【编者按】2015年,国务院学位委员会、教育部正式批准增设“网络空间安全”一级学科授权点,中国信息安全学术界十余年来的不懈努力,终于美梦成真!

然而,像所有新兴学科一样,“网络空间安全”还是只丑小鸭,除密码学等少数分支外,至今还没有自己的基础理论羽翼;在许多人眼里,国内外信息安全专家只不过是能织善补的“巧匠”而已。

当年的冯·诺伊曼理论让“计算机工程”变成了“计算机科学”,香农信息论让“通信工程”这株柔弱的小苗变成了枝繁叶茂的参天大树,如果有人能创建网络空间安全的理论基础,让这门新兴学科插上腾飞的翅膀,把丑小鸭变成白天鹅,无疑是对科学的巨大贡献。

有幸的是,两位中国学者勇敢地站出来,率先冲向《安全通论》的前沿阵地,抛出一系列“砖”,以期引来更多的“玉”!

不管《安全通论》最终能否成为网络空间安全的理论基础,必然引爆通用安全理论研究的热潮,将在这门新兴学科的发展史上留下不可磨灭的印记。

为永久记录这一历史时刻,也为作者“引玉”之初心,本刊从2016年第1期起,每期将从“科学网”上转载2篇《安全通论》的文章,直至这一系列文章载完为止。

文章编号:2096-1618(2016)01-0001-05
稿件来源:科学网
网　　址:http://blog.sciencenet.cn/blog-453322-944217.html
发表时间:2015-12-18

安全通论(1)

——经络篇

杨义先,　钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:本文刷新了传统的安全观念。从安全角度出发,用概率方法严格证明了:任何有限系统,都存在一套完整的“经络树”,使得系统的任何“病痛”,都可以按如下思路进行有效“医治”:首先梳理出“经络树”中“受感染”的带病“树枝”体系,然后,对该“树枝”末梢上的“带病树叶”(“穴位”或“元诱因”)进行“针灸”。医治好“病叶”后,与这些“病叶”相连的“树枝”就治好了;医治好所有“病枝”后,与这些“病枝”相连的“树干”就治好了;医治好所有“病干”后,整棵“经络树”就医治好了,从而,系统的“病痛”就治好了。此处所指的有限系统,既可以是儿童玩具这样的微系统;也可以是芯片、计算机、电信网、互联网、物联网甚至整个赛博空间等复杂巨型有限系统;当然,也可以是消防、抗灾、防病、治安、环保等各类常见的其他系统。

0　引言

“安全”与“信息”都是至今还没有严格定义的概念,但是,这并不意味着就不能对它们进行深入研究,其实,早在60年前,仙农就已经创立了“信息论”,从而为现代通信的飞速发展奠定了坚实的基础。但是,至今人们对“安全”的研究,特别是网络空间安全的研究,还仅仅停留在“兵来将挡,水来土淹”的工程层次或技术层次,既缺乏全面系统的理论指导,又遗留了许多明显的漏洞,比如,虽然大家都承认网络空间安全是“三分技术,七分管理”,但是,全世界都将几乎90%的精力聚焦于那“三分技术”;而“七分管理”竟然无人问津,或者说只是片面地将“管理”理解为“颁布几份规章制度”而已。

我们梦想建立一套基础的通用安全理论,并以此来指导,包括网络空间安全在内的,所有安全保障工作。本文是努力实现该梦想的第一步。

1　不安全事件的素分解

“安全”是一个很主观的概念,与“角度”密切相关。同一个事件,对不同的人,从不同的角度来说可能会得出完全相反的“安全结论”,比如,“政府监听公民通信”这件事,从政府角度来看,“能监听”就是“安全”;而对公民来说,“能监听”就是“不安全”。所以,下面研究“安全”,只锁定一个角度,比如,“我”的角度。(其实,包括“安全”、美、丑、善和恶等在内的每个形容词,都是主观的和相对的。)

“安全”是一个与时间密切相关的概念。同一个系统,在昨天安全,绝不等于今天也安全(比如,若用现代计算机去破译古代密码,简直是易如反掌);同样,在今天安全,也绝不等于明天就安全。当然,一个“在昨天不安全”的系统,今天也不会自动变为安全。因此,下面研究“安全”时,我们只考虑时间正序流动

的情况,即,立足当前,展望未来。(为突出重点,本文中我们只考虑当前时刻的情况。带时间的安全通论,将在后续论文中涉及到。)

"安全"是一个与对象密切相关的概念。若A和B是两个相互独立的系统,若我们只考虑A系统的安全,那么,B系统是否安全就应该完全忽略。比如,若只考虑"我的手机是否安全",那么,"白宫的电脑是否中毒"就可以完全忽略。因此,下面研究"安全"时,只锁定一个有限系统,即,该系统由有限个"元件"组成。

设A是一个封闭的独立系统,如果直接研究其"安全",那么,根本就无处下手!不过,幸好有,"安全"=不"不安全",所以,若能够把"不安全"研究清楚了,那么,"安全"也就明白了。

下面就以概率论为工具,从"我"的角度,沿着时间的正序方向(但只考虑当前状态),来研究系统A的"不安全"。

假定A系统中发生了某个事件,如果它是一个对"我"来说的"不安全"事件,那么,"我"就能够精确且权威地判断这是一个"不安全的事件",因为,该事件的后果是"我"不愿意接受的!(注意:除"我"之外,"别人"的判断是没有参考价值的,因为,本文只从一个角度来研究"安全")。如果将该"不安全事件"记为D,那么,该事件导致系统A"不安全"的概率就记为$P(D)$。为了简化计,我们只考虑$0<P(D)<1$的情况,因为,如果$P(D)=0$,那么,这个"不安全事件"D就几乎不会发生,故可以忽略,因为无论是否对造成事件D的环境进行改进,都不影响系统A的安全性;如果$P(D)=1$,那么,D就是"不安全"的确定原因(没有随机性),这时只需要针对事件D单独进行加固(比如,采用现在所有可能的已知安全技术手段就行了。实际上,当前全球安全界都已经擅长于这种"头痛医头,足痛医足"的方法),就可以提升系统A的安全性了。

从理论上看,给定系统A之后,如果A是有限系统,那么,总可以通过各种手段,发现或测试出当前的全部有限个"不安全事件",比如,D_1、D_2、…、D_n。下面,在不引起混淆的情况下,我们用D_i同时表示"不安全事件"和造成该事件D_i的原因。于是,系统A的"不安全"概率就等于$P(D_1\cup D_2\cup\cdots\cup D_n)$,或者说,系统A的"安全"概率等于$1-P(D_1\cup D_2\cup\cdots\cup D_n)$。

换句话说,本来无处下手的"安全"研究,就转化为了下面的数学问题:

"安全"数学问题:在概率$0<P(D_1\cup D_2\cup\cdots\cup D_n)<1$的情况下,使该概率$P(D_1\cup D_2\cup\cdots\cup D_n)$最小化的问题,或者使$1-P(D_1\cup D_2\cup\cdots\cup D_n)$最大化的问题。

设D和B是系统A的两个"不安全事件",那么,$(D\cup B)$也是一个"不安全事件",但是,$(D\cap B)$或者$(D\backslash B)$等就不一定再是"不安全事件"了。若事件D是B的真子集,并且D的发生会促使B也发生(即,条件概率$P(B\mid D)>P(B)$),则称事件D是事件B的"子事件"。

在时间正序流动的条件下,设系统A的过去全部"不安全事件"集合为D,若当前又发现一个新的"不安全事件"B,那么,系统A的当前"不安全"概率$=P(D\cup B)\geqslant P(D)=$系统A的过去"不安全"概率。于是,

"不安全性"遵从热力学第二定律:系统A的"不安全"概率将越来越大,而不会越来越小(除非有外力,比如,采取了相应的安全加固措施等);或者说"安全"与"信息"一样都是负熵。

热力学第二定律说:热量可以自发地从高温物体传递到低温物体,但不可能自发地从低温物体传递到高温物体;热量将最终稳定在温度一致的状态。那么,有限系统A的"不安全"状态将最终稳定在什么地方呢?

下面就来回答这个问题。

设Z是一个"不安全事件",如果存在另外两个"不安全事件"X和Y(它们都是Z的真子集),同时满足如下两个条件:(1)$X\cap Y=\Phi$(空集);(2)$Z=X\cup Y$。那么,就说"不安全事件"Z是可分解的。此时X和Y都是Z的子事件。如果某个"不安全事件"是不可分解的(即,它的所有真子集都不再是"不安全事件"了),那么,就称该事件为"不安全的素事件"。

定理1 ("不安全事件"分解定理):对任意给定的"不安全事件"D,都可以判断出D是否是可分解的,并且,如果D是可分解的,那么,也可以找到它的某种分解。

证明:由于有限系统A的全部"不安全事件"只有有限个,D_1、D_2、…、D_n,所以,至少可以通过穷举法,对每个$D_i(i=1,2,\cdots,n)$测试一下$D\backslash D_i$,看看它是否也是"不安全事件"。如果至少能够找到某个这样的i,那么,D就是可分解的,而且,D_i与$(D\backslash D_i)$就是它的一个分解;否则,如果这样的i不存在,那么,D就是不可分解的"不安全素事件",这是因为"D_1、D_2、…、D_n"是全部"不安全事件"。证毕。

定理2 ("不安全事件"素分解定理):若反复使用上述的"不安全事件"分解定理来处理"不安全事件"$(D_1\cup D_2\cup\cdots\cup D_n)$及其被分解后的"不安全子事件",那么,就可以最终得到分解:$D_1\cup D_2\cup\cdots\cup D_n=B_1\cup B_2\cup\cdots\cup B_m$,这里对任意的$i$和$j(i,j=1,2,\cdots,m)$都有$B_i$是"不安全素事件"并且$B_i\cap B_j=\Phi$(空集)。

证明:若 $D=D_1\cup D_2\cup\cdots\cup D_n$,已经是不可分解的了,那么,$m=1$,并且 $D_1\cup D_2\cup\cdots\cup D_n=B_1$

若 D 是可以分解的,并且 X 是 D 分解后的一个"不安全子事件"。如果 X 已经不可分解了,那么,可以取 $B_1=X$;如果 X 还可以再分解,那么,再对 X 的某个"不安全子事件"进行分解。如此反复,直到最终找到一个不能再被分解的"不安全子事件",请将该事件记为 B_1。

仿照上面分解 D 的过程,来试图分解 $D\backslash B_1$,便可以找出不能再被分解的"不安全子事件"B_2。

再根据 $D\backslash(B_1\cup B_2)$ 的分解,便可得到 B_3。

最终,当这个分解过程结束后,全部的 B_i 就已经构造出来了。证毕。

于是,根据"不安全事件"素分解定理,便有 $B_i\cap B_j=\Phi$(空集),并且:$P(D_1\cup D_2\cup\cdots\cup D_n)=P(B_1\cup B_2\cup\cdots\cup B_m)=P(B_1)+P(B_2)+\cdots+P(B_m)$,

因此,换句话说,我们可以将引发有限系统 A 的"不安全事件"D_1、D_2、…、D_n,分解为另一批彼此互不相容的"不安全素事件"B_1、B_2、…、B_m,并且,还将有限系统 A 的不安全概率转化为 $P(B_1)+P(B_2)+\cdots+P(B_m)$。所以,有限系统 A 的"不安全"概率 $P(D_1\cup D_2\cup\cdots\cup D_n)$ 的最小化问题,也就转化成了每个彼此互不相容的"不安全素事件"的概率 $P(B_i)$($i=1,2,\cdots,m$)的最小化问题。换句话说,我们有如下结果:

定理 3　(分而治之定理):任何有限系统 A 的"不安全事件"集合,都可以分解成若干个彼此互不相容的"不安全素事件":B_1、B_2、…、B_m。使得只需要对每个 B_i($i=1,2,\cdots,m$)进行独立加固,即减小事件 B_i 发生的概率 $P(B_i)$,那么,就可以整体上提高系统 A 的安全强度,或者说整体上减少系统 A 的"不安全"概率。

该分而治之定理就回答了前面的"热平衡"问题,即,有限系统 A 的"不安全"状态,将最终稳定成一些彼此互不相容的"不安全素事件"之并。该定理对全球网络空间安全界的启发意义在于:过去那种"头痛医头,足痛医足"的做法虽然值得改进;但也不能盲目地"头痛医足"或"足痛医头",而是应该科学地将所有安全威胁因素,分解成互不相容的一些"专科"(B_1、B_2、…、B_m),然后,再开设若干"专科医院"来集中精力"医治"相应的病症(即,减小 $P(B_i)$)。

专科医院也是要分门诊部的,同样,针对上述的每个"不安全素事件"B_i 也可以再进一步地进行分解,并最终得到系统 A 的完整"经络图",于是,便找到了某些"头痛医足"的依据,甚至给出"头痛医足"的办法。

2　系统"经络图"的逻辑分解

设 X 是 B 的一个真子集,并且,若事件 X 发生,那么将促进 B 也发生(即,$P(B\mid X)-P(B)>0$),那么,就称 X 为 B 的一个诱因。

针对任何具体给定的有限系统 A,因为 B 是有限集,所以,从理论上看,总可以通过各种手段,发现或测试出当前 B 的全部有限个诱因,比如,X_1、X_2、…、X_n,即,$B=X_1\cup X_2\cup\cdots\cup X_n$。

设 X 和 Y 是 B 的两个诱因,而且还同时满足:(1)$X\cap Y=\Phi$(空集);(2)$B=X\cup Y$。那么,就说 B 是可分解的,并且 $X\cup Y$ 就是它的一种分解。如果某个 B 是不可分解的(即,它的所有真子集都不再是其诱因了,或者说对 B 的所有真子集 Z,都有条件概率 $P(B\mid Z)=P(B)$),那么,就称该事件为"素事件"。

若 Y、Y_1、Y_2 都是 B 的诱因,并且,(1)$Y_1\cap Y_2=\Phi$(空集);(2)$Y=Y_1\cup Y_2$。那么,就说 B 的诱因 Y 是可分解的,并且 $Y_1\cup Y_2$ 就是它的一种分解。如果诱因 Y 是不可分解的(即,它的所有真子集都不再是 B 的诱因了),那么,就称该诱因 Y 为"B 的素诱因"。如果诱因 Y 的所有子集 Z,都不再是 Y 自己的诱因了,那么,就称 Y 为"元诱因",或形象地称为"穴位"。

定理 4　(事件分解定理):对任意给定的事件 B,都可以判断出 B 是否是可分解的,并且,如果 B 是可分解的,那么,也可以找到它的某种分解。

证明:由于系统 B 的全部诱因只有有限个,X_1、X_2、…、X_n,所以,至少可以通过穷举法,对每个 X_i($i=1,2,\cdots,n$)测试一下 $B\backslash X_i$,看看它是否也是 B 的一个诱因。如果至少能够找到某个这样的 i,那么,B 就是可分解的,而且,X_i 与($B\backslash X_i$)就是它的一个分解;否则,如果这样的 i 不存在,那么,B 就是不可分解的,这是因为"X_1、X_2、…、X_n"是 B 的全部诱因。证毕。

定理 5　(事件素分解定理):若反复使用上述的"事件分解定理"来处理事件 B,那么,就可以最终得到分解:$B=Y_1\cup Y_2\cup\cdots\cup Y_m$,这里对任意的 i 和 j($i,j=1,2,\cdots,m$)都有 $Y_i\cap Y_j=\Phi$(空集),并且每个 Y_i 都是 B 的素诱因。

证明:若 B 已经是不可分解的了,那么,$m=1$,并且,$B=Y_1$。

若 B 是可以分解的,并且 Y 是 B 分解后的一个诱因。如果 Y 已经是 B 的素诱因了,那么,可以取 $Y_1=Y$;如果 Y 还可以再分解,那么,再对 Y 的某个诱因进行分解。如此反复,直到最终找到一个不能再被分解的素诱因,请将它记为 Y_1。

仿照上面分解 B 的过程,来试图分解 $B\backslash Y_1$,便可以找出 B 的不能再被分解的素诱因 Y_2。

再根据 $B\backslash(Y_1\cup Y_2)$ 的分解,便可得到 Y_3。

最终,当这个分解过程结束后,全部的 Y_i 就已经构造出来了。证毕。

有了上面各定理的准备后,我们现在就可以给出如下的,

有限系统 A 的经络图算法步骤:

第 0 步:针对系统 A 的"不安全事件"D。

第 1 步:利用定理 2,将 D 分解成一些互不相容的"不安全素事件"$B_1\cup B_2\cup\cdots\cup B_m$,这里对任意的 i 和 $j(i,j=1,2,\cdots,m)$ 都有 B_i 是"不安全素事件"并且 $B_i\cap B_j=\Phi$(空集)。(为清晰计,在绘制经络图时,可以从左至右,按照 $P(B_i)$ 的递减顺序排列)。

第 2.i 步$(i=1,2,\cdots,m)$:利用定理 5,把第 1 步中所得到的 B_i 分解成若干"B_i 的素诱因"。(为清晰计,在绘制经络图时,可以从左至右,对 B_i 的素诱因,按照其发生概率大小值的递减顺序排列)为避免混淆,我们将所有第 2 步获得的素诱因,称为"第 2 步素诱因"。这些素诱因中,有些可能已经是"元诱因"(穴位)了。

第 3.i 步$(i=1,2,\cdots,m)$:针对第 2 步所获得的每个不是"元诱因"(穴位)的素诱因,利用定理 5,将其进行分解,由此得到的素诱因,称为"第 3 步素诱因"(这些诱因的从左到右的排列顺序也与前几步相似)。这些素诱因中,有些可能已经是"元诱因"(穴位)了。

……

第 k.i 步$(i=1,2,\cdots,m)$:针对第 $k-1$ 步所获得的每个不是"元诱因"(穴位)的素诱因,利用定理 5,将其进行分解,由此得到的素诱因,称为"第 k 步素诱因"。(这些诱因的从左到右的排列顺序也与前几步相似)。这些素诱因中,有些可能已经是"元诱因"(穴位)了。

……

由于上面各步骤的每次分解,都是针对真子集进行的,所以,这种分解的步骤不会无穷进行下去,即,一定存在某个正整数,比如 N,使得:

第 N.i 步$(i=1,2,\cdots,m)$:针对第 $N-1$ 步所获得的每个不是"元诱因"的素诱因,利用定理 5,将其进行分解,由此得到的素诱因全部都已经是"元诱因"(穴位)了。(每一个素诱因下面的元诱因排列顺序,也是采用概率从大到小进行)

将上面的分解步骤结果,用图形表述出来,我们便得到了有限系统 A 的不安事件"经络图"(由于它的外形很像一棵倒立的树,所以,也称这为"经络树"):

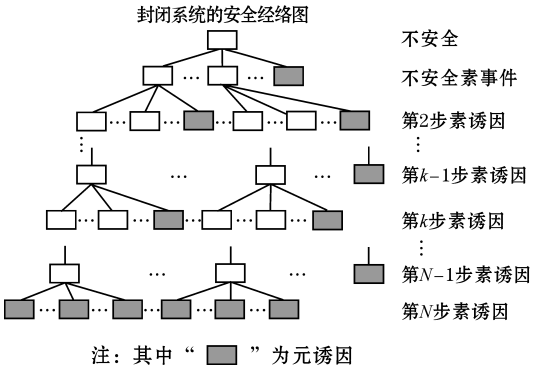

图 1 系统 A 的安全经络树

根据经络树的绘制过程,我们可以知道:

(1)如果系统 A 不安全了,那么,至少有某个"不安全素事件"(甚至可能是"元诱因"(穴位))发生了(见经络树的第二层);

(2)如果某个"不安全素事件"发生了,那么,该事件的至少某个"素诱因"(甚至可能是"元诱因"(穴位))就发生了(见经络树的第三层);

……

(K)如果某个"第 $k-1$ 步素诱因"发生了,那么,该它的至少某个"第 k 步素诱因"(甚至可能是"元诱因"(穴位))就发生了(见经络树的第 $k+1$ 层);

好了,现在就清楚,该如何"头痛医足"了:实际上,只要系统 A"病"了,那么,就一定能够从系统 A 的完整经络图中,找出某个"生病的子经络图"M,使得(1)M 的每层"素诱因"或"元诱因"(穴位)都是"病"的;(2)除了 M 之外,系统 A 的经络图的其他部分都没病。于是,为了治好该"病",只需要将 M 中的所有"元诱因"(穴位)的"病"治好就行了,或形象地说,只需要对这些"元诱因"(穴位)扎针灸就行了。(说明:这里某个第 k 步诱因病了,意指它的至少一个"第 $k+1$ 步诱因"发生了。而如果某个第 k 步诱因的全部第 $k+1$ 步诱因都没有发生,那么,这个第 k 步诱因就没病!可见,除了"元诱因"(穴位)之外,M 中的其它非元诱因是可以自愈的!)

更具体地说,"头痛医足"的过程是:首先将最底层,比如第 N 层,的"元诱因"(穴位)治好,于是,第 $N-1$ 层的"素诱因"就自愈了;然后,再扎针灸治好第 $N-1$ 层的"元诱因"(穴位),于是,第 $N-2$ 层的"素诱因"就自愈了;然后,再扎针灸治好第 $N-3$ 层的"元诱因"(穴位),……,如此继续,最终到达顶层,就行了。

"经络图"的用途显然不仅仅是用来"头痛医足",它还有许多其它重要应用,比如:

1. 只要守住所有相关的"元诱因"(穴位),那么,系统 A 就安然无恙;

2. 同理,将只要所有炮火瞄准相关“元诱因”(穴位),那么,就能够稳准狠地打击对手;

3. 除了元诱因(穴位)之外,经络图中平均概率值大的“经络”是更脆弱的经络(即,安全“木桶原理”中的短板),也是在系统安全保障中,需要重点保护的部分;同时,也是攻击过程中重点打击的部分。

4. 平时就可绘制和补充经络图,在关键时刻就可以排上用场了!

3　结束语

仙农在研究信息论时,虽然发现了信道容量的上限值,但是,非常遗憾,他没能给出如何才能达到该上限值,从而,致使全世界通信界的科学家们在过去六十余年来,使出浑身解数设计各种编码方法,来努力逼近仙农界,至今没成功。

与此相似,本文虽然证明了有限系统的“安全经络图”是存在的,但是,并未给出如何针对具体的系统,来绘制其安全经络图,估计未来的学者们也不得不花费巨大的精力,针对具体系统来绘制具体的经络图。

必须指出,绘制经络图绝非易事,想想看,为了绘制人体经络图,中医界的祖先们奋斗了数千年! 因此,你也别指望在短期内就绘制出“网络空间安全经络图”,虽然这个图肯定存在。

特别猜测:本文虽然借用了“人体经络”来解释我们的结果,但是,人体本身也是一个系统,而且,如果只考虑有限目标的话,人体也可看成一个有限系统。因此,根据本文的结果,对“有限人体系统”的健康来说,也应该存在一张像图 1 那样的“经络图”。我们大胆地猜测:中医发现的“人体经络图”就是这张经络图(类似图 1)的一部分!

下面结合网络空间安全的情况,给出几点注记:(1)漏洞库中的每个漏洞,算是“元诱因”(穴位)了吧,堵住相关漏洞就是对相关“元诱因”(穴位)的加固;(2)口令算是一种“元诱因”(穴位)吧,如果今后能够完全消除口令,代之以综合的个体生理特征,那么,这个“元诱因”(穴位)就会被充分加固了吧;(3)删贴等“信息封堵”手段,虽然可以加固某个“素诱因”,但是,绝非加固“元诱因”(穴位),所以,难免会吃力不讨好;(4)“被穿透”和“被封堵”显然是互不相容的安全事件,而“被窃密”和“口令暴露”却是彼此相容的不安全事件;(5)欢迎所有学者,继续对“网络空间安全经络图”和其它系统的经络图进行更深入的研究。