DOI:10.3969/j.issn.1009-6868.2016.02.013
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20160224.1559.002.html

编者按:网络空间安全作为一项新的全球治理议程,已经成为世界关注的焦点、各国政府的战略目标之一,但人们对网络空间安全的研究,还缺乏全面系统的理论指导,针对该问题,我刊特转载自《科学网》一篇由北京邮电大学杨义先、钮心忻教授编写的《安全通论——攻防篇之“盲对抗”》(原文网址:http://blog.sciencenet.cn/blog-453322-947304.html)。在该文章中,给出了黑客攻击能力和红客防御能力的可达理论极限,并巧妙地构造了一个随机变量$Z=(X+Y)\bmod 2$,将一次真正成功的攻防问题,等价地转换成了攻击信道$(X;Z)$,同时恰到好处地应用了看似并不相关的仙农编码定理。

安全通论——攻防篇之“盲对抗”

The General Theory of Security: Blind Confrontation in Offensive and Defensive

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 02-0057-004

摘要:精确地给出了黑客攻击能力和红客防御能力的可达理论极限。对黑客来说,如果他想真正成功地把红客打败k次,一定有某种技巧,使他能够在k/C次进攻中,以任意接近1的概率达到目的;如果黑客经过n次攻击,获得了S次真正成功,那么一定有$S\leqslant nC$。对红客来说,如果他想真正成功地把黑客挡住R次,一定有某种技巧,使得他能够在R/C次防御中,以任意接近1的概率达到目的;如果红客经过n次防卫,获得了R次真正成功,一定有$R\leqslant ND$。这里C和D分别是攻击信道和防御信道的信道容量。如果$C<D$,则黑客输;如果$C>D$,则红客输;如果$C=D$,则红黑实力相当。

关键词:黑客;红客;进攻;防御;信道

Abstract: In this paper, the limit theory of hacker attack ability and honker defense ability is given. If a hacker wants to beat a honker K times, there must be some skills, so that he can achieve the purpose with probability arbitrarily close to 1 in the k/C times' offensive. If a hacker achieves S successes after n attacks, there must be $S\leqslant nC$. If a honker wants to defend against a hacker R times, there must be some skills, so he can achieve the purpose with probability arbitrarily close to 1 in the k/C times' defensive; If a honker achieve n times' real success after n times' defensive, there must be $R\leqslant ND$. C and D respectively represent the channel capacity of offensive channel and defensive channel. If $C<D$, then the hacker loses. If $C>D$, then the honker loses. If $C=D$, they have considerable strength.

Key words: hacker; honker; offensive; defensive; channel

杨义先/YANG Yixian
钮心忻/NIU Xinxin
(北京邮电大学 信息安全中心,北京 100876)
(Information Security Center, Beijing University of Post and Telecommunication, Beijing 100876, China)

- 攻防是安全的核心,特别是在有红黑双方对抗的场景下,攻防几乎就等于安全
- 在攻防系统中,只有攻方和守方这两个直接利益相关方,但绝没有利益无关的第三方
- 无裁判攻防可分为盲攻防和非盲攻防

1 盲对抗场境

攻防是安全的核心,特别是在有红黑双方对抗的场景下(比如,战场、公安、网络安全等),攻防几乎就等于安全。所以,在安全通论的建立过程中,我们将花费更多的篇幅来研究攻防问题。但是,长期以来,人们并未对攻防场景进行过清晰的整理,再加上攻防一词经常被滥用,从而导致攻防几乎成了一个只能意会不能言传的名词,当然就更无法对攻防进行系统的理论研究了。

因此,为了开始我们的研究,必须首先理清攻防场景。更准确地说,下面我们只考虑无裁判的攻防,因为像日常看到的诸如拳击比赛等有裁判攻防的体育项目,并不是真正的攻防。在攻防系统中,只有攻方和守方这两个直接利益相关方(虽然有时涉及的人员会超过两个),但绝没有利益无关的第三方。所以,对攻防结果

收稿时间:2016-01-22
网络出版时间:2016-02-24

来说，吹哨的裁判员其实是干扰，是噪音，而且还是主观的噪音，因此必须要去除。

无裁判攻防又可以进一步分为两大类：盲攻防、非盲攻防。所谓盲攻防，指每次攻防后，双方都只知道自己的损益情况，而对另一方却一无所知，比如，大国博弈、网络攻防、实际战场、间谍战、泼妇互骂等都是盲攻防的例子；非盲攻防，指每次攻防后，双方都知道本次攻防的结果，而且还一致认同这个结果，比如，石头剪刀布游戏、下棋、炒股等都是非盲攻防的例子。一般来说，盲对抗更血腥和残酷，而非盲对抗的娱乐味更浓。在文章中，我们只考虑盲攻防[1]。

为了更形象地说明，下面我们仍然借用拳击的术语来介绍盲攻防系统。当然，这时裁判已经被赶走，代替裁判的是无所不知的上帝。

攻方（黑客）是个神仙拳击手，永远不知累，他可用随机变量 X 来表示。黑客每次出击后，都会对自己的本次出击给出一个真心盲评价（比如，自认为本次出击成功或失败，当自认为本次出击成功时，记为 $X=1$；当自认为出击失败时，记为 $X=0$），但是，他绝不将这个真心盲评价系统告诉任何人。此处，之所以假定攻方（黑客）的盲自评要对外保密，是因为我们可以因此认定他的盲自评是真心的，不会也没有必要弄虚作假。

守方（红客）也是个神仙拳击手，他也永远不知累，可用随机变量 Y 来表示。红客每次守卫后，也都会对自己的这次守卫给出一个真心盲评价（比如，自认为本次守卫是成功或失败，当自认为守卫成功时，记为 $Y=1$；当自认为守卫失败时，记为 $Y=0$）。这个评价也仍然绝不告诉任何人。同样，之所以要假定红客的盲自评要对外保密，是因为我们可以因此认定他的自评是真心的，不会也没有必要弄虚作假。

裁判员虽然被赶走了，但是我们却把上帝请来了。不过，上帝只是远远地呆在凌霄宝殿看热闹，他知道攻守双方心里的真实想法，因此也知道双方对每次攻防的真心盲自评，于是他可将攻守双方过去 N 次对抗的盲自评结果记录下来：$(X, Y)=(X_1, Y_1)、(X_2, Y_2)、\cdots、(X_N, Y_N)$。

由于当 N 趋于无穷大时，频率趋于概率 P_r，所以只要攻守双方足够长时间对抗之后，上帝便可以得到随机变量 X、Y 的概率分布和 (X, Y) 的联合概率分布：

P_r（攻方盲自评为成功）= $P_r(X=1)=p$

P_r（攻方盲自评为失败）= $P_r(X=0)=1-p$，$0<p<1$

P_r（守方盲自评为成功）= $P_r(Y=1)=q$

P_r（守方盲自评为失败）= $P_r(Y=0)=1-q$，$0<q<1$

P_r（攻方盲自评为成功，守方盲自评为成功）= $P_r(X=1, Y=1)=a$，$0<a<1$

P_r（攻方盲自评为成功，守方盲自评为失败）= $P_r(X=1, Y=0)=b$，$0<b<1$

P_r（攻方盲自评为失败，守方盲自评为成功）= $P_r(X=0, Y=1)=c$，$0<c<1$

P_r（攻方盲自评为失败，守方盲自评为失败）= $P_r(X=0, Y=0)=d$，$0<d<1$

这里，a、b、c、d、p、q 之间还满足式(1) ~ (3)：

$$a+b+c+d=1 \tag{1}$$

$$p=P_r(X=1)=P_r(X=1,Y=0)+P_r(X=1,Y=1)=a+b \tag{2}$$

$$q=P_r(Y=1)=P_r(X=1,Y=1)+P_r(X=0,Y=1)=a+c \tag{3}$$

所以，6 个变量 a、b、c、d、p、q 中，其实只有 3 个是独立的。

足够长的时间之后，上帝看够了，便叫停攻守双方。让他们分别对擂台进行有利于自己的秘密调整，当然某方（或双方）也可以放弃本次调整的机会，如果他（他们）认为当前擂台对自己更有利的话。这里，所谓的秘密调整，指双方都不知道对方做了些什么调整。比如，针对网络空间安全对抗，也许红客安装了一个防火墙，也许黑客植入了一种新的恶意代码等；针对阵地战的情况，也许攻方调来了一去增援部队，也许守方又埋了一批地雷等。

总之，攻守双方调整完成后，双方又在新的擂台上，再开始下一轮的对抗。

不过，我们不研究攻守双方的下一轮对抗，只考虑当前轮，即由上面的 X、Y、(X, Y) 等随机变量所组成的系统。

至此，盲攻防场景的精确描述就完成了。可见，网络战、间谍战、泼妇互骂等对抗性很惨烈的攻防，都是典型的盲对抗。

2 黑客攻击能力极限

根据第 1 节中的随机变量 X 和 Y，上帝再新造一个随机变量 $Z=(X+Y) \bmod 2$。由于任何两个随机变量都可以组成一个通信信道，所以我们把 X 作为输入，Z 作为输出，上帝便可构造出一个通信信道 F，我们称之为攻击信道。

由于攻方（黑客）的目的是要打败守方（红客），所以黑客是否真正成功，不能由自己的盲评价来定（虽然这个盲评价是真心的），而应该是由红客的真心盲评价说了算，所以则有式(4)：

{攻方的某次攻击真正成功}

={攻方本次盲自评为成功∩守方本次盲自评为失败}∪{攻方本次盲自评为失败∩守方本次盲自评为失败}

$=\{X=1,Y=0\}\cup\{X=0,Y=0\}$

$=\{X=1, Z=1\}\cup\{X=0,Z=0\}$

={1 bit 信息被成功地从通信系统 F 的发端 (X) 传输到了收端 (Z)}。 (4)

另一方面，如果有 1 bit 信息被成功地从发端 (X) 传到了收端 (Z)，那么要么是“$X=0$，$Z=0$”，要么是“$X=1$，$Z=1$”。由于 $Y=(X+Z) \bmod 2$，所以由“$X=0$，$Z=0$”推知“$X=0$，$Y=0$”；由“$X=1$，$Z=1$”推知“$X=1$，$Y=0$”。而“$X=0$，$Y=0$”意味着攻防本次盲自评为失败∩守方本次盲自评为失败；“$X=1$，$Y=0$”意味着

攻方本次盲自评为成功∩守方本次盲自评为失败；综合起来就意味着攻方获得某次攻击的真正成功。

简而言之，我们可以知道：如果黑客的某次攻击真正成功，那么攻击信道F就成功地传输1 bit到收端；如果有1 bit被成功地从攻击信道F的发端，传送到了收端，那么黑客X就获得了一次真正成功攻击。

引理1：黑客获得一次真正成功的攻击，其实就对等于攻击信道F成功地传输了1 bit。

根据仙农信息论的著名《信道编码定理》[2]：如果信道F的容量为C，那么对于任意传输率$k/n\leq C$，都可以在译码错误概率任意小的情况下，通过某个n bit长的码字，成功地把k bit传输到收信端；如果信道F能够用n长码字，把S bit无误差地传输到收端，那么，一定有$S\leq nC$。

定理1（黑客攻击能力极限定理）：设由随机变量$(X;Z)$组成的攻击信道F的信道容量为C。那么：如果黑客想真正成功地把红客打败k次，一定有某种技巧（对应于仙农编码），使得他能够在k/C次攻击中，以任意接近1的概率达到目的；如果黑客经过n次攻击，获得了S次真正成功的攻击，一定有$S\leq nC$。

由定理1可知：只要求出攻击信道F的信道容量C，那么黑客的攻击能力极限就确定了。

下面我们需要计算出F的信道容量C。

首先，由于随机变量$Z=(X+Y) \bmod 2$，所以可以由X和Y的概率分布，得到Z的概率分布如下：

$$P_r(Z=0)$$
$$= P_r(X=Y)$$
$$= P_r(\text{攻守双方的盲自评结果一致})$$
$$= P_r(X=0,\ Y=0)+ P_r(X=1,\ Y=1)$$
$$= a+d$$
$$P_r(Z=1)$$
$$= P_r(X\neq Y)$$
$$= P_r(\text{攻守双方的盲自评结果相反})$$
$$= P_r(X=0,\ Y=1)+ P_r(X=1,\ Y=0)$$
$$= b+c$$
$$= 1-(a+d)$$

考虑通信系统F，它由随机变量X和Z构成的，即它以X为输入，Z为输出，它的2X2阶转移概率矩阵为$A=[A(x,z)]=[P_r(z \mid x)]$，这里$x$，$z$=0或1。

$$A(0,0)$$
$$= P_r(Z=0 \mid X=0)$$
$$= [P_r(Z=0,\ X=0)]/\ P_r(X=0)$$
$$= [P_r(Y=0,\ X=0)]/(1-p)$$
$$= d/(1-p)$$
$$A(0,1)$$
$$= P_r(Z=1 \mid X=0)$$
$$= [P_r(Z=1,\ X=0)]/\ P_r(X=0)$$
$$= [P_r(Y=1,\ X=0)]/(1-p)$$
$$= c/(1-p)$$
$$= 1-d/(1-p)$$
$$A(1,0)$$
$$= P_r(Z=0 \mid X=1)$$
$$= [P_r(Z=0,\ X=1)]/\ P_r(X=1)$$
$$= [P_r(Y=1,\ X=1)]/p$$
$$=a/p$$
$$A(1,1)$$
$$= P_r(Z=1 \mid X=1)$$
$$= [P_r(Z=1,\ X=1)]/\ P_r(X=1)$$
$$= [P_r(Y=0,\ X=1)]/p$$
$$=b/p$$
$$=(p-a)/p$$

由于随机变量(X,Z)的联合概率分布为：

$$P_r(X=0,\ Z=0)=P_r(X=0,Y=0)= d$$
$$P_r(X=0,\ Z=1)=P_r(X=0,Y=1)= c$$
$$P_r(X=1,\ Z=0)=P_r(X=1,Y=1)= a$$
$$P_r(X=1,\ Z=1)=P_r(X=1,Y=0)= b$$

所以，随机变量X与Z之间的互信息为：

$$I(X,\ Z)$$
$$=\sum_x\sum_z p(x,\ z)\log(p(x,\ z)/[p(x)p(z)])$$
$$=d\log[d/[(1-p)(a+d)]] +$$
$$c\log[c/[(1-p)(b+c)]] +$$
$$a\log[a/[p(a+d)]] +b\log[b/[p(b+c)]] \quad (5)$$

由于此处有：$a+b+c+d=1$，$p=a+b$，$q=a+c$，$0<a,b,c,d,p,q<1$，所以式(5)可以进一步转化为只与变量a和p有关的式(6)（注意：此时q已不再是变量，而是确定值了）：

$$I(X,\ Z)$$
$$=[1+a-(p+q)]\log[[1+a-$$
$$(p+q)]/[(1-p)(1+2a-p-q)]] +$$
$$(q-a)\log[(q-a/[(1-p)(p+q-2a)])] +$$
$$a\log[a/[p(1+2a-p-q)]] +$$
$$(p-a)\log[(p-a)/[p(p+q-2a)]] \quad (6)$$

利用此$I(X,\ Z)$就可知：以X为输入，Z为输出的信道F的信道容量C就等于$\text{Max}[I(X,\ Z)]$（这里最大值是针对X为所有可能的二元离散随机变量来计算的）。更简单地说：容量C等于$\text{Max}_{0<a,p<1}[I(X,Z)]$（这里的最大值是对仅仅两个变量$a$和$p$在条件$0<a$，$p<1$下之取的），所以该信道容量的计算就很简单了。

3 红客守卫能力极限

设随机变量X、Y、Z和(X,Y)等都与前面相同。

根据随机变量Y（红客）和Z，上帝再组成另一个通信信道G，称为防御信道，即把Y作为输入，把Z作为输出。

由于守方（红客）的目的是要挡住攻方（黑客）的进攻，所以红客是否真正成功，不能由自己的盲评价来定，而应该是由黑客的真心盲评价说了算，所以就应该有如式(7)中的等式成立：

$$\{\text{守方的某次防卫真正成功}\}$$
$$=\{\text{守方本次盲自评为成功}\cap\text{攻方本次盲自评为失败}\}\cup\{\text{守方本次盲自评为失败}\cap\text{攻方本次盲自评为失败}\}$$
$$=\{Y=1,\ X=0\}\cup\{Y=0,\ X=0\}$$
$$=\{Y=1,\ Z=1\}\cup\{Y=0,\ Z=0\}$$
$$=\{1\text{ bit信息被成功地从防御信道G的发端}(Y)\text{传输到了收端}(Z)\}。 \quad (7)$$

与攻击信道的情况类似，反过来，式(7)也就意味着：如果在防御信道G中，1 bit信息被成功地从发端(Y)传到了收端(Z)，那么红客就获得了一次真正成功的防卫。

引理2：红客获得一次真正成功

的守卫，其实就是防御信道G成功地传输了1 bit。

定理2（红客守卫能力极限定理）：设由随机变量$(Y;Z)$组成的防御信道G的信道容量为D。那么则有：如果红客想真正成功地把黑客挡住R次，那么一定有某种技巧（对应于仙农编码），使得他能够在R/C次防御中，以任意接近1的概率达到目的；如果红客经过N次守卫，获得了R次真正成功的守卫，那么，一定有$R\leqslant ND$。

考虑通信系统G，它由随机变量Y和Z构成的，即它以Y为输入，Z为输出，它的2X2阶转移概率矩阵为$B=[B(y,z)]=[P_t(z \mid y)]$，这里$y,z=0$或1。

$$
\begin{aligned}
&B(0,0)\\
&=P_t(Z=0 \mid Y=0)\\
&=[P_t(Z=0,Y=0)]/P_t(Y=0)\\
&=[P_t(X=0,Y=0)]/(1-q)\\
&=d/(1-q)\\
&B(0,1)\\
&=P_t(Z=1 \mid Y=0)\\
&=[P_t(Z=1,Y=0)]/P_t(Y=0)\\
&=[P_t(X=1,Y=0)]/(1-q)\\
&=b/(1-q)\\
&B(1,0)\\
&=P_t(Z=0 \mid Y=1)\\
&=[P_t(Z=0,Y=1)]/P_t(Y=1)\\
&=[P_t(X=1,Y=1)]/q\\
&=a/q\\
&B(1,1)\\
&=P_t(Z=1 \mid Y=1)\\
&=[P_t(Z=1,Y=1)]/P_t(Y=1)\\
&=[P_t(X=0,Y=1)]/q\\
&=c/q
\end{aligned}
$$

由于随机变量(Y,Z)的联合概率分布为：

$$
\begin{aligned}
&P_t(Y=0,Z=0)=P_t(X=0,Y=0)=d\\
&P_t(Y=0,Z=1)=P_t(X=1,Y=0)=b\\
&P_t(Y=1,Z=0)=P_t(X=1,Y=1)=a\\
&P_t(Y=1,Z=1)=P_t(X=0,Y=1)=c
\end{aligned}
$$

所以，随机变量Y与Z之间的互信息为：

$$
\begin{aligned}
&I(Y,Z)\\
&=\sum_y\sum_z p(y,z)\log(p(y,z)/[p(y)p(z)])\\
&=d\log[d/[(1-q)(a+d)]]+\\
&b\log[b/[(1-q)(b+c)]]+\\
&a\log[a/[q(a+d)]]+c\log[c/[q(b+c)]] \qquad (8)
\end{aligned}
$$

由于此处有：$a+b+c+d=1$，$p=a+b$，$q=a+c$，$0<a,b,c,d,p,q<1$，所以式(8)可以进一步转化为只与变量a和q有关的式(9)（注意：此时p不再是变量，而是确定值了）：

$$
\begin{aligned}
&I(Y,Z)\\
&=(1+a-p-q)\log[(1+a-p-q)/\\
&[(1-q)(1+2a-p-q)]]+(p-a)\log[(p-a)/\\
&[(1-q)(p+q-2a)]]+a\log[a/\\
&[q(1+2a-p-q)]]+(q-a)\log[(q-a)/\\
&[q(p+q-2a)]] \qquad (9)
\end{aligned}
$$

利用此$I(Y,Z)$可知：以Y为输入，Z为输出的防御信道G的信道容量D就等于$\mathrm{Max}[I(Y,Z)]$（这里最大值是针对Y为所有可能的二元离散随机变量来计算的）或者更简单地说，容量D等于$\mathrm{Max}_{0<a,\ q<1}[I(Y,Z)]$（这里的最大值是对仅仅两个变量$a$和$q$在条件$0<a,q<1$下之取的），所以该信道容量的计算就很简单。

4 攻守双方的实力比较

由于信道容量是在传信率k/n保持不变的情况下，系统所能够传输的最大信息比特数，而每成功传输1 bit，就相当于攻方的一次攻击真正成功（或守方的一次防守真正成功），所以从宏观的角度来看，我们可以推导出定理3。

定理3（攻守实力定理）：设C和D分别表示攻击信道F和防御信道G的信道容量，如果$C<D$，那么整体上黑客处于弱势；如果$C>D$，那么整体上红客处于弱势；如果$C=D$，那么红黑双方实力相当。

我们需要注意到：攻击信道的容量C，其实是q的函数，所以可以记之为$C(q)$；同理，防御信道的容量D是p的函数，可以记之为$D(p)$。由此，在盲对抗中，红黑双方可以通过对自己预期的调整，即改变相应的概率分q和p，从而改变$C(q)$和$D(p)$的大小，并最终提升自己在盲对抗中的胜算情况。换句话说，我们证明了一个早已熟知的社会事实，即定理4。

定理4（知足常乐定理）：在盲对抗中，黑客（或红客）有两种思路来提高自己的业绩，或称为“幸福指数”。增强自身的相对打击（或抵抗）力，即增加b和d（或c和a）；降低自己的贪欲，即增加p（或q）。但是，需要注意你可能无法改变外界，即调整b和d（或c和a），但却可以改变自身，即调整p（或q）。由此可见：知足常乐是盲对抗中的一个真理。

5 结束语

我们的诀窍有两点：巧妙地构造了一个随机变量$Z=(X+Y)\mathrm{mod}2$，并将一次真正成功的攻防问题，等价地转换成了攻击信道$(X;Z)$（或者防守信道$(Y;Z)$）的1 bit成功传输问题；恰到好处地应用了看似风马牛不相关的仙农编码定理。以上两点，任缺一项，就不会找到让“黑客悟空”永远也跳不出去的“如来手掌”。

参考文献

[1] THOMAS M C, THOMAS J A.信息论基础[M]. 阮吉寿, 张华, 译. 北京：机械工业出版社出版, 2007

[2] SHU L, DANIEL J C. 差错控制编码[M]. 晏坚, 何元智, 潘亚汉, 等译. 北京：机械工业出版社出版, 2007

作者简介

杨义先，灾备技术国家工程实验室主任，北京邮电大学教授、博士生导师，信息安全中心主任，首批长江学者特聘教授，首届国家杰出青年基金获得者，中国密码学会副理事长；目前研究方向为网络空间安全、现代密码学和纠错编码等；获得包括国家发明奖和省部级科技进步奖等在内的各类科技奖励20余项，授权发明专利4项，主持和参与多项国家“863”、国家自然科学基金、省部级等科研项目；发表高水平论文500余篇，出版专著及教材20多部。

钮心忻，北京邮电大学计算机学院教授、博士生导师；长期从事网络与信息安全、信号与信息处理等方面的研究工作。