

网络安全评估与分析模型研究

刘文彦, 霍树民, 仝青, 张淼, 齐超

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 网络安全评估有助于清楚掌握其网络信息系统目前与未来的风险所在, 并给出相应的安全建议和对策。网络安全评估与分析模型是其中重要的研究方向和内容, 当前尚无对此进行全面总结和分析的综述文章。对常用的网络安全评估与分析模型进行综述, 首先介绍了以攻击为中心的模型, 如攻击树、攻击图、攻击链等; 然后阐述以防御或攻防交互为中心的模型, 如攻击面、网络传染病、Petri网、自动机等, 对这些模型, 分别介绍了其基本概念、适用领域、建模分析过程以及优势和不足, 同时给出数个典型案例说明模型在网络防御技术评估分析中的应用。

关键词: 网络安全; 模型; 有效性; 评估与分析

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018019

Research on models of network security evaluation and analysis

LIU Wenyan, HUO Shumin, TONG Qing, ZHANG Miao, QI Chao

National Digital Switching Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract: Network security assessment helps to grasp the current and future risks of the network information system clearly, and gives corresponding security suggestions and countermeasures. Model of network security assessment and analysis is an important research direction and content, for which there is no review to give a comprehensive summary or analysis. A review of common network security evaluation and analysis model was given. The model that focus on attack was introduced, such as the attack tree, attack graph and kill chain, then the model that focus on network defense or offensive and defensive interaction was explained, such as attack surface, cyber epidemic model, Petri nets and automation machine, giving introduction to the basic concept, application field, modeling analysis process, advantages and disadvantages of the models. Then, typical examples were given to illustrate the application of the models in network defense technology evaluation and analysis.

Key words: network security, model, effectiveness, assessment and analysis

1 引言

网络安全评估对建立安全的网络信息系统是

一种非常有价值的方法, 也是网络安全主动防御中的一项重要基础支撑技术, 可以有效地发现系统中的安全缺陷, 对网络安全技术的研究具有重

收稿日期: 2017-12-07; 修回日期: 2018-01-09

通信作者: 刘文彦, lwyndsc@163.com

基金项目: 国家自然科学基金资助项目 (No.61602509); 国家自然科学基金创新群体基金资助项目 (No.61521003); 国家重点研发计划基金资助项目 (No.2016YFB0800100, No.2016YFB0800101)

Foundation Items: The National Natural Science Foundation of China (No.61602509), The Innovative Research Group of the National Natural Science Foundation of China (No.61521003), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101)

要的意义,是目前的研究热点和难题之一,而网络安全评估模型并基于该模型进行安全分析是其中重要的研究内容。虽然网络安全技术已经有几十年的发展历程,但无论是学术界还是产业界尚没有统一的方法对各类安全技术进行安全评估和分析。目前,网络安全评估主要有 4 类方法^[1]:基于安全评估标准、资产价值、弱点检测和网络安全模型的评估方法。其中,在学术研究领域用得比较多的是基于网络安全模型的评估方法。基于模型的方法可以更加深入地理解网络中防御的行为特征、攻防过程,为网络系统安全体系的构建提供科学依据,进而提升网络系统应对复杂网络环境下各种突发网络攻击事件的生存能力。即基于模型的评估分析方法中的安全模型可以表达系统行为和状态,可根据模型产生测试例,从而达到对系统整体的安全进行评估的目的。本文从学术研究的角度重点介绍基于模型的评估与分析方法及其使用。

本文通过分析大量的学术论文和著作,调研已有研究,给出了一些常用的评估分析模型。目前,对网络安全进行分析的主要模型有攻击树(attack tree)、攻击图(attack graph)、攻击链(kill chain)、攻击面(attack surface)、网络传染病模型(cyber epidemic model)、Petri 网(Petri net)、自动机(automation machine)等,这些方法有助于分析网络攻防过程及在攻防过程中的系统变化和系统安全性能,对网络防御具有较好的指导作用。例如,给定一个网络防御系统,从某一角度或利用某一手段对其进行定性或定量的计算得到系统的安全性,即抵抗网络攻击的能力以及攻击者可能的攻击途径,同时基于模型分析的结果指导防御系统的设计和改进。这些模型常见于各类论文中,也有不少研究者以此为方向开展课题研究,同时也有一些文章对部分模型进行简单的分析。如高翔^[2]在其博士论文中简单介绍了攻击树模型、攻击图模型、有限状态机模型、Petri 网模型和博弈论模型,《信息网络安全测试与评估》^[3]一书对网络攻击建模中的攻击树、攻击图和攻击网进行了分析和总结,类似的研究还有文献^[1,4,5]。但目前已有文献对上述模型的分析存上一定的局限性。因此本文以此为切入点,在

已有文献的基础上介绍网络安全评估与分析常用模型,及其简单应用。

2 网络安全目标(属性)和指标

在介绍具体的模型之前,首先介绍网络安全评估的属性指标。基于模型的网络安全评估首先要明确分析目的。网络安全目标(属性)及指标在网络信息系统设计中具有重要的指导意义。其中,网络安全目标(属性)是网络安全评估标准的出发点,而网络安全评价指标是网络安全(风险)评价的工具,是反映评价对象安全目标(属性)的指示标志,评价指标的选取和建立是进行综合评价的前提和基础^[3,6]。

网络安全基本目标就是保证网络系统的 3 个基本安全属性得以实现,即机密性(confidentiality)、完整性(integrity)和可用性(availability),简称为 CIA 三合一基本原则。CIA 是所有组织在制定信息安全标准时的出发点。通俗地讲,安全目标就是实现网络信息的可信、可控、可用,这些也是网络安全的基本特征。根据有关网络安全的文献和著作,除上述 3 个属性外,网络安全目标还有其他一些属性,如可靠性、可控性、不可抵赖性、可审查性等^[2]。

但是,简单直接地以网络安全目标(属性)来评估网络安全十分困难。网络安全评估指标是对网络安全目标的内涵进行分析和量化的结果,更具可操作性,在不同的角度有不同的指标^[7]。常用的一些网络安全评估指标有攻击成功率(如概率)、攻击(防御)代价(如成本、损失等)、防御有效性、网络熵、安全增益、攻击检测率等,上述指标中用的比较多的是攻击成功率、防御有效性、攻防代价。除此之外,研究者往往会依据不同的场景下自身需求提出更为合理的评价指标,如王国良等^[3]提出了直接依据专家评估的三性量化指标体系。但是,目前尚无统一的网络安全评估指标。

3 常用网络安全评估模型及分析

常用的网络安全评估与分析模型分类方法是从定量或定性或二者结合的角度来展开,这种方法从结果的性质上进行直观的分析 and 分类,方法

简单直接,但却缺乏对模型内在的分析和反映。本文从一个新的角度,即根据侧重于攻防的程度及建模对象的不同,将网络安全评估常用模型进行如下划分:攻击树、攻击图、攻击链模型等侧重于以攻击者或者攻击为中心进行建模分析,如攻击图、攻击树往往基于假设已知系统中存在的漏洞,且常以攻击者为中心进行度量,以攻击者为中心的方法需要对攻击者能力和资源做出假设,而这些信息防御者及系统是不知道的,在实际应用中有局限;攻击面、网络传染病、Petri 网、自动机侧重于从防御或攻防交互的角度评估分析,攻击和防御手段则是其中状态变化的影响因素,此类方法需要同时对攻击和防御及系统本身进行一定的抽象。上述分类方法在应用中不是绝对的,如 Petri 网等同样可以直接用于分析网络攻击过程。同时, Petri 网和自动机 2 个模型本身并不是为网络攻防而设计的,它们的应用领域非常广泛,也有研究者用这 2 个模型分析进行网络安全评估^[7~12],这些研究多是基于经典的模型改进以对特定攻防情形进行分析。

3.1 以攻击为中心的模型

3.1.1 攻击树

攻击树模型是一种图形化的描述方式,采用树结构的形式描述系统攻击过程,能够很直观地表明和辅助分析系统存在的风险,并可定量评估系统风险。其中,树的根节点表示攻击者希望达到的目标节点,而叶节点表示为实现该攻击目的而可能采取的攻击手段^[13]。每一条从根节点到叶节点的路径表示完成攻击目标所要进行的一次具体的完整攻击过程。有时能影响系统运行的攻击不止一种,此时系统的攻击树不止一棵,而是由多棵攻击树组成的攻击森林^[14]。攻击树模型适合于描述多阶段的网络攻击行为,总的攻击目标由一系列的子目标通过“与/或”关系复合而成。

攻击树可以抽象为一个具有根节点的无环有向图。它的构造过程是一个后向推理的过程。首先,确定针对系统的一个入侵目标,并将入侵目标作为攻击树的根节点。然后,回溯分析出促使根节点事件发生的前提条件或事件组合,将它们作为根节点的子节点。在下一层攻击树中通过

“与”或者“或”关系表示出来;再类似地对攻击树中的每一个节点进行拆分。直到攻击树中的叶节点不能再进行拆分操作,或者已经是某具体实现中的原子攻击(最基本的攻击操作)。

基于攻击树的评估方法比较简单,得到攻击树后,可依据较权威的相关评分标准对叶子节点和系统风险值计算^[15],进而可评估系统整体安全性和分析攻击者最易采用的攻击手段和场景。例如,为了计算攻陷目标节点的概率,可给树的节点赋予不同的属性,如攻击成功率、攻击代价等。假定攻击者可从系统的任意一层发起攻击,且攻击目标所在层数越高,攻击难度越大,攻击成功率越低。最终计算得到的根节点出现的概率就是攻击者实现最终目标的概率。攻击树除了能对系统面临的整体风险大小进行度量,还可对攻击场景展开分析,如哪种攻击场景下攻击者最容易达成目标。这能更加全面地揭示和认识攻击者的攻击选择,然后针对性地进行防御部署。

3.1.2 攻击图

攻击图模型由Cunningham等于1985年提出^[16],是描述网络或信息系统中存在的脆弱点以及脆弱点之间的关联关系最有效的模型之一,可很好地描述攻击行为以及系统行为的变化趋势和规律,被广泛应用于网络的安全分析与评估中。攻击图是攻击者实施攻击过程中所经历的多条攻击路径所形成的图结构^[17]。攻击图方法是从攻击者的角度出发,根据网络和系统中的脆弱点情况模拟推测攻击者的攻击行为,按照攻击的步骤将攻击的过程逐步分解,将攻击过程中的系统状态变化或者攻击成功的必要条件组成一张有向图^[1]。其中,每一条攻击路径是攻击者为达到相应的攻击目标所经历的一系列攻击活动序列。攻击者在对网络进行攻击时首先攻击目标主机网络中具有弱点的主机,当攻击成功之后,其在被攻击的主机就具有了一定的权限,在访问能力允许的条件下,攻击者可能从已经攻克的主机上再次发起攻击,如此往复,直到攻击者达到其攻击的最终目的。这样就构成了一条条攻击路径。在攻击图模型中,一个节点代表一个可能的攻击状态或条件,节点内容通常包括主机名、用户权限、攻击的因果等,

每条边代表一个单一行为引起的状态改变, 行为的执行者可能是攻击者、后门程序等。

从攻击有向图中可分析出如何利用其中若干个脆弱点达到某个攻击目标, 即将网络配置信息和脆弱性信息作为输入, 依托脆弱性知识库, 分析在攻击发生时, 目标网络中的漏洞将如何被利用并造成何种后果, 然后模拟攻击者的行为步骤以分析网络中所有可能的攻击路径。这是一种采用正向搜索的建模方法, 可使用模型检测工具生成此类攻击图; 另外一种是采用反向搜索方法, 即首先指定一个攻击目标, 然后从指定的攻击目标出发, 递归寻找相关的攻击动作, 直到找到在初始网络状态下攻击者就可以发动的攻击动作。

利用攻击图分析网络系统的安全性主要分为 3 个阶段: 首先, 依据建模方法针对特定网络系统和攻击类型生成攻击图; 其次, 为图中的各节点赋值; 最后, 通过推导计算得到定性或定量的安全指标, 如攻击成功率和脆弱节点可达性。当然, 防御者同样可以基于攻击图分析攻击目标与网络固有属性之间的依赖关系, 发现网络中存在的潜在威胁攻击路径及其概率大小, 此即为安全评估, 同时找到网络中的薄弱点进行针对性防御, 如动态改变网络或主机的固有属性。

3.1.3 攻击链

攻击链是入侵者随着时间的推移穿透信息系统对目标进行攻击所采取的路径及手段的集合^[18], 是对攻击者入侵行动和预期效果的建模和分析。需要注意的是, 攻击链是一个过程、模型而非技术。攻击链概念最早由洛克希德公司于 2011 年提出^[19]。攻击链模型提供了一个描述网络攻击的模型, 其将复杂的攻击分解为相互非独有的阶段或层。通过调研在国内外相关已公开研究文献和资料发现很多研究均采用由洛克希德公司提出的攻击链模型描述攻击^[19], 同时该攻击链模型也是美国国家标准与技术研究院 (NIST, National Institute of Standards and Technology) 的官方模型, NIST 称之为网络攻击生命周期^[17~19] (二者的阶段划分完全相同, 只是名称不同), 所以本文称之为经典攻击链。经典攻击链是包含 7 个攻击阶段的模型; 通常, 攻击者不可避免地遵循这些阶段来规划和执行入侵^[17~19]。

目标侦察 (reconnaissance): 选择目标, 收集有关目标的信息, 如目标使用的技术、社会关系、潜在的漏洞等。

武器化 (weaponize): 开发恶意代码以尝试利用已识别的漏洞, 将开发的代码与可交付有效载荷 (如 pdf、doc 和 ppt) 相结合。

交付 (delivery): 将武器化的有效载荷传送到目标环境。常见交付手段如电子邮件附件、钓鱼攻击、下载、USB / 传输介质、DNS 缓存攻击等。

漏洞利用 (exploitation): 基于目标系统的漏洞执行恶意代码。

安装 (installation): 远程访问控制通常需要安装控制 (木马) 程序等恶意软件, 使攻击者可以长期潜伏在目标系统中。

命令和控制 (C2, command and control): 攻击者需要一个通信通道来控制其恶意软件并继续其操作。因此, 需要连接到 C2 服务器。

行动 (act on objective): 它是攻击链的最后一个阶段, 攻击者执行所需要的攻击行为, 如通过数据窃取和篡改、控制链接等操作实现其目标。

为了攻破更复杂的防御系统, 攻击者可能需要执行一个或多个链来规避不同的防御策略。通过了解对手的攻击链, 防御者有更多的机会发现和回应攻击。表 1 描述了 DoD 信息操作指南中的检测、拒绝、中断、降级、欺骗和摧毁等行动矩阵^[18], 在不同攻击阶段的不同防御阶段使用了不同的具体防御方法。例如, 该矩阵在漏洞利用阶段使用主机入侵检测系统 (HIDS, host intrusion detection system) 被动地检测攻击, 同时通过打补丁拒绝攻击。该矩阵显示了防御者可以使用的防御能力范围。矩阵包括了传统的防御者法, 如网络入侵检测系统 (NIDS, network intrusion detection system)、防火墙访问控制列表 (ACL, access control list)、系统强化措施 (日志审计、蜜罐等)。同时, 在矩阵中, 本文还加进了新型主动防御技术, 这些技术具有更多的功能, 如移动目标防御 (moving target defense)^[20]、拟态防御^[21], 防御效果更佳。

3.2 以防御或攻防交互为中心的模型

如前文所言, 以防御或攻防交互为中心的模型也可以描述攻击, 但更多是从系统整体的角度

表 1 行动矩阵

阶段	检测	拒绝	中断	降级	欺骗	摧毁
目标侦察	网页分析	防火墙 ACL	MTD 拟态防御	重定向 蜜罐	蜜罐 拟态防御	—
武器化	NIDS	NIPS	—	—	蜜罐 拟态防御	—
交付	警惕的用户	代理过滤	反病毒 MTD 拟态防御	排队	蜜罐 拟态防御	—
利用	HIDS	补丁	数据执行保护 MTD 拟态防御	限制账号权限	蜜罐 拟态防御	—
安装	HIDS	‘chroot’ jail	反病毒 MTD 拟态防御	—	蜜罐 拟态防御	—
命令和控制	NIDS	防火墙 ACL	NIPS MTD 拟态防御	SinkHole	DNS 重定向 SinkHole 蜜罐 拟态防御	—
行动	日志审计 入侵容忍 拟态防御 可信计算	可信计算	MTD 拟态防御	服务质量 入侵容忍 拟态防御	蜜罐 拟态防御	入侵容忍 拟态防御

描述网络攻防以及系统防御效果。

3.2.1 攻击面

为了更直观地刻画系统安全性能，从系统本身资源等考虑，其攻击面大小也可作为一个参考指标^[22]。即一个系统的攻击面越大，一般其脆弱点越多，被攻陷的可能性越高，安全性也会越差。系统攻击面是系统受攻击的风险指标。根据对以往攻击类型的总结，大多数攻击，如缓冲区溢出攻击，都是攻击者通过系统操作环境向系统发送数据或从系统发送到环境中造成的，有两类典型的攻击场景。一类攻击者通过系统通道（如 sockets）连接到系统，而后调用系统方法（如 API）将数据项（如输入字符串）发送到系统或者从系统中接收数据项。方法包括系统入口点和出口点，系统入口点指系统中代码的函数方法，该方法可从系统环境中直接或间接地接收数据。如果系统方法可将数据发送到环境中，则称其为系统的出口点。另一类攻击者可以通过借用共享的对系统和用户均可见的持久性数据项（如文件、cookies、数据库记录和注册表项等），间接地发送（接收）数据到（从）系统中。因此，攻击者可以通过使用系统方法、通道以及保存在系统环境中的数据项等资源与系统进行连接交互，从而达到

破坏系统的目的。所以，可以将系统方法、通道和数据项看成系统资源，并将可用于系统攻击的系统资源的子集定义为攻击面^[23]。需要注意的是，并非所有资源都是攻击面的一部分，只有攻击者利用某种资源攻击系统时，该资源才算攻击面的一部分。

与攻击图等模型侧重于攻击不同，攻击面的概念独立于攻击者的能力，仅取决于系统的设计和固有属性，与系统中出现的任何漏洞无关，攻击面对所有入口点和出口点的检视包括所有已知漏洞以及尚未发现和利用的潜在漏洞。对于具体的系统，可明确其方法、通道和数据，并从这 3 个维度对攻击面展开量化度量，同时考虑各类资源对攻击面的贡献。对于 2 个系统的攻击面比较而言，攻击面越大，该系统安全性越差。

3.2.2 网络传染病模型

传播行为在许多实际网络中都广泛存在，如社会网络中的疾病传播、信息传播，电力网络的相继故障等。一些相关研究者发现疾病传播和谣言传播行为的研究可以借鉴到 Internet 网络中病毒传播行为分析中（如传播特点、传播过程），即计算机网络中的传染病模型，研究如何更有效地

降低病毒的扩散范围。通过研究计算机网络中病毒或攻击的传播行为,从而提出相对应的策略控制或消除网络中的攻击,使网络达到安全的状态。这对于降低病毒或攻击对网络的损害具有重要意义。计算机网络中传染病模型的基础是复杂网络,把网络中的节点看成图中的顶点,节点间的关系用图中的边表示。目前,学术界对于复杂网络中的传染病传播动力学研究较为深入,这些模型可以分析网络上病毒的传播建模。迄今为止,已有多重传染病模型被提出,其中 SI、SIS、SIR 和 SIRS 这 4 种经典模型应用最广^[24],模型中字母 S (susceptible) 表示易感染状态、I (infected) 表示受感染状态、R (removed) 表示免疫状态或被移除状态。不同模型的假设和使用范围不同,这方面资料很多,不再介绍。

使用传染病模型的关键在于传播控制策略方面,其中免疫策略和隔离策略是 2 种基本的控制策略,分别从控制传播节点(消除解决病毒节点)和控制传播路径(阻止病毒扩散)的角度应对病毒传播。不同网络结构有可能会产生截然相反的网络传播,如计算机病毒更新补丁属于免疫策略,主要是通过保护网络中部分节点进而切断病毒传播途径。免疫策略中有一个重点概念,即感染临界值 σ_c 。如果有效感染率大于等于该临界值,则病毒可以传播扩散,并使全网感染节点数量达到动态平稳状态;反之,若小于该值,则感染节点数量将大幅衰减,无法大范围扩散。最基本的免疫策略有 3 种:随机免疫、目标免疫和熟人免疫。隔离策略是受自然界中传染病的启发提出来的,为了消除由于检测系统产生的误警所带来的负面影响,抑制病毒、蠕虫等的快速传播,当一台主机的行为(如流量)可疑时,先把它隔离(如封掉其通信端口、断开网络连接等),网络管理人员检查,经过一定时间后,如果没有问题,再释放回网络中。在实际中,可以根据不同的情况选择不同的免疫策略,同时选择确定不同的参数,如隔离时间、免疫比例等。

结合网络传染病模型的网络防御分析一般过程为:首先分析网络防御系统的特点,选择适合的传染病模型或者对已有模型进行改进;然后结合实际系统进行建模,确定各参数(建

立网络与实际网络系统的对应关系,如复杂网络图中的顶点对应于网络中的节点,图的边对应于节点之间的连接关系或属性),求解传播阈值条件以及不同状态间的最终平衡状态,同时可采取防御策略使最终达到安全状态,即无感染节点。

3.2.3 Petri 网

Petri 网是一种用于描述和分析具有并发、同步和冲突等特性系统的建模机制,由于其具有直观的图形表现能力和严密的数学基础,利用 Petri 网的各种拓展形式,不仅有助于定性理解系统的动态行为,还可以定量地计算各种性能指标,为检验系统可靠性和安全性等提供依据,在多个领域得到广泛应用^[2]。有研究者将 Petri 网及其改进形式应用于网络安全评估与分析中,如分析网络攻击、入侵检测、入侵容忍和 MTD 等^[7],实现了对网络防御系统的建模和分析^[2,7-10]。如 Mcdermott 在渗透测试过程中使用 Petri 网对网络攻击过程建模,并将其提出的模型命名为攻击网^[25]。

经典 Petri 网在实际应用中存在许多局限性,例如,没有明确考虑时间因素并定量化分析,以及描述复杂系统时模型繁琐等问题,因此后续研究者对经典 Petri 网模型进行了拓展,如随机 Petri 网、广义随机 Petri 网、有色 Petri 网、模糊 Petri 网等^[2,26],其中应用比较多的是随机 Petri 网(SPN, stochastic Petri net)和有色 Petri 网(CPN, colored Petri net)。随机 Petri 网^[27]是在经典 Petri 网中引入时间概念,而有色 Petri 网^[28]则是引入了“颜色”(颜色可以被看作是数据类型)表示方法。这些扩展有的通过与矩阵方法结合在一起建立系统状态方程、代数方程,有的与随机过程论、信息论中的方法结合在一起描述和分析系统运行的不确定性或随机性,如对 SPN 的性能分析建立在其状态空间与马尔可夫链同构的基础之上。SPN 为系统的性能模型提供了良好的描述手段,随机马尔可夫过程为模型的评价提供了坚实的数学基础。下面主要对基于随机 Petri 网的网络防御系统性能评估过程进行简单介绍^[2]。

1) 分析网络防御系统,对应到 SPN 的各个元素,给出系统的 SPN 模型。

2) 构造与 SPN 模型同构等价的马尔可夫链。

3) 基于马尔可夫链的稳态状态概率进行网络防御系统性能评估, 当稳态概率难以求解时, 可使用随机 Petri 网仿真软件, 获得系统可能的行为和状态变化以及系统的可用性、安全性和可靠性等。

3.2.4 自动机

自动机阐述了计算的数学模型的定义与性质, 广泛应用于形式语言、计算机编译和操作系统等各个方面^[29]。自动机是有限状态机 (FSM, finite-state machine) 的数学模型, 亦称有限自动机, 它具有有限数目的内部状态, 在不同输入序列的作用下, 系统内部的状态不断地转换^[30]。鉴于其对状态和转移过程和条件的刻画能力, 不少研究者将其应用于描述网络攻防系统^[12,30,31]。网络空间中的攻击和防御是一个动态变化的对抗过程, 双方通过实施各种行为或控制手段推动安全平衡状态的不断变化, 攻击者试图破坏安全平衡, 防御者则努力保持安全平衡, 可使用自动机对网络攻防进行状态变化描述, 并构造网络防御系统的自动机模型, 以模拟网络系统的运行状态及其动态迁移的条件和过程, 尤其是由各种安全事件导致的安全状态转移。对网络攻防系统而言, 状态表示攻防双方的安全形势, 用状态迁移表征攻防双方各种行为带来的安全形势变化, 通过对安全状态的调节和控制实现安全形势稳定。

有限自动机是实际系统的抽象模型, 因而可以用来对网络防御系统或攻防过程进行建模, 只要将系统的各个状态、转移条件等对应到有限自动机的各个元素即可, 要明确系统的状态 (含初试状态及终止状态) 以及导致系统发生状态转移的方向和原因, 将系统建模为一个 FSM, 依据模型用状态转换图表达^[32], 并对其进行安全分析, 如基于自动机对网络攻击模型的基本过程进行描述^[12], 对攻击者入侵 Web 服务器时系统的状态转换过程进行描述^[33]等。

除了上述典型常用的风险评估模型外, 还有研究者采用故障树模型、层次化分析法 (AHP)、特权图模型、渗透图模型和贝叶斯网络模型等方法展开分析。这些模型相对于前述的几个模型, 使用较少, 不再分析。

4 应用举例

4.1 基于攻击面模型的 MTD 评估分析

文献[21]结合基于配置参数的攻击面转移模型说明如何基于攻击面对 MTD 进行性能分析。该模型从系统描述入手, 使用配置参数刻画 MTD 系统, 进而 MTD 系统状态可用与系统运行息息相关的混合配置参数集合表示。以主机为例, 其配置参数可用主机的内存大小、硬盘大小、CPU 类型、运行系统版本和 IP 地址等描述。此时, 每次系统运行所采用的配置参数即为其攻击面大小, 而攻击面转移则通过系统在不同配置参数间切换实现。当得到 MTD 系统的配置参数空间后, 如何评价不同 MTD 系统间的有效性差异。例如, A 系统的配置空间为 {IP:10.10.0.1, OS: Window XP; IP:10.10.0.2, OS: Window7; IP:10.10.0.3, OS: Window8}, 而 B 系统的配置空间为 {IP:10.10.0.1, OS: Window XP; IP:10.10.0.2, OS: Linux; IP:10.10.0.3, OS: Mac}。为比较 A 和 B 这 2 个 MTD 系统的安全性, 文献[21]引入了系统配置熵 H 的概念刻画攻击面大小, 而配置熵取得最大值的条件是子配置需要相互独立, 即在不影响系统正常工作的情况下, 当系统调整前后所呈现的攻击面完全独立时, MTD 带给系统的安全防护性能最佳, 即使不能保证系统调整前后所呈现的攻击面完全独立, 也要尽量多样化扩大差异。基于上述分析, 系统 B 将比系统 A 具有更大的系统配置熵, 因为系统 B 中的 3 个 OS 较为独立, 而系统 A 中 OS 之间的相关性较强。

4.2 基于网络传染病模型的 MTD 评估分析

文献[34]利用复杂网络的网络病毒动力学理论的 SIS 模型, 给出了 MTD 的有效性评估和最佳配置调度优化方法, 验证 MTD 对攻击持续和传播的阻止或延缓作用, 其背景是网络攻击常从受到损害的计算机发起, 然后攻击易受攻击的计算机。这意味着存在一个 (攻击者, 受害者) 关系, 其中攻击者 (如受感染的计算机) 可以直接攻击受害者 (如易受伤害的) 计算机。在任何计算机可以攻击任何其他计算机的极端情况下, 这种关系可以对应到一个完整的图形结构。所得到

的图形结构称为攻击防御结构, 其中被修复的受损计算机/节点也可能会再次受到攻击, 防御的最终目的是希望所有节点都不受攻击或对攻击免疫。这种模式可以自然地将攻击和防御能力抽象为与攻击防御结构的节点和边缘相关联的参数。网络传染病模型的核心概念是传播阈值, 即疫情动态收敛于无病毒状态的充分条件。这样就可以把该情景与 SIS 模型对应起来, 进而用 SIS 分析 MTD 效能。

4.3 基于攻击链模型的 Wannacry 攻击分析

基于攻击链模型可对“WannaCry”勒索攻击过程进行分析。

1) 目标侦察: 攻击节点或者被感染节点对公网随机 IP 地址主机 445 端口进行扫描; 而对于局域网, 则直接扫描当前计算机所在的网段上的所有主机, 查看其 445 端口是否开放服务等信息。

2) 武器制作 (离线已完成): 该勒索软件来自“永恒之蓝”(EternalBlue) 漏洞利用工具, 主要利用微软 Windows 操作系统的 MS17-010 漏洞进行自动传播。“永恒之蓝”利用 Windows 系统在 445 端口的 MS17-010 安全漏洞潜入计算机对多种文件类型加密并添加.onion 后缀, 使用户无法打开。

3) 交付、漏洞利用及安装: 攻击者连接 445 端口, 成功后通过网络对未打补丁的主机进行漏洞攻击, 目标被成功攻陷后会从攻击机下载 WannaCry 木马、安装并进行感染。木马程序包含 2 个部分, 分别是母体 mssecsvc.exe 和敲诈者程序 tasksche.exe。

4) 命令和控制: 勒索软件进行攻击后, 会自动释放 TOR 网络组件, 用于敲诈者程序与攻击者的网络通信; 同时赎金使用比特币支付, 使勒索过程难以追踪溯源。TOR 组件为匿名代理, 该组件启动后会监听本地 9050 端口, 木马通过本地代理通信实现与服务器连接。受害者在单击“Check Payment”按钮后, 由服务端判断是否下发解密所需私钥。若私钥下发, 则会在本地生成解密所需要的 dky 文件。

5) 行动: 对被感染的主机, 木马程序母体 mssecsvc.exe 运行后会扫描随机 IP 的互联网机

器, 尝试感染, 也会扫描局域网相同网段的机器进行感染传播, 此外会释放敲诈者程序 tasksche.exe, 对磁盘文件进行遍历搜索, 对多种文件类型加密并添加.onion 后缀。敲诈程序使用 AES128 加密文件, 使用 RSA2048 公钥加密 AES 密钥。加密后系统会不断弹出勒索声明以及交付赎金的窗口。

基于上述分析, 可以对攻击进行针对性防御, 以斩断攻击链。从攻击链角度, 可在侦察阶段切断内外网连接、关闭 445 端口等, 同时通过抓包分析及时定位扫描发起点, 对扫描设备进行病毒木马查杀, 一旦发现被感染主机, 立即断网防止扩散; 在交付、漏洞利用及安装阶段, 可通过及时打补丁阻止漏洞利用, 同时也可将所有 445 端口的流量暂时引导到一个清洗中心, 隔离感染; 在命令控制阶段, 可通过将其域名进行接管, 打破 C2 连接, 但这仅是一个临时措施, 因为该攻击软件的变体可以更改域名突破封锁。

5 结束语

对网络信息系统及防御技术进行评估和分析是网络安全领域的重要研究内容之一。通过评估可以获悉系统的安全性能及防御手段的防御效果, 评估结果还可用于指导设计防御策略。基于模型的网络安全评估与分析已经成为评估和分析网络防御者法及系统必不可少的有效手段, 在以阻止网络攻击为目的或者以网络安全性评估为目的的网络防御领域都有广泛的应用。表 2 对每个模型的适用领域和不足之处进行简单总结。

当前网络安全评估与分析仍在不断发展之中, 理论和实践研究都非常活跃, 新的模型不断涌现, 在未来一段时间内其仍将是网络安全领域的重点发展方向之一。

1) 统一的评估分析指标和通用的评估分析模型。关于网络安全性评估分析研究的大部分工作针对网络局部或特定系统, 还没有形成一套通用的理论方法, 即目前尚无较为通用的网络信息系统攻防评估分析模型; 同时, 尽管目前很多模型或方法都给出了相关评估与分

表 2

网络安全评估与分析常用模型总结

模型特性	定性或定量	适用领域	特色及优势	不足
攻击树	定量	适于描述系统攻击过程,可用于推断系统面临的安全威胁	直观地表明和辅助分析系统存在的风险,易于理解	对大型、复杂、动态的网络防御系统难以灵活有效描述,状态空间爆炸
攻击图	定量	适于描述网络或信息系统中存在的脆弱点以及脆弱点之间的关联关系	直观展示攻击者利用目标网络脆弱性实施网络攻击的各种可能攻击路径,可自动发现未知的系统脆弱性及其之间的关系,进而全方位地对系统各类风险展开评估	状态空间爆炸,不适用于对并发性和协作性的攻击过程进行建模和分析
攻击链	定性	适于对攻击过程进行建模	从链的角度较为细致刻画了一般攻击过程,有助于防御者针对性制定防御手段	仅描述了攻击,缺乏量化手段
攻击表面	定性	适于对不同版本不同配置的软件系统安全性进行比较	评价方式与系统所采用的具体实现方式无关,仅取决于系统的设计和固有属性	仅定性分析,具有相对性,类型不同系统难以严格度量和对比,未考虑攻击者能力等
网络传染病模型	定量	适于描述计算机病毒网络传播分析和控制	可实现对网络系统的整体分析和评估	抽象度较高,对节点的特殊性考虑不足
Petri 网	定量	适于描述符合 Petri 网特性(如并发、同步和冲突等)的网络攻防系统	直观的图形表现,数学基础严密,有专门的可视化仿真建模分析工具	状态空间爆炸,对不符合 Petri 网特性的系统难以描述
自动机	定性	适于描述有状态转移的网络攻防系统	可以较好地模拟网络系统的运行状态及其动态转移的条件和过程,尤其是由各种安全事件导致的安全状态转移	对攻防细节如状态转移条件、属性和状态的概括等刻画不足,对复杂系统难以描述

析数值。但是,由于缺乏统一的安全性度量指标,因而难以对各种结果进行分析与比较,即不同方法分析的结果之间无法进行横向的比较。因此需要建立通用的评估分析模型,并制定统一的度量指标。

2) 理论分析与实验分析相结合。理论模型要结合实验进行验证分析,对系统进行广泛的攻防测试以改进理论。很多理论模型仅基于仿真进行测试,缺少具体的攻防场景测试。当前的大多数非实验类评估模型均过于抽象,对实际的指导意义有限;而纯粹实验的评估分析方法针对的目标系统又过于具体,难以直接扩展应用到其他系统中。因此,需要二者相结合、相适应,用模型指导实验分析,同时结合实验分析的数据改进建模过程及分析结果。

3) 评估与分析中考虑人的因素的影响。在网络安全评估与分析中要考虑人的因素。网络攻击是一种人为行为,不管其形式如何多样、随机,其形成的根本原因与人的利益驱动有很大关系。单靠防御技术无法彻底解决网络安全问题,解决此类问题可能会和法规政策、法律、管理等多方面相关。所以,在评估与分析模型中也应考虑攻

防的人为影响,特别是攻击者的作用,以更好地采取防御措施,提高防御性能。

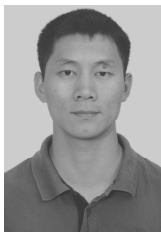
参考文献:

- [1] 井维亮. 基于攻击图的网络安全评估技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2008.
JING W L. Research on network security assessment based on attack graph[D]. Harbin: Harbin Engineering University, 2008.
- [2] 高翔. 网络安全评估理论及其关键技术研究[D]. 郑州: 信息工程大学, 2014.
GAO X. Research on the theory of network security and its key technology[D]. Zhengzhou: Information Engineering University, 2014.
- [3] 王国良, 鲁智勇. 信息网络安全测试与评估[M]. 北京: 国防工业出版社, 2015.
WANG G L, LU Z Y. Testing and evaluation of information network security[M]. Beijing: National Defense Industry Press, 2015.
- [4] 代廷合, 吴开贵. 攻击树在多层网络攻击模型中的应用[J]. 网络安全技术与应用, 2009(1):75-76.
DAI T H, WU K G. Application of attack tree in multi level network attack model [J]. Network security technology and Application, 2009(1):75-76..
- [5] 尚大鹏, 周渊, 杨武, 等. 用于评估网络整体安全性的攻击图生成方法[J]. 通信学报, 2009, (3):1-5.
QIONG D P, ZHOU Y, YANG W. Method to generate attack graphs

- for assessing the overall security of networks[J]. *Journal on Communications*, 2009,(3):1-5..
- [6] 鲁智勇, 冯超, 余辉, 等. 网络安全定量评估模型研究[J]. *计算机工程与科学*, 2009, 31(10):18-22.
- LU Z Y, FENG C, YU H, et al. A study of the quantitative evaluation model for network security[J]. *Computer Engineering & Science*, 2009,31(10):18-22.
- [7] SANDOVAL J E, HASSELL S P. Measurement, identification and calculation of cyber defense metrics[C]//IEEE Military Communications Conference. 2010:2174-2179.
- [8] CAI G, WANG B, LUO Y, et al. A model for evaluating and comparing moving target defense techniques based on generalized stochastic Petri net[M]. Springer Singapore, 2016: 184-197.
- [9] JASIUL B, SZPYRKA M, LIWA J. Detection and modeling of cyber attacks with Petri nets[J]. *Entropy*, 2014,16(12):6602-6623.
- [10] JASIUL B, SZPYRKA M, ŚLIWA J. Malware behavior modeling with colored Petri nets[C]//The International Conference Computer Information Systems and Industrial Management. 2014, 8838: 667-679.
- [11] 杨艳峰, 李洁. 基于有限状态自动机的安全评估模型分析[J]. *企业家天地*, 2013(6):125-126.
- YANG Y F, LI J. Analysis of safety assessment model based on finite state automata[J]. *Entrepreneurs World*, 2013(6):125-126.
- [12] 张峰, 秦志光. 基于有限自动机的网络攻击系统研究[J]. *计算机科学*, 2002,29(21):160-162.
- ZHANG F, QIN Z G. Research on network attack system based on finite-state automata[J]. *Computer Science*, 2002,29(21):160-162.
- [13] 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 J J, HUANG L S, WU S F. Network attack modeling method based on attack tree[J]. *Computer Engineering and Applications*, 2003, 39(27): 160-163.
- [14] 陈建明, 龚尧尧. 基于 SSE-CMM 的信息系统安全工程模型[J]. *计算机工程*, 2003,29(16):35-36.
- CHEN J M, GONG Y W. Security engineering model of information system based on SSE-CMM[J]. *Computer Engineering*, 2003, 29(16): 35-36.
- [15] DANIEL GEER J, HOO K S, JAQUITH A. Information security: why the future belongs to the quants[J]. *IEEE Security & Privacy Magazine*, 2003,1(4):24-32.
- [16] CUNNINGHAM W H. Optimal attack and reinforcement of a network[J]. *Journal of the ACM*, 1985,32(3):549-561.
- [17] BRYANT B, SAIEDIAN H. A novel kill-chain framework for remote security log analysis with SIEM software[J]. *Computers & Security*, 2017.
- [18] YADAV T, RAO A M. Technical aspects of cyber kill chain[C]//The International Symposium on Security in Computing and Communication. 2015: 438-452.
- [19] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. *Leading Issues in Information Warfare & Security Research*, 2011, 1(1): 80.
- [20] 蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展[J]. *计算机研究与发展*, 2016, 53(5):968-987.
- CAI G L, WANG B S, WANG T Z, et al. Research and development of moving target defense technology[J]. *Journal of Computer Research and Development*, 2016, 53(5): 968-987.
- [21] 郭江兴. 网络空间拟态防御研究[J]. *信息安全学报*, 2016,1(4):1-10.
- WU J X. Research on cyber mimic defense[J]. *Journal of Cyber Security*, 2016,1(4):1-10.
- [22] MANADHATA P K, WING J M. An attack surface metric[J]. *IEEE Transactions on Software Engineering*, 2011, 37(3): 371-386.
- [23] MANADHATA P, WING J, FLYNN M, et al. Measuring the attack surfaces of two FTP daemons[C]// ACM Workshop on Quality of Protection. ACM, 2006:3-10..
- [24] Vargasdeleón C. On the global stability of SIS, SIR and SIRS epidemic models with standard incidence[J]. *Chaos Solitons & Fractals*, 2011, 44(12):1106-1110.
- [25] MCDERMOTT J P. Attack net penetration testing[C]//The Workshop on New Security Paradigms. 2001: 15-21.
- [26] PAN P, ZHU X, MAO X. Research on security test for application software based on SPN[J]. *Procedia Engineering*, 2017, 174: 1140-1147.
- [27] MARSAN M A. Stochastic Petri nets: an elementary introduction[C]//European Workshop on Applications and Theory in Petri Nets. 1988: 1-29.
- [28] JENSEN K, KRISTENSEN L M, WELLS L. Coloured petri nets and CPN tools for modelling and validation of concurrent systems[J]. *International Journal on Software Tools for Technology Transfer*, 2007, 9(3-4):213-254.
- [29] MAJI P, GANGULY N, SAHA S, et al. Cellular automata machine for pattern recognition[J]. *Lecture Notes in Computer Science*, 2002, 2493:270-281
- [30] 秦志光, 刘锦德. 安全系统的有限自动机[J]. *电子科技大学学报*, 1996(1):72-75.
- QIN Z G, LIU J D. Finite automata of security system[J]. *Journal of University of Electronic Science and Technology of China*, 1996(1): 72-75.
- [31] 郭威, 郭江兴, 张帆, 等. 基于自动机理论的网络攻防模型与安全性能分析[J]. *信息安全学报*, 2016,1(4):29-39.
- GUO W, WU J X, ZHANG F, et al. A cyberspace attack and defense model with security performance analysis based on automata theory[J]. *Journal of Cyber Security*, 2016,1(4):29-39.

- [32] 张峰, 秦志光. 基于有限自动机的网络攻击系统研究[J]. 计算机科学, 2002,29(z1):160-162.
ZHANG F, QIN Z G. Research on network attack system based on finite automata[J]. Computer Science, 2002,29(z1):160-162.
- [33] 彭文灵, 王丽娜, 张焕国. 基于有限自动机的网络入侵容忍系统研究[J]. 小型微型计算机系统, 2005,26(8):1296-1300.
PENG W L, WANG L N, ZHANG H G. Research on network intrusion tolerance system based on finite automata[J]. Journal of Chinese Computer Systems, 2005,26(8):1296-1300.
- [34] HAN Y, LU W, XU S. Characterizing the power of moving target defense via cyber epidemic dynamics[C]//The 2014 Symposium and Bootcamp on the Science of Security. 2014: 10.

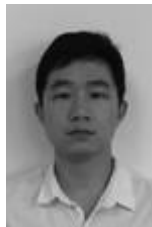
[作者简介]



刘文彦(1986-), 男, 河南周口人, 博士, 国家数字交换系统工程技术研究中心助理研究员, 主要研究方向为网络空间安全、云安全。

霍树民(1985-), 男, 山西长治人, 博士, 国家数字交换系统工程技术研究中心助理研究员, 主要研究方向为网络空间安全、SDN 安全。

仝青(1992-), 女, 河南郑州人, 国家数字交换系统工程技术研究中心博士生, 主要研究方向为网络空间安全防护技术、主动防御技术。



张淼(1994-), 男, 湖北孝感人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为网络安全防御。

齐超(1991-), 男, 江西南昌人, 国家数字交换系统工程技术研究中心博士生, 主要研究方向为网络空间拟态防御技术。