

基于期望收益率攻击图的网络风险评估研究

刘文甫^{1,2}, 庞建民¹, 周鑫¹, 李男¹, 岳峰¹

(1. 信息工程大学, 河南 郑州 450001; 2. 电子信息系统复杂电磁环境效应重点实验室, 河南 洛阳 471003)

摘要: 随着互联网应用和服务越来越广泛, 层出不穷的网络攻击活动导致信息系统的安全面临极大的风险挑战。攻击图作为基于模型的网络安全风险分析技术, 有助于发现网络节点间的脆弱性和评估被攻击的危害程度, 已被证实是发现和预防网络安全问题的有效方法。攻击图主要分为状态攻击图和属性攻击图, 由于状态攻击图存在状态爆炸的问题, 研究者大多偏向于基于属性攻击图的网络风险评估研究。针对现有的属性攻击图研究过度依赖网络节点本身脆弱性和原子攻击本质属性进行量化分析, 忽略了理性攻击者通常以攻击利益最大化来选择具体的攻击路径, 提出了基于期望收益率攻击图的网络风险评估框架和攻击收益率量化模型。所提网络风险评估框架以公开的漏洞资源库、漏洞挖掘系统发现的新漏洞以及与网络攻防相关的大数据为基础数据源, 以开源大数据平台为分析工具, 挖掘计算攻击成本和攻击收益相关要素; 借用经济学中的有关成本、收益以及收益率等概念构建原子攻击期望收益率计算模型; 通过构建目标网络的属性攻击图, 计算攻击路径上的原子攻击期望收益率, 生成所有可能攻击路径的期望收益率列表; 以期望目标为出发点, 依据特定的优化策略(回溯法、贪心算法、动态规划)展开搜索, 得到最大收益率的完整攻击路径, 为网络风险评估提供依据。仿真实验结果表明了所提期望收益率攻击图网络风险评估方法的有效性及合理性, 能够为发现和预防网络安全问题提供支撑。

关键词: 攻击图; 风险评估; 攻击路径; 期望收益率; 收益率攻击图

中图分类号: TP309.1

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022047

Research on network risk assessment based on attack graph of expected benefits-rate

LIU Wenfu^{1,2}, PANG Jianmin¹, ZHOU Xin¹, LI Nan¹, YUE Feng¹

1. Information Engineering University, Zhengzhou 450001, China

2. State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang 471003, China

Abstract: As Internet applications and services become more and more extensive, the endless network attacks lead to

收稿日期: 2021-03-19; 修回日期: 2021-07-28

通信作者: 庞建民, jianmin_pang@hotmail.com

基金项目: 国家自然科学基金(61802433); 之江实验室“先进工业互联网安全平台”项目(2018FD0ZX01)

Foundation Items: The National Natural Science Foundation of China (61802433), Zhijiang Laboratory Advanced Industrial Internet Security Platform(2018FD0ZX01)

引用格式: 刘文甫, 庞建民, 周鑫, 等. 基于期望收益率攻击图的网络风险评估研究[J]. 网络与信息安全学报, 2022, 8(4): 87-97.

Citation Format: LIU W F, PANG J M, ZHOU X, et al. Research on network risk assessment based on attack graph of expected benefits-rate[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 87-97.

great risks and challenges to the security of information systems. As a model-based network security risk analysis technology, attack graph is helpful to find the vulnerability between network nodes and the harm of being attacked. It has been proved to be an effective method to find and prevent network security risks. Attack graph is mainly divided into state-based attack graph and attribute-based attack graph. Due to the problem of state explosion in state-based attack graph, most researchers prefer the attribute-based attack graph for network risk assessment. In view of the existing researches on attribute-based attack graph, they excessively rely on the vulnerability of network nodes and the essential attributes of atomic attack. However, they ignore that rational attackers usually choose specific attack paths by maximizing attack benefits. Then, a network risk assessment framework and a quantification method of attack benefits-rate based on expected benefits-rate attack graph were proposed. The network risk assessment framework took the open vulnerability resource database, the new vulnerabilities found by the vulnerability mining system and the big data related to network attack and defense as the basic data source. The network risk assessment framework also took the open source big data platform as the analysis tool to mine and calculate the elements related to attack cost and attack benefit. Using the concepts of cost, benefit and benefit-rate in economics, the calculation model of expected benefit-rate of atomic attack was constructed. By constructing the attribute-based attack graph of the target network, the expected benefit-rate of atomic attack on the attack path was calculated, and the expected benefit-rate list of all possible attack paths was generated. Furthermore, taking the expected goal as the starting point, the search was carried out according to the specific optimization strategy (backtracking method, greedy algorithm, dynamic programming). And the complete attack path with the maximum benefit-rate was obtained, which provided the basis for network risk assessment. The simulation results show the effectiveness and rationality of the proposed expected benefit-rate attack graph network risk assessment method, which can provide support for discovering and preventing network security problems.

Keywords: attack graph, risk assessment, attack path, expected benefits-rate, attack graph of benefits-rate

0 引言

随着网络技术的日新月异,以及基于互联网的应用和服务越来越广泛,网络中的攻击活动愈演愈烈,信息系统的安全风险面临极大的挑战。信息系统遭受网络攻击的主要原因是网络及其服务应用系统在设计、开发、升级等过程中存在或衍生出安全缺陷或隐患,这些缺陷一旦被恶意入侵者成功利用,就会导致入侵者非法访问系统,进而引发一系列安全事故,造成极大的危害。通常一个理性的攻击者会有目的、有步骤、综合权衡利弊后才决定从哪一网络节点对目标网络发起攻击。因此,以网络中的脆弱性利用为基本出发点、以攻击期望收益率作为攻击节点、攻击路径和攻击目标选择的重要依据,并结合属性攻击图在网络安全评估方面的方法和优势,对评估网络安全风险、构建安全的网络环境以及提高信息安全性有着重要意义。

网络安全风险评估研究主要分为 3 类:单个漏洞脆弱性评估、基于规则的网络脆弱性评估和

基于模型的网络安全风险综合评估^[1-5]。基于攻击图的网络安全风险评估方法能够明确攻击的危害程度以及节点与节点之间的危险关系,在基于模型的网络安全风险综合评估中应用最为广泛^[6-10]。攻击图研究主要分为状态攻击图^[11]和属性攻击图,由于状态攻击图存在状态爆炸等问题,近年来的研究者大多偏向于采用属性攻击图评估网络风险^[12-14]。在属性攻击图的基础上,Zhang 等^[15]改进了近似贝叶斯后验算法(似然加权算法),解决了贝叶斯网络中不允许有环、只能使用一个贝叶斯网络来推断网络的当前和未来安全状态等问题。Wang 等^[16]为了防御高速网络中的多步骤入侵,提出了一种新颖的队列图方法,可以将任意距离的警报关联起来,但该方法并未解决动态的网络问题。文献[17-19]利用攻击图虽然解决了网络风险动态评估问题,但过于依赖网络本身漏洞,而未考虑一次攻击行动的发生往往是有意识或潜意识的综合权衡利益得失之后再做的决定。

本文在研究属性攻击图的基础上,提出了一

种基于期望收益率攻击图的模型。采用大数据分析挖掘影响攻击收益率的因素，即攻击成本和预期收益的主要组成要素，在此基础上构建了期望收益率计算模型，并依据收益率计算结果将属性攻击图转换为期望收益率攻击图，最终实现对网络系统的风险评估。

本文的主要工作和贡献包括4个方面。

1) 提出了一个基于期望收益率攻击图的网络风险评估框架。

2) 定义了网络安全要素，设计了网络主机画像标签并定义了期望收益率攻击图模型。

3) 量化了收益率影响因素，构建了原子攻击期望收益率计算模型。

4) 验证了基于期望收益率和属性攻击图在

网络安全风险评估中的有效性和合理性。

1 网络安全风险评估框架

本节在介绍网络风险评估原理的基础上，提出了一种基于期望收益率攻击图的网络安全风险评估框架。

1.1 风险评估基本原理

风险评估的最基本要素是资产、威胁及脆弱性^[6]。传统的风险评估是通过识别外部威胁出现的概率、查找内部脆弱性的严重程度、判断资产价值（机密性、完整性和可用性），进而得出安全事件发生的可能性以及可能造成的损失，最终得到安全风险情况。风险评估的基本原理如图1所示。

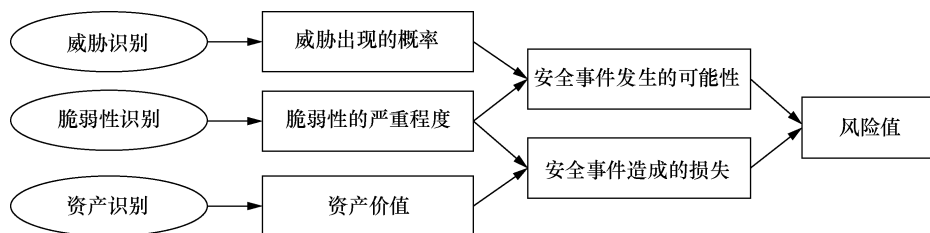


图1 风险评估的基本原理
Figure 1 Basic principle of risk assessment

从图1可以发现，安全事件发生的可能性及安全事件造成的损失都与脆弱性的严重程度有关。因此，传统风险评估中如何识别脆弱性以及脆弱性的严重程度是风险评估研究中最重要的工作之一。大多数目标网络节点多、拓扑结构复杂、提供服务丰富且可靠性要求高，这对预测、发现及消除目标网络的威胁提出了更高要求。现实中大多数目标网络的管理人员身兼数职，导致不能及时应对所有威胁。因此，依据网络风险评估基本原理，以攻击者的视角分析网络威胁并进行风险评估具有一定的必要性和紧迫性。

1.2 基于期望收益率的网络安全风险评估框架

定义1 攻击期望收益率：一个理性攻击者对某个目标网络发起攻击的过程中，期望从目标网络节点中得到的价值与必要支出的比值。

本文在对攻击期望收益率及其要素量化和模型构建研究的基础上，结合属性攻击图生成方法，提出了一种基于期望收益率攻击图的网络安全风险评估框架，如图2所示。

基于期望收益率攻击图的网络安全风险评估框架以公开漏洞库资源、漏洞挖掘系统发现的新漏洞以及与网络攻防相关的大数据为基础数据源，以基于Spark的大数据挖掘平台为分析得到与攻击成本和收益相关的要素，借用经济学中的有关成本、收益以及收益率等概念设计攻击期望收益率计算模型；在定义相关安全要素的基础上，计算基于属性攻击图生成的全部攻击路径上的期望收益率，用以生成期望收益率攻击图并最终服务于网络安全风险分析。

2 期望收益率攻击图模型

本节以属性攻击图为建模基础，增加期望收益率作为攻击者选择攻击路径的衡量标准，用于构建期望收益率攻击图模型，进而为网络攻击带来的风险评估提供支撑。

2.1 网络安全要素定义

依据文献[13]中属性攻击图的网络要素定义，本文将期望收益率攻击图的网络要素

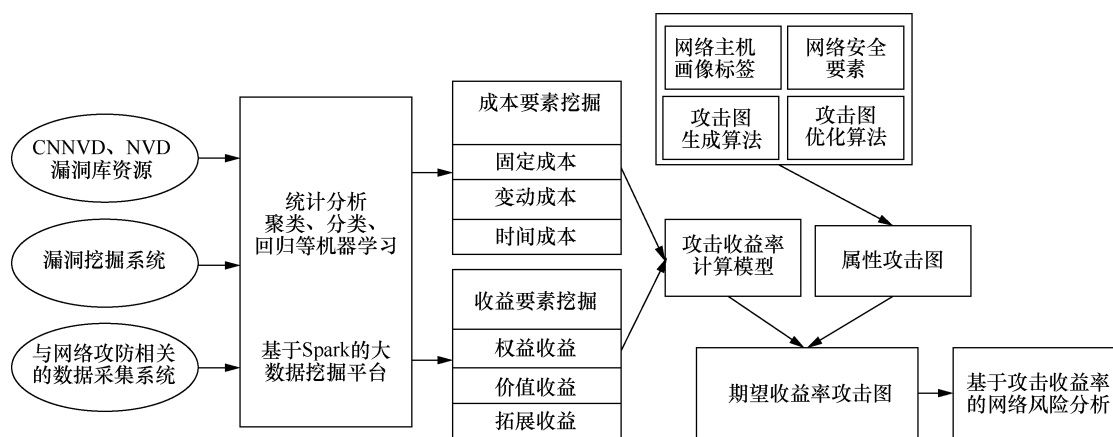


图 2 基于期望收益率攻击图的网络安全风险评估框架

Figure 2 Network security risk assessment framework based on attack graph of expected benefits-rate

扩展为: 主机资产(host asset)、网络服务(network service)、可利用元素(useful element)、网络连接(network connection)、信任关系(trust relationship)、访问权限(access privilege)和收益(expected benefit)。具体定义如下。

定义 2 主机资产主要从机密性、完整性和可用性方面描述主机所具有的价值, 用二元组表示为<host, value>。

1) host 表示被评估的主机, 用 IP 地址描述。

2) value 表示主机机密性、完整性和可用性方面的综合价值。

定义 3 网络服务描述主机上运行的服务, 用五元组表示为<host, service, protocol, port, generality>。

1) host 表示服务所在主机, 用 IP 地址描述。

2) service 表示服务的名称。

3) protocol 表示服务使用的网络协议, 如 TCP、UDP、ICMP 等。

4) port 表示服务监听的端口。

5) generality 表示该服务的通用性, 即广泛性。

定义 4 可利用元素描述了网络中固有的可供攻击者利用的漏洞, 用三元组表示为<host, service, cveid>。

1) host 表示服务所在主机, 用 IP 地址描述。

2) service 表示服务的名称。

3) cveid 表示服务中该漏洞被利用程度的唯一标识, 用可利用性在 CVE 中对应的编号描述。

定义 5 网络连接描述攻击者与主机间及主

机与主机间的连接关系, 这种连接关系可以表示物理上的连通关系, 也可详细描述在哪个协议哪个端口上连接, 用四元组表示为<start_host, to_host, protocol, port>。

1) start_host 表示发起连接的源主机, 用主机 IP 地址描述。

2) to_host 表示连接的目的主机, 用主机 IP 地址描述。

3) protocol 表示源主机连接到目的主机所使用的网络协议, 如 TCP、UDP、ICMP 等。

4) port 表示目的主机提供的连接端口, 用实际端口号描述。

定义 6 信任关系描述主机间可以不经认证而直接访问, 用二元组表示为<trusted_host, coop_host>。

1) trusted_host 表示受信任的主机, 它可以在不经认证的情况下访问目的主机, 用 IP 地址描述。

2) coop_host 表示目的主机, 受信任主机可以不经认证访问自己, 采用主机 IP 地址描述。

定义 7 访问权限表示攻击者在特定主机上所拥有的权限, 用二元组表示为<host, privilege>。

1) host 表示特定主机, 可以采用主机 IP 地址描述。

2) privilege 表示攻击者在特定主机已具备的访问权限, 它的取值范围定义为{none, user, root}。

定义 8 收益表示攻击者一次攻击行为的预期收益, 用三元组表示为<attack_host, attacked_host, benefit>。

1) attack_host 表示攻击发起主机, 用主机 IP 地址描述。

2) attacked_host 表示被攻击主机, 用主机 IP 地址描述。

3) benefit 表示攻击者一次攻击行为所能获取被攻击主机的收益。

2.2 原子攻击及其模式

原子攻击指的是在满足一定的网络安全要素集合的前提下, 对网络中存在的脆弱性的一次具体利用, 从而产生或获取相应的安全要素结果。原子攻击模式指的是对一类脆弱性的利用的描述, 同时这些脆弱性利用有着类似的前提和结果。攻击模式示例如图 3 所示。

名称	远程缓冲区溢出
前置要素	network service <host, service, protocol, port, generality>
	useful elements <host, service, cveid>
	network connection <start_host, to_host, protocol, port>
	access privilege <host, USER>
结果要素	access privilege <host, ROOT>
	host assets <host, value>
脆弱性编号	CVE-2017-5577, CVE-2017-9445, CVE-2019-12527
期望收益率	X%, Y%, Z%

图 3 攻击模式示例

Figure 3 Examples of attack patterns

本文将原子攻击模式表示为一个五元组

<name, pre-conditions, post-conditions, cveidset, expected benefits-rate>。

1) name 表示攻击模式的名称。

2) pre-conditions 表示攻击模式被利用所需的各类网络安全要素前提条件, 如网络连接前提、脆弱性前提及访问权限前提等。

3) post-conditions 表示攻击模式被利用后得到的新网络安全要素, 如信任关系、特权提升等。

4) cveidset 表示适用于该攻击模式的所有脆弱性 cve 编号的集合。

5) expected benefits-rate 表示如果利用该攻击模式进行攻击所能获取的期望收益和成本的比率, 用百分比表示。

2.3 网络主机画像标签设计

为了使网络安全要素快速实例化, 进而为攻击图构建提供必要的网络安全要素支撑, 本文为网络主机设计了一组层次结构的画像标签集, 如图 4 所示。

网络主机画像标签主要包括: 基本属性画像标签、连接关系画像标签、脆弱性画像标签和服务画像标签。其中, 基本属性画像标签用于描述该主机的基本信息, 如 IP 地址、经过评估后的资产信息、主机系统信息等。连接关系画像标签描述该主机与其他主机相连的信息, 如 IP 地址、连接协议、端口号、是否需要认证等。脆弱性画

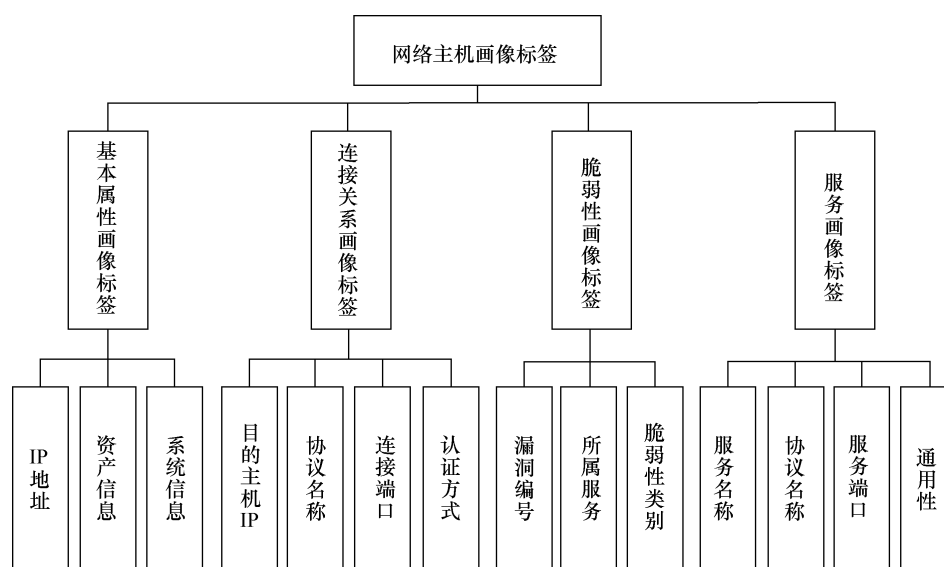


图 4 网络主机画像标签

Figure 4 Portrait labels for network host

像标签描述该主机存在的已知漏洞信息以及带来该漏洞的服务相关信息。服务画像标签描述该主机提供的服务信息，以及与该服务相关的一些基本信息。

2.4 期望收益率攻击图模型

2.4.1 模型定义

定义 9 期望收益率攻击图 $BAG=(S,A,E,B)$,

其中, S 表示属性节点集合, 包括初始属性和可达属性; A 表示攻击节点集合; E 为有向边集合; B 表示期望收益率集合; $E \subset ((S \times A) \cup (A \times S))$, 其中, $S \times A$ 表示集合 S 和 A 的笛卡尔积, $A \times S$ 表示集合 A 和 S 的笛卡尔积。其中, 属性节点由网络中的安全要素组成, 如网络连接、信任关系、访问权限等; 攻击节点指的是依照攻击模式产生的原子攻击, 且以原子攻击的期望收益率作为攻击选择的依据。属性节点与攻击节点之间用有向边连接, 攻击节点是属性节点之间转换的必要前提, 是当前的前提和产生的直接结果, 且攻击节点只有在它所有的前提都满足的情况才能发生攻击, 产生结果。期望收益率攻击图应满足以下约束条件。

1) 对 $\forall p \in S$, 令 $Pat(p)$ 为 p 的父节点集合, 父节点间为“或”关系, 满足 $(\bigvee Pat(p)) \rightarrow p$, 表示只要任何一个父攻击节点被执行, 都会使 p 属性节点被满足。如果 p 为初始属性节点, 则它的父节点为 $\emptyset$ 。

2) 对 $\forall q \in A$, 令 $Pre(q)$ 为 q 的前提节点集合, $Post(q)$ 为 q 的结果节点集合, 前提节点间为“与”关系时, 有 $(\bigwedge Pre(q)) \rightarrow Post(q)$, 表示当全部前提属性被满足后, 可成功完成攻击, 从而使其结果属性被满足。

3) $B(S_i - S_j, A_k)$ 表示攻击的期望收益率, 其中, i 和 j 为属性节点的下标, k 为攻击节点的下标; $S_i - S_j$ 表示从属性 S_i 到 S_j , A_k 表示该属性转换的原子攻击。

4) 期望收益率攻击图 $BAG=(S,A,E,B)$, BAG 的初始属性集指的是 S 的子集 $S_0 = \{c \mid \text{不存在 } a \in A, (a, c) \in E\}$, BAG 的可达属性集指的是 S 的子集 $S_d = \{r \mid r \in S - S_0\}$ 。

2.4.2 期望收益率攻击图分类

根据属性攻击图中原子攻击之间以及原子攻击条件之间关系, 可将属性攻击图中的原子攻击

划分为: “或”关系属性攻击图(包括攻击“或”和条件“或”)、“与”关系属性攻击图(包括攻击“与”和条件“与”)。

“或”关系属性攻击图如图 5 所示。图中方框表示属性节点, 椭圆表示攻击节点。

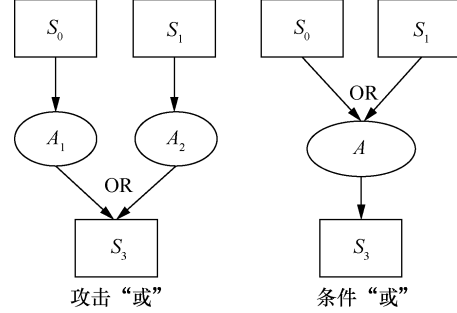


图 5 “或”关系属性攻击图
Figure 5 “OR” relationship attribute-based attack graph

“与”关系属性攻击图如图 6 所示。

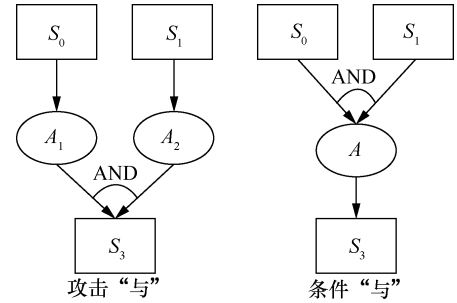


图 6 “与”关系属性攻击图
Figure 6 “AND” relationship attribute-based attack graph

根据期望收益率攻击图模型定义, 只需增加期望收益率计算结果便可以将相应的属性攻击图转换为期望收益率攻击图。此外, 对于期望收益率攻击图而言, 不同的收益率意味着对不同的攻击。因此, 图 5 所示的“或”关系属性攻击图转换成“或”关系期望收益率攻击图后是等价的, 如图 7 所示。图 6 所示的“与”关系属性攻击图转换成“与”关系期望收益率攻击图后是等价的, 如图 8 所示。图 8 中 $B(S_i - S_j, A_k)$ 表示 A_k 攻击的期望收益率。

3 攻击收益率量化及计算模型

3.1 原子攻击成本及其量化

定义 10 攻击成本 (AC, attack cost) 指攻击者为了成功入侵某一目标系统, 所需要的平均

时间、基本要素或工具以及攻击者自身所具备的能力等。

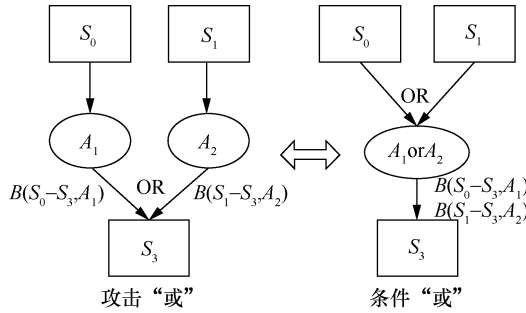


图7 “或”关系期望收益率攻击图

Figure 7 “OR” relationship attack graph of expected benefits-rate

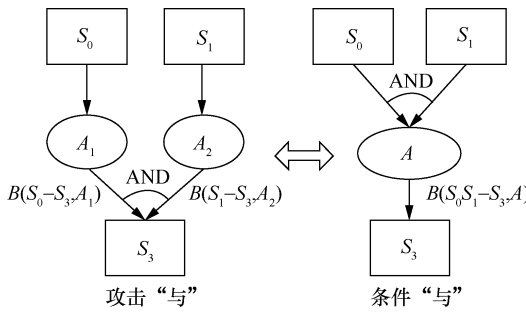


图8 “与”关系期望收益率攻击图

Figure 8 “AND” relationship attack graph of expected benefits-rate

借鉴经济学中关于固定成本和变动成本的定义，将攻击成本划分为攻击固定成本（AFC，attack fixed cost）、攻击变动成本（AVC，attack variable cost）和攻击时间成本（ATC，attack time cost）。参考马春光等^[13]提出的关于攻击压力要素的划分及量化方法，本文将 AFC 划分为攻击损耗包括损耗系数（LF，loss factor）、攻击代码信息（SI，shellcode information）、攻击代码平台（SP，shellcode platform）；AVC 包括攻击操作需求（OR，operation requirement）和攻击信息需求（IR，information requirement）。AC 层次化要素如图 9 所示。AC 要素量化如表 1 所示。

借鉴 AC 的定义，在其组成要素量化的基础上，本文将 AC 的计算模型定义为 AFC、AVC、ATC 所有成本的总和。AC 计算模型如式(1)所示。

$$AC = AFC + AVC + ATC \quad (1)$$

其中， A_{FC} 的取值取决于 SI、SP 以及 LF，并通过 LF 作为每次攻击对 SI、SP 的折旧提取，这样可以对不同的攻击、不同阶段的攻击，灵活模拟攻击固定成本。AFC 的计算模型如式(2)所示。

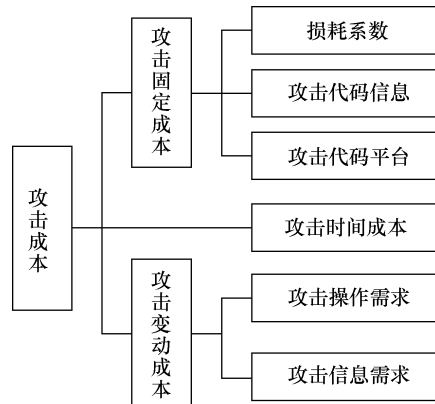


图9 AC 层次化要素

Figure 9 AC hierarchical elements

$$A_{FC} = LF \cdot (SI + SP) \quad (2)$$

表1 AC 要素量化
Table 1 Quantification of AC elements

分类	要素	可选值	分值
AFC	SI	Complete Code/Function Code/Null	0.3/0.5/0.7
	SP	Common/Special/Particular	0.3/0.5/0.7
	LF	Reuse/Modify/Disposable	0.2/0.6/1.0
AVC	OR	Tool/Script/Corporation	0.3/0.5/0.8
	IR	Regular Information/Configuration/Critical Information	0.3/0.5/0.8
ATC	AT	Short/Normal/Long	0.2/0.5/0.7

3.2 原子攻击收益分析及其量化

定义 11 攻击收益（AB，attack benefit）：攻击收益指攻击者通过投入一定的攻击成本，以某种方式入侵某一目标系统，进而在该攻击过程中所获得的一系列收益。

根据攻击收益的定义将其划分为攻击权限收益（APB，permission benefits by attack）、攻击价值收益（AVB，value benefits by attack）和攻击拓展收益（AEB，expansion benefits by attack）。其中 APB 指的是攻击者在入侵目标网络系统时能够获取的权限及其度量，根据权限从低到高划分为远程注册（RR，remote registration）、认证绕过（CB，certified bypass）、有限访问（LA，limited access）和完整权限（full access）。AVB 指的是攻击者在入侵目标网络系统时能够直接获取或破坏的资产价值，主要包括 CV（confidentiality value）、IV（integrity value）、AV（availability value），其取值分别由专家评价获取。AEB 表示攻击目标的通用程度，进而影响对其他目标系统的收益情况。AB

层次化要素如图 10 所示。AB 要素量化如表 2 所示。

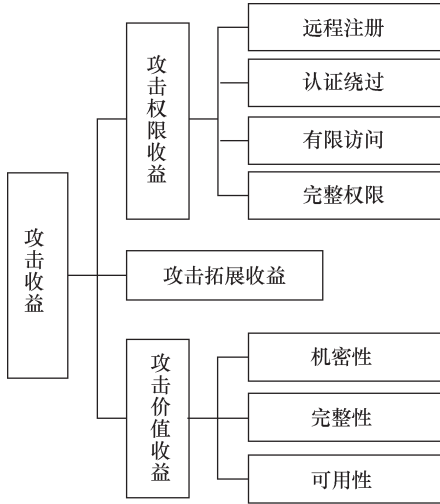


图 10 AB 层次化要素
Figure 10 AB hierarchical elements

表 2 AB 要素量化
Table 2 Quantification of AB elements

分类	要素	可选值	分数
APB	RR	/	0.55
	CB	/	0.75
	LA	/	0.85
	FA	/	1.0
AVB	CV	Normal/Medium/High	0.2/0.5/0.7
	IV	Normal/Medium/High	0.2/0.5/0.7
	AV	Normal/Medium/High	0.2/0.5/0.7
AEB	EB	Low/Medium/High	0.2/0.4/0.6

注：“/”表示不适用。

AB 计算模型如式(3)所示。

$$AB=APB+AVB+AEB \quad (3)$$

式(3)中 AVB 可通过 CV、IV 和 AV 综合反映得到。根据实际经验 CV、IV 和 AV 这 3 种价值中最高一个对资产的价值影响最大，且不同行业由于业务、职能和行业背景差别较大，故安全风险评估和安全保障的要求也不同，本文的 AVB 计算模型增加了权重，用于区别不同行业的安全风险评估。

AVB 计算模型如式(4)所示。

$$AVB = \ln[e \cdot (\alpha \cdot e^{CV} + \beta \cdot e^{IV} + \gamma \cdot e^{AV}) / \delta] \quad (4)$$

式(4)中采用指数的形式是为了体现最高要

素的主导性。其中 α 、 β 、 γ 分别为 CV、IV 和 AV 的权重系数。 e 为自然常数、与常量 δ 一起作为调节系数，目的是将 AVB 的取值映射到 1.0 以内。为了便于计算分析和关注模型本身，本文将 α 、 β 、 γ 取值设定为 1，此时常量 $\delta = 6.04$ 。

3.3 原子攻击期望收益率计算模型

定义 12 折现率 (DR, discount rate) 指的是攻击者利用目标网络脆弱性并最终获取收益的程度，折现率与漏洞的可利用性直接相关，可利用性大则最终期望收益率大，反之则小。

根据 DR 的定义以及通用漏洞评分系统 (CVSS) 中关于漏洞可利用性的组成要素及其度量，可以发现 DR 与 CVSS 中可利用性正相关。因此，本文直接采信 CVSS 中可利用性的组成要素及其量化值，并在此基础上构建 DR 的计算模型。DR 组成要素及其量化如表 3 所示。

表 3 DR 组成要素及其量化
Table 3 DR components and quantification

要素	可选值	分数
Attack Vector(AV)	Local/Network	0.7/1.0
Attack Complexity(AC)	High/Medium/Low	0.6/0.8/1.0
Authentication(AU)	Required/Null	0.6/1.0

DR 计算模型如式(5)所示。

$$DR = AV \cdot AC \cdot AU \quad (5)$$

定义 13 原子攻击期望收益率 (ARB, atomic attack rate of benefit) 指的是攻击者依据攻击节点将某一属性节点转换或获取为另一属性节点时期望的收益与付出的成本的比率。其基本计算模型如式(6)所示。

$$ARB = DR \cdot \frac{AB}{AC} \cdot 100\% \quad (6)$$

即

$$ARB = DR \cdot \frac{APB+AVB+AEB}{AFC+AVC+ATC} \cdot 100\%$$

在基于期望收益率的攻击图中，原子攻击期望收益率计算主要分为两种情况，即“或”关系的基本期望收益率和“与”关系的基本期望收益率，也就是本文图 7 和图 8 所描述的情况。

(1) “或”关系的期望收益率计算

图 7 描述的“或”关系期望收益率攻击图

中，由于两种攻击的最终收益都取决于 S_3 节点，故收益不变，而 $S_0 \rightarrow A_1 \rightarrow S_3$ 和 $S_1 \rightarrow A_2 \rightarrow S_3$ 的攻击成本则很大可能不同。因此，可依据式(1)~式(6)，分别计算攻击期望收益率，假设计算结果为

$$B_1(S_0 - S_3, A_1) = ARB^1$$

$$B_2(S_1 - S_3, A_2) = ARB^2$$

若 $ARB^1 \geq ARB^2$ ，显然一个理性的攻击者会将攻击节点 A_1 作为攻击路径选项，同理，作为一个理性的网络安全管理者在有限的精力和时间内，也将首先针对 $S_0 \rightarrow A_1 \rightarrow S_3$ 加强网络防御。

(2) “与”关系的期望收益率计算

图8描述的“与”关系期望收益率攻击图，虽然是一次原子攻击，但 A 攻击节点需要 S_0 和 S_1 属性节点同时满足的情况下才能达到目的节点 S_3 。通过图8中“与”关系期望收益率攻击图的转换，可以转换成 $S_0 \rightarrow A_1 \rightarrow S_3$ 和 $S_1 \rightarrow A_2 \rightarrow S_3$ 攻击，由于是“与”的关系，单一的攻击无实际意义，只有在计算期望收益率时，才考虑将两种攻击的收益等同，即都等于 S_3 最终收益。设攻击最终期望收益率为 ARB 、最终收益为 AB 、折现率为 DR ， $S_0 \rightarrow A_1 \rightarrow S_3$ 攻击的成本为 AC_1 、期望收益率为 ARB^1 ， $S_1 \rightarrow A_2 \rightarrow S_3$ 攻击的成本为 AC_2 、期望收益率为 ARB^2 ，则各期望收益率计算过程如下。

$$ARB^1 = DR \cdot \frac{AB}{AC_1} \cdot 100\% \quad (7)$$

$$ARB^2 = DR \cdot \frac{AB}{AC_2} \cdot 100\% \quad (8)$$

$$ARB = DR \cdot \frac{AB}{AC_1 + AC_2} \cdot 100\% \quad (9)$$

式(7)、式(8)代入式(9)可得

$$\frac{1}{ARB} = \frac{1}{ARB^1} + \frac{1}{ARB^2} \quad (10)$$

在式(10)的基础上延伸至“与”关系期望收益率攻击图，攻击图含 n 个属性（攻击）“与”的情况，则期望收益率计算模型为

$$\frac{1}{ARB} = \frac{1}{ARB^1} + \frac{1}{ARB^2} + \dots + \frac{1}{ARB^n} \quad (11)$$

3.4 攻击路径确定

依据已知节点属性和状态、攻击方法等构建属性攻击图，在原子攻击成本与收益量化的基础上，计算各原子攻击期望收益率及攻击原子攻击间的逻辑关系，生成期望收益率列表，最后将期望目标作为出发点，依据某一策略（如回溯法、贪心算法、动态规划）展开搜索，最终得到收益率最大的路径作为首选攻击路径。

4 仿真实验及分析

本文研究的重点是在属性攻击图的基础上加入攻击期望收益率，为了简化和更好地理解本文提出的期望收益率攻击图及其相关研究，本节采用仿真实验的方法。

实验的主要方法为：设计一个包含多种“OR”和“AND”关系的属性攻击图；转换为期望收益率攻击图并进行收益率量化（赋值）；结合期望收益率量化情况，舍去期望收益率较低的攻击路径并生成最优收益率攻击图。

4.1 实验假设

假设针对某网络系统的安全分析所生成的属性攻击图，如图11所示。图中 S_8 为网络攻击的最终节点，矩形方框代表属性节点，椭圆代表攻击节点，“OR”和“AND”分别代表“或”和“与”关系。

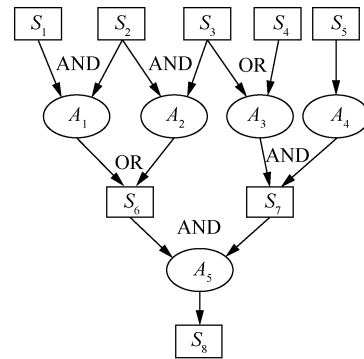


图11 实验网络的属性攻击图
Figure 11 Attribute attack diagram of experimental network

4.2 期望收益率攻击图

图11所示的属性攻击图添加期望收益率后可转换为期望收益率攻击图，如图12所示。

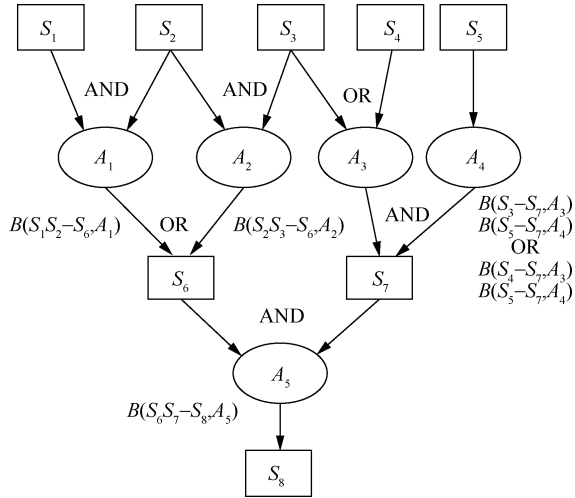


图 12 实验网络的期望收益率攻击图
Figure 12 Benefits-rate of the experimental network

为了便于分析,图 12 中的各期望收益率结果如表 4 所示。

表 4 期望收益率情况
Table 4 The results of benefits-rate

变量名	变量名缩写	收益率
$B(S_1S_2-S_6, A_1)$	$B(A_1)$	65%
$B(S_2S_3-S_6, A_2)$	$B(A_2)$	55%
$B(S_3-S_7, A_3)$	$B(A_3)$	40%
$B(S_4-S_7, A_3)$	$B(A_{30})$	60%
$B(S_5-S_7, A_4)$	$B(A_4)$	30%
$B(S_6S_7-S_8, A_5)$	$B(A_5)$	50%

4.3 期望收益率攻击图简化

从图 12 期望收益率攻击图中可以发现共两处存在“OR”的情况,转换为期望收益率“OR”的情况即 $B(A_1) \text{ OR } B(A_2)$, $B(A_3) \text{ OR } B(A_{30})$ 。依据表 5 期望收益率量化情况,显然应该保留 $B(A_1)=65\%$ (保留 $S_1S_2 \rightarrow A_1 \rightarrow S_6$, 舍去 $S_2S_3 \rightarrow A_2 \rightarrow S_6$) 和 $B(A_{30})=60\%$ (保留 $S_4 \rightarrow A_3 \rightarrow S_7$, 舍去 $S_3 \rightarrow A_3 \rightarrow S_7$)。

此外,设“与”关系攻击路径 $S_4 \rightarrow A_3 \rightarrow S_7$ 和 $S_5 \rightarrow A_3 \rightarrow S_7$ 攻击期望收益率为 $B(A_6)$,依据式(11),则 $B(A_6)$ 计算结果为

$$\frac{1}{B(A_6)} = \frac{1}{B(A_{30})} + \frac{1}{B(A_4)} = \frac{1}{0.6} + \frac{1}{0.3} = 5 \quad (12)$$

即

$$B(A_6) = \frac{1}{5} \cdot 100\% = 20\% \quad (13)$$

简化后的期望收益率攻击图如图 13 所示。

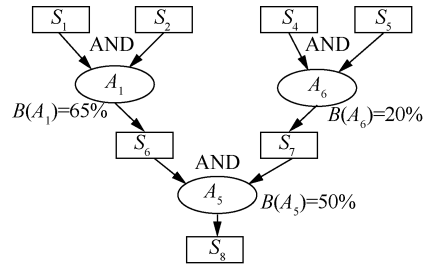


图 13 简化后的期望收益率攻击图
Figure 13 Simplified attack graph of benefits-rate

5 结束语

随着网络技术的快速发展,网络面临的攻击威胁在不断增加,特别是 APT 攻击,具有极强的隐蔽性和针对性,能够对目标网络造成持久且有效的威胁。为了更好地保护重要的网络节点,准确识别攻击目标和攻击路径,为管理人员提供安全策略支撑,本文提出了一种基于期望收益率攻击图的网络安全风险评估模型。首先,通过采集网络漏洞信息、网络攻防等相关网络安全数据,依据 Spark 大数据分析评估平台得到攻击成本和攻击收益的相关要素;其次,依据经济学中相关概念构建攻击成本、攻击收益和原子攻击期望收益率计算模型,提出属性攻击图向期望收益率攻击图的转换方法;最后,利用属性攻击图生成目标网络的全部攻击路径,并计算攻击节点上的期望收益率大小,进而依据期望收益率简化和预测最可能的攻击路径,为网络安全风险分析提供重要依据。仿真实验表明,将期望收益率模型和属性攻击图相结合进行网络风险评估具有可行性和可信性。

本文将期望收益率的概念应用到网络风险评估中,提出基于期望收益率攻击图的网络安全评估方法,该方法不但具备属性攻击图的优点,而且在此基础上构建的期望收益率攻击图,可以依据不同的策略优化攻击路径,进而为使用方提供优先防护/攻击策略。此外,该方法的关键点和难点是攻击成本和收益要素的分类、量化以及期望收益率模型构建,由于模型构建过程中涉及的要素较多,对要素的分类及其量化提出了较高的要求。期望收益率模型涉及的要素及其量化直接影响了模型计算的科学性和准确性,下一步需加强研究、优化模型。

参考文献:

- [1] 吴迪, 冯登国, 连一峰, 等. 一种给定脆弱性环境下的安全措施效用评估模型[J]. 软件学报, 2012, 23(7): 1880-1898.
WU D, FENG D G, LIAN Y F, et al. Efficiency evaluation model of system security measures in the given vulnerabilities set[J]. Journal of Software. 2012, 23(7): 1880-1898.
- [2] MAIO F D, MASCHERONA Z E. Risk analysis of cyber-physical systems by GTST-MLD[J]. IEEE Systems Journal, 2020, 14(1): 1333-1340.
- [3] LEE J, MOON D, KIM I, et al. A semantic approach to improving machine readability of a large-scale attack graph[J]. The Journal of Supercomputing, 2018.
- [4] SCARFONE K, MELL P. An analysis of CVSS version 2 vulnerability scoring[J]. IEEE Computer Society, 2009.
- [5] KERAMATI M, AKBARI A. CVSS-based security metrics for quantitative analysis of attack graphs[C]//2013 3th International Conference on Computer and Knowledge Engineering (ICCKE). 2013.
- [6] KHOUZANI M, LIU Z, MALACARIA P. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs[J]. European Journal of Operational Research, 2019.
- [7] LIU X G. A network attack path prediction method using attack graph[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, (1): 1-8.
- [8] ZANG T, GAO S, LIU B, et al. Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks[J]. Reliability Engineering & System Safety, 2019, 189(SEP.): 232-241.
- [9] OBERT J, CHAVEZ A. Graph theory and classifying security events in grid security gateways[J]. International Journal of Semantic Computing, 2020, 14(1): 93-105.
- [10] 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 F, ZHANG Y, SU J S, et al. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4): 838-848.
- [11] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]//IEEE Symposium on Security & Privacy. 2002.
- [12] INGOLSK, CHU M, LIPPMANN R, et al. Modeling modern network attacks and countermeasures using attack graphs[R]. 2009.
- [13] 马春光, 汪诚弘, 张东红, 等. 一种基于攻击意愿分析的网络风险动态评估模型[J]. 计算机研究与发展, 2015, 52(9): 2056-2068.
MA C G, WANG C H, ZHANG D H, et al. A dynamic network risk assessment model based on attacker's inclination [J]. Journal of Computer Research and Development. 2015, 52(9): 2056-2068.
- [14] 闫峰. 基于攻击图的网络安全风险评估技术研究[D]. 长春: 吉林大学, 2014.
YAN F. The technology research of network security risk assessment based on attacks graphs[D]. Changchun: Jilin University, 2014.
- [15] ZHANG S, SONG S. A novel attack graph posterior inference model based on bayesian network[J]. Journal of Information Security, 2011, 2(1): 8-27.
- [16] WANG L, LIU A, JAJODIA S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts[J]. Computer Communications, 2006, 29(15): 2917-2933.
- [17] 周余阳, 程光, 郭春生. 基于贝叶斯攻击图的网络攻击面风险评估方法[J]. 网络与信息安全学报, 2018, 4(6): 11-22.
ZHOU Y Y, CHENG G, GUO C S. Risk assessment method for network attack surface based on Bayesian attack graph[J]. Chinese Journal of Network and Information Security, 2018, 4(6): 11-22.
- [18] LALLIE H S, DEBATTISTAK, BAL J. Evaluating practitioner cyber-security attack graph configuration preferences[J]. Computers & Security, 2018, 79: 117-131.
- [19] LIN P, CHEN Y. Dynamic network security situation prediction based on bayesian attack graph and big data[C]//2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). 2018.

[作者简介]



刘文甫 (1986-), 男, 河南卫辉人, 信息工程大学博士生, 主要研究方向为大数据分析、自然语言处理、信息安全。



庞建民 (1964-), 男, 河北沧州人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为数据库理论、数据挖掘、机器学习、高性能计算、信息安全。



周鑫 (1994-), 男, 辽宁沈阳人, 信息工程大学博士生, 主要研究方向为人工智能、漏洞挖掘、信息安全。



李男 (1977-), 男, 河北保定人, 博士, 信息工程大学副教授, 主要研究方向为高性能计算和大数据隐私保护。



岳峰 (1985-), 男, 山西长治人, 博士, 信息工程大学讲师, 主要研究方向为高性能计算、信息安全、大数据挖掘。