警报关联图:一种网络脆弱性量化评估的新方法*

张 怡,赵 凯,来 犇
(国防科技大学 计算机学院,湖南 长沙 410073)

摘 要:作为一种基于模型的脆弱性分析技术,攻击图能够识别网络中存在的脆弱性和它们之间的相互关系,分析出可能的攻击路径和潜在威胁。论文在攻击图的基础上提出了警报关联图的概念,利用攻击图中蕴含的脆弱性先验知识,将实时IDS警报信息映射到攻击路径,动态反映攻击进程和攻击者意图。在此基础上提出了一种基于警报关联图的网络脆弱性量化评估方法,通过计算警报关联边的权值对网络脆弱性进行动态分析,这种方法结合了静态的网络脆弱性先验知识和动态变化的攻击者意图,能有效反映网络脆弱性在动态攻击情况下的变化。

关键词:攻击图;警报关联图;脆弱性评估
中图分类号:TP393.08 **文献标志码**:A **文章编号**:1001-2486(2012)03-0109-04

Alert correlation graph: a novel method for quantitative vulnerability assessment

ZHANG Yi, ZHAO Kai, LAI Ben
(College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: As a model-based vulnerability analysis technology, attack graphs can identify network vulnerabilities and their interactions; they can also reveal all possible attack paths and potential threats. Based on the attack graphs, alert correlation graphs are proposed in the paper. An alert correlation graph maps real-time IDS alerts into attack paths using prior knowledge encoded in attack graph, and reveals attack progresses and attackers' intention dynamically. A novel quantitative network vulnerability assessment method is presented based on the alert correlation graph, which analyzes network vulnerabilities by dynamically computing the weight of alert correlation edges. The research also demonstrates, by examples, that the proposed method combines static prior knowledge about network vulnerabilities with dynamic attackers' intentions, and reveals the change of network vulnerability under real-time attacks.

Key words: attack graph; alert correlation graph; vulnerability assessment

网络脆弱性是影响网络安全的关键因素。网络中的脆弱性表现在设计、实现和运行管理的各个环节[1]。完全消除脆弱性是不现实的,也是不可能的,重点是对网络脆弱性进行分析和度量,找出影响网络的关键脆弱性,有的放矢地进行处理。攻击图是基于模型的网络脆弱性分析技术,它从攻击者的角度出发,在综合分析网络配置和脆弱性相关信息的基础上,枚举出所有可能的攻击路径,反应了网络中各个脆弱性之间,以及脆弱性与安全配置之间的相互依赖和相互作用关系,能够深层次地揭示网络中存在的潜在威胁。攻击图技术已被证明在网络脆弱性分析、网络加固、攻击响应等研究领域具有良好的应用前景。

目前,攻击图建模和自动生成技术研究取得较大进展[2-4],越来越多的研究集中在基于攻击图的网络脆弱性分析技术上,即根据攻击图中节点的实际含义,采用各种模型或算法对网络脆弱性进行分析。如文献[5]为攻击图中每个原子攻击指派成功发生的概率值,利用马尔科夫模型计算攻击目标被攻击者成功入侵的最大概率。文献[6]通过配置网络中关键信息资产的价值,对网络的脆弱性进行度量。文献[7]利用专家经验确定攻击图中每个节点独立发生的概率,并计算从攻击初始节点到达每个属性节点的累计概率。上述各种方法中,对攻击图中节点或边的参数分配依赖于管理人员的经验,主观性强,可操作性较差。考虑到IDS(Intrusion Detection System)警报反映了网络中客观存在的攻击行为,文献[8]中首次将攻击图与IDS警报关联相结合,提出了基于队列图(queue graphs)结构的警报关联计算方法,不但提高了警报关联计算的效率,而且还基于攻击图信息,将警报关联(correlation)、假设

* **收稿日期**:2011-09-20
基金项目:国家863计划资助项目
作者简介:张怡(1973—),女,山西五台人,副研究员,博士,硕士生导师,E-mail:zhangyi@nudt.edu.cn

(hypothesis)和预测(prediction)进行了统一。

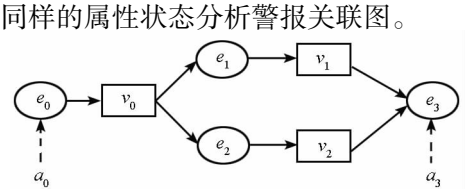
受队列图的研究启发,本文提出警报关联图思想。警报关联图不但包含了 IDS 警报间的关联关系,而且还对这些关联发生的次数进行量化。由于攻击者能主动分析各种因素,智能地进行攻击规划,因此警报关联图可真实反映攻击者意图,可用来对网络脆弱性进行动态的评估。本文提出的方法可应用于分析攻击规律、提取攻击模式,蜜网分析、安全策略验证和部署调整以及使用历史警报数据对攻击图进行预先模拟分析等。与其他分析方法相结合,警报关联图可以为进一步的网络脆弱性分析提供基础数据,指导确定网络防护措施。

1 警报关联图

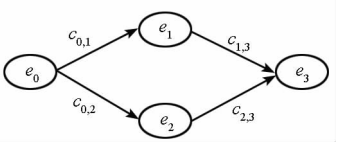
警报关联图的基本思想是在攻击图提供的先验知识基础上,根据 IDS 警报信息动态生成警报关联,并基于警报关联的次数计算关联边的权值。

图 1(a)所示为简单的攻击图。其中 e_0、e_1、e_2 和 e_3 为表示原子攻击的利用节点,v_0、v_1 和 v_2 为表示利用条件和后果的属性节点。e_0 攻击后进入 v_0 状态,在 v_0 状态分别可通过实施 e_1 和 e_2 攻击进入 v_1 和 v_2 状态,而只有 v_1 和 v_2 状态同时达到时,攻击者才可以实施 e_3 攻击。文献[9]中给出了攻击图的形式化定义。图 1(b)是图 1(a)对应的警报关联图,其节点集合是攻击图中利用节点(原子攻击节点)集合,有向边反映了利用节点对应的 IDS 警报之间的关联关系,边的权值(如 $c_{0,1}$)代表警报间的关联次数。显然,警报关联图的有向边也反映了攻击路径,边的权值越大说明攻击者沿着该路径进行攻击的次数越多。

基于攻击图可对 IDS 的警报进行关联。由于 IDS 的警报信息是相互独立的,并且可能存在缺失,因此需要对缺失的警报进行推断。文献[8]将攻击图的属性节点分为 TRUE、FALSE 和 HYP 三个状态。TRUE 表示该节点的属性得到满足,可以根据该属性实施下一步的攻击。FALSE 状态表示该节点的属性不满足,无法实施后续攻击。而 HYP 节点代表根据推断可以假设该节点属性已经满足,但还没有相应的警报信息证实。本文采用同样的属性状态分析警报关联图。



(a)攻击图



(b)警报关联图

图 1 警报关联的基本原理

Fig. 1 Principle of alert correlation

在图 1(a)中,假设在 t_1 时刻系统得到对应原子攻击 e_0 的警报 a_0,由于攻击 e_0 直接导致属性 v_0 可达,因此警报 a_0 触发将 v_0 状态改为 TRUE。假设 t_2 时刻对应 e_3 的警报 a_3 出现,说明攻击者已经获得 v_1 和 v_2 属性,由于此时系统尚未收到警报 a_1 和 a_2,因此只能将 v_1 和 v_2 的状态设置为 HYP,即可推断 e_1 和 e_2 发生,造成属性 v_1 和 v_2 的满足。而当 t_3 时刻警报 a_2 出现时,v_2 的状态由 HYP 变为 TRUE。在上述 IDS 警报序列下,属性节点的状态变化以及警报关联图边权值的变化如图 2 所示。警报关联图边权值的计算方法将在下一节中详细介绍。

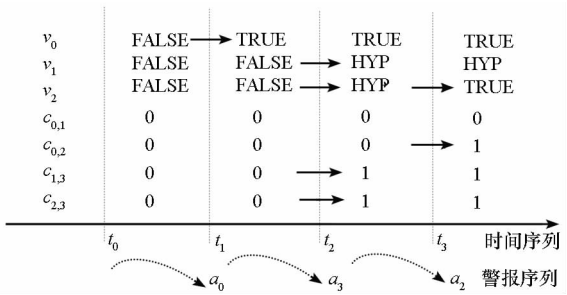


图 2 警报关联中的状态与权值变化

Fig. 2 Change of state and weights in alert correlation

因此,警报关联图可定义为三元组$\langle V,E,C\rangle$,其中顶点集合 $V=\{v_i \mid i=0,1,\cdots,n-1\}$,对应攻击图中的利用节点集合,边集合 $E\subseteq V\times V$ 表示警报之间的关联关系,关联度集合 $C=\{c_{i,j} \mid v_i,v_j\in V\}$,定义了根据 IDS 警报动态计算的关联边的警报关联次数。

2 警报关联度计算

警报关联度计算是指当一个 IDS 警报发生时,根据攻击图(队列图)当前状态和警报关联结果,修改警报关联图中相应边的关联度的过程。根据攻击图的定义[9],属性节点的父节点(利用节点)之间为或关系,表示父节点中任何一个原子攻击实施成功,都会使该属性节点被满足;利用节点的父节点(属性节点)之间为与关系,表示利用节点的全部前提属性必须都被满足,才能实施相应的原子攻击。因此,计算警报关联度需要考虑图 3 中(a)、(b)、(c)3 种情况,其中实心矩形

表示属性节点,空心圆形表示利用节点,e_0 为当前警报对应的利用节点,其余为 e_0 的前续利用节点,也是在警报关联图中具有出边连接 e_0 的节点。

图 3 中,对于情况(a),e_0 攻击发生,必然有 e_1 攻击先发生,因此 e_0 对应的警报发生时,将 $c_{1,0}$ 加 1;对于情况(b),e_0 攻击发生,必然有 e_1 和 e_2 攻击先发生,因此 e_0 对应的警报发生时,将 $c_{1,0}$ 和 $c_{2,0}$ 分别加 1;而对于情况(c),e_1 和 e_2 攻击有一个发生,就可能使 e_0 的前续属性节点状态变为 TRUE,因此,当 e_0 警报发生时,无法直接推断其前续攻击是 e_1 还是 e_2,此时采用的计算方法是若 e_1 对应的警报存在,而 e_2 对应的警报不存在,$c_{1,0}$ 加 1,$c_{2,0}$ 不变,反之,$c_{2,0}$ 加 1,$c_{1,0}$ 不变;若 e_1 和 e_2 对应的警报都存在或都不存在,则 $c_{1,0}$ 和 $c_{2,0}$ 各加 0.5。当然,在警报关联计算时需要考虑(a)、(b)、(c)3 种情况混合存在的情况,如图 3(d)所示。

为实现警报关联计算,定义 $N \times N$ 的关联度矩阵 C 和警报状态向量 S,其中 N 为警报关联图中的节点个数,$c_{i,j}$ 表示节点 e_i 和 e_j 之间的关联度。s_i 为 1 表示 e_i 对应的警报已经出现,为 0 表示未出现。对于每个利用节点,都对应一个用于警报关联计算的数据结构。例如,图 3(d)中节点 e_0 对应的数据结构如图 3(e)所示。

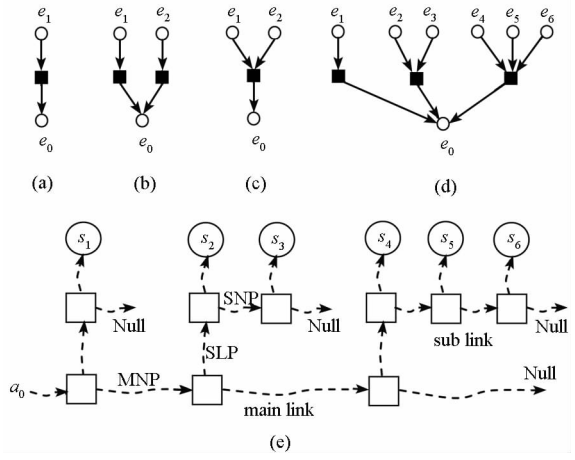


图 3　警报关联值的计算

Fig. 3　Computation of alert correlation values

该结构包含 2 级链表,主链表 ML(main-link)的每个控制块称为主链表控制块,对应每个节点在攻击图中的前序属性节点。每个前序属性节点对应的前序利用节点由子链表 SL(sub-link)维护。每个子链表上的控制块包含指向该前序利用节点的状态(0 或 1)。每个主控制块指向下一主控制块的指针记为 MNP(Main-link Next Pointer),指向对应子链表的指针记为 SLP(Sub-Link Pointer),子链表控制块中指向下一控制块的指针记为 SNP(Sub-link Next Pointer)。基于上述数据结构,警报关联度的计算方法如图 4 所示。

算法依次遍历主链表和子链表,并确保每个子链表中指向所有前序利用节点边的警报关联度增加和为 1。若子链表中有状态为 1 的节点,增加值在这些状态为 1 的节点间均分,否则在所有节点间均分。显然,上述算法具有 $O(N)$ 的计算复杂度和 $O(N^2)$ 的存储复杂度。警报状态向量初始值全为 0,其维护比较简单,此处不再赘述。

输入:关联矩阵 $\boldsymbol{C}$,状态向量 $\boldsymbol{S}$,警报 a_i

输出:关联矩阵 $\boldsymbol{C}$

变量:temp,记录每个 sub link 中有多少个警报的状态为 TRUE

(1)　根据警报 a_i 查找相关 main link 入口,获取指向 main link 控制块的 MNP 指针;

(2)　若 MNP = Null,转到(3);否则开始执行步骤(2.1);

(2.1)　从 main link 控制块中获取 SLP 指针,temp = 0;

(2.2)　读取 SL 控制块,若相应警报状态为 TRUE,则 temp = temp + 1;

(2.3)　若 SNP = Null,转步骤(2.4),否则将 SNP 指向的 SL 控制块作为当前控制块,转到步骤(2.2);

(2.4)　根据 2.1 获得的 SLP 指针,重新遍历 sub link,若 s_j = TRUE,则 $c_{i,j} = c_{i,j} + \frac{1}{temp}$;

(2.5)　读取当前 ML 控制块 MNP 指向的下一个 ML 控制块作为当前 ML 控制块,转步骤(2);

(3)　算法结束

图 4　警报关联度的计算方法

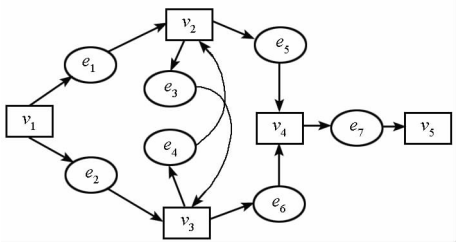
Fig. 4　Algorithm of alert correlation weights computation

3　网络脆弱性量化评估

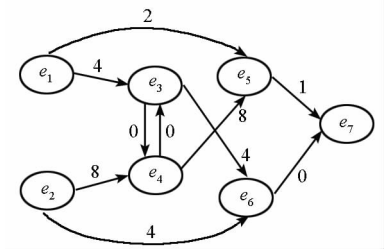
图 5(a)反映了一个用攻击图描述的网络攻击场景。属性 v_1 到 v_5 分别表示拥有主机 1 到主机 5 的 root 权限。其中 v_1 为初始属性,v_5 为最终攻击结果。e_1 和 e_2 表示主机 1 和 2 分别具有脆弱性 CVE-2008-4250(服务器远程代码执行漏洞)。主机 2 和主机 3 可以相互访问且都能访问主机 4,主机 4 可以访问攻击目标主机 5。而主机 4 和 5 分别存在脆弱性 CVE-2006-3747(Apache 缓冲区溢出漏洞)和 CVE-2004-0330(Serv-U FTP 服务器缓冲区溢出漏洞)。

由图 5(a)所示攻击图生成的警报关联图如图 5(b)所示。设根据产生的网络 IDS 警报计算的每条边的警报关联度如图 5(b)所示。根据上述警报关联度可以计算攻击者沿着每条攻击路径

进行攻击的情况。如表 1 所示。



(a)攻击图



(b)警报关联图

图 5 警报关联图应用示例

Fig. 5 Example of the application of alert correlation graph

表 1 攻击路径的度量值计算

Tab. 1 Computation of attack path weights

攻击路径	度量值
$e_1 - e_5 - e_7$	2 + 1 = 3
$e_1 - e_3 - e_6 - e_7$	4 + 4 + 0 = 8
$e_1 - e_3 - e_4 - e_5 - e_7$	4 + 0 + 8 + 1 = 13
$e_2 - e_6 - e_7$	4 + 0 = 4
$e_2 - e_4 - e_5 - e_7$	8 + 8 + 1 = 17
$e_2 - e_4 - e_3 - e_6 - e_7$	8 + 0 + 4 + 0 = 12

由于每条关联边的度量值计算依据 IDS 真实的警报信息,因此表 1 中攻击路径的度量值计算真正反映了攻击者的攻击行为。特别是 $e_2 - e_4$ 以及 $e_4 - e_5$ 间的关联值较大,反映了攻击者沿主机 1 到主机 3,再到主机 2 的攻击次数较多。针对这一特点,在网络防护时可采取专门的措施进行安全加固。

与文献[8]中反映 IDS 警报关联的结果图(result graph)相比,警报关联图没有记录每个警报关联的具体信息,而是根据攻击图中描述的攻击路径记录警报之间关联的次数,不但减小了计算和存储开销,而且结果更加宏观,更有利于动态分析攻击者的攻击行为。

由于关联边权值计算的复杂度为 $O(N)$,只与攻击图中利用节点的数目有关,而与 IDS 警报的数目无关,因此警报关联图可以在线计算、分析、展示并预测攻击者的攻击路径,实时反映受保护网络的安全状况,及时地根据攻击者的行为对网络进行加固。同时,根据警报关联图对 IDS 警报的历史数据进行分析,可以获取攻击者真正关心、也是最需要防护的网络脆弱点。

4 结束语

本文提出的警报关联图概念实质上是对攻击图在时间上进行扩展,把 IDS 检测到的警报信息映射到攻击路径上,通过计算警报关联边的权值对网络脆弱性进行分析。

本文只是提出警报关联图的基本概念,更多的因素需要在下一步研究中考虑。一是目前度量值计算方法中,只考虑状态向量中记录的前序警报是否发生,而在基于攻击图的 IDS 警报推测中,每个属性节点都可能处于 TRUE、HYP 或 FALSE 状态。因此可以利用 IDS 警报对应的前序属性节点的状态进一步地对其前序警报进行区分,优化警报关联度的计算。更加重要的是 IDS 警报的缺失对警报关联计算影响很大,如何有效利用警报的预测和推断信息进行关联度计算对提高网络脆弱性分析准确度也具有重要意义。

参考文献(References)

[1] 林闯,任丰原. 可控可信可扩展的新一代互联网[J]. 软件学报, 2004,15(12):1815 - 1821.
LIN Chuang, REN Fengyuan. Controllable, trustworthy and scalable new generation internet[J]. Journal of Software, 2004,15(12):1815 - 1821. (in Chinese)

[2] Ammann P, Wijesekera D, Kaushik S. Scalable graph-based network vulnerability analysis[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002:217 - 224.

[3] Ou X M, Boyer W F, McQueen M A. A scalable approach to attack graph generation[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006: 336 - 345.

[4] Chen F, Su J S, Zhang Y. A scalable approach to full attack graphs generation[C]// Proceedings of the 1st International Symposium on Engineering Secure Software and Systems, 2008:150 - 163.

[5] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs[C]// Proceedings of 15th IEEE Computer Security Foundations Workshop, 2002:49 - 63.

[6] Wang L Y, Singhal A, Jajodia S. Toward measuring network security using attack graphs[C]// Proceedings of 3rd International Workshop on Quality of Protection, 2007: 49 - 54.

[7] Wang L Y, Islam T, Long T, et al. An attack graph-based probabilistic security metric[C]// Proceedings of 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2008:283 - 296.

[8] Wang L Y, Liu A Y, Jajodia S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts[J]. Computer Communications, 2006,29:2917 - 2933.

[9] 陈锋, 张怡,苏金树,等. 攻击图的两种形式化分析[J]. 软件学报, 2010,21(4):838 - 848.
CHEN Feng, ZHANG Yi, SU Jingshu, et al. Two formal analyses of attack graphs[J]. Journal of Software, 2010,21(4): 838 - 848. (in Chinese)