第 44 卷 第 3 期 计 算 机 工 程 2018 年 3 月
Vol. 44 No. 3 Computer Engineering March 2018

·安全技术· 文章编号：1000-3428(2018)03-0151-05 文献标志码：A 中图分类号：TP391.06

基于 Rete 算法的攻击图构建方法

樊子华，常朝稳，韩培胜，潘冬存

（信息工程大学 三院，郑州 450000）

摘 要： 针对现有攻击图构建方法适用的网络规模受限的问题，通过分析现有方法存在的缺陷及构建过程中的特点，使构建攻击图转化为威胁行动属性之间的模式匹配，将 Rete 引入到攻击图构建过程中，提出基于 Rete 的攻击图构建方法。实验结果表明，该方法具有较好的构建效率，能够适用于大规模网络的攻击图构建。

关键词： 网络安全；攻击图；Rete 算法；大规模网络；攻击图构建；模式匹配

中文引用格式： 樊子华，常朝稳，韩培胜，等. 基于 Rete 算法的攻击图构建方法[J]. 计算机工程，2018，44(3)：151-155，165.

英文引用格式： FAN Zihua，CHANG Chaowen，HAN Peisheng，et al. Generation Method of Attack Graph Based on Rete Algorithm[J]. Computer Engineering，2018，44(3)：151-155，165.

Generation Method of Attack Graph Based on Rete Algorithm

FAN Zihua，CHANG Chaowen，HAN Peisheng，PAN Dongcun

（The Third Academy，Information Engineering University，Zhengzhou 450000，China）

【Abstract】 Aiming at the problem that the applicable network scale for existing attack graph generation methods is limited，through analysis of the shortage of the existing attack graph construction methods and the characteristics of the construction process，the constructed attack graph is transformed into a pattern matching between the threat action properties. Rete is introduced into the construction process of attack graph，an attack graph building method based on Rete is proposed. Experimental results show that the method has better construction efficiency and can be applied to the construction of attack graph in large-scale network.

【Key words】 network security；attack graph；Rete algorithm；large-scale network；attack graph generation；pattern match

DOI： 10.3969/j.issn.1000-3428.2018.03.026

0 概述

计算机及网络技术的飞速发展使得计算机网络的规模越来越大，随着计算机网络更加广泛和深入地应用到社会生活的方方面面，针对计算机网络的恶意攻击所造成的后果也日益严重。攻击图能够反映网络中存在的威胁路径，因此为网络的安全防护提供重要的支撑。

现有攻击图构建方法的构建时间随网络中主机数目的增加而迅速增长，因此无法有效地应用到大规模网络中，其主要原因是网络环境中大量的属性使得需要较长的时间去寻找攻击之间的关联关系。针对这一问题，本文将寻找攻击之间的关系归结为属性之间的模式匹配，将 Rete 算法引入攻击图构建过程中。首先根据网络中属性种类的不同对所有属性进行处理，得到环境网络；其次将攻击模式作为事实与环境网络进行匹配，产生有效的原子攻击及攻击之间的关联关系，进而生成攻击图。

1 相关研究

攻击图构建方法从手工构建[1]开始，发展到现在的自动构建；从为较小规模计算机网络[2]构建开始，发展到现在的为较大规模计算机网络构建[3]。计算机网络规模的不断扩展使得攻击图的构建代价越来越大[4]，现有的攻击图构建方法[5-6]已经不能很好地应用到大规模网络当中[7]。

文献[8]提出一种原子攻击搜索算法，主要针对攻击模式中的所有变量，根据变量取值的不同实例化攻击模式知识库中的每一个攻击模式，得到可能被利用的原子攻击集合，遍历该集合找到前提条件已经满足的原子攻击。该算法在构建时间方面具有较大的缺陷，时间复杂度高达 $O(N^6)$，其中 N 为网络中的主机数目，因此无法应用于大规模网络。

为了降低攻击图构建所需要的时间，文献[9]借鉴 IP 地址中无类别域间路由记法，提出了基于 CIDR 的属性压缩方法，通过主机间的相互关系转化

作者简介：樊子华(1993—)，男，硕士研究生，主研方向为网络态势感知；常朝稳，教授；韩培胜，副教授；潘冬存，教授。

收稿日期：2017-02-09 修回日期：2017-03-19 E-mail：fanzihua1993@163.com

为虚拟子网间的相互关系,压缩网络中的属性数量,提高构建效率。但当网络中主机与外部网络的连接关系存在差异时,该属性压缩方法就无法使用。

文献[10]采用反向搜索策略,以攻击目标为基础,反向推导出攻击路径,进而生成部分攻击图。由于构建部分攻击图所需任务量明显较小,因此该方法能够应用于大规模网络,文献中的实验也表明了这一点。但部分攻击图在理解网络整体的安全性方面存在缺陷,且只能应用于攻击目标确定的情况下。

文献[11]针对网络中巨大的属性数量显著提高攻击图构建代价的特点,采用属性的预处理技术对属性进行分类,并利用攻击实例化技术生成攻击图。但预处理技术只是对网络中的属性进行简单分类,在攻击实例化时仍具有较大的输入量,增加了攻击图构建的时间消耗,时间复杂度达到 $O(N^4)$,其中 N 为网络中的主机数目。

综合上述方法的优缺点,针对攻击图构建方法存在的不足,本文将构建攻击图过程中的重要过程——寻找攻击之间的关联关系转化为模式匹配问题,将 Rete 算法引入攻击图构建中,用于寻找攻击之间的关联关系,提出基于 Rete 的攻击图构建方法并分析时间复杂度,最后给出算法的实验和分析。

2 Rete 算法

Rete 算法[12]是一种高效的模式匹配算法,主要用于产生式系统。Rete 算法的主要思想是以空间换时间,基于规则本身及规则之间的结构相似性共享匹配结果,以此消除重复的匹配过程,提高模式匹配效率。

一个产生式系统程序[13]是由一系列 If-Then 结构的规则组成,需要匹配规则的数据称为事实,被保存在一个全局数据库工作存储器(Working Memory)中[14]。一条规则可分为 If、Then 两部分,If 部分称为 LHS,Then 部分称为 RHS[15]。If 部分包含若干个正或负模式,代表成功匹配该规则时需要具有的属性,如果某一规则 If 部分中的每一个正模式得到匹配且每一个负模式均不匹配,则称这条规则被满足;Then 部分包含一系列动作,代表成功匹配该规则时将要执行的动作。Rete 算法的功能是基于 Working Memory 中存储的事实,找到产生式系统中所有匹配的规则。

在匹配之间首先根据所有规则的 LHS 构造一个判别网络,表示所有规则各属性之间的依赖关系,利用了规则之间的属性结构相似性。假设有规则 1:If $c0 \wedge c1 \wedge c2 \wedge c3 \wedge c4$ Then $P1$。判别网络定义了多种节点,包括根节点、类型节点、α 节点、β 节点、终端节点,不同的节点具有不同的功能。

建立好判别网络后,将 Working Memory 中的事实经过根节点送入判别网络中进行匹配,当事实能够满足某一规则的 LHS 时,就会到达该规则对应的终端节点将其触发。匹配过程通过以下操作实现:

1)匹配:从 Working Memory 选出一个事实,评估规则 LHS 的每个属性,判断事实满足的属性;

2)冲突解决:从所有满足 LHS 的规则中选择一个,如果不存在能够满足 LHS 的规则,则停止匹配;

3)执行:执行所选中规则的 RHS 中的动作;

4)跳转到 1)继续执行。

通过上述过程,可以将规则的 LHS 集合与元素 WME 相比较找到所有的实例。如图 1 所示为规则 1匹配过程示意图,表示当属性 $c0$、$c1$、$c2$、$c3$ 与 $c4$ 均满足时到达终端节点触发 $P1$。

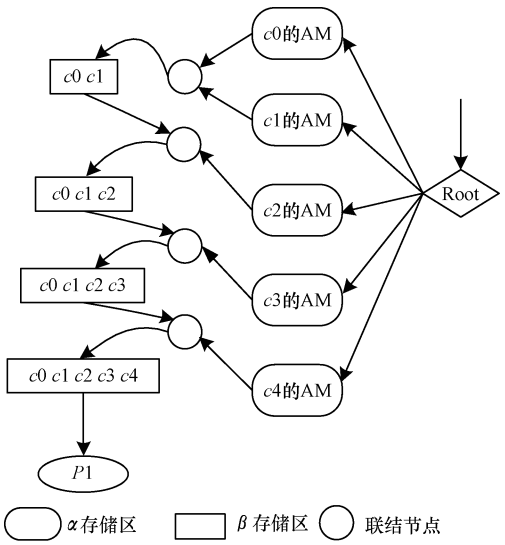

图 1 Rete 规则网络示例

3 攻击图和相关概念的定义

生成攻击图之前,本文首先对网络中的安全要素进行定义。

定义 1(攻击图)攻击图是网络的一个状态转换图,表现了攻击造成的状态及这些状态之间的关联关系,体现了网络中潜在的威胁路径。攻击图可以用一个四元组来表示(N,E,N_0,N_g),其中,N_0是初始状态集合,代表网络的初始状态。N_g是目标状态集合,代表攻击者最终想要达到的状态。N 为中间状态集合,代表网络中主机的状态。

攻击者在达到目标状态之前,需要通过攻击主机取得所需条件,这个过程所产生的状态就是中间状态。攻击图中的节点集合就是网络的状态集合,可以定义为 $N \cup N_0 \cup N_g$,用如下四元组来表示(Id,$Hostid$,Vul,P)。其中,Id 为状态节点标识,$Hostid$ 是使网络状态发生变化的主机标识,Vul 为该状态下存在的弱点,P 是攻击者成功到达该网络状态的概率。

E 是边集合,代表状态之间的转移。在攻击图中,边集合可以定义为 $E \subseteq (((N_0 \times N) \times N) \cup (N \times N_g))$。

定义 2(弱点) 弱点是指可以被攻击者利用,从而进行攻击的漏洞,可用如下五元组来表示(*Vid*, *Range*,*Type*,*Service*,*Result*)。其中,*Vid* 为该弱点在 CVE 漏洞库的唯一标识,*Range* 为弱点的利用范围,*Type* 为弱点类型,*Service* 为弱点所对应服务的名称,*Result* 为成功利用该弱点的后果。

定义 3(威胁行动) 能够改变网络状态的活动称为威胁行动,体现为攻击图中的边集合 E,本质上就是攻击者的攻击,可用如下三元组来表示(*Src_host*, *Dst_host*,*AP*)。其中,*Src_host* 为攻击起点所在的主机,*Dst_host* 为受到攻击的主机,*AP* 为威胁行动采用的攻击模式。

定义 4(攻击模式) 攻击模式是指攻击者攻击方法的总结,可用如下四元组来表示(*Name*,*Vuls*,*Pre*, *Eff*)。其中,*Name* 是攻击模式的名称,*Vuls* 是攻击模式所能利用的弱点,*Pre* 为该攻击模式发生的先决条件集合,*Eff* 为该攻击模式被利用的后果集合。

定义 5(威胁路径) 对于一个目标状态 $N_n \in N_g$,如果从非目标状态 N_0 开始,存在一个状态序列 N_1, $N_2,\cdots,N_{n-1}$,使得 $(N_{i-1},N_i) \in E, 0 < i < n-1$,就称该序列为一条威胁路径。非目标状态 N_0 指该状态可以是初始状态或中间状态,威胁路径反映了攻击者从初始状态到目标状态的整个攻击过程。

攻击图的构建过程是通过威胁行为将状态节点连接起来,本质是攻击者的威胁行动使得网络安全状态不断变化,并且一个威胁行动所用攻击模式的 *Eff* 属性满足其他威胁行动中攻击模式的 *Pre* 属性。可以将构建攻击图的过程转化为寻找威胁路径的过程,而威胁路径是通过威胁行动中攻击模式的先决条件和后果之间的对应关系、主机之间的连接关系共同分析得到,因此可以将构建攻击图转化为攻击模式及网络环境属性之间的模式匹配。

由于在攻击图的构建过程中需要多次遍历整个网络,因此攻击图的构建时间随着网络规模的增长也在快速增加,攻击图构建所需时间是一个重要的指标。为此,本文将模式匹配算法 Rete 引入攻击图的构建过程中,首先对目标环境中的属性进行处理,得到环境网络;将攻击模式作为事实与环境网络进行匹配,产生有效的原子攻击及攻击之间的关联关系,进而生成攻击图。

4　基于 Rete 算法的攻击图构建方法描述

假设威胁行动 TA_i 和威胁行动 TA_j 在攻击图中处于同一威胁路径中的相邻位置,且 TA_i 在前,那么 TA_i 中攻击模式的后果集合 *Eff* 满足 TA_j 中攻击模式的先决条件集合 *Pre*,即 $Eff(i)$ 能够匹配 $Pre(j)$;TA_i 和 TA_j 中 *Src_host* 属性所对应主机相互之间应具有连接关系。通过匹配威胁行动及其相关的 *Pre*、*Eff* 等属性可以明确威胁行动之间的相互关系,完成威胁路径的搜索,进而构建出完整的攻击图。

根据 Rete 算法的流程,可以将攻击图的构建过程分为建立环境网络和威胁行动匹配 2 个步骤。

环境网络的建立是将威胁行动的 *Eff* 集合分解为单个属性,与 *src_host* 对应的 HostID 等属性共同构建环境网络,代表当前网络环境,通过建立环境网络可以减少匹配过程中无效的匹配数量,进而降低攻击图构建所需时间。

威胁行动匹配是将威胁行动的 *Pre* 集合作为事实进入环境网络进行匹配,当到达环境网络的终端节点时,表明 *Pre* 集合对应的威胁行动与终端节点存储的威胁行动具有关联关系,在同一个威胁路径中并处于相邻的位置。重复进行该步骤能够得到现有环境下可能会发生的威胁行动以及与这些威胁路径具有关联关系的威胁行动,进而完成威胁路径的搜索,再进而完成攻击图的构建。

4.1　环境网络构建

基于威胁行动中属性的特点,将不同的属性对应不同的环境网络节点,包括根节点、类型节点、α 节点、β 节点和终端节点,各节点定义如下:

定义 6(根节点) 根节点是环境网络的起点,任意一个需要匹配的 *Pre* 属性都要通过根节点进入环境网络。

定义 7(类型节点) 类型节点紧跟根节点,目的是筛选匹配项,任何不属于该类型的 *Pre* 集合属性不需要与后续节点继续匹配,从而减少不必要的匹配过程。在网络中只有当 2 个主机具有连接关系时,这 2 个主机上的威胁行动才会在同一威胁路径中并处于相邻位置,也就是说具有关联关系的威胁行动所在主机具有连接关系。根据这一特性,将与某台主机具有连接关系的所有主机的 HostID 集合作为类型节点。当某威胁行动的 *Pre* 集合属性经过根节点后,只能通过包含威胁行动 *Src_host* 属性对应的 HostID 的类型节点继续匹配。

定义 8(α 节点) α 节点紧跟类型节点之后,用于判断表现形式为名称、数字等定值的属性是否相等。如表 1 所示为部分采用 α 节点形式进行表达的属性。每个 α 节点维护一个内存表,用于存储与该节点匹配的 *Pre* 属性。当相同的 *Pre* 属性再次到达该节点时可直接匹配,提高匹配效率。

表 1　部分利用 α 节点进行匹配的属性

类型	描述
Protocal	A transport or application layer protocol, such as tcp, udp and rpc
VulID	Vulnerability information which is marked by the CVE ID
Remote	Remote or Local
Privilege	Access permission, such as user and root
Data	Data Type

定义 9(β 节点) β 节点是变量判断节点,用于判断属性之间等于、大于、小于等相互关系,只有对应属性符合相互关系时才能继续匹配,比如在某一主机上,攻击者现有权限必须大于操作所需权限才能成功完成操作。如表 2 所示为部分采用 β 节点进行表达的属性。与 α 节点相同,β 节点也通过维护内存表来提高匹配效率。

表 2 部分利用 β 节点进行匹配的属性

类型	描述
lHasPrivilege(cpriv,npriv)	Attacker has Privilege of cpriv level and the operate need Privilege of npriv level
HasProtocol(pro1,pro2)	src_host has Protocol pro1 which is the same as Protocol pro2 of dst_host
Trust(dst_host,src_host)	The dst_host trust the src_host

定义 10(终端节点) 终端节点位于环境网络的末端,存储一个威胁行动。当 *Pre* 集合属性到达终端节点时,表明 *Pre* 集合对应的威胁行动与终端节点中的威胁行动匹配成功,相互之间具有关联关系,这 2 个威胁行动在同一威胁路径中并处于相邻位置。

通过建立环境网络将现有威胁行动及相关属性存储在一个网状结构中,利用环境网络进行匹配的好处是在寻找威胁路径时不需要匹配所有的威胁行动属性,*Pre* 集合属性每成功匹配一个节点,就相应地排除了其他部分节点及其后续节点,减少了不必要的搜索和匹配过程,提高了攻击图构建算法的性能。

根据上述节点定义,本文设计了环境网络构建算法 CrEvirNet,具体描述如下:

算法 1 CrEvirNet 算法(环境网络构建算法)

输入 威胁行为包含攻击模式的 *Eff* 集合及网络的相关属性

输出 环境网络

1. 创建一个根节点。

2. 根据主机之间的连接关系创建相应的类型节点并连接到根节点上。

3. 取一个攻击模式的 Eff 集合。

1)根据 src_host 属性选取对应的类型节点。

2)针对 Eff 集合中的单个属性,建立集合 A 和集合 B。符合 α 节点的单个属性放入集合 A,符合 β 节点的单个属性放入集合 B。

3)从集合 A 中取出一个属性,如果环境网络中存在对应的 α 节点,则将该节点作为后续节点与上一个节点相连;如果不存在对应的 α 节点,则创建该节点并作为后续节点。

4)重复步骤 3)直至集合 A 为空。

5)从集合 B 中取出一个属性,如果环境网络中存在对应的 β 节点,则将该节点作为后续节点与上一个节点相连;如果不存在对应的 β 节点,则创建该节点并作为后续节点。

6)重复步骤 5)直至集合 B 为空。

7)创建终端节点用于存储匹配的威胁行为,并将终端节点连接到对应的最后一个 β 节点。

4. 重复步骤 3 直到完成所有的攻击模式。

4.2 威胁行动匹配

环境网络构建算法能够根据当前网络状态和威胁行动建立完整的环境网络。根据建立的环境网络,针对攻击模式 APi,将其 *Pre* 集合属性作为事实送入环境网络进行匹配,如果能达到某个终端节点则攻击模式 APi 加上对应的源主机和目标主机的 HostID 就是可能发生的威胁行动,且与终端节点内存储的威胁行动具有关联关系,处于同一威胁路径的相连位置;针对所有攻击模式重复这一过程就能得到当前环境下可能发生的威胁行动集合及与现有威胁行动的关联关系;根据可能的威胁行动集合能够得到威胁路径,最后利用开源绘图工具 Graphviz 绘制攻击图。

首先建立一个派遣队列 queue,将攻击模式集合放入 queue 中,算法运行时不断从 queue 中取出一个攻击模式作为事实送入环境网络中进行匹配,得到可能的威胁行动集合,并将这些威胁行动的后果集合添加到环境网络中且将威胁行动添加到攻击图中,重复上述操作直到队列 queue 为空。

根据上述描述,本文设计了攻击图构建算法 APMCAG,具体描述如下:

算法 2 APMCAG 算法

输入 环境网络和攻击模式集

输出 攻击图

1. 建立一个派遣队列 queue 并放入攻击模式集。

2. 当派遣队列不为空时

1)从攻击模式集中选取一个攻击模式 APi,将其 *Pre* 集合送入环境网络中进行匹配。

2)如果可以匹配,则将对应终端节点中的威胁行为加入 PTA 集中。

3)如果不能匹配,则从攻击模式集合中选取另一个攻击模式并进行步骤 1)。

3. 重复步骤 2 直至攻击模式集为空。

4. 用 PTA 集中威胁行为的 *Eff* 集合更新环境网络。

5. 利用匹配到的威胁行为构建攻击图。

4.3 算法时间复杂度分析

设网络中主机数量为 N,描述主机连接关系的属性数目为 Nc,攻击模式数目为 M,攻击模式中 *Pre* 属性和 *Eff* 属性包含的元素数目上限为 U,匹配队列的数量为 A,则本文提出的攻击图的构建算法的时间消耗应该介于 $O(N^2)$ 和 $O(N^3)$ 之间。

证明:攻击图的生成算法中的派遣队列需要匹配的数量为 A,A 与主机数目 N 成线性关系。算法第 1 步寻找适合的类型节点,类型节点的总数量与 Nc 有关,Nc 与主机数目 N 成线性关系。经过类型节点后,在匹配的类型节点后进行匹配。在单个类型节点后的匹配时间复杂度与攻击模式中 *Pre* 属性和 *Eff* 属性包含的元素数目有关。算法最好的情况为只有一个适合的类型节点,此时时间复杂度为 $O(U)$;最坏的情况是所有类型节点均匹配,即网络

中所有的主机互相联通,此时时间复杂度为 $O(NcU)$。因此本文算法的总的时间复杂度为 $O(ANcU)-O(ANc^2U)$,由于 U 存在上限,是一个常数,A 和 Nc 与主机数目 N 线性相关,因此复杂度应介于 $O(N^2)$ 和 $O(N^3)$ 之间,也就是说算法的时间复杂度为 $O(N^3)$。

5　实验验证

5.1　实验环境

为了证明所提出算法的有效性,本文进行了仿真实验,其拓扑结构如图 2 所示。通过改变子网个数、每个子网中的主机个数可以改变网络规模,得到不同规模下算法的有效性。同时,每台主机上存在的弱点数量也可手动设置或随机分配。原型系统在下面的环境下进行测试:CPU 是 Corei5 3.2 GHz,内存 RAM 是 4 GB,操作系统是 Windows XP。

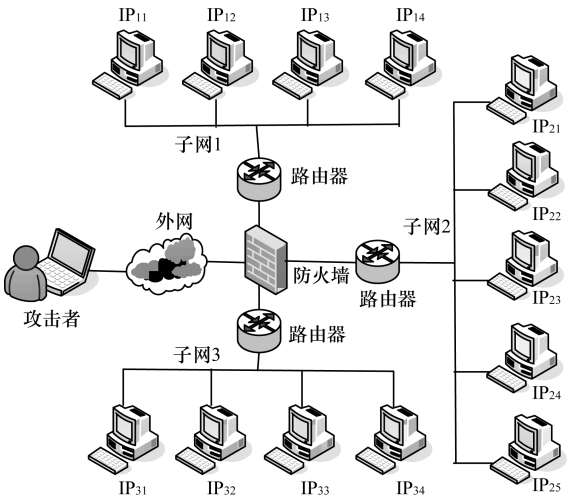

图 2　实验网络拓扑

5.2　实验结果与分析

当前存在较多的攻击图构建方法,本文选取由文献[16]提出的较为经典的方法进行比较。实验构建了模拟网络,网络中只有一个子网且没有防火墙,各主机之间是相互连接的,各主机上脆弱性的最大数量为 5。如图 3 所示为各个方法所用的 CPU 时间,单位为 s。

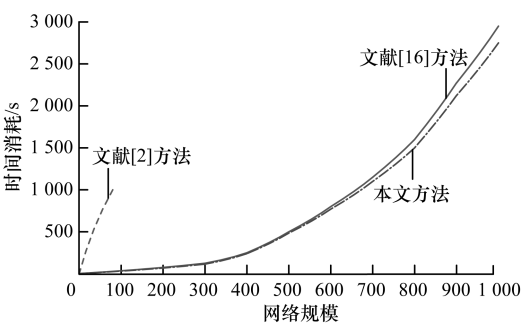

图 3　网络规模对攻击图构建时间的影响

分析图 3 可知,文献[2]方法的时间复杂度较高,CPU 消耗时间随着网络规模呈指数增长;本文方法和文献[16]方法时间复杂度较好,随着网络规模的增长,CPU 消耗时间呈多项式增长,但本文方法要优于文献[16]方法,主要原因是本文方法产生了完整的攻击图,而文献[16]方法仅产生部分攻击图。

由实验结果可以看出,本文方法具有良好的时间复杂度,能够适用于大规模网络的攻击图构建,为评估大规模网络的安全提供基础。主要原因是将攻击图的构建过程归结为攻击属性之间的模式匹配,通过对当前环境进行处理,构建环境网络,减少攻击图构建过程需要匹配的对象数量,降低时间消耗。

6　结束语

针对现有攻击图构建方法时间消耗过大的不足,本文分析了网络中安全要素的特点,将构建攻击图过程中寻找攻击之间的关联关系转化为模式匹配问题,并在攻击图构建中引入 Rete 算法,提出基于 Rete 的攻击图构建算法。对于所提出的方法,本文进行了时间复杂度分析和模拟实验验证。得到的结果均表明该方法具有较好的效率。在下一步的工作中,需要在大规模的真实网络中进一步验证本文方法的可扩展性。

参考文献

[1] PHILLIPS C, SWILER L. A Graph-based System for Network Vulnerability Analysis[C]//Proceedings of the 7th Workshop on New Security Paradigms. New York, USA:ACM Press,1998:71-79.

[2] SHEYNER O. Scenario Graphs and Attack Graphs[D]. Pittsburgh,USA:Carnegie Mellon University,2004.

[3] 苘大鹏,张　冰,周　渊,等. 一种深度优先的攻击图生成方法[J]. 吉林大学学报(工学版),2009,39(2):446-452.

[4] GHOSH N,GHOSH S K. A Planner-based Approach to Generate and Analyze Minimal Attack Graph [J]. Applied Intelligence,2012,36(2):369-390.

[5] 宋舜宏,陆余良,夏　阳,等. 基于贪心策略的网络攻击图生成方法[J]. 计算机工程,2011,37(2):126-128.

[6] 朱　明,殷建平,程杰仁,等. 基于贪心策略的多目标攻击图生成方法[J]. 计算机工程与科学,2010,32(6):22-25.

[7] 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.

[8] AMMANN P,WIJESEKERA D,KAUSHIK S. Scalable Graph-based Network Vulnerability Analysis [C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. New York, USA: ACM Press,2002:217-224.

[9] 陈　锋. 基于多目标攻击图的层次化网络安全风险评估方法研究[D]. 长沙:国防科学技术大学,2009.

[10] 赵　豹. 基于攻击图的网络脆弱性分析技术研究[D]. 长沙:国防科学技术大学,2009.

[11] 叶　云,徐锡山,齐治昌,等. 大规模网络中攻击图自动构建算法研究[J]. 计算机研究与发展,2013,50(10):2133-2139.

(下转第 165 页)

[34] NIKIFORAKIS N, INVEMIZZI L, KAPRAVELOS A, et al. You Are What You Include: Large-scale Evaluation of Remote Javascript Inclusions [C]//Proceedings of ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2012: 736-747.

[35] ABDELHAMID N, AYESH A, THABTAH F. Phishing Detection Based Associative Classification Data Mining[J]. Expert Systems with Applications, 2014, 41(13): 5948-5959.

[36] MARCHAL S, FRANCOIS J, STATE R, et al. PhishStorm: Detecting Phishing with Streaming Analytics [J]. IEEE Transactions on Network and Service Management, 2014, 11(4): 458-471.

[37] JR I W. Website Forgery: Understanding Phishing Attacks and Nontechnical Countermeasures for Ordinary Users, IN 47907-2086[R]. West Lafayette, USA: Center for Education and Research of Purdue University, 2015.

[38] DHARMAADI I P A, BAKHRUN A, SAPUTRA D, et al. Typo-squatting Crime in Indonesia Online Banking[C]// Proceedings of International Conference on Information Technology Systems and Innovation. Washington D. C., USA: IEEE Press, 2014: 269-272.

[39] SPAULDING J, KANG A R, UPADHYAYA S, et al. A User Study of the Effectiveness of Typosquatting Techniques [C]// Proceedings of 2016 IEEE Conference on Communications and Network Security. Washington D. C., USA: IEEE Press, 2016: 360-361.

[40] LIN E, GREENBERG S, TROTTER E, et al. Does Domain Highlighting Help People Identify Phishing Sites? [C]// Proceedings of International Conference on Human Factors in Computing Systems. Washington D. C., USA: IEEE Press, 2011: 2075-2084.

[41] FINKE C. URL Fixer-download[EB/OL]. [2017-04-06]. https://github.com/cfinke/URL-Fixer.

[42] CHEN G C G, JOHNSON M F, MARUPALLY P R, et al. Combating Typo-squatting for Safer Browsing [C]// Proceedings of the 2 3 rd International Conference on Advanced Information Networking and Applications. Washington D. C., USA: IEEE Computer Society, 2009: 26-29.

[43] 薛　虹. 网络时代的知识产权法[M]. 北京:法律出版社,2000.

[44] ICANN. The Internet Corporation for Assigned Names and Numbers [EB/OL]. [2017-04-06]. https://www.icann.org/ policy.

[45] Cybertelecom: Anticyberquatting Consumer Protection Act [EB/OL]. [2017-04-04]. http://www.cybertelecom.org/dns/acpa.htm.

[46] 豪威特,王菲萍. 域名争议与商标侵权[J]. 国外社会科学文摘,1999(6):45-48.

[47] Pengelola Name Domain Internet Indonesla. Tentang Pandi[EB/OL]. [2017-04-28]. http://www.pandi.id/.

[48] Wikipedia Indonesia: Undang-undang Informasi dan Transaksi Elektronik[EB/OL]. [2017-04-16]. http://id.wikipedia.org/wiki/Undangundang_Informasi_dan_Transaksi_Elektronik.

[49] 郅　飞. 网络域名抢注法律问题研究[D]. 呼和浩特:内蒙古大学,2012.

[50] 朱旻卿. 略论域名抢注与商标保护[D]. 上海:华东政法大学,2012.

[51] 程永顺. 审理域名注册纠纷案件的若干问题[J]. 知识产权,2001,11(1):53-54.

[52] 刘艺工,周久人. 域名抢注的法律问题探析[J]. 长春理工大学学报(社会科学版),2012,25(10):20-22.

[53] 最高人民法院审判委员会. 最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释[J]. 中华人民共和国最高人民法院公报,2001(10):21-22.

[54] 国务院信息化工作领导小组办公室. 中国互联网络信息中心宣布成立——《中国互联网络域名注册暂行管理办法》发布[J]. 中国教育信息化,1997(8):61-62.

[55] 中国互联网络信息中心. 中国互联网络信息中心域名争议解决办法[EB/OL]. [2017-04-26]. http://www.cnnic.cn/ggfw/fwzxxgzcfg/2012/01207/t20120731_32910.htm.

编辑　吴云芳

(上接第 155 页)

[12] FORGY C L. Rete: A Fast Algorithm for the Many Pattern /Many Object Pattern Match Problem [J]. Artificial Intelligence, 1982, 19(1): 17-37.

[13] 庞伟正,金瑞琪,王成武. 一种规则引擎的实现方法[J]. 哈尔滨工程大学学报,2005,26(3):385-389.

[14] CALIFF M E, MOONEY R J. Relational Learning of Pattern-match Rules for Information Extraction [C]// Proceedings of the 16th National Conference on Artificial Intelligence and the 11th Innovative Applications of Artificial Intelligence Conference. [S.l.]: American Association for Artificial Intelligence, 2002: 328-334.

[15] LEI Feng, WANG Jianqiang. Research on the WSN Intrusion Detection System Based on Improved BM Pattern Match Algorithm [J]. Journal of Convergence Information Technology, 2012, 7(17): 109-115.

[16] OU Xinming, BOYER W, MCQUEEN M. A Scalable Approach to Attack Graph Generation[C]//Proceedings of the 13th ACM Conference on Computer and Communication Security. New York, USA: ACM Press, 2006: 336-345.

编辑　顾逸斐