DOI:10.3969/j.issn.1009-6868.2016.01.010
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20160112.1457.002.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》(原文网址:http://blog.sciencenet.cn/blog-453322-944217.html)。在该文章中,作者提出需要建立一套基础的通用安全理论,来指导包括网络空间安全在内的所有安全保障工作;并从安全角度出发,形象地将系统比作完整的"经络树",认为对系统的任何"病痛"都可进行有效的"医治"。

安全通论——经络篇

The General Theory of Security: Meridian

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0038-004

摘要: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。

关键词:网络空间安全;国家安全;健康防御;人体经络

Abstract: From a security point of view, and proved by probability method, we point out that in any finite system there are a complete set of " meridian trees" that makes any "pain" effectively cured according to the following ideas: Firstly, we need to find out the "infected branch" system, then do the "acupuncture" to the "sick leaves (acupoint) " at the end of the bunch. After curing the sick leaves, the branch that is connected with these leaves is cured; after curing the sick leaves, the "trunk" that is connected with these branches is cured; after curing all the "sick trunks", the whole tree is cured, so the pain of system is cured. The system here refers to the finite system, and it can be both a micro system, and also a chip, computer, telecommunication network, Internet, Internet of things or even the cyber space of complex giant system; of course, it can also be a fire, disaster, disease prevention, public security, environmental protection and other types of common other systems.

Key words: network space security; national security; health defense; human meridian

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)

- 安全是一个与角度、时间、对象都密切相关的概念
- 不安全性遵从热力学第二定律
- 经络图中平均概率值大的"经络"是更脆弱的经络,是在系统安全保障中需要重点保护的部分,也是攻击过程中重点打击的部分
- 绘制出网络空间的安全经络图需要投入很多的精力并耗费很长的时间

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",但全世界都将几乎90%的精力

收稿日期:2016-01-04
网络出版时间:2016-01-12

聚焦于那三分技术，七分管理竟然无人问津，或者说人们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。文章是努力实现该梦想的第1步，希望能够激发学者们更多的后续研究。

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，我们研究安全，只锁定一个角度，比如，“我”的角度。

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，我们研究安全时，只考虑时间正序流动的情况，即立足当前，展望未来。

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，B系统的安全就应该完全忽略。因此，我们研究安全时，只锁定一个有限系统，即该系统由有限个“元件”组成。

假设A是一个封闭的独立系统，如果直接研究其安全，根本就无处下手！不过，幸好有“安全”=不“不安全”，所以，若能把不安全研究清楚了，安全也就明白了。

假设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！需要注意：除“我”之外，“别人”的判断是没有参考价值的，因为，文中只从一个角度来研究安全。如果将该不安全事件记为D，该事件导致系统A不安全的概率就记为$P(D)$。我们只考虑$0<P(D)<1$的情况，因为如果$P(D)=0$，这个不安全事件就几乎不会发生，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$P(D)=1$，D则是不安全的确定原因，这时只需要针对事件D单独进行加固，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，则可以通过各种手段，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。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$P(D_1\cup D_2\cup...\cup D_n)$，或者说，系统A的安全概率等于$1-P(D_1\cup D_2\cup...\cup D_n)$。

换句话说，本来无处下手的安全研究，就转化为了安全数学问题，即在概率$0<P(D_1\cup D_2\cup...\cup D_n)<1$的情况下，使该概率$P(D_1\cup D_2\cup...\cup D_n)$最小化的问题，或者使$1-P(D_1\cup D_2\cup...\cup D_n)$最大化的问题。

假设D和B是系统A的两个不安全事件，$(D\cup B)$则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。如果事件D是B的真子集，并且D的发生会促使B也发生，则称事件D是事件B的“子事件”。

在时间正序流动的条件下，假设系统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，则有系统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。

假设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：$X\cap Y=\varnothing$（空集）；$Z=X\cup Y$，我们就认为不安全事件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，我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是否可分解，如果是可分解的，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，即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$D_1,D_2,\cdots,D_n$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$(D_1\cup D_2\cup...\cup D_n)$及其被分解后的不安全子事件，那么就可最终得到分解$D_1\cup D_2\cup...\cup D_n=B_1\cup B_2\cup...\cup B_m$，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$B_i\cap B_j=\varnothing$（空集）。

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

如果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，则可以取$B_1=X$；如果X还可以再分解，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$B_i\cap B_j=\emptyset$（空集），并得出$P(D_1\cup D_2\cup...\cup D_n)=P(B_1\cup B_2\cup...\cup B_m)=P(B_1)+P(B_2)+...P(B_m)$，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$P(B_1)+P(B_2)+...+P(B_m)$。所以，有限系统A的不安全概率$P(D_1\cup D_2\cup...\cup D_n)$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。

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$P(B_i)$，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。

分而治之定理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$P(B_i)$）。

2 系统“经络图”的逻辑分解

设X是B的一个真子集，如果事件X发生，将促进B也发生（即$P(B|X)-P(B)>0$），我们就称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$B=X_1\cup X_2\cup...\cup X_n$。

设X和Y是B的两个诱因，而且还同时满足：$X\cap Y=\emptyset$（空集）；$B=X\cup Y$。我们则认为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$P(B|Z)=P(B)$），我们就称该事件为素事件。

若Y、Y_1、Y_2都是B的诱因，并且$Y_1\cap Y_2=\emptyset$（空集）；$Y=Y_1\cup Y_2$，我们则认为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），我们就称该诱因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，我们就称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，都可以判断出其是否是可分解的，如果是可分解的，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，即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；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，就可以最终得到分解，即$B=Y_1\cup Y_2\cup...Y_m$，这里对任意的i和j（$i,j=1,2,\cdots,m$）都有$Y_i\cap Y_j=\emptyset$（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，则有$m=1$，$B=Y_1$。

假设B是可以分解的，且Y是B分解后的一个诱因。如果Y已经是B的素诱因了，则可以取$Y_1=Y$；如果Y还可以再分解，则再对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$B_1\cup B_2\cup...\cup B_m$，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$B_i\cap B_j=\emptyset$（空集）。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，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$k-1$步所获得的不是元诱因（穴位）的

每个素诱因，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，使得在第$N.i$步（i=1，2，…，m）中，针对第N−1步所获得的不是元诱因的每个素诱因，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，也是采用了概率从大到小进行）。

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，所以我们也称这为“经络树”，如图1所示。

现在我们就比较清楚，该如何头痛医足了：实际上，只要系统A“病”了，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。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，即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，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！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，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），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，就可以了。

经络图的用途显然不仅仅是用来头痛医足，它还有许多其他重要应用，比如：

（1）只要守住所有相关的元诱因（穴位），系统A就安然无恙。

（2）同理，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。

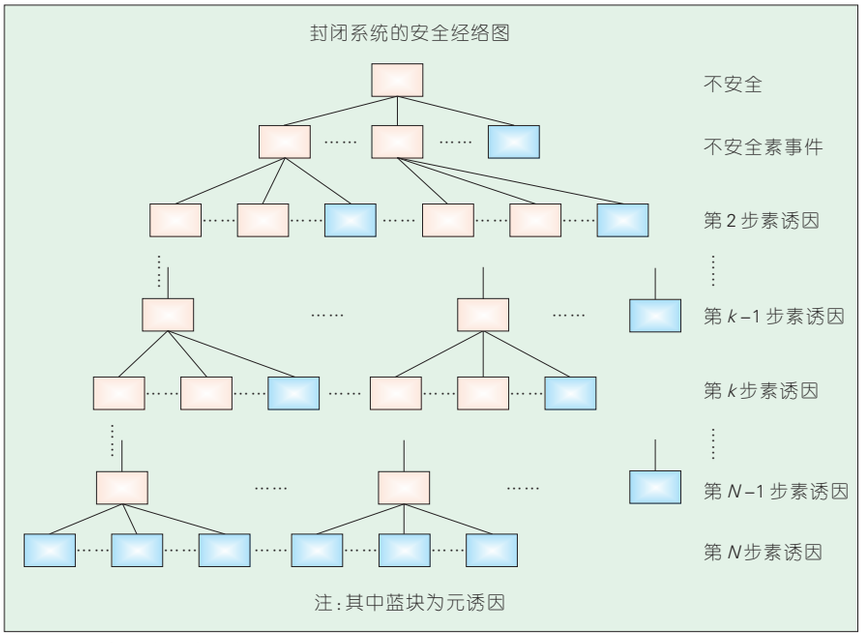
（4）平时就可绘制和补充经络图，在关键时刻就可以排上用场了！

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，但是他没能给出如何才能达到该上限值，从而使全世界通信界的科学家们在过去60余年里，设计各种编码方法来努力逼近仙农界，至今没有成功。

与此相似，文章中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！如今我们也需要很长时间才能绘制出网络空间安全经络图。



▲图1 系统A的安全经络树

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。