文章编号：2096-1618(2016)01-0006-06
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-947304.html
发表时间：2016-01-01

安全通论(2)

——攻防篇之“盲对抗”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：本文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，那么，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，那么，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。反过来，如果红客经过 N 次防卫，获得了 R 次“真正成功”，那么，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 $C<D$，那么黑客输；如果 $C>D$，那么红客输；如果 $C=D$，那么，红黑实力相当。

0　引言

谁都承认，以网络安全、领土安全、环境安全、粮食安全、身体健康、公共安全、国家安全等为代表的“安全问题”是头等大事。但是，直到现在为止，无论是国内还是国外，对安全问题都没有真正系统研究过。虽然，各国都花费了大量的人力和物力，去研究具体的安全问题，但是，大家都几乎是“只见树木，不见森林”，从来没有人提出过一整套，适合于所有安全问题的，系统的“安全基础理论”，甚至，根本就不相信这样的理论会存在！

作者不信邪，非要试图来研究一套“放之四海而皆准”的安全基础理论，称之为“安全通论”，当然，我们很清楚，这样的理论绝非能轻易建立和完成的。在文献[1]中，我们已经证明了一个出人意料的结果：针对任何有限系统，若从安全角度去考虑，那么，它的所有“不安全”问题，都可以很清晰地分解成一棵有限的“倒立树”。使得，

(1)只要用心维护好这棵“倒立树”的安全，那么，整个系统的安全就可以得到充分保障了；

(2)如果系统出现了某个安全问题，那么，就一定可以从这棵“倒立树”中分离出一个或几个“树枝”，满足：(A)除了这些“树枝”外，“倒立树”的所有其它“树枝”都是无病的；(B)对有病的“树枝”，只需要对其底部的带病末端进行“医治”，然后，其它上层的“分枝”等都会自愈。

此处之所以要限定“系统是有限的”，是因为，在现实工程中，所遇到的系统(比如，网络系统、消防系统、实际战场等)都是有限的。

实际上，文献[1]已经展示了“安全通论”的冰山一角，更使我们相信：“放之四海而皆准的”安全理论是存在的！

本文再继续对“安全通论”进行更深入的挖掘。

由于本文读者面也很广，上可以包括国家元首，中可以包括网络黑客，下可以包括骂街泼妇等；也更由于当前国内学术界过于看重 SCI 等机械指标，所以，与文献[1]的处理方法一样，我们带头挑战 SCI，直接将论文实名发表在网络上，欢迎各界安全专家批评指正。

同时，更欢迎大家一起来研究“安全通论”，无论你是信息安全专家、军事家、政治家、医生、股神、拳王、泼妇等需要考虑对抗问题的任何人。

1　盲对抗场境描述

“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”:其实,“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,必须去除。

“无裁判攻防”又可以进一步地分为两大类:盲攻防、非盲攻防。所谓“盲攻防”,意指每次攻防后,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。所谓“非盲攻防”,意指每次攻防后,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。本文只考虑“盲攻防”;有关“非盲攻防”的研究,将在后续文章中给出。

为形象计,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。他每次出击后,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,这个“真心盲评价”他绝不告诉任何人,只有他自己才知道(当然,上帝也知道)! 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 来表示他。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,只有红客自己才知道!(当然,上帝本来就知道)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。

注:这里“盲评价”的“盲”,主要意指双方都不知道对方的评价,而只知道自己的评价,但是,这个评价却是任何第三方都不能“说三道四”的。比如,针对“黑客一拳打掉红客假牙”这个事实,也许吹哨的那个“裁判员”会认定“黑客成功”。但是,当事双方的评价可能会完全不一样,比如:也许黑客的“盲自评”是“成功,$X=1$”(如果他原本以为打不着对方的),也许黑客的“盲自评”是“失败,$X=0$”(如果他原本以为会打瞎对方眼睛的);也许红客的“防卫盲自评”是“成功,$Y=1$”(如果他原本以为会因此次攻击毙命的),也许红客的“防卫盲自评”是“失败,$Y=0$”(如果他原本以为对方会扑空的)。总之,到底攻守双方对本次“打掉假牙”如何评价,只有他们自己心里才明白! 你看,我们“把那个吹哨的裁判员赶走”是正确的吧,谁敢说他不会“吹黑哨”呢?

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) 的联合概率分布如下:

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 之间还满足如下三个线性关系等式:

$$a+b+c+d=1;$$

$$p=P_r(X=1)=P_r(X=1,Y=0)+P_r(X=1,Y=1)=a+b$$

$$q=P_r(Y=1)=P_r(X=1,Y=1)+P_r(X=0,Y=1)=a+c$$

所以,6 个变量 a,b,c,d,p,q 中,其实只有三个是独立的。

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”,即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,双方又在新擂台上,

再开始“下一轮”的对抗。

不过,本文不研究攻守双方的“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

根据上节中的随机变量 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,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,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,就应该有如下事件等式成立:

$\{$攻方的某次攻击真正成功$\}$

$=\{$攻方本次盲自评为成功$\cap$守方本次盲自评为失败$\}\cup\{$攻方本次盲自评为失败$\cap$守方本次盲自评为失败$\}$

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

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

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

另一方面,反过来,如果有 1 比特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$\cap$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$\cap$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,我们知道:(1)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 个比特到收端;反之,(2)如果有一个比特被成功地从“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”。即,我们有:

引理 1:黑客获得一次“真正成功的攻击”,其实就对等于说:“攻击信道”F 成功地传输了一个比特。

根据仙农信息论的著名“信道编码定理”[2][3]:如果信道 F 的容量为 C,那么,对于任意传输率 $k/n\leqslant C$,都可以在译码错误概率任意小的情况下,通过某个 n 比特长的码字,成功地把 k 个比特传输到收信端。反过来,如果信道 F 能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S\leqslant nC$。

利用引理 1,就可把这段话翻译成如下重要定理:

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,1)如果黑客想“真正成功”地把红客打败 k 次,那么,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。反过来,(2)如果黑客经过 n 次攻击,获得了 S 次“真正成功”的攻击,那么,一定有 $S\leqslant nC$。

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。

下面来计算 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:

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

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 2×2 阶转移概率矩阵为 $\mathbf{A}=[A(x,z)]=[P_r(z\mid x)]$,这里 $x,z=0$ 或 1,

$$
\begin{aligned}
&\mathrm{A}(0,0)\\
&=P_r(Z=0\mid X=0)\\
&=[P_r(Z=0,X=0)]/P_r(X=0)\\
&=[P_r(Y=0,X=0)]/(1-p)\\
&=d/(1-p);\\
&\mathrm{A}(0,1)\\
&=P_r(Z=1\mid X=0)\\
&=[P_r(Z=1,X=0)]/P_r(X=0)\\
&=[P_r(Y=1,X=0)]/(1-p)\\
&=c/(1-p)\\
&=1-d/(1-p);\\
&\mathrm{A}(1,0)\\
&=P_r(Z=0\mid X=1)\\
&=[P_r(Z=0,X=1)]/P_r(X=1)
\end{aligned}
$$

$= [P_r(Y=1,X=1)]/p$

$=a/p$;

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

$I(X,Z)$

$=\sum_x\sum_z p(x,z)\log(p(x,z)/[p(x)p(z)])$

$=d\log[d/[(1-p)(a+d)]]$

$+c\log[c/[(1-p)(b+c)]]$

$+a\log[a/[p(a+d)]]$

$+b\log[b/[p(b+c)]]$

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,上述公式可以进一步转化为只与变量 a 和 p 有关的如下公式(注意:此时 q 已不再是变量,而是确定值了)

$I(X,Z)$

$=[1+a-(p+q)]\log[[1+a-(p+q)]/[(1-p)(1+2a-p-q)]]$

$+(q-a)\log[(q-a/[(1-p)(p+q-2a)])]$

$+a\log[a/[p(1+2a-p-q)]]$

$+(p-a)\log[(p-a)/[p(p+q-2a)]]$

于是,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 $\mathrm{Max}[I(X,Z)]$(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)或者更简单地说:容量 C 等于 $\mathrm{Max}_{0<a,p<1}[I(X,Z)]$(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。

好了,"攻"的量化研究就到此。下面再来考虑"守"的情况。

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,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,就应该有如下事件等式成立:

{守方的某次防卫真正成功}

={守方本次盲自评为成功∩攻方本次盲自评为失败}∪{守方本次盲自评为失败∩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 比特信息被成功地从防御信道 G 的发端(Y)传输到了收端(Z)}。

与"攻击信道"的情况类似,反过来,上述事件等式也就意味着:如果在"防御信道"G 中,1 比特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。

与引理 1 类似,我们有:

引理 2:红客获得一次"真正成功的守卫",其实就对等于说:"防御信道"G 成功地传输了一个比特。

与定理 1 类似,我们也可得到如下重要定理:

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,(1)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。反过来,(2)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 $R\leqslant ND$。

下面再来计算"防御信道"G 的"信道容量"D:

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 2×2 阶转移概率矩阵为 $B=[B(y,z)]=[P_r(z \mid y)]$,这里 $y,z=0$ 或 1,

$B(0,0)$

$= P_r(Z=0 \mid Y=0)$

$= [P_r(Z=0,Y=0)]/P_r(Y=0)$

$= [P_r(X=0,Y=0)]/(1-q)$

$= d/(1-q)$;

$B(0,1)$

$= P_r(Z=1 \mid Y=0)$

$= [P_r(Z=1,Y=0)]/P_r(Y=0)$

$= [P_r(X=1,Y=0)]/(1-q)$

$= b/(1-q)$;

$B(1,0)$

$= P_r(Z=0 \mid Y=1)$

$= [P_r(Z=0,Y=1)]/P_r(Y=1)$

$= [P_r(X=1,Y=1)]/q$

$=a/q$;

B(1,1)

$= P_r(Z=1 \mid Y=1)$

$= [P_r(Z=1,Y=1)]/P_r(Y=1)$

$= [P_r(X=0,Y=1)]/q$

$=c/q$。

由于随机变量(Y,Z)的联合概率分布为:

$P_r(Y=0,Z=0)=P_r(X=0,Y=0)= d$

$P_r(Y=0,Z=1)=P_r(X=1,Y=0)= b$

$P_r(Y=1,Z=0)=P_r(X=1,Y=1)= a$

$P_r(Y=1,Z=1)=P_r(X=0,Y=1)= c$

所以,随机变量 Y 与 Z 之间的互信息为:

$I(Y,Z)$

$= \sum_Y \sum_Z p(y,z)\log(p(y,z)/[p(y)p(z)])$

$= d\log[d/[(1-q)(a+d)]]$

$+b\log[b/[(1-q)(b+c)]]$

$+a\log[a/[q(a+d)]]$

$+c\log[c/[q(b+c)]]$

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,上述公式可以进一步转化为只与变量 a 和 q 有关的如下公式(注意:此时 p 不再是变量,而是确定值了)

$I(Y,Z)$

$= (1+a-p-q)\log[(1+a-p-q)/[(1-q)(1+2a-p-q)]]$

$+(p-a)\log[(p-a)/[(1-q)(p+q-2a)]]$

$+a\log[a/[q(1+2a-p-q)]]$

$+(q-a)\log[(q-a)/[q(p+q-2a)]]$

于是,利用此 $I(Y,Z)$ 就可知,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了。

到此,我们也给出了红客防卫能力的极限。

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 比特,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,从宏观角度来看,我们就有:

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",那么,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,难分伯仲。

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(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":其一,增强自身的相对打击(或抵抗)力,即,增加 b 和 d(或 c 和 a);其二,降低自己的贪欲,即,增加 p(或 q)。但是,请注意,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"不仅仅是一个成语,而且也是"盲对抗"中的一个真理。

5 结束语

我们的诀窍有两点:其一,巧妙地构造了一个随机变量 $Z=(X+Y) \bmod 2$,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 比特成功传输"问题;其二,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"。

其实,排除"事后诸葛亮"因素,屠呦呦获诺贝尔奖还真与她老父亲取名有关系。因为,任何人,如果他姓名与"青蒿"有关,那么,他都会在碰到与"青蒿"所有相关的事情上,比其它人更多一分关注。

类似的歪打正着,最近也被我们给碰上了。二十几年前读研时,我们就看过仙农的著名论文"Communication Theory of Secrecy Systems",后来,就一直从事网络安全的科教工作。由于仙农的这篇文章中,有一个词"Secrecy",所以,冥冥之中,总觉得仙农理论与安全有关,虽然明知其中的牵强多过实际,因为:一来,仙农的"Secrecy"仅仅是现在信息安全的很小一部分,更与本文中研究的"广义安全"相差十万八千里;二来,在本文中扮演核心角色的仙农编码定理其实是发表在仙农的另一篇著名论文"Mathematical Theory of Communication"中,根本就没带"Secrecy"字眼。但是,像

屠呦呦会特别关注“青蒿”一样,我们在考虑安全问题时,也特别关注仙农,这不,我们这对“瞎猫”,就真的“碰到死耗子”了!

特别说明:这本该是一篇高影响因子的 SCI 论文,但是,如今国人已被 SCI 绑架了,所以,老夫想带头摆脱 SCI 的束搏,故将此文在这里发表。本文欢迎所有媒体转载。

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

[3] Shu Lin,Daniel J,Costello Jr. 差错控制码[M]. 晏坚,何元智,潘亚汉,等译. 北京:机械工程出版社,2007.