基于 Rough 集理论的主机安全评估模型研究

汪贵生[1,2],夏 阳[3]
(1.安徽大学 计算机科学与技术学院,安徽 合肥 230039;
2.铜陵学院 计算机系,安徽 铜陵 244000;
3.解放军电子工程学院 网络工程系,安徽 合肥 230037)

摘 要:针对网络安全技术的发展现状,目前大部分网络安全评估方法从本质上来看,都是从安全漏洞的角度进行网络安全评估,然后给出相应的评估结果和解决方案。但主要不足是没有针对网络安全的实际情况对模型的粒度进行深入分析,其模型对网络安全的分析过于理想化。提出了基于粗糙集理论的主机安全评估模型的方法,该方法模型能够利用历史评估记录,把漏洞作为安全要素,在基于粗糙集理论的属性约简能力基础上,建立安全评估模型。

关键词:网络安全;安全评估;粗糙集理论;漏洞
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)12-0156-03

Host Computer Security Evaluation Model Research Based on Rough Set Theory

WANG Gui-sheng[1,2],XIA Yang[3]
(1.College of Computer Science and Technology,Anhui University,Hefei 230039,China;
2.Department of Computer Science,Tongling College,Tongling 244000,China;
3.Department of Network Engineering, Institute Electronic Engineering of PLA,Hefei 230037,China)

Abstract:Aiming at safe technical development present condition of network, the greatly parts of network safety valuation method comes up to see from the essence currently, carrying on the network safety valuation from of the safe vulnerability, then giving an analyzing result and the solution. But the main shortage is the grain degree that didn't aim at the actual circumstance of the network safety to the model to carry on thorough analysis, its idealizes of model too. Host computer security evaluation model research based on rough set theory was put forward. This model considered the vulnerability as a security factor and the security evaluation model was built from historical evaluation records by using attribute reduction.

Key words:network security; security evaluation; rough set theory; vulnerabilities

0 引 言

目前大部分网络安全评估方法从本质上来看,都是从安全漏洞的角度进行网络安全评估,通过扫描网络中是否存在某些已知漏洞,然后给出相应的评估结果和解决方案。这类方法的缺点是耗时长、占用大量带宽,干扰网络的正常运行。为了寻找更好的网络安全评估方法,不少研究者做了许多有益的工作。文献[1,2]从图论的角度对网络安全进行了量化分析,但主要不足是没有针对网络安全的实际情况对模型的粒度进行深入分析,其模型对网络安全的分析过于理想化,在实际网络特别是大型网络中难以使用。为了保证网络安全运行,在过去人们一直倾向采取被动式防护策略,如防火墙、入侵侦测等[3],但从近年来网络蠕虫、木马等利用软件漏洞造成病毒式攻击造成大量损失的情况来看,单靠被动式防护只能忍受亡羊补牢的损失,已显得安全防御力度不足,必须进而采取主动防范的策略,找出自己的网络主机安全漏洞并消除它才能有效降低风险。为此,网络研究人员提出了主动安全评估技术,通过事先检查是否存在被黑客利用的漏洞来评估系统安全状况[4],并对发现的问题提出解决建议。

文中把安全漏洞作为安全要素,引入 Rough 集理论来分析漏洞扫描器记录的海量历史信息,对系统安全要素进行约简和重要性度量,自动建立基于规则的安全评估模型,进而建立主机定量安全风险度量模型,

收稿日期:2008-03-20
基金项目:安徽省自然科学研究项目(KJ2008B23ZC)
作者简介:汪贵生(1973-),男,安徽枞阳人,讲师,硕士研究生,研究方向为网络安全、数据挖掘等。

以分析系统安全态势。

1　基于 Rough 集理论的安全评估系统

粗糙集(rough set)理论是 20 世纪 80 年代初由波兰科学家 Z. Pawlak 提出的一种处理模糊性和不确定性的数学工具[5]。它从一个新的角度将知识定义为对论域的划分能力,并将其引入数学中的等价关系来进行讨论,从而为数据分析,特别是不精确、不完整数据分析提供了一套新的数学方法。目前,粗糙集理论已经被广泛应用于数据挖掘、机器学习、网络安全和模式识别等众多领域。基于 Rough 集理论的安全评估系统分为在线和离线两大部分,主要由扫描器、攻击测试、知识发现、逻辑推理和安全态势分析模块组成[6],如图 1 所示。在该系统中,扫描器和攻击测试用于获取系统的脆弱信息,并将结果存入漏洞库;知识发现使用 Rough 集理论对漏洞库的历史数据进行离线分析,约简系统安全要素并度量其重要性,生成基于规则的安全评估模型且存于知识库;逻辑推理利用知识库中安全评估模型对当前扫描结果进行在线推理,得到评估结果;安全态势分析利用漏洞数据库和知识发现模块的安全要素重要性信息,建立系统安全风险评估模型,分析系统安全演化状况。该系统具有自适应性能,可定期使用 Rough 集理论对历史评估记录进行知识发现,及时更新知识库,以实现对新漏洞的评估。

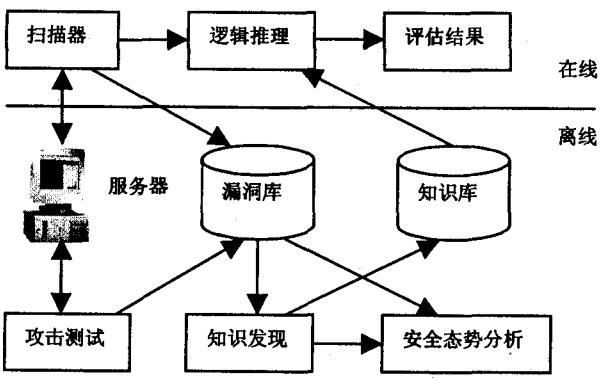

图 1　基于 Rough 集理论的安全评估系统

2　基于 Rough 集理论的安全评估模型

漏洞扫描器对一台主机每次扫描大量的记录,因此长时期的扫描结果将是海量数据。由于 Rough 集理论借助于信息系统 $S = < U, R = C \cup d, V, f: U \times R \rightarrow V >$ 来表达和处理知识,具有能从海量数据中发现有用规律并可转化这些规律为逻辑规则的优势,因此采用 Rough 集理论从长期扫描记录中发现影响系统安全的要素,挖掘出安全要素组合的潜在威胁规则,利用安全要素重要性建立主机安全风险度量模型。

2.1　建立安全评估模型

假定主机扫描记录对应对象集 U,安全要素集 F 对应条件属性集 C,威胁评估结果集 r 对应决策属性集 d。把主机中各个服务存在的漏洞 V 作为系统安全要素,威胁评估结果集的严重程度 r = {高,中,低} 的取值根据漏洞可能对系统造成的直接威胁程度来确定[7],选定条件属性集 $C = \{V_1, V_2, \cdots, V_k\}$ 对系统进行 n 次评估,建立评估信息决策表,见表 1。在评估信息决策表的基础上,充分利用 Rough 集理论的属性约简能力来度量安全要素的重要性,删除对安全评估结果无影响的系统安全要素,使得评估信息决策表中的一个记录代表一类具有相同规律特性的样本。

表 1　评估信息决策表

U	条件属性				r
	V_1	V_2	…	V_k	
1	V_{11}	V_{12}	…	V_{1k}	r_1
2	V_{21}	V_{22}	…	V_{2k}	r_2
⋮	⋮	⋮	⋮	⋮	⋮
n	V_{n1}	V_{n2}	…	V_{nk}	r_n

设 R 是由威胁评估结果集 r 的严重程度导出的分类,安全要素 V_i 在 F 中的重要性[8] 为

$$I(V_i) = \frac{| P_F(R) | - | P_{F \setminus |V_i|}(R) |}{| U |} \tag{1}$$

式中:$P_F(R)$ 为 R 的 F 正域,即根据知识 F 论域 U 中所有一定能归入集合 R 的元素构成的集合,表达式为

$$P_F(R) = U\{Y_i \mid (Y_i \in U \mid N(F) \cap Y_i \subset R)\} \tag{2}$$

式中:$U \mid N(F)$ 是不分明关系 F 对 U 的划分,即

$$U \mid N(F) = \{(x,y) \mid (x,y) \in U^2 \cap \forall f \in F(f(x) = f(y))\} \tag{3}$$

评估信息决策表经过安全要素约简,就可得到与安全评估决策规则相对应的结果,即就是所需要的评估模型,其形式为"$A \rightarrow B$"。另外,为了对评估决策规则 $A \rightarrow B$ 推出的正确结论概率进行估计,引入评估决策规则 $A \rightarrow B$ 的可信度

$$K_{A \rightarrow B} = \frac{| X \cap Y |}{| X |} \tag{4}$$

式中:X 为安全要素值满足 A 的实例集合;Y 为威胁评估结果的严重程度值满足 B 的实例集合。

2.2　主机安全风险评估

主机及网络安全性的根源在于其存在的脆弱性(vulnerability)[9],即网络协议、网络软件、网络服务、主机操作系统及各种主机应用软件在设计及实现上存在种种安全隐患和安全缺陷。漏洞之间的关联性、网络主机之间的依赖性、网络服务的动态性及网络联接的

复杂性决定了主机及网络脆弱性分析是一项非常复杂的工作。一台主机的安全取决于运行服务的安全，同时服务存在的漏洞影响服务的安全。为了对主机安全作出整体量化评估[10]，分析系统配置改变对系统安全的影响，提出了基于安全要素的重要性度量，从构成主机安全的安全要素层、服务层和主机层进行分析，建立了层次化主机安全风险评估模型，如图 2 所示。主机层和服务层的安全风险度量可由它的下层各个子节点的安全风险指数加权和得到，具体分析如下。

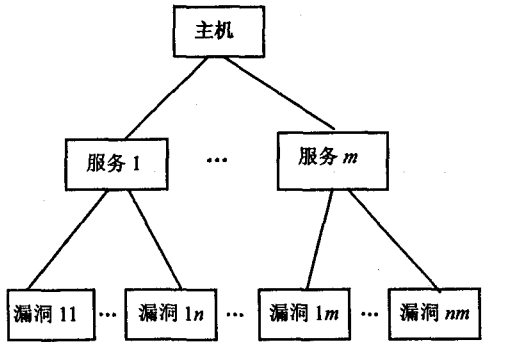

图 2 系统安全风险评估模型

主机 H 的安全风险 Q_H 定义为系统中服务所占的比重向量 $\boldsymbol{\beta}$ 与服务层安全风险向量 Q_S 的内积

$$Q_H = \boldsymbol{\beta} \cdot Q_S \tag{5}$$

其中 $\boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_m)$，$m$ 为主机 H 运行的服务数，元素 β_i 为系统中各项服务所占的重要性比重，可由管理员根据各个服务在系统中的重要性来确定；$Q_{s_i} = (Q_{s_1}, Q_{s_2}, \cdots, Q_{s_m})$ 是服务 S_i 的安全风险值，是各安全要素在系统安全中所占比重向量 W_i 与安全风险等级向量 V_i 的内积，即

$$Q_{s_i} = W_i \cdot V_i \tag{6}$$

其中 $W_i = (W_{i_1}, W_{i_2}, \cdots, W_{i_n})$ 应来自于样本客观信息，即利用安全要素的重要性信息并进行归一化处理，得到服务 S_i 的第 j 个安全要素在系统安全中所占比重：

$$w_{ij} = I(v_{ij}) / \sum_{k=1}^{m} \sum_{t=1}^{n_k} I(v_{kt}) \tag{7}$$

$V_i = (V_{i_1}, V_{i_2}, \cdots, V_{i_n})$ 是服务 S_i 的第 j 个安全要素的风险等级，按照漏洞本身的直接威胁等级进行赋值，对严重性为高、中、低的漏洞风险分别赋值为 7、5、3。主机 H 的安全风险 Q_H 的意义在于，计算出一段时期内的安全风险态势，以便清晰地看出系统配置变化对系统安全状况的影响。

3 结束语

文中提出的基于 Rough 集理论的主机安全评估模型与已有方法模型相比，具有度量安全要素重要性、发现和评估多个安全要素组合的威胁以及评估分析一段时间内安全态势的特点，能够反映出系统配置对系统安全的影响，使得安全评估结果更加准确、直观。该方法模型适用范围广，只要更改相应的条件和决策属性，就能够应用于各种操作系统。今后还将进一步研究：实现网络拓扑结构的自动探测，从而实现网络安全态势的可视化直观显示；研究对大量扫描信息的智能挖掘和推理技术；研究主机之间漏洞的组合对系统威胁的评估规则，为扩展和完善网络安全评估打下基础。

参考文献：

[1] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security [J]. IEEE Transactions on Software Engineering, 1999, 25 (5): 633 - 650.

[2] Dacier M, Deswarte Y, Kaaniche M. Quantitative Assessment of Operational Security: Models and Tools[R]. USA: LAAS Research Report 96493, 1996.

[3] 匿 名. 网络安全技术内幕[M]. 前导工作室译. 北京：机械工业出版社，1999.

[4] 杨守君. 黑客技术与网络安全[M]. 北京：中国对外翻译出版公司，2000：145 - 160.

[5] 刘 清. Rough 集及 Rough 推理[M]. 北京：科学出版社，2001.

[6] 陈秀真，郑庆华. 基于粗糙集理论的主机安全评估方法[J]. 西安交通大学学报，2004，38(12)：1229 - 1230.

[7] Stardust. 计算机网络系统安全漏洞分类研究[EB/OL]. 2003 - 03 - 03[2003 - 11 - 13]. http://www.xfocus.net/artic - les/200103/126.html.

[8] Pawlak Z. Rough sets[J]. International Journal of Computer and Information Science, 1982(11): 341 - 356.

[9] 陆余良，夏 阳. 主机网络安全量化融合模型研究[J]. 计算机学报，2005，28(5)：918 - 920.

[10] 夏 阳，陆余良，蒋 凡. 网络安全量化评估系统的研究与应用[J]. 计算机科学，2003，30(2)：101 - 103.

(上接第 155 页)

[C]// In the 2002 International Conference on Parallel Processing. Los Alamitos: IEEE Computer Society Press, 2002: 379 - 384.

[11] Tzeng Wen - Guey. Effcient 1 - out - n oblivious transfer schemes[C]// In Proceedings of the Public - Key Cryptography (PKC'02). [s. l.]: Springer - Verlag, 2002: 159 - 171.

[12] 姜正涛，郝艳华，王育明. 对不经意传输协议的分析[J]. 西安电子科技大学学报，2005，32(1)：130 - 138.