文章编号: 2096-1618(2016)04-0337-05
稿件来源:科学网
网 址: http://blog.sciencenet.cn/blog-453322-956051.html
发表时间:2016-02-14

安全通论(7)

——黑客篇之“战术研究”

杨义先, 钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:精确地描述了黑客的静态形象,即,黑客可用一个离散随机变量 X 来描述,这里 X 的可能取值为 $\{1,2,\cdots,n\}$,概率 $P_r(X=i)=p_i$,并且,$p_1+p_2+\cdots+p_n=1$。此外,还给出了在一定假设下,黑客的最佳动态攻击战术,即,当黑客的资源投入比例为其静态概率分布值时,黑客的“黑产收入”达到最大值。特别是,在投入产出比均匀的前提下,黑客 X 的熵若减少1比特,那么,他的“黑产收入”就会翻一倍,换句话说,若黑客 X 的熵 $H(X)$ 越小,那么,他就越厉害,他能够通过攻击行为获得的“黑产收入”就越高!

0 引言

如果说安全的核心是对抗,那么,在对抗的两个主角(攻方与守方)中,攻方(黑客)又是第一主角,因为,红客(守方)是因黑客(攻方)而诞生的。所以,很有必要对黑客,特别是他的攻击策略,进行更深入的研究。

广义地说,系统(或组织)的破坏者,都统称为“黑客”。他们以扰乱既有秩序为目的。因此,癌细胞、病菌、敌对势力、灾难、间谍等都是黑客。但是,为了聚焦,本文以常言的“网络黑客”为主要研究对象,虽然这里的结果和研究方法其实适用于所有黑客。

黑客的攻击肯定是有代价的,这种代价可能是经济代价、政治代价或时间代价。同样,黑客想要达到的目标也可能是经济目标、政治目标或时间目标。因此,至少可以粗略地将黑客分为经济黑客、政治黑客和时间黑客。

经济黑客:只关注自己能否获利,并不在乎是否伤及对方。有时,自己可以承受适当的经济代价,但是,整体上要赢利。赔本的买卖是不做的,他们肯定不是“活雷锋”。因此,经济黑客的目标就是:以最小的开销来攻击系统,并获得最大的收益。只要准备就绪,经济黑客随时可发动进攻。

政治黑客:不计代价,一定要伤及对方要害,甚至有时还有更明确的攻击目标,不达目的不罢休。他们随时精确瞄准目标,但是只在关键时刻,才“扣动扳机”。最终成败取决于若干偶然因素,比如,目标突然移动(红客突然出新招)、准备不充分(对红客的防御情况了解不够),或突然刮来一阵风(系统无意中的变化)等。

时间黑客:希望在最短的时间内,攻破红客的防线,而且,使被攻击系统的恢复时间尽可能地长。

从纯理论角度来看,其实没必要去区分上述3种黑客。下面为了形象计,也为了量化计,我们重点考虑经济黑客,即,黑客想以最小的经济开销来获取最大的经济利益。

1 黑客的静态描述

先讲一个故事:我是一个“臭手”,面向墙壁射击。虽然,我命中墙上任一特定点的概率都为零,但是,只要扳机一响,我一定会命中墙上某点,而这本来是一个“概率为零”的事件。因此,“我总会命中墙上某一点”这个概率为1的事件,就可以由许多“概率为零的事件(命中墙上某一指定点)”的集合构成。

再将上述故事改编成“有限和”情况:我先在墙上画满(有限个)马赛克格子,那么,“我总会命中某一格子”这个概率为1的事件,便可以由有限个“我命中任何指定格子”这些“概率很小,几乎为零的事件”的集合构成。或者,更准确地说,假设墙上共有 n 个马赛克格子,那么,我的枪法就可以用随机变量 X 来完整地描述:如果我击中第 $i(1\leqslant i\leqslant n)$ 个格子的事件(记为 $X=i$)的概率 p_i,那么,$p_1+p_2+\cdots+p_n=1$。

现在,让黑客代替“我”,让(有限)系统代替那面墙。

安全界有一句老话,也许是重复率最高的话,说:“安全是相对的,不安全才是绝对的”。可是,过去大家仅将这句话当成“口头禅”,而没有意识到其实是一个很重要的公理:

安全公理:对任何(有限)系统来说,安全都是相对的,不安全才是绝对的,即,“系统不安全,总可被黑客攻破”这个事件的概率为1。

根据该安全公理,我们可知,虽然黑客命中“某一点”(攻破系统的指定部分)的概率虽然几乎为零,但是,黑客“击中墙”(最终攻破系统)是肯定的,概率为1。

黑客可以有至少两种方法在“墙上”画马赛克格子:

画马赛克格子的第一种办法:锁定目标,黑客从自己的安全角度出发,画出系统的安全经络图(见参考文献[1]),然后,以每个“元诱因”(或“穴位”)为一个“马赛克格子”。假如,系统的安全经络图中共有 n 个“元诱因”,那么,黑客的(静态)攻击能力就可以用随机变量 X 来完整地描述:如果黑客摧毁第 $i(1\leqslant i\leqslant n)$ 个“元诱因”,记为 $X=i$,的概率为 p_i,那么,$p_1+p_2+\cdots+p_n=1$。

这种“元诱因马赛克画法”的根据是:在文献[1]中,已经知道,系统出现不安全问题的充分必要条件是某个(或某些)“元诱因”不安全。

“元诱因马赛克”的缺点是参数体系较复杂,但是,它的优点很多,比如,可以同时适用于多目标攻击,安全经络可以长期积累、永远传承等。根据安全经络图,我们可知:“安全”同时具有“波”和“粒子”的双重性质,或者说,具有“确定性”和“概率性”两种性质。更具体地说,任何不安全事件的“元诱因”的“确定性”更浓,而“素诱因”和“素事件”的“概率性”更浓。充分认识安全的波粒二象性,将有助于深刻理解安全的实质,有助于理解《安全通论》的研究方法和思路。

画马赛克格子的第二种办法:经过长期准备和反复测试,黑客共掌握了全部 n 种可能攻破系统的方法,于是,黑客的攻击能力可以用随机变量 X 完整地描述为:当黑客用第 i 种方法攻破系统,记为 $X=i(1\leqslant i\leqslant n)$,的概率为 p_i,这里,$p_1+p_2+\cdots+p_n=1$,$0<p_i<1(1\leqslant i\leqslant n)$。

说明:能够画出这“第二种马赛克格子”的黑客,肯定是存在的,比如,长期以“安全检测人员”这种红客身份掩护着的卧底,就是这类黑客的代表。虽然,必须承认,要想建立完整的武器库,即,掌握攻破系统的全部攻击方法,或完整地描述上述随机变量 X,确实是非常困难的,但是,从理论上看是可行的。

当然,也许还有其他方法来画“马赛克格子”,不过它们的实质都是一样的,即,黑客可以静态地用一个离散随机变量 X 来描述,这里 X 的可能取值为 $\{1,2,\cdots,n\}$,概率 $P_r(X=i)=p_i$,并且,$p_1+p_2+\cdots+p_n=1$。

2 黑客的动态描述

上节中用离散随机变量来表示的“黑客的静态描述”,显然适合于包括经济黑客、政治黑客、时间黑客等各种黑客。由于政治黑客的业绩很难量化,比如,若黑客获取了元首的私人存款金额,那么,这样的业绩对美国来说一钱不值,而对朝鲜等后封建国家来说,就是无价的国家机密。因此,本节中的量化分析主要针对经济黑客。

黑客的动态行为千变万化,必须首先清理场景,否则,根本无法下手。

为使相关解释更形象,本节采用上述第一种“马赛克格子画法”,即黑客是一个离散随机变量,他攻破第 i 个“元诱因”,记为 $X=i(1\leqslant i\leqslant n)$,的概率为 p_i,这里,$p_1+p_2+\cdots+p_n=1$,$0<p_i<1(1\leqslant i\leqslant n)$。特别强调,其实下面的内容适用于包括第二种方法在内的所有“马赛克格子画法”。

任何攻击都是有代价的,并且,如果黑客已经技术最牛了,那么,整体上来说是“投入越多,收益越多”。

设黑客攻破第 i 个“元诱因”的“投入产出比”为 $d_i(1\leqslant i\leqslant n)$,即,若为攻击第 i 个“元诱因”,黑客投入了1元钱,那么,一旦攻击成功(其概率为 p_i)后,黑客将获得 d_i 元的收入;当然,如果攻击失败,那么,黑客的这1块钱就全赔了。

根据文献[1]可知,任何一个“元诱因”被攻破后,系统也就被攻破了,不再安全了。因此,为了尽量避免被红客发现,尽量少留“作案痕迹”,我们假定:在攻击过程中,黑客只要发现有一个“元诱因”被攻破了,那么,他就立即停止本次攻击,哪怕继续攻破其他“元诱因”还可以获得额外的收入,哪怕对其他“元诱因”的“攻击投资”被浪费。

设黑客共有 M 元用于攻击的“种子资金”,如果他把这些资金全部投入到攻击他认为最有可能成功的某个“元诱因”(比如,最大的那个 p_i),那么,假如黑客最终成功地攻破了第 i 个“元诱因”(其概率为 p_i),则此时黑客的资金总数就变成(Md_i),但是,假如黑客的攻击失败(其概率为 $1-p_i$),则他的资金总数就瞬间变成

了零。可见,从经济上来说,黑客的这种“孤注一掷”战术的风险太大,不宜采用。

为增加抗风险能力,黑客改变战术,将他的全部资金分成 n 部分,b_1、b_2、…、b_n,其中 b_i是用于攻击第 i 个“元诱因”的资金在总资金中所占的比例数,于是,$\sum_{i=1}^{n} b_i=1$,这里 $0\leqslant b_i\leqslant 1$。如果在本次攻击中,第 i 个“元诱因”首先被攻破(其概率为 p_i),那么,本次攻击马上停止,此时,黑客的总资产变为(Mb_id_i),同时,投入到攻击其他“元诱因”的资金都白费了。由于 $\sum_{i=1}^{n} p_i=1$,即,肯定有某个“元诱因”会被首先攻破,所以,只要每个 $b_i>0$,那么,本次攻击结束后,黑客的总资产肯定不会变成零,因此,其抗风险能力确实增强了。

我们还假定:为了躲开红客的对抗,黑客选择红客不在场时,才发起攻击,比如,黑客每天晚上对目标系统进行(一次)攻击。当然,这里还有一个暗含的假设,即,黑客每天晚上都能够成功地把系统攻破一次,其实,这个假设也是合理的,因为,如果要经过 K 个晚上的艰苦攻击才能攻破系统,那么,把这 K 天压缩成“一晚”就行了。

单看某一天的情况,很难对黑客的攻击战术提出任何建议。不过,如果假定黑客连续 m 天晚上对目标系统进行“每日一次”的攻击,那么,确实存在某种攻击战术,能使得黑客的盈利情况在某种意义上,达到最佳。

为简化下足标,本文对 b_i和 $b(i)$交替使用,不加区别。

如果黑客每天晚上,都对他的全部资金按相同的分配比例 $b=(b_1,b_2,\cdots,b_n)$,来对系统的各“元诱因”进行攻击。那么,m 个晚上之后,黑客的资产就变为

$$S_m=M\prod_{i=1}^{m}S(X_i)=M\prod_{i=1}^{m}[b(X_i)d(X_i)]$$

这里 $S(X)=b(X)d(X)$,X_i是 1 到 n 之间的某个正整数,表示在第 i 天晚上,被(首先)攻破的那个“元诱因”的编号,所以,$X_1,X_2,\cdots,X_m$是独立同分布的随机变量,设该分布是 $p(x)$,于是有如下定理。

定理 1　若每天晚上黑客都将其全部资金,按比例 $b=(b_1,b_2,\cdots,b_n)$分配,来对系统的各“元诱因”进行攻击,那么,m 天之后,黑客的资产就变为

$$S_m=M2^{mw(b,p)}$$

这里 $W(b,p)=E(\log S(X))=\sum_{k=1}^{m}p_k\log(b_kd_k)$,称为“双倍率”。

证明　由于独立随机变量的函数,也是独立的;所以,$\log S(X_1)$、$\log S(X_2)$、…、$\log S(X_m)$也是独立同分布的,由弱大数定律,可得:

$\log S_m/m=[\sum_{i=1}^{m}\log S(X_i)]/m\to E(\log S(X))$,依概率

于是,$S_m=M2^{mw(b,p)}$。证毕。

由于黑客的资产按照 $2^{mw(b,p)}$方式增长(这也是把 $W(b,p)$称为“双倍率”的根据),因此,只需要寻找某种资金分配战术 $b=(b_1,b_2,\cdots,b_n)$,使得双倍率 $W(b,p)$能够最大化就行了。

定义 1　如果某种战术分配 b,使得双倍率 $W(b,p)$达到最大值 $W^*(p)$,那么,就称该值为最优双倍率,即

$$W^*(p)=\max_b W(b,p)=\max_b\sum_{k=1}^{m}p_k\log(b_kd_k)$$

这里的最大值 max 是针对所有可能的满足 $\sum_{i=1}^{n}b_i=1$,$0\leqslant b_i\leqslant 1$ 的 $b=(b_1,b_2,\cdots,b_n)$而取的。

双倍率 $W(b,p)$作为 b 的函数,在约束条件 $\sum_{i=1}^{n}b_i=1$之下,求其最大值。可以写出如下拉格朗日乘子函数并且改变对数的基底(这不影响最大化 b),则有:

$$J(b)=\sum p_k\ln(b_kd_k)+\lambda\sum b_i$$

关于 b_i求导得到

$$\partial J/\partial b_i=p_i/b_i+\lambda,\ i=1,2,\cdots,n$$

为了求得最大值,令偏导数为 0,从而得出:

$$b_i=-p_i/\lambda$$

带入约束条件 $\sum_{i=1}^{n}b_i=1$,可得到 $\lambda=-1$ 和 $b_i=p_i$。从而可知,$b=p$ 为函数 $J(b)$的驻点。

定理 2　最优化双倍率 $W^*(p)=\sum_{i=1}^{n}p_i\log d_i-H(p)$,并且,按比例 $b^*=p=(p_1,p_2,\cdots,p_n)$分配攻击资金的战术进行攻击,便可以达到该最大值。这里 $H(p)$是描述静态黑客的那个随机变量的熵,即,$H(p)=-\sum_{i=1}^{n}p_i\log p_i$。

证明　将双倍率 $W(b,p)$重新改写,使得容易看出何时取最大值:

$$\begin{aligned}W(b,p)&=\sum p_k\log(b_kd_k)\\&=\sum p_k\log[(b_k/p_k)p_kd_k)]\\&=\sum p_k\log d_k-H(p)-D(p\mid b)\\&\leqslant\sum p_k\log d_k-H(p)\end{aligned}$$

这里 $D(p\mid b)$是随机变量 p 和 b 的相对熵[7]。而当 $b=p$ 时,可直接验证上述等式成立。证毕。

从定理 2 可知:对于一个可用离散随机变量 $X(P_r(X=i)=p_i$,并且,$p_1+p_2+\cdots+p_n=1)$来静态描述的黑客,他的动态最佳攻击战术也是$(p_1,p_2,\cdots,p_n)$,即他将其攻击资金按比例$(p_1,p_2,\cdots,p_n)$分配后,可得到最多的"黑产收入"。

下面再对定理 2 进行一些更细致的讨论,我们有:

定理 3 如果攻破每个"元诱因"的投入产出比是相同的,即,各个 d_i彼此相等,都等于 a,那么此时的最优化双倍率 $W^*(p)=\log a-H(p)$,即最佳双倍率与熵之和为常数,并且,若按比例 $b^*=p$ 分配攻击资金,那么,此种战术的攻击业绩便可达到该最大值。此时,第 m 天之后,黑客的财富变成 $S_m=M2^{m[\log a-H(p)]}$。而且,黑客的熵若减少 1 比特,那么,他的财富就会翻一倍!

如果并不知道每个 d_i的具体值,而只知道 $\sum 1/d_i=1$,此时,记 $r_i=1/d_i$于是,双倍率可以重新写为:

$$\begin{aligned}W(b,p)&=\sum p_k\log(b_kd_k)\\&=\sum p_k\log[(b_k/p_k)p_kd_k)]\\&=D(p\mid r)-D(p\mid b)\end{aligned}$$

由此可见双倍率与相对熵之间存在着非常密切的关系。

由于黑客每天晚上都要攻击系统,他一定会总结一些经验来提高他的攻击效果。更准确地说,可以假设黑客知道了攻破系统的某种边信息 Y,也是一个随机变量。

设 $X\in\{1,2,\cdots,n\}$为第 X 个"元诱因",攻破概率为 $p(x)$,而攻击投入产出比为 $d(x)$。设(X,Y)的联合概率密度函数为 $p(x,y)$。用 $b(x\mid y)\geqslant 0,\sum_x b(x\mid y)=1$ 记为已经边信息 Y 的条件下,黑客对攻击资金的分配比例。此处 $b(x\mid y)$理解为:当得知信息 y 的条件下,用来攻击第 x 个"元诱因"的资金比例。对照前面的记号,将 $b(x)\geqslant 0,\sum_x b(x)=1$ 表示为无条件下,黑客对攻击资金的分配比例。

设无条件双倍率和条件双倍率分别为

$$W(X)=\max_{b(x)}\sum_x p(x)\log[b(x)d(x)]$$

$$W(X\mid Y)=\max_{b(x\mid y)}\sum_{x,y}p(x,y)\log[b(x\mid y)d(x)]$$

再设

$$\Delta W=W(X\mid Y)-W(X)$$

对于独立同分布的"攻击元诱因"序列(X_i,Y_i),可以看到:当具有边信息 Y 时,黑客的相对收益增长率为 $2^{mw(X\mid Y)}$;当黑客无边信息时,他的相对收益增长率为 $2^{mw(X)}$。

定理 4 由于获得攻击"元诱因"X 的边信息 Y,而引起的双倍率增量 ΔW 满足 $\Delta W=I(X;Y)$。这里 $I(X;Y)$是随机变量 X 和 Y 的互信息。

证明 在有边信息的条件下,按照条件比例分配攻击资金,即,$b^*(x\mid y)=p(x\mid y)$,那么关于边信息 Y 的条件双倍率 $W(X\mid Y)$可以达到最大值。于是:

$$\begin{aligned}W(X\mid Y)&=\max_{b(x\mid y)}E[\log S]=\max_{b(x\mid y)}\sum p(x,y)\log[d(x)b(x\mid y)]\\&=\sum p(x,y)\log[d(x)p(x\mid y)]=\sum p(x)\log d(x)-H(X\mid Y)\end{aligned}$$

当无边信息时,最优双倍率为

$$W(X)=\sum p(x)\log d(x)-H(X)$$

从而,由于边信息 Y 的存在,而导致的双倍率的增量为

$\Delta W=W(X\mid Y)-W(X)=H(X)-H(X\mid Y)=I(X;Y)$。证毕。

此处双倍率的增量,正好是边信息 Y 与"元诱因"X 之间的互信息。因此,如果边信息 Y 与"元诱因"X 相独立,那么,双倍率的增量就为 0。

设 X_k是黑客第 k 天攻破的"元诱因"的序号,假如各$\{X_k\}$之间不是独立的,又假设每个 d_k彼此相同,都等于 a。于是,黑客根据随机过程$\{X_k\}$来决定第$(k+1)$天的最佳攻击资金分配方案(即,最佳双倍率)为

$$W(X_k\mid X_{k-1},X_{k-2},\cdots,X_1)=E[\max E[\log S(X_k)\mid X_{k-1},X_{k-2},\cdots,X_1]]=\log a-H(X_k\mid X_{k-1},X_{k-2},\cdots,X_1)$$

这里的最大值 max 是针对所有满足如下条件的边信息攻击资金分配方案而取的:$b(x\mid X_{k-1},X_{k-2},\cdots,X_1)\geqslant 0,\sum_x b(x\mid X_{k-1},X_{k-2},\cdots,X_1)=1$。

而且,该最优双倍率可以在 $b(x_k\mid x_{k-1},x_{k-2},\cdots,x_1)=p(x_k\mid x_{k-1},x_{k-2},\cdots,x_1)$时达到。

第 m 天晚上的攻击结束后,黑客的总资产变成

$$S_m=M\prod_{i=1}^{m}S(X_i)$$

并且,其增长率的指数为

$$\begin{aligned}&(E\log S_m)/m=[\sum E\log(S(X_i))]/m\\&=[\sum(\log a-H(X_i\mid X_{i-1},X_{i-2},\cdots,X_1))]/m\\&=(n/m)\log a-[H(X_1,X_2,\cdots,X_m)]/m\end{aligned}$$

这里$[H(X_1,X_2,\cdots,X_m)]/m$ 是黑客 m 天攻击的平均熵。对于熵率为 $H(\chi)$的平衡随机过程,对上述增长率指数公式的两边取极限,可得

$$\lim_{m\to\infty}[E\log S_m]/m+H(\chi)=\log a$$

这再一次说明,熵率与双倍率之和为常数。

3 结束语

文献[1]~[6]奠定了《安全通论》的两个重要基

石:安全经络、安全攻防。

本文开始,我们将努力奠定《安全通论》的第三块重要基石:黑客。

没有黑客就没有安全问题,也更不需要《安全通论》。可惜,黑客不但有,而且还越来越多,而且其外在表现形式还千奇百怪,因此,有必要专门对黑客进行系统深入的研究。

本文虽然彻底解决了黑客的静态描述问题,即,黑客其实就是一个随机变量 X,它(他)的破坏力由 X 的概率分布函数 $F(x)$(或概率密度函数 $p(x)$)来决定。但是,关于黑客的动态描述问题,还远未解决,本文只是在若干假定之下,给出了黑客攻击的最佳战术。欢迎有兴趣的读者来研究黑客的其他攻击行为的最佳战术。

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] Thomas M Cover, Joy A Thomas. 信息论基础[M]. 阮吉寿,张华,译. 北京:机械工业出版社出版,2007.