基于DBN的计算系统动态安全分析模型

赵 峰 章 勤 李 敏
(华中科技大学计算机科学与技术学院 武汉 430074)
(服务计算技术与系统教育部重点实验室 武汉 430074) (集群与网格计算湖北省重点实验室 武汉 430074)

摘 要 计算系统脆弱性分析是系统安全领域研究的热点问题之一。随着多核技术的出现,计算系统呈现开放性和动态性的特征。有鉴于此,在研究现有系统安全风险分析的基础上,提出了面向动态计算系统的安全分析模型,它利用动态贝叶斯网络构建攻击图,以解决计算系统脆弱性动态转移的问题。最后,以虚拟计算系统为实例验证了所提方法的效率和性能。实例仿真表明,该方法是动态系统安全风险分析的一种新的有效途径。

关键词 系统安全,安全分析,攻击图,动态贝叶斯网络
中图法分类号 TP393 **文献标识码** A

Novel Dynamic Security Analysis Model for Computing System Based on DBN

ZHAO Feng ZHANG Qin LI Min
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)
(Services Computing Technology and System Lab, Wuhan 430074, China)
(Cluster and Grid Computing Lab, Wuhan 430074, China)

Abstract In recent years, computing system vulnerability analysis attracts more and more researchers, which has become a hot spot in the field of system security. With the emergence of multi-core technology, computing systems become more open and dynamic. An attack graph-based dynamic security analysis model was proposed, which can measure combined effect of dynamic computing system vulnerabilities. An improved attack map generation algorithm was also presented to improve performance and simplify further security analysis by system administrators. Moreover, a virtual computing system-based example shows the analysis process of the proposed method and validates its efficiency and performance. The experimental results show that our method is an effective way to dynamic system security risk analysis.

Keywords System security, Security analysis, Attack graph, Dynamic baysian network

1 引言

计算系统的安全分析技术一直是国内外众多学者关注的焦点之一。通过定性和定量的风险评估,可分析计算系统潜在的威胁,对系统资源配置进行有效指导,以提高系统对恶意攻击的抵抗能力,从而提升系统的生存性和可信性。近年来,多核技术的出现使得计算系统的处理能力得到迅猛提升,计算系统开放性和动态性的特征日益明显,其下的系统脆弱性分析问题也更加复杂。一方面,随着工作站数量的剧增,操作系统和应用软件的使用和升级过程中的风险分析更为复杂;另一方面,复杂计算系统具有动态性,可以随时随地创建、销毁和迁移应用实例,因此在动态变化过程中进行计算系统的安全分析也更为困难。

传统系统安全分析技术多采用基于模型的方法为整个系统建模,通过模型获得系统所有可能的行为和状态,然后利用模型分析工具产生测试用例,对系统整体的安全性进行评估。这种分析方法无法适应复杂计算系统的动态扩展和攻击行为的动态演变,因此不再适用。有鉴于此,本文针对复杂计算系统的动态性和开放性,提出了一种基于攻击图的系统动态安全分析模型,利用动态贝叶斯网络(DBN, Dynamic Baysian Network)对系统攻击序列进行动态建模,并设计了一种改进的攻击图生成算法。实例仿真表明,该方法是动态系统安全风险分析的一种有效途径。

2 相关工作

国内外众多学者对计算系统的脆弱性分析方法和理论展开了广泛的研究,取得了一系列成果。

Swiler等人提出了基于图的网络安全分析模型,使用攻击图描述入侵过程,根据攻击者的特征、网络配置和攻击模板,从目标状态出发反向匹配攻击模板,以发现存在的隐患和计算最大入侵成功概率[1],但其攻击图采用手工绘制,且最短路径算法受限于攻击图的结构。Sheyner等人提出了一种利

到稿日期:2009-03-26 返修日期:2009-06-10 本文受国家自然科学基金(60803114),国家重点基础研究发展计划(973项目:2007CB310900)资助。

赵 峰(1976-),男,博士后,副教授,CCF会员,主要研究方向为网络安全、系统安全、数据挖掘等,E-mail:jimmyzf@gmail.com;章 勤(1955-),女,硕士,教授,主要研究方向为网格与高性能计算;李 敏(1985-),男,硕士生,主要研究方向为网络安全。

用模型检测器 NumSMV 自动生成攻击图的方法[2]，但该攻击图生成方法的效果受模型检测器表达能力的制约。

CVSS 系统(Common Vulnerability Scoring System)通过打分方式测量系统单个缺陷，但无法将整个系统或网络的缺陷进行整合以便总体分析[3]。Suvajit 等人提出在系统设计之初，使用攻击图作为辅助优化系统体系结构，以容忍系统缺陷及弥补 CVSS 的不足[4]。Wang Lingyu 等人在 CVSS 的基础上提出利用贝叶斯网络对攻击图建模，分析系统缺陷之间的依赖关系，以进行整体安全分析[5,6]。该方法能连续有效地评测动态环境下的网络安全，但其计算成本过高且计算准确性受 CVSS 的时序规律限制。

国内有学者提出了分布式系统的脆弱性分析模型和基于推理的网络脆弱性的分析模型[7-9]。对动态计算系统安全分析模型的研究刚起步，鲜见相关文献。

3 基于 DBN 的动态安全模型

3.1 问题描述

为使本文概念上自包，现给出相关定义。

定义 1 攻击脆弱性是指计算系统中因硬件、软件或者安全策略上的错误而引起的缺陷，攻击者可利用这些缺陷入侵成功，是违背安全策略的系统特征。

以虚拟计算系统(Virtual Computing System)为例，系统的攻击脆弱性主要由以下因素构成：①虚拟机(VM, Virtual Machine)的状态，包括入侵者在该 VM 上获得的权限、客户操作系统(Guest OS)上存在的漏洞情况以及当前能被利用的攻击方法等；②虚拟机管理器(VMM, Virtual Machine Monitor)状态，攻击者在 VMM 层上获得的权限以及能被利用的攻击方法；③攻击者的状态，亦即攻击者发起攻击和攻击过程中所在的 VM；④攻击关联关系，亦即攻击者使用的攻击方法的前置条件和后置条件。

文献[2]对攻击模型和攻击图给出了形式化的描述，本文引用如下。

定义 2 攻击模型 M 是一个有限状态自动机，$M=(S,\tau,s_0,l)$。其中 S 是状态集合；$\tau\subseteq S\times S$ 是状态转换关系矩阵；$s_0\in S$ 是初始状态；$l:S\to 2^{AP}$ (AP 是原子命题集合)是对状态的标记，在该状态上是一些命题为真的集合。

定义 3 攻击图是攻击模型的子图，可用五元组 $AG=(S,\tau,s_0,E,l)$ 表示。其中 S 是状态集；$\tau\subseteq S\times S$ 是状态转换关系矩阵；$s_0\in S$ 是初始状态；$E\subseteq S$ 是错误状态集合；$l:S\to 2^{AP}$ (AP 是原子命题集合，$|AP|$ 是原子命题集合个数)是对状态的标记，在该状态上是一些命题为真的集合。

贝叶斯概率(Baysian probability)是观察者对某一事件发生的相信程度，是事件发生的动态预测。在攻击模型中，它是 M 中不同状态转换关系概率的直观体现。因此，我们对攻击模型 M 做了改进，将贝叶斯概率引入攻击模型的状态转换中，以适应虚拟计算系统的动态性，提出了基于贝叶斯概率的攻击模型 M_B。

定义 4 贝叶斯概率攻击模型是一个四元组，$M_B=(S,\tau_B,s_0,l)$。其中 S 是状态集；$\tau_B\subseteq S\times S\to[0,1]$ 是状态转换关系矩阵，表示状态之间的可达概率关系(用贝叶斯概率表示)，若 $\forall s,s'\in S$，则 $\sum_{S}\tau_B(s,s')=1$；$s_0\in S$ 是初始状态；$l:S\to 2^{AP}$ (AP 是原子命题集合)是对状态的标记，在该状态上是一些命题为真的集合。

开放计算系统中，系统缺陷的不确定性导致了攻击行为演变过程的动态变化。因此，在攻击模型 M_B 的基础上，采用动态贝叶斯网络来描述攻击行为的动态演变，以监视和更新系统，并获取攻击序列之间的潜在联系。DBN 用于计算系统的脆弱性评估中，可以通过系统中已知的缺陷以及已经受到的攻击事件来推断潜在的安全关系，从而对攻击事件发生的可能性做出量化的评估。

基于攻击模型 M_B 和 DBN，我们对传统攻击图模型做了改进，提出了一种新的攻击图模型 AG_B。AG_B 的目的是描述攻击行为在计算系统中的动态演化过程，定义如下。

定义 5 攻击图可表示为 $AG_B=(S,\tau_B,s_o,R,l)$，其中，

(1)状态集 S 表示攻击行为在计算系统中的实施情况。任何状态 $s=(obj,state,env)$，其中 obj 是攻击实体；$state$ 是用户行为的类别，包括正常行为、攻击行为、入侵行为；env 是攻击生存环境条件。

(2) $\tau_B\subseteq S\times S\to[0,1]$ 是状态转换关系矩阵，表示不同状态之间的转移概率关系。

(3) $s_0\in S$ 是计算系统初始状态。

(4) $R=(v,e,p)$ 是描述攻击序列过程的 DBN，$v\subseteq S$ 是 DBN 节点集合；e 是 DNB 有向边集合，表示攻击过程中的先后和因果关系；p 是 DBN 在 τ_B 上的条件概率。

(5) $l:S\to 2^{AP}$ (AP 是原子命题集合)是对状态的标记，在该状态上是一些命题为真的集合。

3.2 AG_B 生成算法

开放性的动态计算系统中，现有攻击图生成算法存在两方面的问题：①随着应用实例规模的增大，算法的状态空间呈指数级增长，算法的时间复杂度和空间复杂度太高；② 当应用程序的个数动态变化时，算法的适应性太差，无法完整搜索出攻击图中的攻击路径，降低了计算系统安全分析的准确性。本文对文献[2]提出的攻击图生成算法进行了改进，提出了一种具有动态适应性的攻击图生成算法，算法如下所示：

输入：S,τ_B,s_0,l；

输出：AG_B；

算法步骤：

①根据 s_0 和 S，构建 DBN 结构，并生成初始攻击图 (S,τ_B,s_0,R,l)，DBN 生成方法如下：

初始化：令 DBN 结构为 $R=(v,e)$，其中 $v=S,e=\emptyset;n=|S|$，表示元素个数；临时线性表 $L=\emptyset$；

for $(i=1;i<(n+1)/2;i++)$

{ root=$v[i]$;//根节点

while $(i\neq j)$ and $(v[j]\in v)$

{

计算 $I(v[i],v[j])$，其中

$$I(x_1,x_2)=\sum_{x_1,x_2}p(x_1,x_2)\log\frac{p(x_1,x_2)}{p(x_1)p(x_2)};$$

将所有 $I(v[i],v[j])>\frac{1}{2^{|AP|}}$ 的节点对按递减顺序存入 L；

}

while $(L\neq\emptyset)$

{

从 L 中依次取出节点对，连接两节点，将边添加到 e 中；

}

}

②根据计算系统的动态变化，调整行为序列的 DBN 结构，并计算新的条件概率 p，计算方式如下：

$$p(v)=p(v|pre(v))=\prod p(x,x\in S|pre(v))$$

其中，$pre(v)$是节点 v 的先序节点集合。

③根据 DBN 的动态变化调整 S，$l: S \rightarrow 2^{AP}$ 和 $R=(v,e,p)$，重新生成 AG_B。

④周期性监测计算系统状态变化，如发生改变执行③，无变化执行⑤。

⑤返回 AG_B。

算法中主要考虑 DBN 的以下变化。

节点删除：当计算系统状态个数减少时，DBN 中对应的节点需要删除。与此同时，DBN 中与此节点对应的边也要删除。这种情况下 DNB 的结构不会发生变化，只是精简，需要重新计算 p；

节点增加：当计算系统状态个数增加时，DBN 中节点需要加入。这种情况下需要重新构建 DBN 的网架，采用文献[10]中的算法更新 DBN 结构，并计算 p；

节点变迁：当计算系统状态值发生变化时，需要更新 DBN 结构，并重新计算 p。

4 虚拟计算系统实例分析

基于虚拟机的虚拟计算环境(Virtual Computing Environment)具有开放性、一体性、复杂性、动态性等特征，能更有效地整合分散的计算资源，为用户和应用提供一体化的服务环境，实现资源共享和有效利用，是动态计算系统的典型代表：一方面，只要计算资源许可，虚拟计算环境中虚拟机(VM, Virtual Machine)的数量可无限制增加；另一方面，虚拟机具有动态性，可以随时随地创建、销毁和迁移。有鉴于此，我们以虚拟计算系统为实例环境对本文提出的方法予以验证。

4.1 实验环境

我们在 Linux 平台(Fedora8, Xen3.1, 内核 2.6.23)上构建一个小型虚拟计算系统作为原型，实验环境包括 1 台双 CPU(每个 CPU4 核、频率 1.6G, cache 4MB, 内存 2G)的服务器和 1 台 P2.0GHz/512M/Cache128K 的 PC。创建了 3 个 VM，通过在 VM 上部署 MySQL 数据库，通过新建、删除、迁移 VM 与数据库服务来验证本文提出的模型。可仿真实验中的系统漏洞如表 1 所列。

表 1 系统漏洞及入侵效果

系统缺陷	攻击方式	成功概率	入侵效果
Func 漏洞	直接利用	70%	提升权限
远程登录	端口监听	90%	提升权限
IF 查询拒绝服务漏洞	空指针引用	35%	服务崩溃
zlib 漏洞	注入攻击	40%	应用程序失效

利用本文提出的安全分析方法，可找出虚拟计算系统中攻击序列成功入侵的可能概率，从而判定计算系统的脆弱点。

例如，模拟实验中，假设系统受攻击后的状态更新如图 1 所示。虚线是创建 VM 与数据库服务后攻击路径的变化序列，则表 2 列出了不同攻击序列可能成功的概率。可见，S_0—S_2—S_3—S_4 的入侵成功概率最高，是系统最脆弱的环节。

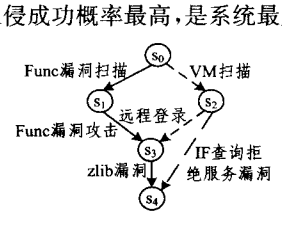

图 1 攻击状态更新

表 2 攻击序列入侵概率

攻击序列	入侵概率
S_0—S_1—S_3—S_4	0.28
S_0—S_2—S_3—S_4	0.36
S_0—S_2—S_4	0.35

4.2 基于 AG_B 的入侵检测效率

考虑到攻击行为的序列关系，我们在新墨西哥大学 Computer Immune Systems Data sets[11] 中的 sendmail 数据集(包含 71760 个进程和 44,500,219 个系统调用序列)上验证了 AG_B 方法的入侵检测效率。表 3 列出了 AG_B 方法与基于贝叶斯网络、基于数据挖掘、基于系统调用序列的入侵检测效率对比结果。实验结果表明：①AG_B 方法的检测率要优于其它方法；②系统动态变化时，AG_B 方法的检测率和误报率与静态检测效率变化不大，表明 AG_B 方法能较好地适应计算系统的动态变化。

表 3 入侵检测效率对比

方法		检测率	误报率
静态 AG_B 方法		87.5%	0.79%
AG_B 方法	VM 删除	87%	0
	VM 增加	86.7%	0.16%
	VM 迁移	87.9%	1.1%
传统贝叶斯网络方法[10]		70.23%	5.30%
数据挖掘方法	分类[12]	81%	2.7%
	序列模式[13]	82.5%	3.6%
系统调用序列方法(长度=6)[14]		86%	0

4.3 性能分析

为验证本文提出方法的性能，在虚拟计算平台上将本文方法与基于 NuSMV 的系统安全分析方法[2] 进行了比较，对比结果如表 4 所列。实验结果表明，基于 DBN 的分析方法在攻击图生成时间上远低于基于 NuSMV 的分析方法，时间缩短了近 2.5 倍，克服了 NuSMV 方法攻击图构建的时间瓶颈。

表 4 性能对比

安全分析方法	状态数	错误率	执行时间	
			生成	运行
基于 NuSMV 的方法[2]	101	3.91%	2h	5s
基于 DBN 的方法	90	4.2%	47min	6s

此外，同基于 Baysian Network 的安全分析方法[6] 相比，本文方法克服了 BN 方法不能动态获取系统信息的缺点；同基于 Ranking 的系统安全分析方法[15] 相比，本文方法的错误率为 4.2%，小于基于 Ranking 攻击图分析的 15%的错误率。

结束语 传统基于攻击图的安全评估模型无法适应动态计算系统的动态扩展和攻击行为的动态演变。利用 DBN 描述攻击行为的动态演变，提出了基于 DBN 的动态安全模型，并提出了一种具有动态适应性的攻击图生成算法，为计算系统的安全评估提供了自动化的手段。通过改进的攻击图模型可以对计算机网络系统脆弱环节、易受攻击环节、攻击路径等进行有效的分析与预测。本文今后的研究工作包括利用提出的分析模型找出确保计算系统安全的原子攻击集以及分析模型在入侵检测与入侵容忍中的应用。

参 考 文 献

[1] Swiler L, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system[R]. SAND 97-3010/1. 1998

[2] Sheyner O, Haines J, Lippmann R, et al. Automated generation

and analysis of attack graphs[C]// Proceeding of the 2002 IEEE Symposium on Security and Privacy. Oakland, CA, May 2002

[3] Mell P, Scarfone K, Romanosky S. Common Vulnerability Scoring System[J]. IEEE Security & Privacy, 2006, 4(6): 85-89

[4] Suvajit G, Winstead J. Using Attack Graphs to Design Systems [J]. IEEE Security & Privacy, 2007, 5(4): 80-83

[5] Frigault M, Wang L. Measuring Network Security Using Bayesian Network-based Attack Graphs [C] // Proceedings of the 32nd Annual IEEE International Computer Software and Applications Conference (COMPSAC2008). August 2008: 698-703

[6] Frigault M, Wang L, Singhal A, et al. Measuring Network Security Using Dynamic Bayesian Networks[C]// Proceedings of the 4th ACM Workshop on Quality of Protection. Alexandria, Virginia, USA, October 2008: 23-30

[7] 冯萍慧，连一峰，戴英侠，等. 基于可靠性理论的分布式系统脆弱性模型[J]. 软件学报，2006，17(7)：1633-1640

[8] 王永杰，鲜明，刘进，等. 基于攻击图模型的网络安全评估研究[J]. 通信学报，2007，28(3)：29-34

[9] 贾炜，连一峰，冯登国，等. 基于贝叶斯网络近似推理的网络脆弱性评估方法[J]. 通信学报，2008，29(10)：191-198

[10] Chen J, Greiner R, Kelly J, et al. Learning Bayesian networks from data: An information-theory based approach[J]. Artificial Intelligence, 2002, 137(1/2): 43-90

[11] Computer Immune Systems Data sets[EB/OL]. http://www.cs.unm.edu/~immsec/data-sets.htm

[12] Abbes T, Bouhoula A, Rusinowitch M. A Traffic Classification Algorithm for Intrusion Detection[C]// Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshops. May 2007: 188-193

[13] 赵峰，李庆华，金莉. 多维流序列并行预测算法研究[J]. 小型微型计算机系统，2007，28(2)：333-336

[14] Warrender C, Forrest S, Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Models[C]// Proceedings of 1999 IEEE Symposium on Security and Privacy. Oakland, USA, September 1999: 133-145

[15] Mehta V, Bartzis C, Zhu H, et al. Ranking Attacking Graphs[C]// Proceedings of 9th International Symposium on Recent Advances in Intrusion Detection (RAID2006). Hamburg, Germany, September 2006: 127-144

(上接第 22 页)

参 考 文 献

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4): 393-422

[2] 刘敏珏，吴泳，伍卫国. 无线传感器网络(WSN)研究[J]. 微电子学与计算机，2005，22(7)：58-61

[3] 孙利民，李建中，陈渝，等. 无线传感器网络[M]. 北京：清华大学出版社，2005

[4] Doherty L, Warneke B A, Boser B E, et al. Energy and performance considerations for smart dust[J]. International Journal of Parallel and Distributed Systems and Networks, 2001, 4: 121-133

[5] Pradhan S, Kusuma J, Ramchandran K. Distributed compression in a dense micro-sensor network[J]. IEEE Signal Processing Magazine, March 2002: 51-60

[6] Shrivastava N, Mudumbai R, Madhow U, et al. Target Tracking with Binary Proximity Sensors: Fundamental Limits, Minimal Descriptions, and Algorithms[A]// Proceedings of the 4th International Conference on Embedded Networked Sensor Systems [C]. 2006: 251-264

[7] 袁红梅，杨震. 基于无线传感器网络的活动目标跟踪[J]. 现代电子技术，2006(19)：7-10

[8] 宋超凡，董慧颖. 基于传感器网络的分段线性拟合跟踪算法研究[J]. 沈阳理工大学学报，2007，26(2)

[9] Mechitov K, Sundresh S, Kwon Y, et al. Cooperative Tracking with Binary-Detection Sensor Networks[R]. UIUCDCS-R-2003-279. Department of Computer Science, University of Illinois at Urbana-Champaign, 2003

[10] Kim WooYoung, Mechitov K, Chol J-Y, et al. On Target Tracking with Binary Proximity Sensors [A] // 4th International Conference on Information Processing in Sensor Networks[C]. Los Angeles, CA, USA, April 2005

[11] Arulampalam M S, Maskell S, Gordon N, et al. A Tutorial on Particle Filters for Online/Non-Gaussian Bayesian Tracking[J]. IEEE Transactions on Signal Processing, 2002, 50(2)

[12] Aslam J, Butler A, Comstantin F, et al. Tracking a Moving Object with a Binary Sensor Network[A]// Proc. ACM Conference on Embedded Networked Sensor Systems[C]. 2003: 150-161

[13] Djuric P M, Vemula M, Bugallo M F. Signal Processing by Particle Filtering for Binary Sensor Networks[A]// Proc. IEEE 11th Digital Signal Processing Workshop & IEEE Signal Processing Education Workshop. 2004: 263-267

[14] Singh J, Kumar R, Cagler R. Tracking Multiple Targets Using Binary Proximity Sensors[A]// Proceedings of the 6th International Conference on Information Processing in Sensor Networks [C]. April 2007: 529-538

[15] Vemula M, Bugallo M F, Djuric P M. Particle Filtering - based Target Tracking in Binary Sensor Networks Using Adaptive Thresholds[A] // Proc. 2th IEEE International Workshop on Computational Advances in Multi-sensor Adaptive Processing [C]. Dec. 2007: 17-20

[16] Djuric P M, Vemula M, Bugallo M F. Target Tracking by Particle Filtering in Binary Sensor Networks[J]. IEEE Transactions on Signal Processing, 2008, 56(6): 2229-2238