们的偏好是各不相同的,即要么 $x^{h,q}\succ_h x^{h,g}$,要么相反 $x^{h,g}\succ_h x^{h,q}$。由核配置的帕累托有效性与 T_3 即可获得这一性质。若从偏好角度来看,$x^{h,q}$ 和 $x^{h,g}$ 无差异,由 T_3 可知有:$[(x^{h,q}+x^{h,g})/2]\succ_h x^{h,q}\backsim_h x^{h,g}$。这意味着配置 $\{x^{h,q},h\in H,q=1,2,\cdots,Q\}$ 不是帕累托有效的,因而不在核内。该矛盾说明:必定成立 $x^{h,q}\succ_h x^{h,g}$,或者相反 $x^{h,g}\succ_h x^{h,q}$。因此,对 h 类用户中的每个用户,都可以根据所持有钱袋数量的偏好 $\angle_h$ 来排序。

对每一类 h 用户,令 x^{h*} 表示 h 类核配置 $x^{h,q},q=1,2,\cdots,Q$ 中,偏好优先程度最低的那个。对某 h 类用户,其中每个用户的钱袋子向量都是相同的,此时 x^{h*} 就表示偏好的平均水平。对钱袋子向量不同的类别,x^{h*} 则表示偏好排序水平最低的配置。现在来构造由每类用户中的这样一些用户组成的联盟:该用户的钱袋子向量配置 x^{h*} 在该类用户中的偏好排序最低。我们的证明策略是,这一联盟将阻碍原来的核配置,从而证明了这样的配置不可能真的在核配置集合中。

考虑 h 类用户的核配置偏好排序平均水平,并标记为 b^h,其中,$b^h=(\sum_{q=1}^{Q}x^{h,q})/Q$。由偏好的严格凸性($T_3$)有:对那些 $x^{h,q}$ 不同的 h 类用户,有:

$$b^h=(\sum_{q=1}^{Q}x^{h,q})/Q\succ_h x^{h*}$$

对那些 $x^{h,q}$ 相同的 h 类用户,有:

$$x^{h,q}=b^h=(\sum_{q=1}^{Q}x^{h,q})/Q\backsim_h x^{h*}$$

根据核配置的可行性,我们有:

$$\sum_{h\in H}b^h=\sum_{h\in H}[\sum_{q=1}^{Q}x^{h,q}]/Q=[\sum_{h\in H}\sum_{q=1}^{Q}x^{h,q}]/Q\leqslant\sum_{h\in H}r^h$$

换句话说,由每用户中(偏好排序水平最低)的那个用户组成的联盟,便可达到配置 b^h。对联盟中的每个用户而言,对所有的 h,有 $x^{h*}\angle_h b^h$,而对某些 h,有 $b^h\succ_h x^{h*}$。因而,每类用户偏好排序水平最低的用户组成的联盟,便阻碍了原来的配置 $x^{h,q}$。这便出现了矛盾,从而证明了定理成立。证毕。

为了证明定理 1 的可逆性,我们还要对用户冲进竞技场之前的钱袋子向量,做如下合理假设。

假设 T_4:每个用户 $h\in H$ 的初始禀赋 r^h,都是他的所有可行钱袋子向量集合 X^h 的一个内点(即,不是集合 X^h 的边界点)。如果 $X^h=R_+^N$,则 $r^h\gg 0$,即,对所有 $k=1,2,\cdots,N$,都有 $r_k^h>0$。

该假设的合理性是这样的,如果用户在冲进竞技场前,已经对自己身上的钱袋子向量有最高偏好了(即,r^h 是边界点了),那么,他的最佳策略就应该是:拒绝进入竞技场。换句话说,将他的所有攻击费都转变为建设费,全力以赴保护已有的钱袋子;当然,也可能由于自己力量不够(比如,另有人出价高于他的建设费,来雇佣机器黑客攻击他),那么,他也只能眼睁睁丢掉自己的钱袋子。如果用户对别人的所有钱袋子都感兴趣(即,$X^h=R_+^N$),那么,他当然应该对每个钱袋子都分配一定的攻击费(即,第 k 个钱袋子的攻击费 $r_k^h>0$),否则,机器黑客是不会无赏提供服务的。

引理 1(闵科瓦斯基超平面定理):令 K 是一个凸集,它也是 R^N 的一个子集。若 z 不是 K 的内点,则必存在一个约束 K 的边界穿过 z 的超平面 H。也就是说,存在 $p\in R^N,p\neq 0$,对所有的 $x\in K$,满足 $p.x\geqslant p.z$。

由于该引理 1 是一个现成的数学结论(见文献[20]中的定理 2.11),所以,这里就略去了证明过程。该引理将应用于下面定理 2 的证明过程。

定理 3(德布鲁-斯卡夫定理):若有假定 T_1,T_2,T_3,T_4,并且对所有的 $Q=1,2,\cdots$,令 $\{b^h,h\in H\}\in$ 核(Q),则对所有的 Q,$\{b^h,h\in H\}$ 都是复制用户集 QH 的竞争性均衡配置。

证明 我们将证明存在一个机器黑客的佣金价格向量 p,对每一类用户 h,均满足 $p.b^h\leqslant p.r^h$,并且 b^h 在攻击费的预算约束下,依据偏好 $\angle_h$ 获得最大化的偏好排序。我们的证明策略是,构造一个配置集,它优于 $\{b^h,h\in H\}$。接下来,证明后者是一个有超平面支撑的凸集,取该超平面的法向量为 p,再证明 p 就是支撑 $\{b^h,h\in H\}$ 的竞争均衡价格向量。

对每个 $i\in H$,令 $\Gamma^i=\{z:z\in R^N,z+r^i\succ_i b^i\}$。向量集 Γ^i 是 i 类用户的一个配置集,对该类用户,其配置的偏好,严格好于 b^i-r^i。根据配置 b^i-r^i,用户可以达到核配置状态。现在定义一族 Γ^i 集,$i\in H$ 的凸结合集(凸壳)。令

$$\Gamma=\{\sum_{i\in H}a_iz^i:z^i\in\Gamma^i,\ a_i\geqslant 0,\ \sum a_i=1\}$$

表示更优的配置集 Γ^i 凸结合而得的集合。集合 Γ 是

集合 Γ^i 的并集的凸壳。

现在再证明:由集合 Γ^i 构成的集类 Γ 严格排列在穿过原点的超平面上方。该超平面的法向量就是要寻找的均衡佣金价格向量。

首先证明 0 不属于 Γ。其证明方法是,将 $0\in\Gamma$ 的概率与构造一个阻碍核配置 b^i 的联盟的概率相对应,而后者是一个矛盾,概率为 0。假设 $0\in\Gamma$,由假定 T_3(偏好的连续性)可知,对每个 i,Γ^i 总是开集,因而,Γ 也是开的(为方便计,此处忽略了 Γ^i 与由 X^i 导引的边界相重合的那一部分区域。更准确地说:在假定 T_1 和 T_3 下,Γ^i 与 Γ 具有非空内部域,并且,0 不属于内部域(Γ)。若 $0\in\Gamma$,则在 0 附近存在一个含于 Γ 中的 ε 邻域($\varepsilon>0$)。Γ 中的典型元素可表示为 $\sum a_i z^i$,其中 $z^i\in\Gamma^i$。令 R_-^N 表示 R^N 的非正象限,取交集 $\Gamma\cap R_-^N$,也就是说,取 Γ 的非正部分。选择 $z\in\Gamma\cap R_-^N$,满足 $z=\sum a_i z^i$,其中,对所有的 i,a_i 都是有理数。这是可能的,因为 $\varepsilon>0$,我们可以用有理数序列来任意逼近所有真实的 a_i。接着,找 a_i 的公分母。考虑取 a_i 的公分母为 Q(大倍数 Q 复制的用户集可克服单个用户的不可分问题),我们有 $\sum a_i z^i\leqslant 0$(在各坐标分量上成立)。还须证明的是,由前述结论可知:存在一个联盟,它阻碍配置 b^i 在复制用户集 QH 中的建立,其中,Q 为 a_i 的公分母。构造一个联盟 S,它由 Qa_i(整数)个 $i(i\in H)$ 类用户集合中的用户组成。考虑 S 中用户的配置为 $d^i=r^i+z^i$。根据 Γ^i 的定义,有 $d^i>_i b^i$。由 $\sum a_i z^i\leqslant 0$,有 $\sum(Qa_i)z^i\leqslant 0$,从而,得到 $\sum(Qa_i)(d^i-r^i)\leqslant 0$,或等价地,$\sum(Qa_i)d^i\leqslant\sum(Qa_i)r^i$,这意味着 d^i 在 S 中是可行的。根据用户 $i\in S$ 的偏好,d^i 是 b^i 的一个增进。从而,S 阻碍 b^i,这就出现了矛盾。因此,只能有:0 不属于 Γ。

在证明了 0 不属于 Γ 后,还需要证明 0 不是非常靠近 Γ。的确,当 $0=\sum_{h\in H}(b^h-r^h)$ 时,$0\in\Gamma$ 的边界,其中等式右边是 Γ 的闭包。因而,0 正好表示了这样一个边界点,穿过该边界点,就可得到引理 1 中的支撑超平面。集合 Γ 是一个凸集,所以,由引理 1,存在 $p\in R^N$,$p\neq 0$,对所有 $v\in\Gamma$,满足 $p.v\geqslant p.0=0$。根据弱单调性假设 T_1,有 $p\geqslant 0$。现在,由于对每个用户 h 都有 (b^h-r^h) 属于 Γ 的闭包,所以有,$p.(b^h-r^h)\geqslant 0$。但是,由于同时还有 $\sum_{h\in H}(b^h-r^h)=0$,进而有 $p.\sum_{h\in H}(b^h-r^h)=0$。因此,对每个用户 h,有 $p.(b^h-r^h)=0$,等价地,$p.b^h=p.r^h$。这实际上就是说,

$$p.0=p.\sum_{h\in H}[b^h-r^h]/\#H=inf_{x\in\Gamma}(p.x)$$
$$=\sum_{h\in H}[\inf(p.z^h)]/\#H$$

这里的 #H,表示用户集 H 中用户的个数;而最后一个等式中 inf( ) 是对满足 $z^h\in\Gamma^h$ 的所有可能 z^h 而言的(主要是为了减少足标的层次)。所以,$p.(b^h-r^h)=\inf(p.z^h)$。

这样,对每个用户 h 和 $y\in\Gamma^h$,有 $p.(b^h-r^h)=\inf(p.y)$。等价地,b^h 依据偏好程度 $b^h\angle_h x$ 最小化 $p.(x-r^h)$。此外,$p.b^h=p.r^h$。进一步地,根据假设 T_4 可知,b^h 附近存在一个 ε 邻域包含于 X^h 中。根据假设 T_1,T_2 和 T_4 可知,“偏好约束下的佣金最小化”等价于“佣金约束下的偏好排序最大化”,从而,b^h,$h\in H$ 就是一个竞争性均衡配置,证毕。

3　结束语

利用经济学的“一般均衡理论”来研究网络空间安全对抗时,最大的难点是建立合适的数学模型,而这一点并不容易。比如,经济学中有一个由“供应厂商、家庭消费方、股份分配返还”构成的完美的资金流动闭环,而在红客、黑客和用户所构成的体系中,却没有此类闭环。而经济学中的整体优化基础,刚好就是由总供给、总需求(含初始禀赋)相减而获得的“超额需求函数”。可惜在网络空间安全对抗中,完全就找不到此类“超额需求函数”的影子。因此,若无合适的数学模型,根本就不知道该从何处下手。但愿经济学家们,能够利用熟悉各种经济模型的优势,进入网络空间安全领域,倒逼一些特定情况下的安全对抗模型。

本文中几个定理的证明过程,其实是从已知的几个经济学结果(比如,[20]的定理 13.1、定理 14.1 和定理 14.2)中抽丝剥茧而得的。之所以要不厌其烦地“抽丝”,是想保持本文的封闭性,特别是方便网络安全界的读者朋友,使大家不必在“网络空间安全”和“经济学”这两个“八竿子打不着”的领域间,来回反复跳跃。

在《安全通论》之前,人们一直咬定:安全对抗就是“水涨船高”、“鱼死网破”或“魔高一尺道高一丈”等。但是,从本文的结论我们知道,其实安全对抗应该更像“潮汐”:来潮时,惊天动地;退潮后,风平浪静。或者说,安全对抗像“间隙式喷泉”:喷时轰轰烈烈,歇时安安静静。也可以说安全对抗像“拳击摆台赛”:轮中打斗,你死我活;轮间休息,却和平相处。总之,无论用什么现象来容易网络空间安全对抗,关键是要明白:有一只“看不见的手”能够安抚各方,最终达到共赢。因此,红客方应该调整自己的战略,使得:和平期尽可能长一些,并且为下一轮的对抗做足准备。

《安全通论》是一个长期而艰难的课题,它的最高境界应该是:只用一篇短短的论文,甚至只用一个公式,就能道破网络空间安全的核心基础理论。就像仙农仅用一篇论文的两个核心定理(信道编码和信源编

码)就建立了《信息论》那样,就像爱因斯坦仅用一个公式($E=MC^2$)就创立《相对论》那样。可惜,如今,《安全通论》的系列论文却已十数篇了。这刚好说明:《安全通论》还仅仅处于婴儿阶段!但是,任何事情总得有个过程,在初级阶段,我们将用多篇论文,从不同的方面,来归纳网络空间安全的基础理论;然后,在高级阶段,再将这些论文凝练,争取逐步逼近最终目标。

创立《安全通论》虽然很苦,但我们也没忘记苦中寻乐!比如,前段时间,研究工作卡壳了,我们便以最笨的办法,对网络安全的所有分支,又一次进行了地毯式的"轰炸"。并出人意料地,顺便写成了一部喜剧作品《安全简史》,一边供男女老少娱乐,一边也让全社会轻松了解信息安全。

参考文献:

[1] 杨义先,钮心忻,安全通论(1)之"经络篇"[EB/OL]. http://blog. sciencenet. cn/blog-453322-944217. html,2015-12-18.

[2] 杨义先,钮心忻,安全通论(2):攻防篇之"盲对抗"[EB/OL]. http://blog. sciencenet. cn/blog-453322-947304. html,2016-01-01.

[3] 杨义先,钮心忻,安全通论(3):攻防篇之"非盲对抗"之"石头剪刀布游戏"[EB/OL]. http://blog. sciencenet. cn/blog-453322-948089. html,2016-01-04.

[4] 杨义先,钮心忻,安全通论(4):攻防篇之"非盲对抗"之"童趣游戏"[EB/OL]. http://blog. sciencenet. cn/blog-453322-949155. html,2016-01-09.

[5] 杨义先,钮心忻,安全通论(5):攻防篇之"非盲对抗"收官作及"劝酒令"[EB/OL]. http://blog. sciencenet. cn/blog-453322-950146. html. 2016-01-13.

[6] 杨义先,钮心忻,安全通论(6):攻防篇之"多人盲对抗"[EB/OL]. http://blog. sciencenet. cn/blog-453322-954445. html,2016-02-04.

[7] 杨义先,钮心忻,安全通论(7):黑客篇之"战术研究"[EB/OL]. http://blog. sciencenet. cn/blog-453322-956051. html. 2016-02-14.

[8] 杨义先,钮心忻,安全通论(8):黑客篇之"战略研究"[EB/OL]. http://blog. sciencenet. cn/blog-453322-958609. html. 2016-02-25.

[9] 杨义先,钮心忻,安全通论(9):红客篇[EB/OL]. http://blog. sciencenet. cn/blog-453322-960372. html. 2016-03-04.

[10] 杨义先,钮心忻,安全通论(10):攻防一体的输赢次数极限[EB/OL]. http://blog. sciencenet. cn/blog-453322-984644. html,2016-06-14.

[11] 杨义先,钮心忻,安全通论(11):信息论、博弈论与安全通论的融合[EB/OL]. http://blog. sciencenet. cn/blog-453322-989745. html,2016-07-11.

[12] 杨义先,钮心忻,安全通论(12):对话的数学理论[EB/OL]. http://blog. sciencenet. cn/blog-453322-993540. html,2016-07-30.

[13] 杨义先,钮心忻,安全通论(13):沙盘演练的最佳攻防对策计算[EB/OL]. http://blog. sciencenet. cn/blog-453322-1000428. html,2016-09-02.

[14] 杨义先,钮心忻,安全通论(14):病毒式恶意代码的宏观行为分析[EB/OL]. http://blog. sciencenet. cn/blog-453322-1001684. html,2016-09-08.

[15] 杨义先,钮心忻,安全通论(15):谣言动力学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1003586. html. 2016-09-18.

[16] 杨义先,钮心忻,安全通论(16):黑客生态学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1005963. html,2016-09-30.

[17] 杨义先,钮心忻,安全通论(17):网络安全生态学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1007253. html,2016-10-07.

[18] 杨义先,刷新你的安全观念[EB/OL]. http://blog. sciencenet. cn/blog-453322-983276. html,2016-06-08.

[19] 亚当·斯密,郭大力,王亚南. 国民财富的性质和原因的研究(简称《国富论》)[M]. 北京:商务印书馆,1972.

[20] 罗斯·斯塔尔. 一般均衡理论[M]. 鲁昌、许永国,译. 上海:上海财经大学出版社,2003.