文章编号：2096-1618(2016)05-0443-04
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-960372.html
发表时间：2016-03-04

安全通论(9)

——红客篇

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：揭示了红客的本质，即维护系统的“安全熵”值，避免其突变，当然，如果能够“使熵减少或不增”就最理想。特别是通过对熵的时变微分方程的讨论，分析了各种情况下，系统的安全态势以及红客的业绩评价等。

0　引言

红客是被黑客逼出来的，没有黑客就不需要红客。但遗憾的是，黑客不但没有绝迹，而且还越来越多，越来越凶！

在某种意义上，黑客代表“邪恶”，因此，黑客的行动都是在隐蔽环境下进行的，不敢对外公开。从而，黑客获胜的主要法宝就是技术和其他“鸡鸣狗盗”。

在某种意义上，红客代表“正义”，因此，红客的行动都是公开的，他们可以光明正大地运用包括法律、法规、标准、管理、技术、教育等一切手段来捍卫系统的安全。

从表面上看，红客的行动包括(但不限于)安装防火墙，杀病毒，抓黑客，加解密，漏洞扫描，制定标准，颁布(或协助颁布)相关法律、法规，而且还经常删帖、封网、雇水军等等。但是，这些都是错觉，如果要单一地考虑红客的这些防卫措施的话，那么，《安全通论》将无立足之地，而且系统的安全防守工作将越来越乱。过去，也许因为没有搞清红客的本质，所以，红客才做了许多事倍功半的事情，甚至还做了不少负功，既没有能挡住黑客的攻击，又把自己的阵营搞得一团糟，甚至逼反了自己的“友军”。比如，其中，最典型的“化友为敌”的代表，恐怕就是新浪小编们的随意删帖，因为，它激发了更多的负面情绪，甚至严重干扰了红客的正常防护活动。其实，红客的本意，是只想做一件事，那就是：维护系统的熵(或秩序)！或更准确地说，最好能够“减少系统的熵”，次之是要“阻止系统的熵被增大”，至少要确保“系统的熵不要过快地增大”。因此，能够维护好熵的红客，才是合格的红客；否则，就是差红客，甚至是帮倒忙的红客。

由于红客可以使用黑客的所有技术，所以，本文不再重复文献[1-8]中提到过的所有技术部分，而是充分运用《系统论》[9]，来揭示红客的本质。

1　安全熵及其时变性研究

考虑由红客、黑客、用户、网络和服务等组成的系统。由“热力学第二定律”，可知该系统的熵(或秩序，或组织性)一定会随着时间的流逝，而不断地自动增大；由文献[1]，这意味着“系统的不安全性”也在不断地增大；特别是黑客的存在，使得这种“熵增大”的趋势更明显，因为，黑客的实质就是搞破坏，就是要搞乱系统的既定秩序；而与之相反，红客的目的就是要有效阻止这种系统崩析(耗散)趋势，确保用户能够按既定的秩序在系统中提供或获得服务。当然，用户的误操作(或者红客的乱操作)也会在实际上搞乱系统，增大系统的熵，不过，为了清晰起见，本文不考虑诸如用户误操作、红客和黑客失误等无意行为所造成的乱序问题。

由于有红客、黑客等人为因素的影响，所以，网络系统显然不是“封闭系统”(如果只考虑设备，那么，系统就可看成是“封闭系统”，实际上，它还是一个“有限系统”)，更由于红客和黑客连续不断的攻防对抗，使得系统熵(秩序的度量)不断地被增大和缩小，即，系统的熵始终是时变的。

设系统的全部不安全因素为 $q_1, q_2, \cdots, q_n$，记 t 时刻系统的熵为 $Q(t, q_1, q_2, \cdots, q_n)$ 或者简记为 $Q(t)$。当 $Q(t)=0$ 时，系统的熵达到最小值，此时系统的安全性就达到最大值(因为，根据文献[1]“安全”是“负熵”，或者说“不安全”是“熵”)。当然，一般情况下，熵总是正数。若 $Q(t)$ 随时间而增长，即微分 $\mathrm{d}Q(t)/\mathrm{d}t>0$，那么，系统将变得越来越不安全；反之，若 $Q(t)$ 随时间而减少，即微分 $\mathrm{d}Q(t)/\mathrm{d}t<0$，那么，系统将变得越来越安全。因此，下面我们将 $Q(t)$ 称为“安全熵”。而红客的目标就是要努力使得“安全熵”越来越小，黑

客则想使“安全熵”越来越大。

对每个 $i(i=1,2,\cdots,n)$，记 $Q(t,q_i)$（更简单地 $Q_i(t)$ 或 Q_i）为在“只存在不安全因素 q_i”的条件下，在 t 时刻，系统的“安全熵”。那么，各个 $Q_i(t)$ 的时变情况便可以用如下 n 个方程（称为方程组 1）来描述：

$$\begin{aligned}
dQ_1/dt &= f_1(Q_1,Q_2,\cdots,Q_n)\\
dQ_2/dt &= f_2(Q_1,Q_2,\cdots,Q_n)\\
&\vdots\\
dQ_n/dt &= f_n(Q_1,Q_2,\cdots,Q_n) \qquad (1)
\end{aligned}$$

这里，任何一个 Q_i 的变化都是所有其他各 $Q_j(j\neq i)$ 的函数；反过来，任一 Q_i 的变化也承担着所有其他量和整个方程组 1 的变化。

下面针对一些特殊情况来仔细讨论方程组 1。

如果各个 Q_i 不随时间而变化，即，$dQ_i/dt=0$，$i=1,2,\cdots,n$（或者说 $f_1(Q_1,Q_2,\cdots,Q_n)=f_2(Q_1,Q_2,\cdots,Q_n)=\cdots=f_n(Q_1,Q_2,\cdots,Q_n)=0$），那么，此时系统的“安全熵”就处于静止状态，即系统的安全性既不变坏，也没有变得更好。如果从系统刚刚投入运行开始（即，$t=0$），红客就能够维护系统，使其“安全熵”永远处于静止状态，那么，这样的红客就是成功的红客！

设 $Q_1^*,Q_2^*,\cdots,Q_n^*$ 是在静止状态下，方程组 1 的一组解。对每个 i，$i=1,2,\cdots,n$，引入新的变量 $Q'_i=Q_i^*-Q_i$，那么，方程组 1 就转变成了如下方程组

$$\begin{aligned}
dQ'_1/dt &= f'_1(Q'_1,Q'_2,\cdots,Q'_n)\\
dQ'_2/dt &= f'_2(Q'_1,Q'_2,\cdots,Q'_n)\\
&\vdots\\
dQ'_n/dt &= f'_n(Q'_1,Q'_2,\cdots,Q'_n) \qquad (2)
\end{aligned}$$

如果这个方程组可以展开为泰勒级数，即得到如下方程组

$$\begin{aligned}
dQ'_1/dt &= a_{11}Q'_1+a_{12}Q'_2+\cdots+a_{1n}Q'_n+a_{111}Q'^2_1+a_{112}Q'_1Q'_2+\\
&\quad a_{122}Q'^2_2+\cdots\\
dQ'_2/dt &= a_{21}Q'_1+a_{22}Q'_2+\cdots+a_{2n}Q'_n+a_{211}Q'^2_1+a_{212}Q'_1Q'_2+\\
&\quad a_{222}Q'^2_2+\cdots\\
dQ'_n/dt &= a_{n1}Q'_1+a_{n2}Q'_2+\cdots+a_{nn}Q'n+a_{n11}Q'^2_1+a_{n12}Q'_1Q'_2+\\
&\quad a_{n22}Q'^2_2+\cdots \qquad (3)
\end{aligned}$$

该方程组的通解是：

$$\begin{aligned}
Q'_1 &= G_{11}e^{\lambda(1)t}+G_{12}e^{\lambda(2)t}+\cdots+G_{1n}e^{\lambda(n)t}+G_{111}e^{2\lambda(1)t}+\cdots\\
Q'_2 &= G_{21}e^{\lambda(1)t}+G_{22}e^{\lambda(2)t}+\cdots+G_{2n}e^{\lambda(n)t}+G_{211}e^{2\lambda(1)t}+\cdots\\
Q'_n &= G_{n1}e^{\lambda(1)t}+G_{n2}e^{\lambda(2)t}+\cdots+G_{nn}e^{\lambda(n)t}+G_{n11}e^{2\lambda(1)t}+\cdots
\end{aligned}$$

此处各个 G 都是常数，$\lambda(i)$，$i=1,2,\cdots,n$，则是如下 nXn 阶矩阵，$\boldsymbol{B}=[b_{ij}]$，的行列式关于 λ 的特征方程的根，即方程 $det(\boldsymbol{B})=0$ 的根，这里 $\boldsymbol{B}=[b_{ij}]$，$b_{ii}=a_{ii}-\lambda$，$i=1,2,\cdots,n$，而 $b_{ij}=a_{ij}$，当 $i\neq j$ 时。

上述特征方程的根 $\lambda(i)$ 既可能是实数，也可能是虚数。下面考虑几种特别情况：

情况(1)，如果所有的特征根 $\lambda(i)$ 都是实数且是负数，那么，根据通解式可知，各 Q'_i 将随着时间的增加，而趋近于 0（因为 $e^{-\infty}=0$），这说明红客正在节节胜利，因为，“安全熵”变化率趋于 0 意味着：各个不安全因素正被逐步控制，系统的秩序也正在恢复之中！

情况(2)，同理，如果所有的特征根 $\lambda(i)$ 都是复数且负数在其实数部分，那么，根据通解式可知，各 Q'_i 也随着时间的增加，而趋近于 0。这时，红客也正在节节胜利中！

由于 $Q_i=Q_i^*-Q'_i$，$i=1,2,\cdots,n$，所以，根据方程组 2 可知，在情况(1)和(2)中，Q_i 逼近静态值 Q_i^*，此时，系统所处的安全平衡状态是稳定的，因为，在一个足够长的时间内，系统愈来愈逼近静态，系统的“安全熵”变化率始终逼近于 0，即系统的秩序是长期稳定的。

情况(3)，如果有一个特征根 $\lambda(i)$ 是正数或 0，那么，系统的平衡就不稳定了，即，系统的安全性也不稳定了，红客就有可能失控。

情况(4)，如果有一些特征根 $\lambda(i)$ 是正数和复数，那么，系统中就包含着周期项，因为，指数为复数的指数函数具有这样的形式：

$e^{(a-ib)t}=e^{at}[\cos(bt)-i\sin(bt)]$，这里 i 为虚数单位

此时，系统的安全状态会出现周期性的振动，即会出现红客与黑客之间的反复“拉锯战”，虽然双方会各有胜负，但是，总体趋势是向着对红客不利的混乱和不安全方向发展。

为了使上面的讨论更加形象，现在考虑 $n=2$ 这个简单，即此时系统的不安全因素主要有两个（比如，“黑客攻击”和“用户操作失误”这两个宏观的因素），那么，方程组 1 就简化为：

$dQ_1/dt=f_1(Q_1,Q_2)$，和 $dQ_2/dt=f_2(Q_1,Q_2)$

在可以展开为泰勒级数的假设下，它的解为：

$$\begin{aligned}
Q_1 &= Q_1^*-G_{11}e^{\lambda(1)t}-G_{12}e^{\lambda(2)t}-G_{111}e^{2\lambda(1)t}-\cdots\\
Q_2 &= Q_2^*-G_{21}e^{\lambda(1)t}-G_{22}e^{\lambda(2)t}-G_{211}e^{2\lambda(1)t}-\cdots
\end{aligned}$$

其中 Q_1^* 和 Q_2^* 是使 $f_1=f_2=0$ 而得到的 Q_1 和 Q_2 的静态解，G 是积分常数；而 $\lambda(1)$ 和 $\lambda(2)$ 是特征方程 $(a_{11}-\lambda)(a_{22}-\lambda)-a_{12}a_{21}=0$ 的根，而此二次方程的根为

$$\lambda=C/2\pm\sqrt{[-D+C^2/4]},$$

其中，$C=a_{11}+a_{22}$，$D=a_{11}a_{22}-a_{12}a_{21}$。

于是，可知

(1)若 $C<0$，$D>0$，$E=C^2-4D>0$，那么，特征方程的两个根都是负的，因而，系统就会随着时间的伸展，趋向于稳定在静止状态 (Q_1^*,Q_2^*)，这时，红客将居于主动地位，系统的安全尽在掌控中。

(2)若 $C<D, D>0, E=C^2-4D<0$,那么,特征方程的两个根都是带有负实数部分的复数解。此时,随着时间的推移,系统的"安全熵"(Q_1, Q_2)就会将沿一个螺旋状的曲线轨迹而逼近静止状态(Q_1^*, Q_2^*),这时,对红客来说,也是有利的。

(3)若 $C=0, D>0, E<0$,那么,特征方程的两个解都是虚数,因此,方程组的解中就包含有周期项,就会出现围绕静止值的摆动或旋转,即,代表"安全熵"的点(Q_1, Q_2)会围绕静止态(Q_1^*, Q_2^*)画出一条封闭的曲线,这时,红客与黑客难分胜负,双方不断地进行着"拉锯战"。

(4)若 $C>0, D>0, E>0$,那么,特征方程的两个解都是正数,此时,完全不存在静态。或者说,此时系统更混乱,红客完全失控,只能眼睁睁地看着系统最终崩溃!

更进一步,下面再来考虑 $n=1$ 这种最简单的情况,此时,系统的不安全因素只有一个(比如,黑客的破坏)。于是,方程组 1 就简化为方程:$\mathrm{d}Q/\mathrm{d}t=f(Q)$。若将 $f(Q)$ 展开为泰勒级数,那么,就得到如下方程:

$$\mathrm{d}Q/\mathrm{d}t=a_1Q+a_{11}Q^2+\cdots$$

此泰勒式中未包含常数项,因为,我们可以假定:"不安全因素"不会自然发生,即,系统刚刚被使用($t=0$)的那一刻,系统不会出现安全问题。

如果粗略地只保留该泰勒级数中的第一项,那就有 $\mathrm{d}Q/\mathrm{d}t=a_1Q$,这说明:系统的安全态势将完全取决于常数 a_1 是正还是负。如果为 a_1 为负,那么,"安全熵"整体上向减少的方向发展,即,系统的安全性会越来越好,对红客有利;如果 a_1 为正,那么,"安全熵"整体上向增加的方向发展,即,系统的安全性会越来越差,对红客不利。而且,系统的这种越来越安全(或越来越不安全)的态势遵从指数定律:$Q=Q_0e^{a(1)t}$,其中,Q_0 表示初始时刻($t=0$)时,系统的"安全熵";而 $a(1)$ 是 a_1 的等价表达式,这主要是为了简化公式中足标体系的复杂度。(这是因为 $Q=Q_0e^{a(1)t}$ 是方程 $\mathrm{d}Q/\mathrm{d}t=a_1Q$ 的解)。该指数定律表明:如果系统的安全态势在向好的方面发展,那么,变好的速度会越来越快;反之,如果系统的安全态势在向坏的方面发展,那么,变坏的速度也会越来越快,甚至瞬间崩溃!

如果再精细一点,即,保留上述泰勒级数的前两项,于是,就有方程:

$$\mathrm{d}Q/\mathrm{d}t=a_1Q+a_{11}Q^2$$

该方程的解为 $Q=[a_1ce^{a(1)t}]/[1-a_{11}ce^{a(1)t}]$。注意,随着时间的延伸,该解所画出的曲线就是所谓的"对数曲线",它是一个趋向于某极限的 S 形曲线,也就是说,此时,从安全性角度来看,系统的变好和变坏,还是有"底线"的。

下面,我们再换一个角度来看系统安全,即跳出系统,完全以旁观的第三方身份,来看红客与黑客之间如何"道高一尺魔高一丈"地"水涨船高"。

此时,影响系统安全性的因素只有两个(即,红客努力使系统变得更安全,使"安全熵"不增;而黑客却努力要使系统不安全,增加"安全熵"),而且,假如这两个因素之间还是相互独立的,即,各方都埋头于自己的"攻"或"守"(实际情况也基本是这样,因为,短兵相接时,双方根本顾不过来考虑其他事情),或者说,红客(黑客)的"安全熵"随时间变化的情况与黑客(红客)的"安全熵"无关,而且还只考虑"主要矛盾",即此时在方程组 3 中,每个方程式里就只保留第 1 项,其他系数都全部为 0。于是,方程组 3 被简化为:

$$\mathrm{d}Q_1/\mathrm{d}t=a_1Q_1 \text{ 和 } \mathrm{d}Q_2/\mathrm{d}t=a_2Q_2$$

解此方程组,可得其解为:$Q_1=c_1e^{a(1)t}$ 和 $Q_2=c_2e^{a(2)t}$,从中再解出时间 t,可得:$t=[\ln Q_1-\ln c_1]/a_1=[\ln Q_2-\ln c_2]/a_2$。设 $a=a_1/a_2, b=c_1/(c_2)^a$,那么就有一个重要的公式,即:

$$Q_1=b(Q_2)^a$$

它说明红客与黑客的"安全熵"(Q_1 和 Q_2)彼此之间是幂函数关系,比如,红客维护系统安全所贡献的"安全熵"是黑客破坏系统安全所增大"安全熵"的幂函数。为更清楚起见,我们将上面的公式组 $\mathrm{d}Q_1/\mathrm{d}t=a_1Q_1$ 和 $\mathrm{d}Q_2/\mathrm{d}t=a_2Q_2$ 再重新写一次如下,即:

$$\{[\mathrm{d}Q_1/\mathrm{d}t][1/Q_1]\}:\{[\mathrm{d}Q_2/\mathrm{d}t][1/Q_2]\}=a \text{ 或者 } \mathrm{d}Q_1/\mathrm{d}t=a(Q_1/Q_2)(\mathrm{d}Q_2/\mathrm{d}t)$$

这里,前一部分说明:在只考虑红客和黑客的"安全熵"(Q_1 和 Q_2)的前提下,红客使其"安全熵"的相对增长率($[\mathrm{d}Q_1/\mathrm{d}t][1/Q_1]$)与黑客的"安全熵"的相对增长率($[\mathrm{d}Q_2/\mathrm{d}t][1/Q_2]$)之间的比值竟然是常数!而后一部分,更出人意料地表示:红客"安全熵"的时变率($\mathrm{d}Q_1/\mathrm{d}t$)与黑客"安全熵"的时变率($\mathrm{d}Q_2/\mathrm{d}t$)之间的关系,竟然是如此简洁!

若 $a_1>a_2$,即,红客"安全熵" Q_1 的增长率大于黑客"安全熵" Q_2 的增长率,那么,$a=a_1/a_2>1$,它表明红客对系统整体安全性走势的掌控力更强;反过来,若 $a_1<a_2$,即,红客"安全熵" Q_1 的增长率小于黑客"安全熵" Q_2 的增长率,那么,$a=a_1/a_2<1$,它表明红客对系统安全性走势的掌控力不如黑客。

再考虑泰勒级数方程组 3 的另一种情况:各个不安全因素彼此之间相互独立(比如,由文献[1]可知,当这些不安全因素就是系统安全"经络图"中的全体"元诱因"时,这些不安全因素之间就是相互独立的),此时,方程组 3 就简化为,对 $i=1,2,\cdots,n$,有:

$$\mathrm{d}Q_i/\mathrm{d}t=a_{i1}Q_i+a_{i11}(Q_i)^2+a_{i111}(Q_i)^3+\cdots$$

此时,不安全因素对系统"安全熵"的整体影响,就等于每个不安全因素对系统"安全熵"各自影响的

累加,即,此时有“整体等于部分和”。

方程组3还有一种特殊情况值得单独说明,即,假如有某个不安全因素 q_s 的泰勒展开式系数在各个方程中都很大,而其他不安全因素的泰勒系数却很小甚至为0,那么,不安全因素 q_s 就是不安全因素的主导部分,系统的不安全性可能主要是由它而引发,因此,这样的不安全因素 q_s 就应该是红客关注的重点,要尽力避免它成为系统崩溃的“导火索”。

2 结束语

经过前面8篇文章(见文献[1]-[8])的努力,我们已经奠定了《安全通论》的前三块重要基石,即,安全经络(见文献[1])、安全攻防(见文献[2-6])、黑客实质(见文献[7-8])。本文开始研究第四块重要基石:红客!

虽然红客与黑客在技术方面几乎没有区别,甚至他们的技术可以彼此通用,但是,作为系统安全的正、反两种力量的代表,他们在角色方面的差别还是很大的,因此,值得专门设立篇幅来进行研究。

如果说黑客的手段杂乱无章,那么,红客的手段更是一团乱麻(甚至红客还会“好心办坏事”,即做一些本该黑客搞的破坏),如何找到一根线索来把“这团乱麻”理清,这真是一个严峻的挑战。幸好我们偶然从文献[1-8]中发现了一个总是伴随着《安全通论》的一个“幽灵”,即,“熵”,而且,运气更好的是:经过分析,“熵”竟然与红客的本质密不可分,而且还是解开“乱麻”的重要线索。贝塔朗菲的《一般系统论》(见文献[9])对系统熵进行了恰到好处的研究,因此,被本文深度参考。文中的许多思路和方法都依赖于“系统论”,只不过贝塔朗菲用它们去研究生物的新陈代谢系统,而我是用它们来研究网络系统;贝塔朗菲研究的生物熵,我研究的是“安全熵”而已。

本文揭示了红客的实质是“维护系统的安全熵”,并详细分析了系统“安全熵”的多种情况下的时变特性。但是,到底应该怎样做才能够有效地阻止“安全熵”变大的趋势呢?这当然是一个重要而又困难的问题,过去全球安全界的同行们做了许多“埋头拉车”的具体工作,但是,在“抬头看路”方面还真的做得不够,比如,

(1) 都说安全是“三分技术,七分管理”,但是,真正落实到行动上时,大家在“安全管理”方面花费的精力远远未达到“七分”。因此,我们希望能够在《安全通论》中,专门开辟“管理篇”来详细研究“如何用管理的办法,来维护系统的安全熵”;

(2) 及时反馈也是红客维护“安全熵”并在必要时对其进行微调的重要办法,因此,维纳的《控制论》在《安全通论》中也应该有特殊的地位,但是,突破口确实很难找。

对红客的研究肯定不仅仅限于本文的这些内容,但是,为了尽快搭建起《安全通论》的核心骨架,吸引全球尽可能多的安全专家来一起“挖金矿”,我们不得不先放弃一些细节,比如,其实开放系统的“安全熵”永远不会处于平衡状态,而是会维持在所谓的“稳态”上,这与有机体的新陈代谢相同,而且,同样具有“异因同果性”,即,由不同的原因导致相同的结果,比如,或者是因为“黑客太弱”,或者是因为“红客太强”,而使得系统的安全无恙;反过来,或者是因为“黑客太强”,或者是因为“红客做了负功”,而使得系统崩溃。系统一旦达到“稳态”,就必定表现出“异因同果性”。

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] 冯. 贝塔朗菲. 一般系统论:基础、发展和应用[M]. 林康义,魏宏森,译. 北京:清华大学出版社,1987.