文章编号:1673-5005(2007)01-0144-04

基于改进攻击树的网络攻击模式形式化研究

段友祥[1], 王海峰[2]

(1. 中国石油大学 计算机与通信工程学院,山东 东营 257061; 2. 山东临沂师范学院 信息学院,山东 临沂 276002)

摘要:攻击树是一种网络攻击形式化描述和建模工具,具有结构化、可重用等优点。通过分析攻击树在实际应用中的缺陷,提出了攻击树新的建立规则,并引入了时间序列和概率的概念,从而更加准确地实现了攻击模式的形式化表示。应用改进后的攻击树描述了一个 WEB 攻击,结果表明该形式化方法具有很好的实用性和有效性。

关键词:攻击模式; 攻击树; 形式化; WEB 攻击; 网络

中图分类号:TP 393.8 文献标识码:A

Formulization of network attack pattern based on improved attack tree

DUAN You-xiang[1], WANG Hai-feng[2]

(1. *College of Computer & Communication Engineering in China University of Petroleum, Dongying* 257061, *Shandong Province, China*;
2. *Department of Information in Shandong Linyi Normal College, Linyi* 276002, *Shandong Province, China*)

Abstract: As a mean for describing network attack pattern and modeling, attack tree is characterized by structure and reutilization. The disadvantages of the attack tree in application were analyzed. A new establishment rule for the attack tree was presented by introducing time-order and probability. It can increase the exactness of the methodology. The improved attack tree was used to describe WEB attack. The results show that the methodology is effective.

Key words: attack pattern; attack tree; formulization; WEB attack; network

网络攻击形式具有多样性,而且目前随着网络防御能力的提高,网络攻击出现了很多变异形式,或者是进化出一些新的形式。此外,协同化攻击与攻击过程的复杂化,致使攻击模式的描述越来越困难。然而,攻击模式的研究对于研究网络安全具有极其重要的价值。近年来出现了一些研究攻击形式的方法,如一阶逻辑谓词语言、自动状态机等,其中最有价值的是攻击树的形式化方法。但在应用中发现,有时攻击并不是通过一个步骤或者方法来实现的,而是按照攻击进程采用了不同的攻击方法,也就是说攻击不完全是并行化或是串行化的过程,存在很复杂的形式[1]。另外,攻击过程中还存在攻击子模式出现的时间序列问题。传统的攻击树不能很好地刻画出攻击的这类特征,从而影响到整个攻击模式的准确性描述。为此,笔者引入时间序列和概率的概念,提出攻击树新的建立规则,以准确实现攻击模式的形式化表示。

1 攻击树模型

为了研究描述安全系统的方法,以对系统的安全性进行精确的估价,Bruce Schneler [2]在 1999 年首次提出攻击树这个概念。它将针对系统的一个攻击表示为"与、或"树的结构形式。树的根节点表示网络攻击要达到的总目标,其他节点则表示实现上一级攻击目标采用的手段或方法,每一条从根节点到叶节点的路径表示了实现攻击目标而进行的一个完整的攻击过程。攻击树的节点分为"与"(AND)节点和"或"(OR)节点两类。其中,"与"节点的逻辑形式为 a AND b = c,即 a 与 b 两种攻击完成后可以达到攻击目的 c,见图 1;"或"节点的逻辑形式为 a OR b = c,即完成攻击 a 或者完成攻击 b 就能达到攻击目的 c,见图 2。

收稿日期:2006 - 06 - 15

作者简介:段友祥(1964 -),男(汉族),山东广饶人,教授,研究方向为计算机网络及应用、信息安全和数据库。

攻击树虽然逻辑形式简单,但是树形结构的先天优势条件使攻击模式可以有很强的扩充性,根据逻辑规则可以实现新攻击子模式的添加和删除,同时,由于采用子模块化的形式表达,子模块可以重复出现在攻击树构成的森林中,因此攻击模式具有很好的复用性[3]。

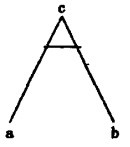

图1 "与"节点

虽然攻击树具有很多优点[4-5],但是在实际的网络攻击研究中发现,攻击树在精确刻画实际攻击模式时还存在一些缺陷,主要表现为不能准确反映攻击子模式的序列关系,不能精确反映子模块在实现攻击目的中的重要程度。

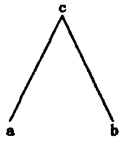

图2 "或"节点

2 攻击树的改进

2.1 改进策略

2.1.1 "与"节点

传统攻击树中,表示"与"逻辑关系的方式存在一个明显的弊端,即其逻辑含义不能精确地反映出子模式 a,b 在达到 c 攻击目标过程中的先后关系,如图3所示。这个缺陷表现在整个攻击树甚至攻击森林中,会使描述出来的攻击模式十分模糊[6-7]。

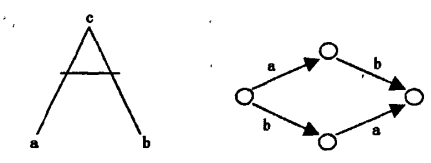

图3 "与"节点及其序列关系

对"与"节点的改进方法是,对"与"节点的生成采用简单的排序规则,将最先发生的攻击子模式放在左孩子节点,然后根据先后顺序将其他的子模式节点插入。利用从左至右的排列反映 a,b 等攻击子模式的先后顺序。虽然规则简单,但是扩大到整个攻击树后能明显地提高形式描述的准确程度。

2.1.2 "或"节点

在传统攻击树中,"或"逻辑体现了达到攻击目的可以有多个子攻击模式,每个子攻击模式的发生概率是有很大的差异的,而研究攻击发生的概率对于安全性评价来说非常重要[8]。攻击发生概率不同主要是由于系统环境的差异和各种攻击技术的难易程度不同而引起的。通常情况下,技术难度低的攻击子模式出现的概率高,安全专家就要对出现频率高的攻击模式制定更合理的安全策略;出现频率低的攻击模式或者是因为网络、系统环境的奇异性,或者是因为对攻击者技术要求高,因此,研究出现频率低的攻击模式对防御隐蔽性强的攻击同样有着积极的意义[9]。

对"或"节点的改进方法是,在"或"节点中添加由安全专家估计的每种攻击子模式出现的概率值,概率值采用模糊化的等级值,即把出现概率分为高、较高、中、较低、低5个模糊等级,分别量化为{1,0.8,0.6,0.4,0.2},同时从左向右按概率值从大到小顺序排列。

这样在改进的攻击树中的"或"节点就能在一定程度上反映攻击模式出现的概率,也能分辨出每种攻击模式的重要程度。

2.2 改进后攻击树的优点

首先,有利于自动处理攻击模式。由于采用"与"节点按发生先后排序规则和"或"节点的按发生概率值排序规则,在改进的攻击树成功建立后,可以采用程序的方法对攻击树进行诸如生成各种攻击模式、剪枝处理等操作。其次,可以从攻击树中提取出现概率高或出现概率低的攻击模式,以做重点研究或处理。再次,可以有利于采用程序完成攻击树的维护工作,实现新攻击子模式的添加和旧模式的删除、更新。

3 应用实例

近年来随着用户网络安全意识的提高,越来越多的网络系统使用防火墙作为保护内部网主机的一个重要屏障,过滤了很多不良 IP 地址,关闭了常用的端口,但是作为 WEB 服务的主机,其 WEB 服务端口(常用 80 或 8080)仍然是要开放的,所以就出现了绕过防火墙的 WEB 攻击模式。WEB 攻击比传统攻击模式更隐蔽,危害性更大,大多数攻击能经过深层渗透获得 root 权限,它能实现一个完整的攻击过程[10]。

图4中给出了一个用改进的攻击树描述的 WEB 攻击。每个节点名字由"G"+节点编号构成,其中 G 是 Goal 的字头,节点编号由父节点编号+子目标顺序号组成,既能体现层次也能体现孩子节点的序号。例如 G2134 表示的路径从根向下为:总目标的第2个孩子→第2个孩子目标的第1个孩子→第1个孩子目标的第3个孩子→第3个孩子目标的第4个孩子。

一些主要子目标的含义说明见表1。

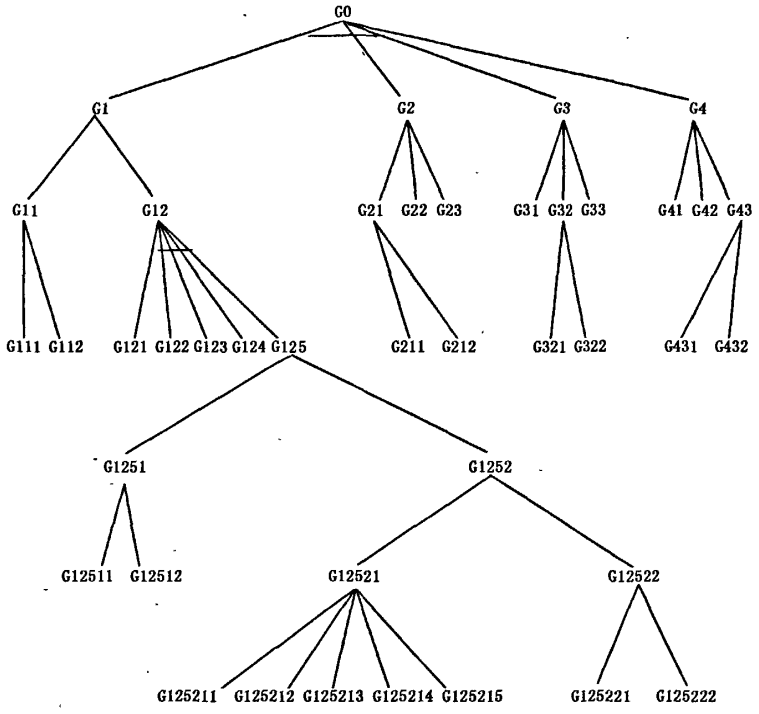

图 4 改进攻击树表示的一个 WEB 攻击实例

表 1 主要子目标符号及其含义

符号	含义	符号	含义
G0	完全攻击一台主机	G321	已知系统漏洞
G1	扫描目标主机	G322	未知系统漏洞
G2	取得目标主机一般权限	G41	DOS
G3	取得目标主机 root 权限	G42	泄密
G4	破坏目标主机	G43	其他
G11	确定目标主机 IP 地址	G431	后门
G111	ping	G432	跳板
G112	SE	G251	目标系统已知漏洞
G12	扫描未知 IP 地址的主机	G1252	目标系统未知漏洞
G121	确定主机域名	G12511	应用程序漏洞
G122	确定防火墙地址	G12512	系统漏洞
G123	确定防火墙规则	G12521	应用程序
G124	确定 WEB 服务器 OS 信息	G12522	系统程序
G125	确定 WEB 主机漏洞情况	G125211	ASP
G21	漏洞利用	G125212	JSP
G22	利用配置错误	G125213	PHP
G23	猜测弱口令	G125214	SQL
G211	已知漏洞利用	G125215	注入
G212	未知漏洞利用	G125221	IIS
G32	系统漏洞	G125222	Apache

从图 4 中可以看出,G12 是“与”子节点,G12 的目的是探测在防火墙后面的主机系统。从 G121 到 G125 的顺序排列说明了完成该攻击目的需要的子攻击模式。首先确定主机的域名,如果该主机未提供 WEB 服务,那么此攻击过程不能继续,接着就是确定防火墙的 IP 地址,然后探测防火墙的访问控制规则,为绕过做准备,再就是探测 WEB 服务器的信息与操作系统的信息。G124 又是 G125 的依赖前提,根据 WEB 服务软件的信息,比如 IIS 或 APACHE 来分析其存在的漏洞。在这里就体现出了各子模式的时间依赖关系,即各攻击子模式出现的先后顺序。对于“与”节点并不添加概率值属性,因为每个子模块必须都出现。

G2 是“或”子节点,G2 的攻击目的是获得主机普通用户权限。G21,G22,G23 每个子节点都有出现的概率值属性,且按概率大小排列。比如 G23 是弱口令攻击,攻击概率最低,因为虽然弱口令攻击最简单,但是随着网络安全意识的提高,弱口令攻击成功的概率降低了,因此出现的概率就低了。G21 是漏洞攻击,它出现的概率相对最高,因为 WEB 程序设计者安全意识仍然很低,多数 WEB 应用程序存在大量可以被黑客利用的漏洞。G22 是利用配置错误的攻击模式,它出现概率为中度。通过为“或”节点的攻击模式增加发生概率属性,就可以用简单的攻击树遍历算法提取出现概率高于一定阈值的攻击模式。

最后,通过访问改进的攻击树的叶子节点就得出一个常见的基于 WEB 的攻击模式。例如:G121

→G122→G123→G124→G125211 →G211 →G321→G431。这个攻击模式是,探测目标主机开放 WEB 服务,利用 WEB 服务端口绕过防火墙,寻找出 WEB 应用程序的漏洞,利用该漏洞取得普通权限后再利用系统已知 RPC 漏洞通过渗透获得系统权限,最后在 WEB 应用程序中放置 ASP 后门,为下次入侵做准备。这是目前出现概率比较高的攻击模式,当然根据攻击树可以生成更多基于 WEB 的攻击模式,从而为网络防御提供准确的信息。

4 结束语

通过在攻击树中引入顺序关系和概率的概念对攻击树进行了改进,较好地解决了攻击顺序和攻击重要程度表示不清楚的问题,从而使攻击树更准确地实现了攻击模式的形式化描述。另外,方便了在攻击树的基础上设计相应的算法来处理攻击模式的操作,例如,添加变异的攻击模式、淘汰过时的攻击模式、细化攻击模式等等,为深入研究攻击和制定安全策略奠定了基础。

参考文献:

[1] 阚流星,鲁鹏俊,王丽娜,等.基于攻击树和 Agent 技术的攻击模型[J].计算机工程,2003,29 (18):80-81.
KAN Liu-xing, LU Peng-jun, WANG Li-na, et al. Attack model based on attack tree and agent technique[J]. Computer Engineering, 2003, 29 (18):80-81.

[2] SCHNEIER B. Attack trees: modeling security threats [J]. Dr Dobb's Journal,1999,24(12): 21-29.

[3] MOORE A P, ELLISON R J, LINGER R C. Attack modeling for information security and survivability[DB/OL]. CMU/SEI-2001-TN-001 (2001-03-01) [2005-10-20]. http://www.cert.org/archive/pdf/01tn001.pdf.

[4] 庄朝晖.基于攻击树的多层次入侵检测及其在 Linux 上的原型[D].厦门:厦门大学计算机系,2002.

[5] 卢继军,黄刘生,吴树峰.基于攻击树的网络攻击建模方法[J].计算机工程与应用,2003,39(27):160-163.
LU Ji-jun, HUANG Liu-sheng, WU Shu-feng. An attack tree approach for network intrusion modeling[J]. Computer Engineering and Applications, 2003, 39(27):160-163.

[6] 张永,陆余良.攻击树在多阶段入侵检测系统中的应用[J].计算机应用与软件,2004, 21(8):103-105.
ZHANG Yong, LU Yu-liang. The applications of atack tree in the multi-stages intrusion detection systems[J]. Computer Applications and Software,2004, 21(8):103-105.

[7] 秦嵘,张尧弼.基于攻击树的协同入侵建模[J].计算机应用与软件,2005, 22(4):116-118.
QIN Rong, ZHANG Yao-bi. Attack tree based coordinated intrusion modeling[J]. Computer Applications and Software, 2005, 22(4):116-118.

[8] KRISTOPER Daley. A structral framework for modeling multi-stage network attacks[C]. IEEE Computer Society, 2002:5-10.

[9] EVANS S, HEINBUCH D, WALLNER J, et al. Risk-based systems security engineering stopping attacks with intention[J]. IEEE Security & Privacy,2004,2(6):59-62.

[10] BRUCE Schneier. 网络信息安全的真相[M].吴世忠,马芳,译.北京:机械工业出版社,2001:9.

(编辑 修荣荣)

"863"计划海洋技术领域课题验收会在中国石油大学(华东)青岛校区顺利召开

2006 年 12 月 26 日至 27 日,"863"计划海洋技术领域课题验收会在中国石油大学(华东)青岛校区顺利召开。此次验收会由科技部主办,中国石油大学(华东)承办,共邀请海洋技术领域专家 17 人,科技部孙清处长主持了会议。

此次验收会共分海洋探测与海洋工程和海洋油气开发工程两个组,分别对中国科学院声学研究所、国家海洋局第一海洋研究所、国家海洋局第二海洋研究所、上海交通大学、利策科技(上海)有限公司、中国科学院地质与地球物理研究所、西安石油大学、长安大学、中国石油大学等 9 个单位承担的 11 个课题进行了验收。专家组听取了课题研究情况、资金使用情况、课题取得的成果及其在海洋技术行业中应用情况的汇报,审核了有关文档资料。经过答辩、审议和讨论,高分辨率测深侧扫声纳系统等 11 个课题顺利通过验收或结题。

(摘自中国石油大学(华东)校园网)