基于攻击图概率的安全度量

Lingyu Wang1, Tania Islam1, Tao Long1, Anoop Singhal2, and Sushil Jajodia3

1 Concordia Institute for Information Systems Engineering Concordia University Montreal, QC H3G 1M8, Canada {wang,t is,ta lon}@ciise.concordia.ca 2 Computer Security Division National Institute of Standards and Technology Gaithersburg, MD 20899, USA anoop.singhal@nist.gov 3 Center for Secure Information Systems George Mason University Fairfax, VA 22030-4444, USA jajodia@gmu.edu

摘要：如今，为了保护网络资源的严谨性，量化潜在的多阶段、多种脆弱性的攻击显得十分重要。一种基于脆弱性之间的因果关系的模型使其变的可行，即攻击图。本篇文章提出了一种基于攻击图概率的网络安全度量模型，并研究了它的效率计算。首先给出了该模型的定义，然后提供了一些关于该模型的简单且有指导作用的解释。接下里，通过带有环的攻击图深入理解该模型的定义，延展其定义。在很多案例中，直接通过定义来计算该度量并不高效，为未来如何提高其高效性提供了启发和方向。

1 介绍

对于日渐复杂的网络环境，传统二进制思想逐渐不再适用于网络安全（无论是攻击或是防守）。实际上，网络中的漏洞被发现后还是会存在，因为各种因素的存在，比如环境因素、开销和代价、网络任务等。为了通过最高效的方式去除漏洞的残余，我们需要评估并测量攻击者利用结合多种漏洞来危害网络环境的可能性。

最近，关于安全度量的研究受到了很大的关注。但是现有的网络安全度量标准一般集中于对个体漏洞进行测量。例如，通用漏洞评分系统（CVSS）从每一个独立的漏洞入手估量了其潜在影响和在环境下的评估。由于影响力、破坏力以及相关性需要在该漏洞危及关键资源的时候才能被测量，而这种攻击行为需要多个漏洞的结合，所以该评价体系存在着一个很大的局限。

另一方面，业界已经对漏洞之间的原理性关系做了很多的工作，这种关系通常以攻击图的形式编制。攻击图帮助人们理解关键资源是否能通过多次复杂的攻击所获取。但是，攻击图作为一个定性模型，其依然把安全问题看作一个非此即彼的问题，即将网络看作是完全安全的（关键资源不可被攻击所得到）或完全不安全的。这个限制是因为通常情况下在各种安全配置中获得一个最好的选择是从业者最希望的。

可以清楚的认识到，目前的安全评估和安全定性模型之间存在着分歧，因为目前的安全评估主要针对单个漏洞而安全定性模型将安全问题定义为非此即彼。为了填补两者之间的界限，我们提出了一种概率度量方法来估量网络安全性。此度量方法从目前的安全评估方法和安全定性模型入手。更具体的说，该工作结合目前度量方法中对单个漏洞的评估度量出一个网络整体的评分。这个结合的过程基于以攻击图方式编制的漏洞之间原理性关系。其中最关键的挑战在于处理带环复杂攻击图。首先本文不考虑环的问题先定义了基础度量且提供了这个度量的直观解释。在这个解释的基础上本文扩展了带环攻击图的定义。最后，本文调研了该度量的时间效率，其中揭示了如果直接通过定义出发计算度量值通常比较低效从而提供了优化计算的一些启发。

本文剩下内容的安排如下。第二章给出了一个动机性的示例。第三张定义了本文提出的度量方法以及探究如何解决攻击图中的环状问题。第四章提供了对度量效率的启发。第五章为相关工作，第六章是本文的总结。

2 攻击图以及动机性示例