文章编号: 2096-1618(2017)03-0231-08
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(17)

——网络安全生态学

杨义先, 钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:一说起网络空间安全治理,几乎每个领导(特别是大领导)都会脱口开出“药到病除”的祖传秘方:抓生态嘛! 但是,到底什么才是网络安全的生态? 可能从来就没人认真思考过,顶多搞一些诸如“管理+技术+法规+教育+…”等定性的综合配套措施而已,这些显然只是皮毛。本文首次定量地研究了,黑客、红客和用户同时并存的复杂网络空间的生态学问题。重点包括:黑客与用户形成的“狮子与牛羊”般的狩猎与被猎生态平衡问题;黑客与红客形成的“牧民与狮子”般的竞争性生态平衡问题;用户与红客形成的“牧民与牛羊”般的互惠互利生态平衡问题;黑客、红客和用户三方共同形成的“狮子、牧民和牛羊”般的捕猎、竞争和互惠共存的复杂生态平衡问题。

doi:10.16836/j.cnki.jcuit.2017.03.001

0 引言

从安全角度来看,在网络空间中主要生活着三种生物:黑客、红客和网络普通用户(简称“用户”)。他们彼此相互作用:或互为竞争(黑客与红客);或为捕猎与被猎(黑客与用户),或互惠互利(红客与用户)。而网络安全生态学就是要仿照古老的生物生态学,用数学模型,从数量上来描述黑客、红客和用户的生存与环境关系,并以此解释一些宏观现象,为确保网络空间安全提供战略借鉴。

为什么能够把黑客、红客和用户当作生物来看待呢?

因为,一方面,他们的功能与角色完全取决于所使用的工具(包括硬件和软件)。比如,依靠黑客工具行事的人,当然就是黑客了;没有工具的黑客,也就不再是黑客了。

另一方面,他们都拥有共同的预装(或预配)基础设施(包括基础软件和核心硬件等,比如,操作系统和CPU等),而其主要区别只体现在更上层的自选应用工具方面。

第三方面,几乎每一种自选应用工具的扩散,都具有口口相传的特性,即,当某人拥有并使用了某应用工具后,如果满意,他会向其朋友推荐;而其朋友中,又有一些人会跟进(拥有并使用该工具,相当于“儿子代工具用户”),甚至再向其朋友推荐;这些朋友中,也许再有一些人跟进(产生了“孙子代工具用户”);如此反复推进,最终,该工具使用者数量的增加模式就完全等同于生物的繁殖模式了。由于这些工具使用者的代际很密集,数量也很大,所以,可以用连续函数来表示任何时刻用户的密度(或数量)。

如果我们把拥有并使用 N 个工具的活人隐去,而只把他等同于这 N 个工具的集合的话,由于这些(非基础设施的)应用工具都是像生物一样繁殖的,那么,由黑客、红客和用户组成的活人网络世界,也就等同于一个软、硬件工具世界,而每一种工具就等同于一种生物。当某工具正被使用时,那就相当于该生物个体是活的;当该工具被主人卸载、放弃或被毁坏(比如,被黑客攻破等)后,就相当于该生物个体死亡了;当该工具虽未被放弃但也暂未被使用时,就相当于该生物个体迁出了;当该工具重新又被使用后,就相当于该生物个体迁入了;当该工具被淘汰后,就相当于该物种灭绝了等。

从安全功能角度看,所有这些生物都可以分为三大类:从事破坏活动的黑客类工具、从事与黑客对抗的红客类工具、从事建设事业的用户类工具。为习惯计,我们仍然用黑客、红客和用户来表示这些工具。更形象地说,在网络空间这个大草原上,生存着食肉类的黑客(并不再细分狮子、狼或豹)、食草类的用户(并不再细分牛、羊或大象等)和牧民红客(并不再细分其肤色、信仰或民族。注意,这里说的是“牧民”而非“猎人”,因为,猎人与狮子的关系不是红客与黑客之间的竞争关系,而是捕猎与被猎的关系,这就与黑客和用户之间的关系重复了)。本文试图利用生态数学来演绎

网络草原上,黑客、红客和用户的恩怨情仇、此消彼长的生死故事。

文献[16]曾专注于黑客生态学,为避免不必要的混乱,那时始终假定“只有一种黑客工具”。但是,相关的思路和结果其实对“多种黑客工具”仍然有效,因为,虽然每一种黑客工具形成了一个生物群体,但由多个黑客工具形成的多个生物群的大目标基本上是一致的,即,躲过红客,侵略用户。所以,站在食草动物的角度,就没必要区分黑客到底是狮子还是花豹了。

文献[16]建立的黑客生态学,其实不仅仅限于黑客,它既是“红客生态学”,也是“用户生态学”,反正,它可以是任何一群大目标基本一致的“单种群动物”的生态学。但是,当黑客和用户被放在一起时,就相当于将狮子和牛羊放一起了,这时无论如何也不应该再将它们视作同一个种群了,所以,文献[16]就失效了,就必须再次借鉴古老的生物生态学,来为它们建立“多种群生态学”。

由于黑客、红客和用户的生存状态相差很大,所以,本文分别根据“黑客+用户”、“黑客+红客”、“红客+用户”、“黑客+红客+用户”等情况,来考虑两种群和三种群的安全生态学。

再次强调,本文研究的是工具,而不是活人,所以,当某个活人同时拥有和使用多个黑客工具、红客工具和用户工具时,我们便将此人割裂成多个虚拟人的集合体,让虚拟人各自扮演黑客、红客和用户的角色。

1 “黑客+用户”生态学

在黑客、红客和用户三者间的所有可能两种群(“黑客+用户”、“黑客+红客”、“红客+用户”)生态学中,“黑客+用户”的生态学最为重要,因为,黑客的真正第一攻击目标是用户,用户的敌人是黑客。所以,我们首先来认真研究“黑客+用户”生态学;而在随后几节中,对其他几个两种群生态学,只做简要介绍。

从生物类比来看,黑客与用户的关系恰如捕猎与被猎:当某黑客成功攻破某用户的系统后,就相当于该用户被猎,我们也说该用户个体死了。作为食肉动物的黑客,在用户这个食草动物面前,当然有绝对优势。在缺乏红客的场合下,用户只能依靠自身防御和运气,努力逃脱黑客的追杀,而不能回击(否则就是红客了)。

设 $x(t)$ 和 $y(t)$ 分别是 t 时刻用户和黑客的密度(或个数),由于它们都具有生物繁殖特性,即,当它们单独生存时,用户的密度 $x(t)$ 满足动力学方程 $(1/x)\,dx/dt=r_1-f_1(x)$,而黑客的密度 $y(t)$ 也满足 $(1/y)\,dy/dt=r_2-g_2(y)$(见文献[16])。但是,当用户和黑客混居时,它们密度的变化不但要遵守自己的规律,而且,还要受另一方的影响。若设相应的影响函数分别为 $g_1(y)$ 和 $f_2(x)$,那么,用户与黑客相互作用的动力学模型,就可表示为如下的微分方程组:

$(1/x)\,dx/dt=r_1-f_1(x)-g_1(y)$ 和 $(1/y)\,dy/dt=r_2-g_2(y)+f_2(x)$

这里和今后,为简捷计,在不引起混淆的情况下,都用 x 代表 $x(t)$,用 y 代表 $y(t)$;而且,各 $f_i(x)$ 和 $g_i(y)$ $(i=1,2)$ 都假定是非负值函数。其中,第一个方程里的“$-g_1(y)$”是因为黑客攻击造成用户减损而致;第二个方程里的“$+f_2(x)$”是因为用户死亡为黑客提供了生存机会(食物)的原因。

1.1 黑客与用户相互线性影响时的生态平衡性

在最简单的情况下,可假定影响函数 $f_i(x)$ 和 $g_i(y)$ 都为线性函数,于是,“黑客+用户”的生态方程为如下 Lotka-Volterra 模型:

$dx/dt=x(a_{10}-b_{11}x-b_{12}y)$ 和 $dy/dt=y(a_{20}+b_{21}x-b_{22}y)$

这里的各个系数 b_{ij} $(i=1,2)$ 均为非负。当 $b_{11}>0$ 时,称用户为密度制约的;当 $b_{11}=0$ 时,称用户为非密度制约的。同理,当 $b_{22}>0$ 时,称黑客是密度制约的;当 $b_{22}=0$ 时,称黑客为非密度制约的。a_{10} 和 a_{20} 分别表示用户和黑客的生长率(出生率减死亡率)。若记 $k=b_{21}/b_{12}$,那么,上述生态方程可重写为:

$dx/dt=x(a_{10}-b_{11}x)-b_{12}xy$ 和 $dy/dt=y(a_{20}+kb_{12}x-b_{22}y)$

由此可见,第一个公式中的 $b_{12}xy$ 表示的含义是:单位时间内用户被黑客攻破的数目,形象地说,在单位时间内用户被黑客吃掉的数目;而黑客的当前数目为 y,所以,$b_{12}x$ 表示每个黑客在单位时间内攻破用户的数目,或形象地称为黑客的捕食率(这里当然暗含捕食率为正),它表示黑客攻击用户的能力。

令上述生态方程的右边等于 0,于是,得到两条直线:

$$L1:a_{10}-b_{11}x-b_{12}y=0 \text{ 和 } L2:a_{20}+b_{21}x-b_{22}y=0$$

如果这两条直线在第一象限内有一个交点 (x',y')(即,该交点的坐标满足 $x'>0$,$y'>0$),那么,根据 Routh-Hurwits 稳定性条件(见文献[18]),有:

渐近稳定性引理:若 $b_{11}b_{22}+b_{21}b_{12}>0$ 并且 $b_{11}x'+b_{22}y'>0$,那么,平衡点 (x',y') 是渐近稳定的,即,无论因何原因,如果用户和黑客的数量偶然落进了 (x',y') 点附近,那么,用户和黑客的数量将最终趋于 x' 和 y'。

那么,什么情况下,这种偶然会变成必然呢?答案之一就是如下,

双密度制约的生态平衡定理(见文献[18]的定理

3.1):如果 $b_{11}>0$ 和 $b_{22}>0$ 同时成立(即,用户和黑客都是密度制约的),那么,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x' 和 y',从而达到生态平衡。

另一个更强的答案(见文献[18]的定理 3.2)是黑客密度制约的生态平衡定理:即使对用户没有密度制约(这对弱者是公平的),即,$b_{11}=0$ 和 $b_{22}>0$(此时 $b_{21}b_{12}>0$ 天然成立),那么,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x' 和 y',从而达到生态平衡。此时,在黑客只攻击本群用户的假定下(即,黑客不迁出),则用户和黑客的生态模型变成如下:

$$dx/dt=x(b-b_{12}y) \text{ 和 } dy/dt=y(-d+Eb_{12}x-b_{22}y)$$

其中各参数均为正常数,b 是用户的出生率,d 是黑客的死亡率,E 是因为用户被攻破而给黑客做的贡献率。此时,唯一的正平衡点(x',y')是

$$x'=(bb_{22}+db_{12})/[E(b_{12})^2] \text{ 和 } y'=b/b_{12}$$

并且它还是全局稳定的,即,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x'和 y',从而达到生态平衡,这便是黑客无迁出时的生态平衡定理。

如果考虑黑客的迁出行为(比如,或者暂不攻击,或者转向攻击本群之外的其它用户),那么,用户和黑客的生态方程变成:

$$dx/dt=x(b-b_{12}y) \text{ 和 } dy/dt=y(f+Eb_{12}x-b_{22}y)$$

这里各参数也为正常数,方程的非平凡平衡点(x',y')

$$x'=(bb_{22}-fb_{12})/[E(b_{12})^2] \text{ 和 } y'=b/b_{12}$$

$f>(bb_{22})/b_{12}$时,$x'<0$,在这种情况下,第一象限中的所有解都趋于$(0,f/b_{22})$,从而导致用户被全部攻破,即,用户灭绝;如果$f<(bb_{22})/b_{12}$,则非平凡平衡位置为正,此时,这个正平衡点是全局稳定的,即,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x'和 y',从而达到生态平衡。这便是有黑客迁出时的用户灭绝与生态平衡定理。

前面的几个结论都基于合理的假定:强者(黑客)受密度制约,而弱者(用户)则不受密度制约。为了理论的完整性,如果我们非要做相反的假定,即,弱者(用户)受密度制约,而强者(黑客)反而不受密度制约,那么,此时"用户+黑客"的生态方程变成:

$$dx/dt=x(b-b_{11}x-b_{12}y) \text{ 和 } dy/dt=y(-d+Eb_{12}x)$$

这里各参数也为正常数,它们的非平凡平衡位置(x',y')为 $X'=d/(Eb_{12})$ 和 $y'=(bEb_{12}-db_{11})/[E(b_{12})^2]'$。如果,$bEb_{12}>db_{11}$,即,平衡点为正,那么,此时,该正平衡点是全局稳定的,即,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x'和 y',从而达到生态平衡。这便是用户密度制约生态平衡定理。

另外,无论是用户还是黑客,都会遇到一些意外情况造成其个体数量的减少,比如,设备的常规升级换代,会造成当前正常用户的减少;公安机关对黑客的专项打击活动,会造成黑客的意外减少等。如果在上述的生态方程中,考虑到这种减员因素(假定被减少的是常数),那么,相应的"用户+黑客"生态方程就可变为

$$dx/dt=x(b-b_{11}x-b_{12}y)-F \text{ 和 } dy/dt=y(-d+Eb_{12}x)-G$$

此时,便有如下,

有意外减损时的生态平衡定理(见文献[18]的定理 3.32):如果该方程组存在正平衡点(x',y'),并且 $F\geqslant 0$,$G\geqslant 0$,那么,(x',y')是全局稳定的,即,无论最初有多少个用户和黑客(当然暗含为正),它们最终的数量都会趋于 x'和 y',从而达到生态平衡。

下面在特殊情况 $G=0$,$F>0$ 下,对该定理给出较形象的解释。此时,平衡点(x',y')为 $x'=d/(Eb_{12}')$ 和 $y'=[1-b_{11}d/(Eb_{12})-EFb_{12}/d]/b_{12}$,因而,只有当 $F<F'$ 时,才有 $y'>0$,这里 $F'=d[b-b_{11}d/(Eb_{12})]/(Eb_{12})$,从而$(x',y')$是全局稳定的。当 $F>F'$时,将导致用户灭绝,故称 F'临界减损率。

1.2　用户和黑客的一般生态平衡性

上一小节的所有结果,都有一个假设前提,即,用户与黑客数量相互之间的影响是线性的。该线性假定的优点是简捷、深入,并且在许多情况下,它确实能够较好地逼近真实结果;而且,根据工程经验,人们能够从实际案例中获得的许多数据也只能是各种比率等,这就暗含了线性假设。

当然,线性假设的局限也是显然的,所以,本小节试图考虑更一般的情况。

用户和黑客相互影响的最一般模型是如下的 Kolmogorov 模型:

$$dx/dt=xF_1(x,y) \text{ 和 } dy/dt=yF_2(x,y)$$

假如曲线 $F_1(x,y)=0$ 和 $F_2(x,y)=0$ 只有一个正交点(x',y'),即,$x'>0$ 和 $y'>0$,它又称为正平衡点。由 Taylor 定理,便可将上述一般模型分解为:

$dx/dt=x[(x-x')\partial F_1/\partial x+(y-y')\partial F_1/\partial y]$ 和 $dy/dt=y[(x-x')\partial F_2/\partial x+(y-y')\partial F_2/\partial y]$

这里分别记偏微分值 $F_{11}=\partial F_1/\partial x$ 、$F_{12}=\partial F_1/\partial y$ 、$F_{21}=\partial F_2/\partial x$ 和 $F_{22}=\partial F_2/\partial y$。

设用户和黑客形成的生态环境,满足如下条件:

A1:$F_{12}<0$(用户受到黑客的抑制);

A2:$F_{21}>0$(黑客得到用户的给养,即,黑客靠攻击用户获利而生存);

A3:当 $y=0$ 时,$F_{11}<0$(若无黑客,用户是密度制约的);

A4:$F_{22}<0$(黑客增长是密度制约的);

A5:存在常数 $A>0$,使得 $F_1(0,A)=0$(A 为用户不存在时,黑客的临界密度);

A6:存在常数 $B>0$,使得 $F_1(B,0)=0$(B 为无黑客时,用户的负载容量);

A7:存在常数 $C>0$,使得 $F_2(C,0)=0$(C 为无黑客时,用户的下临界密度);

A8:$yF_2\leqslant\alpha[xF_1(x,0)-xF_1(x,y)]-\mu y$(即,黑客的增长只依靠它攻破用户的供给,其中,方括号[ ]内表示单位时间内,黑客攻破用户的数量;α 和 μ 是正常数,并且 α 表示黑客的最快攻击系数,μ 表示最小死亡率)。

定义集合 $Q=\{x\geqslant 0,y\geqslant 0\}$ 是全部第一象限,$Q_0=\{x>0,y>0\}$。设 F_1 和 F_2 在 Q 内是连续函数,而在 Q_0 是一阶可导函数,并且它们满足如下两组条件:

条件 P1(a) 存在一个 $x'>0$,使得$(x-x')F_1(x,0)<0$,对所有 $x\geqslant 0$ 且 $x\neq x'$;

条件 P1(b) 存在一个 $y'>0$,使得$(y-y')F_1(0,y)<0$,对所有 $y\geqslant 0$ 且 $y\neq y'$;

条件 P1(c) 偏微分满足$\partial F_1/\partial y<0$ 在集合 Q_0 内;

条件 P1(d) 对每一点$(x,y)\in Q_0$,有 x 8 1$F_1$3/∂x-8 A 3$y\partial F_1/\partial y<0$。

条件 P2(a) 存在一个 $x''>0$,使得$(x-x'')F_2(x,0)>0$,对所有 $x\geqslant 0$ 且 $x\neq x''$;

条件 P2(b) 偏微分满足$\partial F_2/\partial y\leqslant 0$ 在集合 Q_0 内;

条件 P2(c) 对每一点$(x,y)\in Q_0$,有 $x\partial F_2/\partial x+y\partial F_2/\partial y>0$。

根据已知的数学生态学结果(见文献[18]第 3.3 节定理 3.26),可得:

黑客灭绝定理:如果在 Kolmogorov 模型中,函数 F_1 和 F_2 同时满足条件 $P1$ 和 $P''2$,并且设 $x''\geqslant x'$,那么,对所有起始点在 Q_0 内的轨道,当 $t\to\infty$ 时,趋于点$(x',0)$。形象地说,在此种情况下,只要初始时至少有一个用户(当然暗含为正),那么,经过足够长时间之后,黑客将最终灭亡,并且还幸存着 x'个用户。

在 Kolmogorov 模型中还有如下一般性的生态平衡结果(见文献[18]第 3.3 节定理 3.27):

用户与黑客生态平衡定理:如果在 Kolmogorov 模型中,函数 F_1 和 F_2 同时满足条件 P_1 和 P_2,并且还有 $x''<x'$,则在 Q_0 内存在唯一奇点(a,b)。如果(a,b)是不稳定的,则在 Q_0 内至少存在一个周期轨道;若不存在周期轨道,则(a,b)是全局吸引的。形象地说,此种情况下,只要初始时至少有一个用户和黑客(当然暗含为正),那么,经过足够长时间之后,用户数将趋于 a,而黑客数将趋于 b。

2 “黑客+红客”生态学

黑客与红客的关系,当然是你死我活的竞争关系,就像狮子与牧民(注意:不是猎人)的关系:狮子以猎取食草动物(用户)为生,牧民则要保护用户;一般情况下,牧民不会主动去伤害狮子,除非特殊的围猎季节。

设 $x(t)$ 和 $y(t)$ 分别是 t 时刻红客和黑客的密度(或个数),由于它们都具有生物繁殖特性,即,当它们单独生存时,红客和黑客的密度 $x(t)$ 和 $y(t)$ 分别满足 logistic 动力学方程$(1/x)\,\mathrm{d}x/\mathrm{d}t=r_1(K_1-x)/K_1$ 和$(1/y)\,\mathrm{d}y/\mathrm{d}t=r_2(K_2-y)/K_2$(见文献[16]),这里 K_1 和 K_2 分别为红客种群和黑客种群(x 和 y)的最小生存容量(即,低于该容量时,相应的红客或黑客种群将会自行灭绝,见文献[16])。

但是,当红客和黑客混居时,它们密度的变化不但要遵守自己的规律,而且,还要受另一方的影响。若设相应的影响函数都是线性的,分别为 αy 和 βx,那么,红客与黑客相互作用的动力学模型就可表示为如下的微分方程组,Gause-Witt 模型:

$(1/x)\,\mathrm{d}x/\mathrm{d}t=r_1(K_1-x-\alpha y)/K_1$ 和 $(1/y)\,\mathrm{d}y/\mathrm{d}t=r_2(K_2-y-\beta x)/K_2$

其中,α 和 β 称为红客和黑客的竞争系数,即,它们分别给对方造成的杀伤力为“$-\alpha y/K_1$”和“$-\beta x/K_2$”,这里的负号“-”就体现了杀伤性,如果把该负号换为正号,那么相应的关系就由“竞争”变为了“互惠”(这就是下一节将要讨论的红客与用户之间的关系)。令微分方程组的右边为 0,可得两条直线:$L_1(K_1-x-\alpha y=0)$和 $L_2(K_2-y-\beta x=0)$,根据这两条直线在第一象限中的位置特性,已经证明(见文献[18]的 1.2 节或文献[19]的 3.1 节)。

红客与黑客的竞争定理:由 Gause-Witt 模型描述的红客和黑客,彼此厮杀的结果是:(1)如果 $K_1/K_2>\alpha$ 和 $\beta>K_2/K_1$,那么,黑客将被淘汰;(2)如果 $\alpha>K_1/K_2$ 和 $K_2/K_1>\beta$,那么,红客将被淘汰;(3)如果 $\alpha>K_1/K_2$ 和 $\beta>K_2/K_1$,那么,红客或黑客中的某一方将被淘汰,即,不是你死,就是我活;(4)如果 $K_1/K_2>\alpha$ 和 $K_2/K_1>\beta$,那么,红客和黑客将共存,谁也不能淘汰谁,即,它们势均力敌。

从这个定理中可以解读出一些有趣的现象:α 是

黑客给红客造成的伤害;β 是红客给黑客造成的伤害;红客和黑客在竞争中,是否被对方灭绝,不但取决于自己的杀伤力,还取决于两条生死线:它们最小生存容量的比值 K_1/K_2 和 K_2/K_1。即,如果各方给对方的杀伤力都在生死线内,那么,即使竞争很惨烈,大家也都会共存;如果各方给对方的伤害都在生死线外,那么,只能活一方,到底谁死就得看运气了;如果一方给另一方的伤害在生死线之内,但是另一方的反击却在生死线外,那么,反击者获胜并灭掉对方。换句话说,红客若想淘汰黑客,那么,它有两种策略:增大其对黑客的杀伤力 β,或者降低自己的最小生存容量 K_1(即,提高自己的生存力)。黑客若想在竞争中获胜,策略也一样。

现在来考虑红客和黑客混居时的一般生态平衡情况。为简化足标,我们将上面的 Gause-Witt 模型重新写为常用的 Lotka-Volterra 模型生态方程:

$dx/dt=x(a_{10}-b_{11}x-b_{12}y)$ 和 $dy/dt=y(a_{20}-b_{21}x-b_{22}y)$

这里的各个系数 $b_{ij}(i=1,2)$ 均为非负。当 $b_{11}>0$ 时,称红客为密度制约的;当 $b_{11}=0$ 时,称红客为非密度制约的。同理,当 $b_{22}>0$ 时,称黑客是密度制约的;当 $b_{22}=0$ 时,称黑客为非密度制约的。a_{10} 和 a_{20} 分别表示红客和黑客的生长率(出生率减死亡率)。

令上述生态方程的右边等于 0,于是,得到两条直线:

$L1:a_{10}-b_{11}x-b_{12}y=0$ 和 $L2:a_{20}-b_{21}x-b_{22}y=0$

如果这两条直线在第一象限内有一个交点 (x',y')(即,该交点的坐标满足 $x'>0,y'>0$),那么,根据 Routh-Hurwits 稳定性条件(见文献[18]的 3.1 节),有:若 $b_{11}b_{22}-b_{21}b_{12}>0$ 并且 $b_{11}x'+b_{22}y'>0$,那么,平衡点 (x',y') 是渐近稳定的,即,无论因何原因,如果红客和黑客的数量偶然落进了 (x',y') 点附近,那么,红客和黑客的数量将最终趋于 x' 和 y'。由于此时不等式 $b_{11}b_{22}-b_{21}b_{12}>0$ 的必要条件是:$b_{11}>0$ 和 $b_{22}>0$,所以红客和黑客都必须是密度制约的。

由此,根据文献[18]的定理 3.1,我们有:

红客黑客竞争的生态平衡定理:在上面 Lotka-Volterra 模型表示的红客和黑客竞争生态方程中,如果红客和黑客都是密度制约的,那么,它们的正平衡点 (x',y') 是全局稳定的。即,无论最初有多少个红客和黑客(当然暗含为正),它们最终的数量都会趋于 x' 和 y',从而达到生态平衡。

3　“用户+红客”生态学

红客与用户的关系,就是生物中的互惠互利关系,就像牧民保护牛羊那样,红客要保护用户免遭黑客的攻击。

设 $x(t)$ 和 $y(t)$ 分别是 t 时刻红客和用户的密度(或个数),由于它们都具有生物繁殖特性,即,当它们单独生存时,红客和用户的密度 $x(t)$ 和 $y(t)$ 分别满足 logistic 动力学方程 $(1/x)\,dx/dt=r_1(K_1-x)/K_1$ 和 $(1/y)\,dy/dt=r_2(K_2-y)/K_2$(见文献[16]),这里 K_1 和 K_2 分别为红客种群和黑客种群(x 和 y)的最小生存容量(即,低于该容量时,相应的红客或用户种群将会自行灭绝)。

但是,当红客和用户混居时,它们密度的变化不但要遵守自己的规律,而且,还要受另一方的影响。若设相应的影响函数都是线性的,分别为 $b_{12}y$ 和 $b_{21}x$,那么,红客与用户相互作用的动力学模型就可表示为如下的微分方程组:

$(1/x)\,dx/dt=r_1(K_1-x)/K_1+b_{12}y$ 和 $(1/y)\,dy/dt=r_2(K_2-y)/K_2+b_{21}x$

其中 $b_{21}x$ 和 b_{12}y 就分别是用户(红客)给予红客(用户)的互惠。根据文献[19]的 3.3 节,我们有如下生态定理:

红客与用户互惠的生态平衡定理:记 $\delta=1-b_{12}b_{21}$,$a=b_{12}K_2/K_1$ 和 $b=b_{21}K_1/K_2$。如果 $\delta>0$,那么,无论最初的红客和用户个数是多少(当然假定为正数),最终,红客的数量将趋于 $(1+a)/\delta$,而用户的数量将趋于 $(1+d)/\delta$。

虽然从安全角度看,红客与用户基本上是一家人,它们彼此影响的生态问题其实并不重要,但是,为了学术的完整性,我们还是在此节做简要概述。

下面该来考虑用户、红客和黑客三者大团圆时的生态学问题了。

4　“黑客+用户+红客”生态学

综合来考虑黑客、红客和用户在一起的生态环境时,情况就更复杂了:黑客的本意是要从用户处获利,但是,如果红客要挡它财路的话,黑客也会攻击红客;红客并不想主动攻击黑客,但是,如果用户受到伤害,红客就有义务提供保护;用户在黑客面前几乎无论为力,就像牛羊在狮子面前一样,只能靠运气(未被黑客盯上)和红客的保护。

下面来看这三方,如何联袂演唱一出生态学大戏。

设 $x_1(t)$、$x_2(t)$、$x_3(t)$ 分别为 t 时刻用户、红客和黑客的密度(或数量)。当它们独自相处,没有其它两方存在时,它们各自都要满足自己的动力学模型,比如,$dx_i/dt=r_ix_i[1-x_i/K_i]$,$i=1,2,3$(见文献[16]),这里 K_1、K_2 和 K_3 分别为用户种群、红客种群和黑客种群

的最小生存容量(即,低于该容量时,相应的用户、红客或黑客种群将会自行灭绝)。

但是,当用户、红客和黑客三者混居时,它们的密度的变化不但要遵守自己的规律,而且,还要受另两方的影响。设相应的影响函数都是线性的,为了使足标更整齐,我们逐一来考虑各自的密度变化方程。

首先,对用户来说,当它独居时,满足 $dx_1/dt=r_1x_1[1-b_{11}x_1]$,但是,混居后,红客要给它提供互惠($+b_{12}x_2$),黑客却要对它减灭($-b_{13}x_3$),所以,用户最终的密度变化动力学方程为:$dx_1/dt=r_1x_1[1-b_{11}x_1+b_{12}x_2-b_{13}x_3]$。

其次,对红客来说,当它独居时,满足 $dx_2/dt=r_2x_2[1-b_{22}x_2]$,但是,混居后,用户要给它提供互惠($+b_{21}x_1$),黑客却要与它竞争造成减损($-b_{23}x_3$),所以,红客最终的密度变化动力学方程为:$dx_2/dt=r_2x_2[1+b_{21}x_1-b_{22}x_2-b_{23}x_3]$。

最后,对黑客来说,当它独居时,满足 $dx_3/dt=r_3x_3[1-b_{33}x_3]$,但是,混居后,用户要给它提供牺牲($+b_{31}x_1$),红客却要与它竞争造成减损($-b_{32}x_2$),所以,黑客最终的密度变化动力学方程为:$dx_3/dt=r_3x_3[1+b_{31}x_1-b_{32}x_2-b_{33}x_3]$。

综合而言,“用户+红客+黑客”的生态学微分三方程组为:

$$dx_1/dt=r_1x_1[1-b_{11}x_1+b_{12}x_2-b_{13}x_3]$$
$$dx_2/dt=r_2x_2[1+b_{21}x_1-b_{22}x_2-b_{23}x_3]$$
$$dx_3/dt=r_3x_3[1+b_{31}x_1-b_{32}x_2-b_{33}x_3]$$

为考虑该生态系统的稳定性,令上面三式的右边为0,得到线性方程组:

$1-b_{11}x_1+b_{12}x_2-b_{13}x_3=0$, $1+b_{21}x_1-b_{22}x_2-b_{23}x_3=0$, $1+b_{31}x_1-b_{32}x_2-b_{33}x_3=0$

记矩阵 $A=[a_{ij}]$, $i,j=1,2,3$ 为该联立方程的行列式矩阵,即,$a_{11}=-b_{11}$, $a_{12}=b_{12}$, $a_{13}=-b_{13}$; $a_{21}=b_{21}$, $a_{22}=-b_{22}$, $a_{23}=-b_{23}$, $a_{31}=b_{31}$, $a_{32}=-b_{32}$, $a_{33}=-b_{33}$。若 $a=(a_1,a_2,a_3)$ 是该方程组的正解,即,$a_i>0$, $i=1,2,3$,也称 $a=(a_1,a_2,a_3)$ 为该生态方程的正平衡位置。于是,上面的三个生态微分方程可重新写为

$$dx_1/dt=r_1x_1[1-b_{11}(x_1-a_1)+b_{12}(x_2-a_2)-b_{13}(x_3-a_3)]$$
$$dx_2/dt=r_2x_2[1+b_{21}(x_1-a_1)-b_{22}(x_2-a_2)-b_{23}(x_3-a_3)]$$
$$dx_3/dt=r_3x_3[1+b_{31}(x_1-a_1)-b_{32}(x_2-a_2)-b_{33}(x_3-a_3)]$$

于是,平衡位置 (a_1,a_2,a_3) 是局部稳定的充分条件为:矩阵 $[a_ia_{ij}]$ 的所有特征根的实部为负。

下面进一步来考虑全局稳定性问题。

“用户+红客+黑客”三合一生态平衡定理1(见文献[18]定理4.7):上述正平衡位置 (a_1,a_2,a_3) 对“用户+红客+黑客”的生态方程是全局稳定的充分条件是:如果存在一个正的对角线矩阵 $\boldsymbol{C}$,使得 $\boldsymbol{CA}+\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}$ 是负定的,并且函数 $W(X)=[(X-a)^{\mathrm{T}}(\boldsymbol{CA}+\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C})(X-a)]/2$ 不沿上述三微分方程组的一根轨线恒为0($X=a$ 外)。此处 X 表示 (x_1,x_2,x_3), a 表示 (a_1,a_2,a_3), $\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置矩阵。形象地说,如果以上条件满足的话,那么,无论最初用户、红客和黑客的个数是多少(当然假定为正),那么,最终用户的个数会趋于 a_1,红客的个数会趋于 a_2,黑客的个数会趋于 a_3。

为介绍另一个生态平衡定理,我们先引入如下定义:

一个矩阵 $\boldsymbol{C}=[\boldsymbol{C}_{ij}]$ 称为是一个 $\boldsymbol{M}$ 矩阵,如果当 $i\neq j$ 时,$C_{ij}\leqslant 0$,而且下列五个条件中任何一个成立(其实,对于具有非正的非对角线元素的矩阵,这五个条件是彼此等价的):

条件1,矩阵 $\boldsymbol{C}$ 的所有特征值有正实部;

条件2,$\boldsymbol{C}$ 的顺序主子式为正,即,每个顺序子矩阵的行列式值是正的;

条件3,$\boldsymbol{C}$ 是非奇异的,而且 $\boldsymbol{C}^{-1}\geqslant 0$;

条件4,存在一个向量 $x>0$,使 $\boldsymbol{C}x>0$;

条件5,存在一个向量 $y>0$,使 $\boldsymbol{C}^{\mathrm{T}}y>0$。

“用户+红客+黑客”三合一生态平衡定理2(见文献[18]定理4.8):上述正平衡位置 (a_1,a_2,a_3) 对“用户+红客+黑客”的生态方程是全局稳定的充分条件是:1)存在一个矩阵 $\boldsymbol{G}$,使得对所有 $i,j=1,2,3$ 都有 $a_{ii}\leqslant\boldsymbol{G}_{ii}$ 和 $|a_{ij}|\leqslant\boldsymbol{G}_{ij}$ 对 $i\neq j$;2)矩阵 $[-\boldsymbol{G}]$ 的所有顺序主子式为正。形象地说,如果以上条件满足的话,那么,无论最初用户、红客和黑客的个数是多少(当然假定为正),那么,最终用户的个数会趋于 a_1,红客的个数会趋于 a_2,黑客的个数会趋于 a_3。

5 结束语

到目前为止,包括本文在内,经过17篇系列论文的探索,《安全通论》的轮廓已经很清晰了,从而“网络空间安全”一级学科的统一基础理论就不再是天方夜谭了。至于如何广泛使用《安全通论》去促进网络空间安全的教育、科研、产品研发、安全防护、攻防改进等,那就只能靠安全界的各位同仁了。可喜的是,在教育方面,好几年高校已经将《安全通论》当作其研究生教材了,希望它早日成为国内外更多高校信息安全专业的本科生和研究生基础教材;而且业界许多人的安全观念也因《安全通论》而得以刷新,希望它能够为国内外网络安全保障体系的建设和维护做重要贡献。

虽然还有许多工作要做,但是,有必要在此做一个简要归纳,以便《安全通论》能促进网络空间安全一级

学科的健康成长和迅速发展。到目前为止,《安全通论》在回答如下四大支柱性核心问题方面均有进展:

问题 1:什么是安全,什么是攻防,什么是黑客,什么是红客?

问题 2:无论是否失去理智,黑客和红客攻防对抗双方的极限在哪里?

问题 3:如果黑客和红客攻防双方是理智的,那么最佳攻防策略是什么?

问题 4:网络空间安全的生态情况是什么,如何治理?

关于问题 1 的部分答案,包含在文献[1,2,9]中,主要结果可概括为:(1)从安全角度来看,任何有限系统都可以分解成一个逻辑经络树;只要能够保证该经络树中的某些末端点(元诱因)不出问题,那么,整个系统就不会有安全问题。(2)安全也是一种负熵(与信息是负熵类似)。而且,任何有限系统,若无外界的影响,那么,它的"不安全性"总会越来越大,就像熵始终向增大方向发展一样。(3)攻防可以分为两大类:盲攻防和非盲攻防。网络空间中,黑客与红客的攻防基本上都是盲攻防,但是,沙盘演练有助于我们用非盲数据来研究盲状态。(4)黑客的数学本质,其实就是一个离散随机变量 X;而且,黑客的攻击能力可用 X 的熵来度量,即,当这个熵越小时,黑客越厉害;具体地说,X 的熵每少一个比特,该黑客在最佳攻击策略的指导下,他的黑产收入能够增加一倍。(5)红客的唯一目的是控制系统的不安全熵,使该熵不断减少(最理想情况),不再增大(次理想情况),或不要过快增大(保底情况)。因此,判断红客的某行为是否正确的唯一依据,就是该行动最终会导致系统的不安全熵的变化趋势。熵向减少方向发展,就说明红客正确,否则就是帮倒忙。问题 1 的深入研究,还需要借助可靠性理论、容错理论和系统论等知识。

关于问题 2 的部分答案,包含在文献[2-8,10-11]中,主要结果包括:无论彼此对抗的是两人还是多人,无论对抗者是有理智还是因斗争太残酷已经失去了理智,盲对抗都是存在理论极限的,即,攻防各方都不可能突破这些极限。这其实又从另一个角度规劝对抗各方理智行事,即,以争取自身利益最大化为目标,损人不利己的事情别做,因为,失去理智并不能帮助提升你的攻防能力。虽然在不同情况下,相应的理论极限值互不相同(细节在此略去),但是,这些极限基本上都是基于《信息论》中的仙农信道容量定理而得出的,极限值都等于某些特定信道的信道容量。问题 2 的深入研究,还需要继续借助《信息论》和维纳的《赛博学》(即过去常说的维纳《控制论》);同时,反过来,由于通信和对抗在"信道"意义上其实是等价的(即,通信是收发双方的某种对抗,对抗也是攻防各方以输和赢为"比特"的某种通信),因此《信息论》和《安全通论》的许多成果能够彼此借鉴和促进。

关于问题 3 的部分答案,包含在文献[11-13]中,主要结果包括:如果对抗各方都理智行事,即,始终以预定的自身利益最大化为目标,那么,红客与黑客之间其实就是在进行多赢博弈。这时,攻防各方的最佳策略就应该是追求(或将对方逼进)纳什均衡状态。在现实的网络对抗中,无论各方的预定(经济)利益是什么,都一定存在纳什均衡状态。更出人意料的是,我们发现:当达到纳什均衡状态时,其相关攻防也到达了某种特殊信道的信道容量。这就意味着:《信息论》的核心和《博弈论》的核心是强相关的,因此,《信息论》、《博弈论》和《安全通论》原来是可以三论融合的。通信是某种协作式对话,但是,诸如法庭辩论等却是非协作式对话,也是对抗中的一个特例,它们也可纳入基于安全通论的博弈部分,这其实是将信息论扩展到"负信息"领域了。问题 3 的深入研究,还需要继续借助《博弈论》、《策略论》和《运筹学》等理论。可惜目前在国内外的安全界同时精通《博弈论》和《信息论》的人太少,所以,这座金矿还大有潜力可挖。

关于问题 4 的部分答案,包含在本文和文献[14-16]中,主要结果包括:网络空间安全的各涉事方的动力学行为分析,单方或多方相互作用时的生态环境特征等。比如,病毒式恶意代码是如何在网络中传染和为害的、谣言治理的效果如何表现出来、黑客(红客或用户)的生态特性、黑客和红客(黑客和用户、红客和用户)相互作用时的生态特性、黑客红客和用户三者相互作用时的生态特性等。问题 4 的深入研究,还需要充分借鉴《复杂系统理论》、《系统论》等知识,尤其需要数学生态学家的支援,因为,毕竟在国内外安全界谁也不曾想到生物数学能帮上大忙,而且,生物数学对传统的安全专家来说确实太遥远了,不能仅仅依靠安全专家自己的补课。

总之,为庞大的网络空间安全一级学科建立统一的基础理论,绝不是一件容易的事情。到目前为止,我们只是在各个方面,尽量地抛砖,但愿能够引来众多的玉。目前,我们"暂不生产矿泉水,只做大自然的搬运工",所以,我们现在尽量借用已有的理论成果,尽量不去陷入繁杂的数学推导,尽量用最简捷的语言来把复杂的事情说清楚。

再一次邀请国内外各方面专家,与我们一起共同努力,早日完成《安全通论》!

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,

[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,

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

[18] 陈兰荪. 数学生态学模型与研究方法[M]. 北京:科学出版社,1988.

[19] 肖燕妮,周义仓,唐三一. 生物数学原理[M]. 西安:西安交通大学出版社,2012.