故障树分析法在信息安全风险评估中的应用

郑雷雷 宋丽华 郭 锐 张建成

(山东省计算中心 济南 250014) (山东正中计算机网络技术咨询有限公司 济南 250014)

摘 要 信息安全成为人们关注的热点问题,如何定性地构建信息安全风险评估体系以及定量地分析出众多风险因素中的关键部分是关注的首要问题。通过故障树分析法构建了信息安全风险评估模型,然后通过定性分析和定量分析,寻找出导致安全风险爆发的主要因素。初步试验结果标明,该评估模型具有一定的实用性和扩展性。

关键词 信息安全,信息安全风险评估,故障树分析法,定量分析

中图法分类号 TP31 **文献标识码** A

Application of FAT in Information Security Risk Assessment

ZHENG Lei-lei SONG Li-hua GUO Rui ZHANG Jian-cheng

(Shandong Computer Science Center, Jinan 250014, China)

(Shandong Zhengzhong Computer Network Technology Consulting CO., Ltd, Jinan 250014, China)

Abstract Information Security (IS) becomes the focus question that people pay attention to, how to build a qualitative model of Information Security Risk Assessment (ISRA) and how to quantitatively analyze the key parts in a number of risk factors are the primary questions that we concerned. We built the ISRA model using Fault Tree Analysis (FAT), and then by qualitative and quantitative analysis, we analyzed the relationship between risk factors and IS, finding out the main factors that result in Information Security Risk exposure. The result shows the practicability and expandability of this assessment model.

Keywords Information security, ISRA, FAT, Quantitative analysis

随着信息技术的发展,人们迅速进入了信息社会,信息安全问题逐渐成为人们关注的主要问题之一。信息是指由人类活动各个领域产生的、能够以计算机系统存储、检索和管理各种信息的集合。信息安全则是指保证信息的保密性、完整性、可用性,以及保证信息的真实性、可核查性、不可否认性和可靠性等。毫无疑问,信息对于国家、部门、领域乃至个人,都是一种重要的资源,那么,该如何保证信息的安全性呢?首要的一点就是建立信息的安全管理体系,而要建立信息安全管理体系,第一步则是进行信息的安全风险评估工作。

1 信息安全相关概念

保障信息安全,是指在信息安全管理体系下,对可能发生的各种安全事件、可能存在的各种安全漏洞进行分析,从根本上降低危险发生的可能性。因此首要的一步工作就是进行信息安全风险评估,识别、分析可能存在的安全隐患,然后采取应对措施。一般从以下几个方面对一个组织的信息安全进行识别、分析和评估工作:

(1)安全方针。组织是否有自己的信息安全方针、是否对信息安全方针进行评估;

(2)信息安全组织。组织是否有专门的安全组织对内进行信息安全管理,对外保证信息访问受控;

(3)资产管理。组织是否对规定范围内的资产采取了适当的保护措施;

(4)人力资源安全。组织是否有足够的措施确保自己的雇员、其他相关人员的行为没有越限;

(5)物理和环境安全。组织是否采取措施保证自己的设备、设备存放的物理场所等防止被非法物理访问、损毁或干扰;

(6)通信和操作管理。组织是否采取措施保证信息设施被正确、安全地操作;

(7)访问控制。组织是否有访问控制措施,确保用户访问不越界;

(8)信息系统获取、开发和维护。组织是否采取措施保证信息系统的获取、开发、维护工作处于安全状态;

(9)信息安全事件管理。组织是否采取措施保证信息安全事件受控;

(10)业务连续性管理。组织是否采取了有效的措施防止业务活动中断,保护关键业务过程免受信息系统重大失误的影响,并确保它们能及时恢复。

发现安全隐患不是我们的最终目的,发现隐患后,如何对其进行定性定量分析,进而制定应对计划才是我们关心的内容。一般情况下,使用鱼骨图法进行风险分析,鱼骨图法以故

郑雷雷(1984—),男,硕士生,主要研究方向为计算机软件与理论,E-mail:hengll@keylab.net;宋丽华(1983—),女,硕士生,主要研究方向为网络模型及网络环境下应用技术;郭 锐(1979—),男,硕士生,助理研究员,主要研究方向为系统设计开发及信息系统咨询与监理;张建成(1973—),男,硕士生,副研究员,主要研究方向为信息系统咨询与信息标准化。

障现象为结果，以导致该故障发生的因素作为原因。通过鱼骨图法，可以很清晰地分析导致故障发生的各类原因，不过，鱼骨图法无法表示结果与原因之间的定量关系，只能作定性分析。可是尽管某些信息安全风险发生的概率相同，它们的爆发对系统安全出现危险的影响却不相同，出于对资源节约的考虑，不可能同时修复完所有的风险隐患，只能对隐患进行定量分析，确定隐患的优先级，集中力量解决最关键的部分。

2 故障树分析法相关概念

故障树分析法(Fault Tree Analysis，FTA)是用于系统可靠性和安全性分析的工具，是一种由果到因的演绎分析方法。故障树分析法把系统最易观察到的故障现象作为故障树的顶事件，把引发该顶事件故障的最终原因作为底事件，中间事件则反映了顶事件和底事件之间的因果关系。然后通过对各种原因进行详尽分析，按照故障现象与原因之间的因果关系建立起诊断系统故障的数学模型，就可以清楚地分析故障产生的原因和故障的传播过程。

故障树分析包括定性分析和定量分析。定性分析的主要目的是：寻找导致系统不希望发生的事件发生的原因和原因的组合，即寻找导致顶事件发生的所有故障模式，主要从最小割集和结构重要度两个方面进行分析。定量分析的主要目的是：当给定所有的事件发生的概率时，求出顶事件发生的概率及其它定量指标，主要依据概率重要度系数和临界重要度系数或危险重要系数。

割集：是导致顶上事件发生的基本事件的集合，也就是说，故障树中一组基本事件的发生能够导致顶上事件的发生，这组基本事件叫做一组割集。设 C 是一些底事件组成的集合，若 C 中每个事件都发生，即引起顶事件发生，则 C 成为故障树的一个割。

最小割集：若 C 是一个割，从中任意去掉一个事件后就不是割，那么 C 为最小割。最小割集是引起顶事件发生的基本事件的最低限度的集合。

故障树概率函数：在故障树所有底事件相互独立的情况下，顶事件发生的概率 Q 是底事件发生概率 $q_1, q_2, \cdots, q_n$ 的一个函数，记作：$Q=Q(q_1, q_2, \cdots, q_n)$。

结构重要度系数：反映了某一基本事件在整个故障树结构中所占的地位，从结构上反映基本事件的重要程度，用 $I_k(i)$ 表示：

$$I_k(i)=\frac{1}{k}\sum_{i=1}^{k}\frac{1}{m_4(X_1\in E_r)}(i=1,2,\cdots,n) \tag{1}$$

概率重要度系数：反映了基本事件概率的增减对顶事件发生概率的影响的敏感度，用 $I_g(i)$ 表示：

$$I_g(i)=\frac{\partial p(I)}{\partial q_1} \tag{2}$$

临界重要度系数：从结构及概率上反映改善某一基本事件的难易程度，从敏感度和自身发生概率大小双重角度反映基本事件的重要程度。用 $C_g(i)$ 表示：

$$C_g(i)=\frac{q(i)}{Q}I_g(i) \tag{3}$$

一般通过 Fuseell-vesely 算法求解最小割集：从顶事件逐级向下，根据交叉点的不同逻辑关系，将逻辑门的输出事件用输入事件表示，如果是或门，则取输入事件的并集，如果是与门，则取输入事件的交集，直到全部门事件均替换成底事件(基本事件)，这样每一行都由若干底事件组成，构成一个割集。然后利用布尔代数规则中的各类规则 $A+A=A$，$A+AB=A$，$AA=A$ 等进行割集的吸收、简化，最后得到全部最小割集。

3 故障树构建

在故障树分析中，首先将某一系统最不希望的关键故障事件作为“顶事件”，写在第一行；在其下通过因果关系分析寻找所有导致此顶事件发生的直接原因，作为第二行，叫做“中间事件”，把它们用相应的符号表示，并且用适当的逻辑门(与门或或门)与顶事件相连接；接着寻找导致这些中间事件发生的所有直接原因，作为第三行，并且用适当的逻辑门(与门或或门)与第二行相连，以此类推，直到追查到最后一行的基本原因，也就是底事件为止，这样就建成了一棵以顶事件为根，中间事件为节点，底事件为叶的故障树。其中，与门是指仅当所有输入事件发生时，输出事件才发生，而或门是指至少一个输入事件发生时，输出事件就发生。

故障树有助于分析系统的所有可能发生的故障模式和原因，故障树的底事件直观地反映了系统故障点和各模块对系统产生影响的传播路径，而各种逻辑门形式化地表示了各个事件间的内在联系和相互作用。故障树构造过程如图 1 所示。

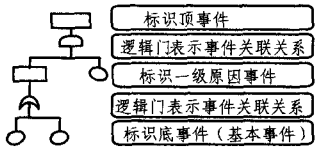

图 1 故障树构造过程

4 信息安全风险评估建模

4.1 前提假设

把信息安全隐患中的一部分拿出来进行建模实验，将信息安全风险评估体系分解成互相独立的若干风险评估模块，将安全事件爆发作为最不期望发生的顶事件，根据风险触发的原因以及各风险之间的相互关系，找出所有导致顶事件发生的一级原因事件，并根据这些原因事件逐步往下一级分析，直到分析到基本的风险隐患，至此构建一棵信息安全风险评估故障树。

假设信息安全体系由若干相互独立的模块组成，各模块的事件状态为两态：发生或者不发生。如下：存在安全体系＝{$T1, I1, I2, M1, M2, M3, M4, M5, M6, M7, M8$}，根据专家经验，各个风险模块以及发生的概率如表 1 和表 2 所列。

表 1 故障树中基本事件的名称

符号	事件	备注
T1	安全事件爆发	顶事件
I1	物理和环境安全存在漏洞	中间事件
I2	访问控制存在漏洞	中间事件
M1	用户访问管理	底事件
M2	用户职责划分	底事件
M3	网络访问控制管理	底事件
M4	操作系统访问控制管理	底事件
M5	物理场所安全性	底事件
M6	设备安全性	底事件
M7	安全方针存在漏洞	底事件
M8	密码控制存在漏洞	底事件

表 2　风险模块发生概率

模块号	M1	M2	M3	M4
发生概率	0.05	0.04	0.05	0.02
模块号	M5	M6	M7	M8
发生概率	0.05	0.06	0.03	0.08

4.2　模型建立

根据各个模块之间的相互作用关系，绘制图 2 所示的故障树。故障树以图形化形式表述了各个事件间的内在联系和相互作用，同时，作为底事件的各个模块直观反映了系统故障点和各模块对系统产生影响的传播路径。

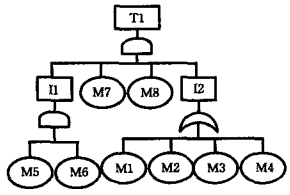

图 2　故障树模型构建

4.3　故障树分析

通过 Fuseell-vesely 算法得到最小割集为：$K1=\{M7\}$，$K2=\{M8\}$，$K3=\{M5,M6\}$，$K4=\{M1,M2,M3,M4\}$，其中每一个 K_i 都代表了系统信息安全发生风险的一种可能性。

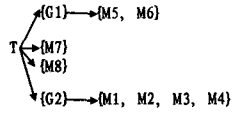

图 3　Fuseell-vesely 算法求解最小割集

那么对于整个系统来说：

(1)故障树分支越少，系统越安全，分支就越多，说明系统面临的信息安全风险越大；

(2)越靠近顶事件，底事件对顶事件的影响越大，例如模型中的 M7 或 M8，一个发生问题，都会导致整个系统面临风险。

针对上述结论，为保证信息安全，可以采取针对性措施，对其中的高阶最小割集进行专门防治，例如可以尽早地建立信息安全方针政策，也可以成立专门的监控小组，保证密码控制的安全性。

通过各风险模块之间的逻辑关系，可以得到每个最小割集发生的概率 $P_{k1}=P_{M7}=0.03$，$P_{k2}=P_{M8}=0.08$，$P_{K3}=P_{M5}+P_{M6}=0.11$，$P_{K4}=P_{M1}*P_{M2}*P_{M3}*P_{M4}=0.000002$，从概率上可以看出，尽管 $M1$ 的概率高于 $M7$ 的概率，但是 $K1$ 发生的概率大于 $K4$ 的概率。这很好地证明了上述结论，而 $K3$ 中的 $M5$、$M6$ 是或门连接，也就是说 $M5$ 或者 $M6$ 发生，都会导致 $K3$ 的发生，所以 $K3$ 发生的概率相当高。

可以得到顶事件发生的概率 $P_{T1}=P_{K1}+P_{K2}+P_{K3}+P_{K4}=0.220002$，如果提前设定阈值为系统信息安全风险发生概率不超过 0.1，就可以判断该系统存在巨大的风险。由于顶事件概率函数是一个多重线性函数，对自变量 P_i 求一次偏导数即可得到各组成模块的概率重要度系数：

$$I_{p(mi)}=\frac{\partial p_{To}}{\partial p_{mi}} \tag{4}$$

$P_{T1}=P(K1+K2+K3+K4)=P_{M7}+P_{M8}+P_{M5}+P_{M6}+P_{M1}*P_{M2}*P_{M3}*P_{M4}$，则 $I_{p(m7)}=I_{p(m8)}=I_{p(m6)}=1$，而 $I_{p(m1)}=0.00004$。

同样地，根据临界度函数 $C_i=q_i*I_i/P_T$，各个节点分别为：$C_{M7}=0.136$，$C_{M8}=0.364$，$C_{M5}=0.227$，$C_{M6}=0.273$。

通过重要度系数的计算，尽管 $M1$ 和 $M5$ 的概率相同（$P_{M1}=P_{M5}=0.05$），但是 $M5$ 在体系中比 $M1$ 重要（$I_{P(m5)}>I_{P(m1)}$），而虽然 $M5$ 和 $M6$ 在体系中的地位相同（$I_{P(m5)}=I_{P(m6)}=1$），但是 $M6$ 要比 $M5$ 优先解决（$C_{M6}>C_{M5}$）。可以了解到：单个模块在整个体系中的重要度，不是取决于它本身的概率大小，而是在于它所在的最小割集在整个体系中所处的位置，对于处于同一地位的模块，则可以通过临界度函数，划分优先级。尽管模块发生的概率差不多，它们在体系中的作用类似，依然可以划分出哪些模块属于应尽早修改的，而哪些模块可以放缓一段时间，而且可以很清晰地了解到各风险模块之间的逻辑关系。

结束语　系统的信息安全问题不是单纯地由某一方面因素引起的，很多安全隐患之间存在各种各样的关联关系。一般的信息安全风险评估更多的是依靠专家经验进行，而很多时候需要进行定量分析，分清原因之间的关系，了解各个因素在整个风险体系中的地位，做到有的放矢，防止资源浪费。

故障树分析法很好地处理了风险因素之间的关联关系，通过与门或者或门以及其他的逻辑关系，形象地表达了风险因素之间的联系，而且可以对各类安全风险进行定性定量分析，可以帮助我们快捷地寻找到亟须整改的安全隐患。在本文的模拟实验中，我们只选取了部分数据进行仿真，并不能反映现实中的实际问题，不过随着我们数据的增多，对安全风险之间的关联关系进行更深层次的发掘，到最后我们可以形象地了解某个组织中存在的各类隐患，并且可很明确地给出整改措施。

参 考 文 献

[1] 郑裕国，张康达. 故障树定性和定量分析的算法[J]. 浙江工业大学学报，1995，(3)：42-47

[2] 肖英柏，向剑文. 软件可靠性稳定增长与安全性测试的故障分析法[J]. 小型微型计算机系统，1999，(9)：668-671

[3] 徐中伟，吴芳美. 形式化故障树分析建模和软件安全性测试[J]. 同济大学学报，2001，29(11)：1329-1302

[4] 纪常伟. 基于故障树的汽车故障诊断系统开发[J]. 车辆与动力技术，2003(1)：52-57

[5] 谭天乐，李平. 基于粗糙集的逻辑故障树方法及其应用[J]. 仪器仪表学报，2004，25(1)：36-41

[6] 陈光宇，黄锡滋. 故障树模块化分析系统可靠性[J]. 电子科技大学学报，2006，35(6)：989-992

[7] 王闯，刘东飞. 故障树分析技术在软件系统测试中的应用[J]. 软件导刊，2008，7(1)：77-79

[8] 朱云鹏. 基于故障树分析法的软件测试技术研究[J]. 计算机工程与设计，2008，29(13)：3387-3390

[9] 沈继忱，李晓光. FSSS 的故障树建模及可靠性分析[J]. 热能动力工程，2010，25(6)：642-647

[10] 漆莲芝，张军. 故障树分析测试用例生成技术研究与应用[J]. 信息与电子工程，2010，8(5)：594-597

[11] 黄丽侠. 故障树分析法在医疗设备故障分析中的应用[J]. 医疗装备，2010，23(7)：71-72

[12] 林跃，马如斌. 故障树与专家规则的车载故障诊断专家系统[J]. 汽车工程师，2010，6：27-29

（下转第 118 页）

首先考虑基于不同局域世界范围 M 并在不同攻击策略下由 SON-LW 模型所建立的网络拓扑的聚簇系数变化情况，如图 5(a)所示。当从网络中移除的节点逐渐增加时，它的聚簇系数则缓慢下降。对于蓄意攻击而言，随机失效对聚簇系数的影响更小。例如，当 $M=20$ 时，网络初始聚簇系数为 0.027。采用随机失效策略移除网络中 40% 的节点后的聚簇系数为 0.0151；移除相同数量的节点，基于局部信息蓄意攻击后导致网络的聚簇系数为 0.0046，而基于全局信息蓄意攻击的结果为 0.0021。图 5(a)中聚簇系数没有像其他统计属性一样产生临界现象，其原因在于移除某一节点后并不影响其邻居节点的连接性。因此，并不存在移除多少节点的特定值使得聚簇系数产生戏剧性的变动。

接下来，就 $M=20$ 采用全局信息蓄意攻击时 SON-LW 模型的网络拓扑特征进行讨论(在其他情况下可以得到相似的结论)。此时，$p_c=0.4\pm0.05$。图 5(b)中，网络介数当移除节点率 $p<p_c$ 时有增加的趋势，这可以解释为网络中度最大节点的失效从整体上造成了经过其他节点的最短路径数目的增加，因而会出现这种情况。当达到临界点 p_c 后，网络介数急剧下降为 0，此时网络中几乎不会有流量存在。图 5(c)中，由于网络中节点的移除造成网络平均路径增加而导致效率降低。当节点移除率超过 p_c 时，网络中的大部分节点之间不存在任何路由而导致效率接近于 0。图中右上部分是 $M=200$ 时，全局信息蓄意攻击对网络效率的影响，此时 $p_c=0.975$。图 5(d)中，当 $p>0.425$ 时有网络可达性 $R<0.001$，即网络中从任一节点到其他节点间几乎都没有路径存在。如果从图 5(e)中对应来看的话，节点移除率 $p>0.6$ 时网络中每一节点单独构成簇，这时网络的最大簇规模 $S=0.001$。因此，我们也可以理解图 5(f)中 $M=20$ 的聚簇直径曲线在 $p=0.6$ 时停止。此外，图 5(f)中显示当 $p<0.35$ 时聚簇直径增加，说明存在可以绕过被移除节点的路径来构成簇。

从图 5 中可以看到全局信息蓄意攻击相比其他情况最具破坏性，即使这样它对于 $M=200$ 时 SON-LW 所形成的网络影响甚小，使得网络有了优良的抗攻击能力。

结束语 许多已有的研究成果主要集中于建立静态拓扑模型和研究复杂网络上的动力学。这些模型中节点间的交互依赖于静态连接机制，比如 BA 模型使用“增长”和“优先连接”来反映真实系统的特征。但是，这仍存在许多问题。真实的网络有较大的聚簇系数和度关联性，而且在网络进化过程中任何细微的变化都将影响拓扑结构的形成。此外，网络拓扑的形成遵循着一定的进化规则，并由内外部因素共同驱动。这是在静态模型中所不能体现的。自组织临界是能够解释上述情形的理论之一。

本文提出了一个局域世界自组织网络模型，它依靠节点适应度变异的外部动力规则来推动网络拓扑结构的形成。我们发现当网络达到稳定状态时，节点适应度表现出了临界值之上的均匀分布和幂律尾特征，而节点度在局域世界范围之上时也出现与适应度相似的幂律性。进而，发现该网络模型随着局域世界范围的扩大而表现出了对随机故障和蓄意攻击的双重容忍特性。本文中对局域世界的选取采用随机方法，这与实际情况并不相符，因此如何选取局域世界将是进一步要做的工作。另外，为了提高网络的故障和攻击容忍能力，该模型与 BA 模型等方法一样并没有人为设计因素的存在，但在工程实践中到处都有设计的痕迹。因此，考虑保障网络可生存性作为网络演化的设计目标来构建模型将是我们考虑的重点。

参 考 文 献

[1] Vázquez A, Pastor-Satorras R, Vespignani A. Large-scale topological and dynamical properties of the Internet[J]. Physical Review E, 2002, 65(6)

[2] Wasserman S, Faust K. Social network analysis: methods and applications[M]. Cambridge: Cambridge University Press, 1994

[3] Jeong H, Tombor B, Albert R, et al. The large-scale organization of metabolic networks[J]. Nature, 2000, 407(6804): 651-654

[4] Williams R J, Martinez N D. Simple rules yield complex food webs[J]. Nature, 2000, 404(6774): 180-183

[5] Redner S. How popular is your paper? An empirical study of the citation distribution[J]. The European Physical Journal B, 1998, 4(2): 131-134

[6] Barabási A L, Albert R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512

[7] Dorogovtsev S N, Mendes J F F. Scaling properties of scale-free evolving networks[J]. Continuous approach. Physical Review E, 2001, 63(5)

[8] Albert R, Barabási A L. Topology of evolving networks: local events and universality[J]. Physical Review Letters, 2000, 85(24): 5234-5237

[9] Bianconi G, Barabási A L. Competition and multiscaling in evolving networks[J]. Europhysics Letters, 2001, 54: 436-442

[10] Li X, Chen G. A local world evolving network model[J]. Physica A, 2003, 328: 274-286

[11] Yook S H, Jeong H, Barabási A L, et al. Weighted evolving networks[J]. Physical Review Letters, 2001, 86(25): 5835-5838

[12] Garlaschelli D, Capocci A, Caldarelli G. Self-organized network evolution coupled to extremal dynamics[J]. Nature Physics, 2007, 3: 813-817

[13] Boccaletti S, Latora V, Moreno Y, et al. Complex networks: Structure and dynamics[J]. Physics Reports, 2006, 424(4): 175-308

[14] Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(6794): 378-382

[15] Costa L F, Rodrigues F A, Travieso G, et al. Characterization of complex networks: A survey of measurements[J]. Advances in Physics, 2007, 56(1): 167-242

[16] Xiao S, Xiao G, Cheng T H. Tolerance of intentional attacks in complex communication networks[J]. IEEE Communications Magazine, 2008, 46(1): 146-152

(上接第 108 页)

[13] 王卓，王晓晔. 基于故障树的空管维修人为差错分析[J]. 天津理工大学学报，2010，26(5)：81-85

[14] 董海鹏，高延滨. 基于故障树与案例相结合的故障诊断方法[J]. 应用科技，2010，37(11)：60-64

[15] 张竞凯，章卫国. 一种基于故障树的自动驾驶仪故障诊断专家系统设计[J]. 测控技术，2010，29(10)：88-92