软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):495−508 [doi: 10.3724/SP.J.1001.2011.03751]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于 Markov 博弈模型的网络安全态势感知方法*

张 勇+, 谭小彬, 崔孝林, 奚宏生

(中国科学技术大学 自动化系,安徽 合肥 230027)

Network Security Situation Awareness Approach Based on Markov Game Model

ZHANG Yong+, TAN Xiao-Bin, CUI Xiao-Lin, XI Hong-Sheng

(Department of Automation, University of Science and Technology of China, Hefei 230027, China)

+ Corresponding author: E-mail: jzhang@mail.ustc.edu.cn

Zhang Y, Tan XB, Cui XL, Xi HS. Network security situation awareness approach based on Markov game model. *Journal of Software*, 2011,22(3):495−508. http://www.jos.org.cn/1000-9825/3751.htm

Abstract: To analyze the influence of propagation on a network system and accurately evaluate system security, this paper proposes an approach to improve the awareness of network security, based on the Markov Game Model (MGM). This approach gains a standard data of assets, threats, and vulnerabilities via fusing a variety of system security data collected by multi-sensors. For every threat, it analyzes the rule of propagation and builds a threat propagation network (TPN). By using the Game Theory to analyze the behaviors of threats, administrators, and ordinary users, it establishes a three player MGM. In order to make the evaluation process a real-time operation, it optimizes the related algorithm. The MGM can dynamically evaluate system security situation and provide the best reinforcement schema for the administrator. The evaluation of a specific network indicates that the approach is suitable for a real network environment, and the evaluation result is precise and efficient. The reinforcement schema can effectively curb the propagation of threats.

Key words: network security situation awareness; threat propagation network; Markov game model

摘 要: 为了分析威胁传播对网络系统的影响,准确、全面地评估系统的安全性,并给出相应的加固方案,提出一种基于 Markov 博弈分析的网络安全态势感知方法.通过对多传感器检测到的安全数据进行融合,得到资产、威胁和脆弱性的规范化数据;对每个威胁,分析其传播规律,建立相应的威胁传播网络;通过对威胁、管理员和普通用户的行为进行博弈分析,建立三方参与的 Markov 博弈模型,并对相关算法进行优化分析,使得评估过程能够实时运行.Markov 博弈模型能够动态评估系统安全态势,并为管理员提供最佳的加固方案.通过对具体网络的测评分析表明,基于 Markov 博弈分析的方法符合实际应用,评估结果准确、有效,提供的加固方案可有效抑制威胁的扩散.

关键词: 网络安全态势感知;威胁传播网络;Markov 博弈模型

中图法分类号: TP393 **文献标识码**: A

随着网络结构的日趋庞杂和各种新型攻击手段的大量涌现,网络安全问题越来越严峻,网络安全技术也在不断变革,从传统的入侵阻止、入侵检测发展到入侵容忍、可生存性研究,从关注信息的保密性发展到关注信

* 基金项目: 国家高技术研究发展计划(863)(2006AA01Z449);中国博士后科学基金资助项目(20070420738)
收稿时间: 2009-06-24; 定稿时间: 2009-10-10

© 中国科学院软件研究所 http://www.jos.org.cn

息的可用性和服务的可持续性,从关注单个安全问题的解决发展到研究网络的整体安全状况及变化趋势,网络安全态势感知(network security situation awareness,简称 NSSA)成为下一代安全技术的焦点.NSSA 起源于态势感知(situation awareness,简称 SA),指对网络安全要素进行获取、理解、显示以及预测未来的发展趋势.1988 年,Endsley 将 SA 定义为感知在一定时间和空间环境中的元素,包括它们现在的状况和它们未来的发展趋势[1].SA 广泛用于商业领域、军事战场、空中交通监管(air traffic control,简称 ATC)和医疗应急调度等领域.1999 年,Bass 首次提出了网络态势感知(NetSA)的概念,将 ATC 态势感知中成熟的模型和技术应用到 NetSA[2],并首次给出 NetSA 的概念模型[3].对 NSSA 的相关研究主要集中在以下 3 个方面:

从网络连接可视化的角度,将网络连接状态以可视化视图的方式呈现出来,安全管理人员据此判断网络是否受到威胁.Lau 等人设计了三维网络流量检测工具 spinning cube[4],以点的形式表示单个网络连接,以三维立方体显示整个网络的连接状况.SIFT 项目组研制了两种可视化工具 NVisionIP[5]和 VisFlowConnect[6],以 NetFlow 审计日志为数据源显示网络连接状况和网络流量.CAIDA 开发了网络可视化工具 AS[7],以极坐标的方式显示网络中的连接.这些方法对网络状况提供了直观的表示,为安全管理员的分析提供很多便利,但都是基于对系统日志的分析,数据来源单一,实时性较差,并且评估结果过多的依赖管理员的经验,尤其当网络连接很多时,很难判断系统是否遭受攻击.

从层次化分析的角度,比较有代表性的是陈秀真等人提出的层次化网络安全态势量化评估方法[10].该方法利用 IDS 海量报警信息和网络性能指标,结合服务、主机本身的重要性及网络系统的组织结构,采用自下而上、先局部后整体的评估策略,将网络分为服务、主机、系统进行分层计算;最后,综合分析得到网络安全态势图,并有集成化的系统实现,具有很好的理论和实用价值.但是,该方法的数据来源仅有系统 IDS 报警数据,在量化评估算法中很多地方都是采用加权分析方法,具有一定的主观性,还需要实际检验.

从数据融合的角度对 NSSA 研究较为广泛和深入,出现了很多数据融合模型,比较有影响力的是 Steinberg 等人提出的 JDL(joint director's laboratories)数据融合模型[8].JDL 提供的逻辑融合框架,将数据融合过程分为数据精炼、对象精炼、态势精炼、影响评估和过程精炼.Endslay 从人类感觉的视角提出了与 JDL 不同的态势感知模型[9],将态势感知过程分为感知、理解和预测.这两种数据融合模型被广泛应用在网络安全态势感知领域,为后续的研究提供了理论指导.Bass 提出了基于分布式多传感器数据融合的网络态势感知[2],给出下一代入侵检测系统框架,为后续的研究提供了指导.该方法的缺点是,当网络系统很复杂时,威胁和传感器的数量以及数据流变得非常巨大而使得模型不可控制.此外,国内在 Bass 的态势感知概念模型和 JDL 数据融合模型的基础上,对 NSSA 的算法进行了一系列的研究.何伟等人提出的基于脆弱性分析的网络态势感知[11]、赵国生等人提出的基于灰色关联分析的网络可生存性态势评估方法[12]等等.这些研究大都停留在评估算法的研究上,很少有成型的系统实现,并且数据来源和安全要素的考虑比较单一.

本文在态势感知概念模型的基础上,提出了一种基于 Markov 博弈分析的网络安全态势感知模型及其实现方法.综合考虑威胁传播、管理员实施安全措施和普通用户行为的影响,准确全面地评估系统当前的安全状态,给出管理员最佳的应对措施.本文的目的在于:通过对威胁传播的分析,建立安全态势量化评估的 Markov 博弈模型,给出态势评估算法,动态评估当前时刻系统的安全态势,并给出最佳加固方案.

1 网络安全态势感知模型

1.1 网络安全态势感知系统框架

网络态势是指由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势[13].NSSA 是在大规模网络环境中,对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势.NSSA 需要考虑多方因素:首先,数据来源要全面和丰富,包括网络结构、资产、脆弱性、威胁等数据;其次,态势感知过程要简洁和客观,尽可能地实现自动化和满足实时性;最后,态势感知结果要到深度广度兼备,满足多种用户需求,提供加固方案给管理员以提高系统安全性.本文在态势感知概念模型基础上,结合数据融合的思想,给出了如图 1 所示的 NSSA 系统框架[14].

© 中国科学院软件研究所 http://www.jos.org.cn

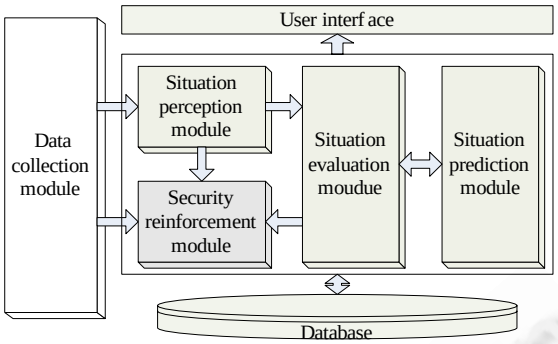

Fig.1 Framework of NSSA

图 1 NSSA 系统框架

该框架通过多传感器检测网络系统的各种安全信息,根据态势感知模型评估系统的安全态势及其变化趋势,并给出安全加固方案,主要包括以下几个模块:

(1) 数据采集:通过多传感器监测网络系统的运行状况,检测大量的原始安全数据;

(2) 态势理解:采用规范化分析、冗余检测和冲突检测等方法,分析原始数据,得到规范化的数据集;

(3) 态势评估:采用态势评估算法,分析态势理解模块的数据,定量描述系统的安全态势;

(4) 态势预测:采用态势预测算法,分析态势的变化规律,预测系统安全态势变化趋势;

(5) 加固方案生成:分析系统最薄弱的节点,给出加固方案,指导管理员提高系统安全性.

1.2 威胁传播分析

网络系统的各个节点相互连接,当系统中某个节点被成功攻击后,威胁可以传播到与该节点相关联的其他节点,从而使这些节点遭受安全威胁.因此,在进行态势感知时不能仅静态考虑系统节点安全状况,还需对威胁传播及其影响进行动态分析.张永铮等人提出了用于风险评估的风险传播模型[15],考虑了风险传播带来的潜在风险,其实质是分析威胁的传播对风险的影响.本文在针对不同威胁分析其传播规律,并结合相关的脆弱性分析对相关资产和相关传播链路的影响,提出威胁传播网络的概念.

1.2.1 相关概念

定义 1(资产). 对系统有价值的资源,单个资产用 $Asset=(id_a,name_a,type_a,value_a,\rho_a)$表示.其中,$id_a$ 为资产标识,$name_a$ 为资产名称,$type_a$ 为资产类型,$value_a$ 为资产价值,ρ_a 资产性能利用率.

资产的类型包括主机、服务器、路由器、网关、防火墙、IDS 等;资产价值表示资产的重要程度,包含资产保密性价值、完整性价值、可用性价值,是一个向量结构,与资产的类型、资产提供的服务、资产所在主机的性能、资产所在的网络位置等因素相关[16];资产的性能利用率是资产所在主机的内存、CPU、可支持连接数等性能的利用率的综合加权,分 5 个等级.随着等级的增长,性能利用率指数增长.

定义 2(威胁). 对资产造成损害的外因,单个威胁用 $Threat=(id_t,name_t,type_t,id_a,id_v,p_t)$表示.其中,$id_t$ 为威胁标识,$name_t$ 为威胁名称,$type_t$ 为威胁类型,id_a 为威胁所在资产的标识,id_v 为威胁利用的脆弱性的标识,p_t 为威胁发生概率.

威胁的类型包括病毒、蠕虫、木马等恶意代码和网络攻击,根据对系统的损害方式将威胁分为两类:一类威胁是占网络资源少的威胁,包括木马、病毒和网络攻击等,对系统节点的保密性、完整性和可用性均有影响,对网络带宽的影响忽略不计;二类威胁是大量耗费系统资源的威胁,以蠕虫和 DDoS 攻击为代表,主要对系统的可用性造成影响.威胁发生的概率表示威胁发生的可能性,在某个资产上,对已检测到的威胁该值为 1;对已检测到某脆弱性但未检测到利用该脆弱性的威胁,根据威胁等级的定义[16],认为该威胁以 p_t 概率发生.

定义 3(脆弱性). 可以被威胁利用的薄弱环节,单个脆弱性用 $Vul=(id_v,name_v,type_v,id_a,id_t,p_v,\mu)$表示.其中,$id_v$ 为脆弱性的标识,$name_v$ 为脆弱性名称,$type_v$ 为脆弱性类型,id_a 为脆弱性所在资产的标识,id_t 为利用该脆弱性的威

© 中国科学院软件研究所 http://www.jos.org.cn

胁的标识,p_v为脆弱性被利用的可能性,μ为脆弱性的影响.

脆弱性的类型包括管理配置脆弱性、漏洞等;脆弱性被利用的可能性表示脆弱性被利用的难易程度,在某个资产上,如果检测到某脆弱性,认为该脆弱性以 p_v 的概率被相应威胁成功利用;脆弱性的影响表示该脆弱性引发的安全事件对资产价值的影响,是一个向量结构,包含对资产保密性价值、完整性价值和可用性价值的影响.通过对检测数据的融合,得到系统中所有的资产、威胁和脆弱性数据,构成资产集合、威胁集合和脆弱性集合.

1.2.2 威胁传播网络

对于威胁集合的每个威胁 t,如果某个网络节点存在 t,则 t 可以通过网络传播到与该节点相邻的其他节点.根据资产集合、脆弱性集合和网络结构信息,首先确定 t 的分布状态,即每个节点是否存在 t,是否存在 t 利用的脆弱性,t 通过每条路径传播的概率;然后分析 t 可能的转播路径和系统的变化状态.威胁的分布状态用威胁传播节点表示,威胁下一步可能的转播方向用威胁传播路径表示.

定义 4(威胁传播节点). 系统中受威胁影响的节点,包括已经被攻击或可能被攻击的节点,用 $Node=(id_a, value_a,\rho_a,t_f,v_f)$表示.其中,$id_a$ 为该节点对应资产的标识,$value_a$ 为该节点对应资产的价值,ρ_a 为该节点对应资产的性能利用率,t_f 表示该节点是否存在威胁,v_f 表示该节点是否存在威胁利用的脆弱性.

定义 5(威胁传播路径). 系统中传播威胁的链路,用有向边 $Path=(id_{as},id_{ad},value_e,\rho_e,p_e)$表示.其中:$id_{as}$ 为路径源节点资产 ID;id_{ad} 为路径目的节点资产 ID;$value_e$ 为路径价值;ρ_e 指路径被切断后对系统造成的损失,是路径带宽利用率,与资产的性能利用率类似,分为 5 个等级;p_e 表示威胁通过该路径成功扩散的概率,分为 5 个等级,每提高一个等级,威胁成功传播概率线性增加.

定义 6(威胁传播网络(threats propagation network,简称 TPN)). 单个威胁 t 的 TPN 包含 t 所有的传播节点和传播路径,用 $TPN(t)=\{Nodes,Paths\}$表示,$Nodes$ 为威胁传播节点集,$Paths$ 为威胁传播路径集.

威胁传播节点集包含系统所有受 t 影响的资产,可以设置包含系统所有资产;威胁传播路径集包含系统所有可以传播 t 的链路,可以设置包含系统所有链路.根据这两个集合建立 t 的传播网络,t 的一步行为指 t 通过威胁传播网络,以一定的概率传播到当前被感染节点的邻居节点.每个威胁通过与之对应的威胁传播网络一步一步地传播到系统其他部分.

1.3 网络安全态势感知流程

根据图 1 给出的 NSSA 系统框架,给出如图 2 所示的 NSSA 流程,态势感知过程分为两部分:基于 Markov 博弈分析的态势量化评估和基于时间序列分析的态势预测.

态势量化评估部分是态势感知的核心.首先,数据采集模块检测的安全数据被融合归类到资产集合、威胁集合、脆弱性集合和网络结构信息,这些数据以规范化数据集的格式保存在数据库中,可以被实时地存取和修改;接着,对威胁集合中的每个威胁建立 TPN;然后,对威胁、管理员和普通用户的行为进行 Markov 博弈分析,评估单个威胁的保密性态势,并给出最佳加固方案;最后,对威胁集合中的所有威胁的保密性态势综合分析评估出系统保密性态势;以同样的方法评估系统完整性态势和系统可用性态势,根据不同的应用背景和需求,对保密性、完整性、可用性态势加权,评估整个系统当前状态的安全态势.

态势预测部分以态势评估结果为基础.系统在不同时刻安全态势彼此相关,可以利用这种相关性分析态势变化规律对系统安全态势进行预测.有很多预测方法,比如神经网络、模糊数学、灰色理论等等.在此,采用时间序列分析方法[14]刻画不同时刻安全态势的前后依赖关系.

© 中国科学院软件研究所 http://www.jos.org.cn

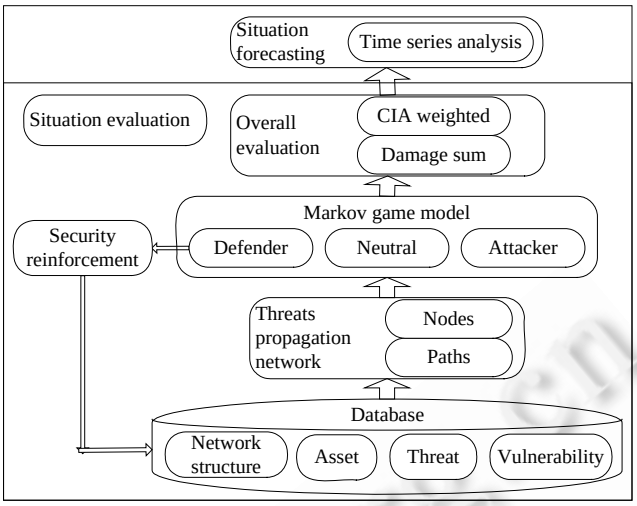

Fig.2 Process of NSSA

图 2 NSSA 流程

2 基于 Markov 博弈分析的态势评估

2.1 Markov博弈模型的建立

博弈论是研究决策者在决策主体各方相互作用下如何进行决策的理论,每个决策主体在考虑其他参与者的反应后选择行动方案[17].Markov 决策过程(MDP)是指决策者根据每个时刻观察到的状态,从可用的行为集合中选用行为的过程.系统下一步的状态是随机的,状态转移概率具有 Markov 性,即下一时刻的状态只与当前时刻相关[18].Markov 博弈是由博弈论和 MDP 综合而来,综合考虑多个参加者的决策.博弈分析方法被广泛用于网络安全性分析,比如,Sallhammar 等人采用博弈模型对攻击者意图进行分析[19],DanShen 等人采用 Markov 博弈模型进行网络安全态势感知和对攻击效果分析[20]等等.这些研究仅对安全态势的某一侧面进行定性分析,在具体实施时很难操作.我们在文献[21]中采用两角色 Markov 博弈分析的方法进行风险评估,考虑了攻防双方的行为对风险的影响,动态地分析威胁的潜在风险,在分析攻击方的行为时,仅考虑威胁自由扩散的特殊情况,并且没有考虑普通用户行为的影响.本文对威胁集合中每个威胁 t 建立如下的 Markov 博弈模型:

(1) 博弈三方:攻击方以威胁的形式存在,通过威胁传播对系统造成损害;防守方以管理员为代表,通过实施加固方案减少威胁利用的脆弱性和切断威胁传播途径,从而提高系统的安全性;中立方以普通用户为代表,通过访问网络资源影响网络的性能,将所有普通用户的统计特性看作一个整体.攻击方的目的是对网络造成最大的损害;防守方的目的相反;中立方只关心己方利益而不管网络状况,比如当发现某个服务器变慢或某条链路出现故障时,中立方可能避开受影响的节点或路径;

(2) 状态空间:$TPN(t)$的所有可能状态组成状态空间,k 时刻状态为 $TPN(t,k)=\{s^i(k),e^j(k)\}$.$i=1,2,\ldots,M$ 为 M 个传播节点,$j=1,2,\ldots,N$ 为 N 条传播路径, $s^i(k)=(id_i,value_{ai},\rho_{aik},t_{fik},v_{fik})$为第 i 个传播节点 k 时刻的状态, $e^j(k)=(id_{js},id_{jd},value_{ej},\rho_{ejk},p_{ej})$为第 j 条传播路径 k 时刻的状态;

(3) 行为空间(策略集):博弈三方所有可能的行为集合.攻击方行为 u^t 是威胁 t 的一步传播,t 以一定的概率按照 $TPN(t)$传播到系统的其他部分,每次只可能传播到当前感染节点的邻居节点;防守方行为 u^v 是管理员执行加固方案,每次只进行一步操作,包括修补某个脆弱性、切断某条传播路径或关闭某个网络节点;中立方行为 u^c 是普通用户访问量统计变化率的升降,简化为网络访问率提高 10%和降低 10%;

(4) 转移概率:随着博弈各方的行为选择,系统的状态不断变化,用 $p(TPN(t,k+1)\,|\,TPN(t,k),u_k^t,u_k^v,u_k^c)$ 描述系统状态变化规律,$TPN(t,k+1),TPN(t,k)$表示系统 $k+1$ 时刻、k 时刻系统的状态, u_k^t,u_k^v,u_k^c 为 k 时刻攻

© 中国科学院软件研究所 http://www.jos.org.cn

击方、防守方和中立方的行为,各方依据一定的概率在行为空间中选取相应的行为;

(5) 报酬函数:博弈结束后各方的得失.由于攻击方的目的是最大程度地对系统造成损害,其报酬用对系统的损害表示,包括对已经存在威胁的节点的一步损害和可能被感染节点的潜在损害;防守方的目的是最大程度地减轻系统损害,其报酬用管理员采取安全措施后所能减少的损害表示;中立方的目的是最大程度地使用网络资源,其报酬用所有普通用户对系统服务的利用程度表示.报酬函数是三方所选策略的函数,下面对博弈过程进行详细的分析得到三方的报酬函数.

2.2 博弈过程

博弈过程是各方参与者根据系统当前状态从行为空间中选取一个行为,然后系统转移到新的状态,参与者再根据新状态做决策,依此反复进行.下面分析在 k 时刻,对某个威胁 t,三方参与者选择行为的策略,并得到各方的一步报酬.在此基础上得到各方的报酬函数,参与者根据己方报酬函数的最大化选择策略.记 $TPN(t,k)=\{s^i(k),e^j(k)\}$为系统 k 时刻状态,$s^i(k)$为第 i 个传播节点 k 时刻的状态,$e^j(k)$为第 j 条传播路径 k 时刻的状态,$TPN(t,k+1)$为系统 $k+1$ 时刻的状态,系统的状态转移具有 Markov 性.

对于攻击方,t 属于不同类型的威胁时对系统的影响不同:对于第 1 类威胁,分别分析 t 对系统的保密性、完整性和可用性影响损害;对于第 2 类威胁,主要分析 t 对系统的可用性造成影响.

A. t 为第 1 类威胁时,t 对节点 i 的保密性、完整性和可用性均有损害,记为 $V^t(s^i(k))=p_t\cdot p_v\cdot(\mu\cdot value_{ai})$.其中,$p_t\cdot p_v$ 表示 t 对应的安全事件在 i 上发生的可能性,$\mu\cdot value_{ai}$ 表示该安全事件对 i 造成的安全性损害,μ 和 $value_{ai}$ 分别取其安全性各个对应分量.对 $TPN(t,k)$中所有节点按同样的方式计算,从而攻击方 t 的一步报酬用公式(1a)表示:

$$V_1^t(TPN(t,k))=\sum_{i\in\Phi_N}V^t(s^i(k)) \tag{1a}$$

B. t 为第 2 类威胁时,t 对节点 i 及其相关路径的可用性造成损害,对 i 可用性造成的损害为 $V^t(s^i(k))=p_t\cdot p_v\cdot\Delta\rho_{ai}\cdot value_{ai}$.其中,$p_t\cdot p_v$ 为 t 对应的安全事件在 i 上发生的可能性,$\Delta\rho_{ai}$ 为 t 对节点性能利用率的改变量,$value_{ai}$ 取节点可用性价值分量;对 i 相关路径可用性造成的损害为 $\sum_{j\in\Phi_i}V^t(e^j(k))$,其中,$V^t(e^j(k))=p_t\cdot p_v\cdot\Delta\rho_{ej}\cdot value_{ej}$ 为 t 对第 j 条路径的可用性损害.对 $TPN(t,k)$中所有节点及其相关路径按同样的方式计算,从而攻击方 t 的一步报酬用公式(1b)表示:

$$V_2^t(TPN(t,k))=\sum_{i\in\Phi_N}V^t(s^i(k))+\sum_{j\in\Phi_i}V^t(e^j(k)) \tag{1b}$$

其中,$i\in\Phi_N$ 表示受 t 影响的节点集,$j\in\Phi_i$ 表示节点 i 的相关路径集.

对于防守方,管理员对节点 i 实施安全措施会带来两方面的影响:减少威胁 t 的损害和影响网络性能.对网络可用性的影响包括安全措施对 i 节点可用性的影响 $V^v(s^i(k))=\Delta\rho_{ai}\cdot value_{ai}$,其中,$\Delta\rho_{ai}$ 为实施安全措施前后对节点性能利用率的改变量,$value_{ai}$ 取节点可用性价值分量;和对 i 相关路径的性能影响为 $\sum_{j\in\Phi_i}V^v(e^j(k))$,其中,$V^v(e^j(k))=\Delta\rho_{ej}\cdot value_{ej}$ 为对第 j 条路径的影响,$\Delta\rho_{ej}$ 为实施安全措施后前后对路径性能利用率的改变量,$value_{ej}$ 为该边的价值.安全措施减少 t 的损害与威胁类型有关:

A. t 为一类威胁时,减少 t 的损害为 $-V^t(s^i(k))$,从而,防守方的一步报酬用公式(2a)表示:

$$V_1^v(TPN(t,k))=-V^t(s^i(k))+V^v(s^i(k))+\sum_{j\in\Phi_i}V^v(e^j(k)) \tag{2a}$$

B. t 为二类威胁时,减少 t 的损害为 $-V^t(s^i(k))-\sum_{j\in\Phi_i}V^t(e^j(k))$,从而防守方的一步报酬用公式(2b)表示:

$$V_2^v(TPN(t,k))=-V^t(s^i(k))-\sum_{j\in\Phi_i}V^t(e^j(k))+V^v(s^i(k))+\sum_{j\in\Phi_i}V^v(e^j(k)) \tag{2b}$$

其中,$j\in\Phi_i$ 表示与节点 i 相关的路径集.

对于中立方,普通用户根据网络的延迟、服务的可访问性等改变访问率.中立方的一步报酬为 N 个节点和

© 中国科学院软件研究所 http://www.jos.org.cn

M 条路径的利用率之和,用公式(3)表示:

$$V^c(TPN(t,k))=\sum_{i=1}^{N}\rho_{ai}\cdot value_{ai}+\sum_{j=1}^{M}\rho_{ej}\cdot value_{ej} \tag{3}$$

威胁通过 $TPN(t,k)$向未感染的节点传播,根据公式(1a)、公式(1b)得到一类威胁的报酬函数,根据公式(2a)、公式(2b)得到二类威胁的报酬函数,统一用公式(4)表示:

$$R_*(TPN(t,k))=V_*^t(TPN(t,k))+V_*^v(TPN(t,k))+\beta\sum_{s(k+1)}p(TPN(t,k+1)\,|\,TPN(t,k),u_k^t,u_k^v,u_k^c)R(TPN(t,k+1)) \tag{4}$$

其中,*表示 1 或者 2;$\beta(0\leqslant\beta<1)$是折扣因子,描述将来威胁传播带来的潜在损害对当前损害的影响;$p(TPN(t,k+1)\,|\,TPN(t,k),u_k^t,u_k^v,u_k^c)$ 是状态转移概率.管理员通过相应的措施抑制威胁的传播,攻防双方的报酬函数近似认为相反,防守方报酬函数用$-R(s(k))$表示.

中立方根据当前的网络状况选择己方行为,报酬函数用公式(5)表示:

$$R^c(TPN(t,k))=V^c(TPN(t,k))+\beta^c\sum_{s(k+1)}p(TPN(t,k+1)\,|\,TPN(t,k),u_k^t,u_k^v,u_k^c)R^c(TPN(t,k+1)) \tag{5}$$

其中,β^c 是中立方折扣因子.

上述的博弈过程近似认为是三角色非零完全信息静态非合作博弈.下面以一个简单网络为例说明博弈过程,该网络具有 4 个节点和 5 条有向边.对该网络威胁集合的某个威胁 t,建立 t 的 TPN.博弈三方是威胁 t、管理员和普通用户,攻击方的行为是按照 TPN 向未感染的节点传播 t,防守方的行为是管理员修补系统节点上 t 利用的脆弱性,中立方的行为是普通用户增加或减少对该网络的访问率,系统状态是 t 对应 TPN 的所有可能的状态.博弈各方根据系统的状态和己方的报酬函数动态地选择己方行为,系统根据各方行为的影响以一定的概率跳转到下一状态,博弈过程如图 3 所示.

(1) k 时刻,只在节点 1 上检测到 t,系统处于状态 A;

(2) k+1 时刻,t 向节点 3 传播,管理员加固节点 3,普通用户访问率不变.系统如果跳转到状态 B,表示加固方案执行没有成功并且威胁成功传播;如果跳转到状态 C,表示加固方案执行成功或 t 在该方向传播失败;

(3) k+2 时刻,以状态 B 为例,t 向节点 2、节点 4、节点 1 传播,管理员加固节点 1,普通用户访问率不变.系统如果跳转到状态 D,表示威胁成功传播到节点 2 和节点 4,节点 1 加固方案执行成功或 t 在该方向传播失败.

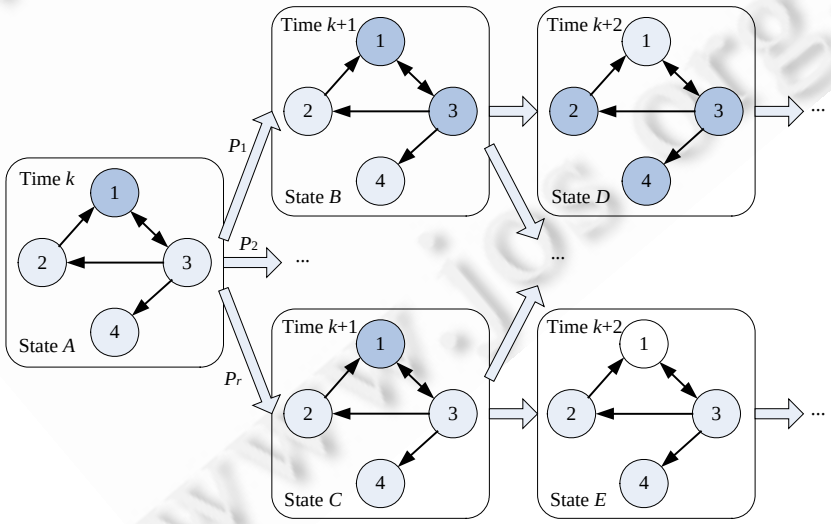

Fig.3 Sketch map of Markov game process

图 3 Markov 博弈过程示意图

© 中国科学院软件研究所 http://www.jos.org.cn

接下来,系统按照上述过程不断变化.对于有限步(*K* 步)博弈过程,从 *k* 时刻~*k*+*K* 时刻,系统的状态变化过程构成一个如图 3 所示的树形结构,每一条从根节点到叶节点的路径都是系统状态的可能的变化过程.*k* 时刻,各方的报酬函数为所有状态的报酬的综合.

2.3 用Markov博弈模型进行态势评估

对于威胁集合中的某个威胁 *t*,分析 *t* 对系统状态的影响,评估系统各个安全态势分量.安全态势评估过程评估系统安全性的最大损害值,此时管理员不采用任何安全措施,威胁对系统造成的损害最大,普通用户对系统的利用率最低,为系统最大损害评估.管理员生成加固方案时,威胁 *t* 按照 TPN 定义的路径传播,加固方案的目标是防守方和中立方的报酬函数最大化,为威胁最大损害情况下的防守方最佳加固方案,系统状态变化如图 4 所示.

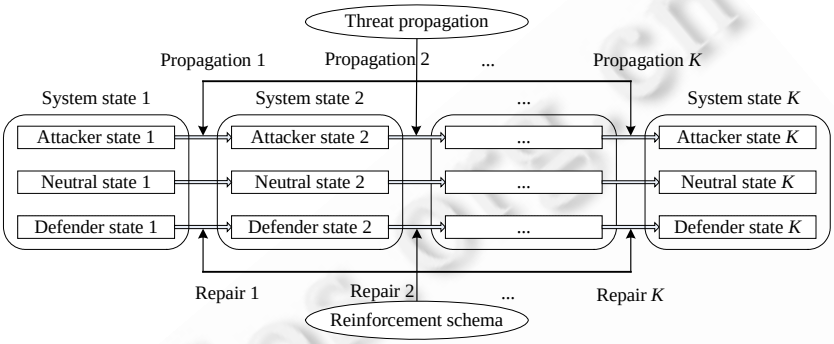

Fig.4 Sketch map of system state transformation

图 4 系统状态变化示意图

针对不同类型的威胁和不同类型的安全态势分量要分别分析.

(1) 系统 *k* 时刻,*t* 为一类威胁时,*t* 的保密性态势和完整性态势的评估方法类似,不计中立方行为的影响,用公式(6a)表示,相应的加固方案用公式(7a)表示:

$$R_{tk} = \max_{u^t}\{R_1(TPN(t,k))\} \tag{6a}$$

$$\pi(s(k)) = \arg\min_{u^v} \max_{u^t}\{R_1(TPN(t,k))\} \tag{7a}$$

(2) 系统 *k* 时刻,在对 *t* 的可用性态势评估时,需要考虑中立方行为的影响,并且需要区分 *t* 属于不同类型的威胁,可用性态势用公式(6b)表示,相应的加固方案用公式(7b)表示.其中,*表示 1 或者 2:

$$R_{tk} = \max_{u^t,u^c}\{R_*(TPN(t,k)) - R^c(TPN(t,k))\} \tag{6b}$$

$$\pi(s(k)) = \arg\min_{u^v} \max_{u^t,u^c}\{R_*(TPN(t,k)) - R^c(TPN(t,k))\} \tag{7b}$$

2.4 态势评量化估算法

网络安全态势评估算法主要包括 3 个步骤:检测数据融合、威胁传播网络(TPN)建立、Markov 博弈模型评估.整个算法流程见算法 1.

算法 1. 网络安全态势量化评估算法.

输入:数据采集模块检测到的各类安全数据;

输出:网络安全态势.

1. 对检测模块测得得安全数据进行融合,得到资产集合、威胁集合、脆弱性集合和网络结构信息;
2. 根据检测模块得到的网络信息,综合资产集合、威胁集合和脆弱性集合,对威胁集合中每个威胁 *t* 建立该威胁的威胁传播网络 *TPN*(*t*);
3. 根据 *TPN*(*t*),对 *t* 建立 Markov 博弈模型,计算 *t* 的保密性损害,评估 *t* 的保密性态势;
4. 根据 *TPN*(*t*),对 *t* 建立 Markov 博弈模型,分析管理员应对 *t* 保密性损害的最佳加固方案;

© 中国科学院软件研究所 http://www.jos.org.cn

5. 按照步骤(3)、步骤(4)类似的方法,评估 t 的完整性态势和可用性态势,并分析相应的最佳加固方案;
6. 将威胁集合中所有威胁的保密性损害求和,评估网络保密性态势;
7. 按照步骤(6)同样的计算方法,评估系统的完整性态势和可用性态势;
8. 根据不同应用需求,采用加权模型评估网络的整体安全态势.

在算法 1 中,根据 $TPN(t)$建立 Markov 博弈模型的第 3 步、第 4 步是整个态势评估算法的核心.在这里,采用有限阶段的值迭代算法.考虑 K 步以内的系统状态变化,在实际应用中,K 根据算法效率和评估效果来定,一般 K 取值小于 $TPN(t)$的直径.下面以保密性分析为例,子算法 2 给出保密性态势评估的流程,子算法 3 给出对应情况下最佳加固方案生成的流程.

子算法 2. 单个威胁保密性态势评估算法.

输入:威胁集合中某个威胁的 $TPN(t)$;

输出:该威胁保密性态势.

A. 令 $k=K$,取 $R(TPN(t,K+1))=0$,$R^c(TPN(t,K+1))=0$, $u_k^t=0$;
B. 如果 $k=0$,则跳转到步骤 E;否则,令 $k=k-1$ 后进入下一步;
C. 对每个 TPN 状态和每个历史依次计算公式(4);
D. 返回步骤 B;
E. 该威胁保密性态势按照公式(6a)计算输出.

子算法 3. 单个威胁的保密性最佳加固方案生成算法.

输入:威胁集合中某个威胁的 $TPN(t)$;

输出:防守方对最大损害的最佳加固方案.

A. 令 $k=K$,取 $R(TPN(t,K+1))=0$,$R^c(TPN(t,K+1))=0$;
B. 如果 $k=0$,则跳转到步骤 E;否则,令 $k=k-1$ 后进入下一步;
C. 对每个 TPN 状态和每个历史依次计算公式(4);
D. 返回步骤 B;
E. 防守方最佳加固方案按照公式(7a)生成输出.

在算法 1 中,第 6 步对威胁集合中所有威胁的保密性态势求和得到网络保密性态势.由于两个低等级安全事件的整体损害没有一个高一级安全事件的损害大,这里的求和不能简单地线性相加,我们采用指数求和的方法[22],

$$R_{Ck}=\log_B \sum_{t\in Therats} B^{R_{Ctk}} \tag{8}$$

其中,B 是基数,根据资产、威胁和脆弱性的等级关系[16],取 $B=5$.

在算法 1 中,第 5 步和第 7 步采用类似的分析方法,求得网络 k 时刻完整性态势 R_{Ik} 和可用性态势 R_{Ak}.不同的应用背景对网络的保密性、完整性和可用性的要求不一样,比如对于政府机关来说,保密性是最重要的;对银行部门来说,完整性是至关重要的,而诸如 VOD 的娱乐行业则最关心可用性.因此,算法 1 的第 8 步采用公式(9)加权评估方法,根据不同的加权参数,评估不同应用需求下的系统安全态势:

$$R_k=R_{Ck}\cdot w_C+R_{Ik}\cdot w_I+R_{Ak}\cdot w_A \tag{9}$$

其中,w_C,w_I,w_A 为保密性、完整性和可用性权重.

3 实验分析

3.1 网络安全态势感知的应用

为了阐明威胁传播分析的原理、验证网络安全态势感知模型设计的合理性、演示基于 Markov 博弈分析的态势评估过程,本文给出态势感知系统在一个具体公司网络测评中的应用,网络主要结构如图 5 所示.网络中的 FTP 和 HTTP 两个服务器通过交换机放置在 DMZ 区;内网办公区主机由交换机划分为 2 个 VLAN,并与外界

© 中国科学院软件研究所 http://www.jos.org.cn

通过防火墙相隔离.远程办公室主机经交换机相连后远程访问公司网络,NetScreen204 是带防火墙的路由器,Internet 用户通过该路由器访问公司网络资源,整个公司部署一个硬件 IDS.

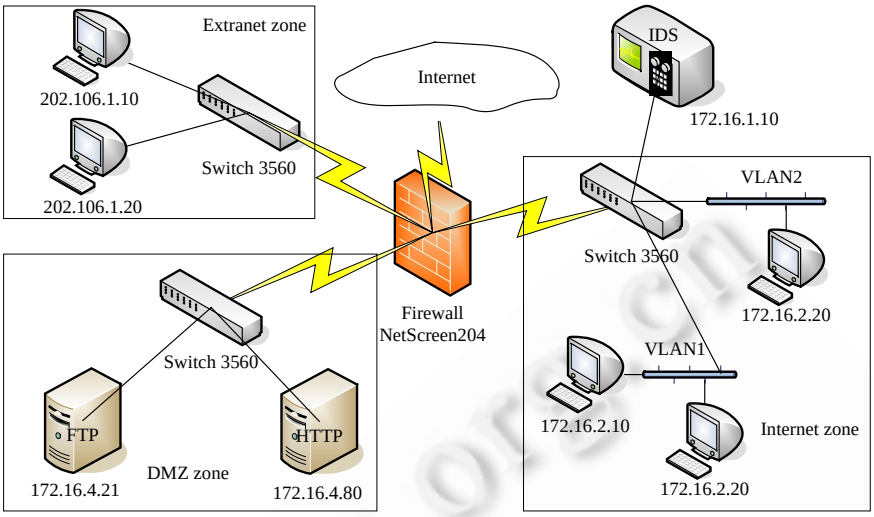

Fig.5 Structure of network system for evaluation

图 5 待评估的网络系统结构

态势感知系统首先进行安全数据检测,包括对每个网络节点部署资产识别,对每个主机和两个服务器部署恶意代码检测和脆弱性扫描,对 IDS、防火墙、路由器和交换机部署渗透测试和在线测试,同时收集 IDS 报警日志数据;接着,根据检测数据融合得到资产集合、威胁集合、脆弱性集合.然后,对威胁集合中的每个威胁建立 TPN,根据 TPN 建立 Markov 博弈模型,分析威胁的安全态势;最后,由每个威胁的安全态势评估网络安全态势.下面以威胁集合中的某个威胁 t 的保密性态势评估过程为例进行描述.

首先建立威胁 t 的 TPN,如图 6 所示,传播节点和传播路径由检测模块测得.

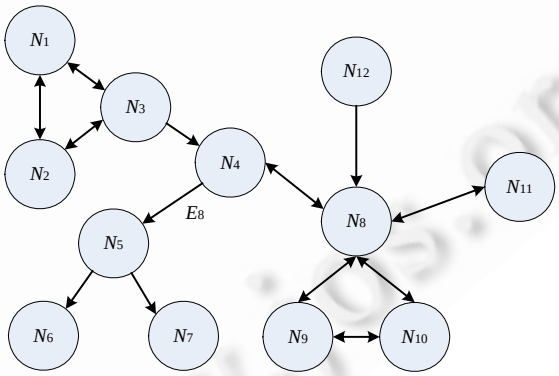

Fig.6 TPN of threat t

图 6 威胁 t 的 TPN

传播节点的状态见表 1,资产的保密性价值和资产的性能利用率均以等级的形式表示.例如,$N_4(N_4,5,4,0,1)$ 节点表示路由防火墙保密性价值很高,被成功入侵后造成的保密性损害很大.目前的性能利用率在 10%~30%之间,还未感染威胁 t,但是存在 t 利用的脆弱性.

© 中国科学院软件研究所 http://www.jos.org.cn

Table 1 State of propagation nodes of threat *t* (partly show)

表 1 威胁 *t* 传播节点的状态(部分显示)

ID	ValueOfC	Efficiency	ThreatOrNot	VulOrNot
N_1	1	1	1	1
N_2	1	1	0	1
N_3	2	2	0	1
N_4	5	4	0	1
N_5	3	2	1	0
N_6	5	3	0	1

传播路径的状态见表 2,路径的价值以等级的形式表示切断该条路径后造成的损失;路径性能利用率与资产性能利用率也类似地分为 5 个等级;威胁通过该传播路径成功传播的概率也分 5 个等级.例如,$E_8(N_4,N_5,5,4,2)$路径表示威胁 *t* 以 20%~40%的概率通过该路径从节点 4 传播到节点 5,该路径非常重要,如果切断对网络造成很大损害,该路径目前处于 10%~30%的利用率.

Table 2 State of propagation paths of threat *t* (partly show)

表 2 威胁 *t* 传播路径的状态(部分显示)

IDS	IDD	ValueOfPath	Efficiency	Probability
N_1	N_3	1	1	4
N_3	N_1	1	1	4
N_3	N_4	3	2	1
N_4	N_5	5	4	2
N_5	N_6	5	3	2
N_5	N_7	5	3	2

接着建立威胁 *t* 的 Markov 博弈模型,攻击方为威胁 *t*,动作为通过 TPN 进行传播;防守方为系统管理员,动作为修复 TPN 中传播节点上的脆弱性或切断 TPN 中某条传播路径;中立方为所有普通用户的统计特性,状态转移概率矩阵可以根据各方动作影响确定.

最后,利用 Markov 博弈模型评估威胁 *t* 的保密性态势(子算法 2).以同样的方法评估威胁集合中所有威胁的保密性态势,并按照公式(8)和公式(9)的方法通过加权求和,得到网络安全态势.图 7 为模型对系统保密性态势评估和预测,包括采用基于传播分析的 Markov 博弈模型评估结果和未考虑威胁传播的静态评估结果.

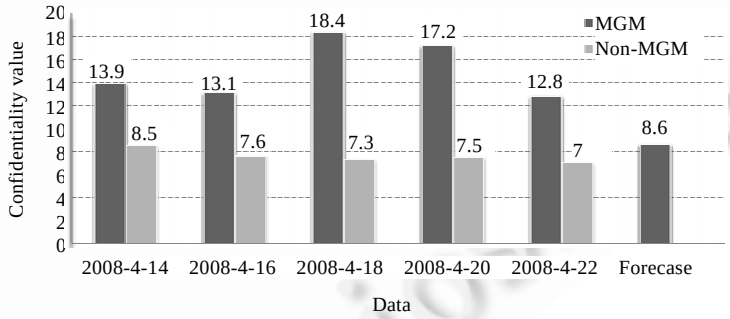

Fig.7 Situation evaluation and forecasting of confidentiality

图 7 保密性态势评估与预测

同时,采用子算法 3 得到应对 *t* 保密性损害的最佳加固方案.以同样的方法,威胁集合中的每个威胁找出应对该威胁保密性损害的最佳加固方法.图 8 为测评系统提供的针对保密性损害的加固方案.

© 中国科学院软件研究所 http://www.jos.org.cn

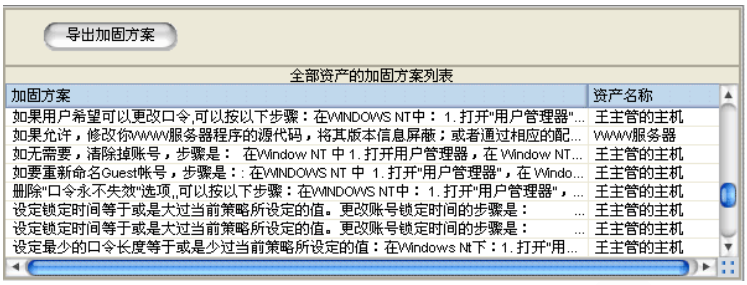

Fig.8 Reinforcement of confidentiality

图 8 保密性加固方案

3.2 优势分析及性能优化

通过上述测评过程的分析可以发现,本文提出的网络安全态势感知模型具有下列优点:

(1) 评估数据来源丰富,采用的多种异构检测模块从多个侧面检测网络的安全因素;

(2) 采用基于 Markov 博弈分析的态势评估算法,增加了对威胁传播分析和对普通用户行为影响分析.比起将各个网络节点孤立的静态分析,能发现系统的潜在危害,更贴近实际;

(3) 采用基于 Markov 博弈分析的安全加固方案生成算法,对威胁传播和普通用户行为动态分析,找到危害程度最大的节点和路径,给出最佳加固方案;

(4) 对不同类型的威胁区别对待,从保密性态势、完整性态势和可用性态势 3 个方面评估系统的安全态势,评估结果细致全面,针对性强.

此外,本文提出的基于 Markov 博弈模型的分析方法考虑了攻击方、防守方和中立方三方的博弈过程,在建立 TPN 的时候考虑了传播节点和传播路径的双重影响,因此在做决策时状态空间会很大.在执行子算法 2 和子算法 3 的迭代时,将会耗费大量的资源.尤其在网络的节点和路径较多时,很难做到实时评估分析,需要考虑性能优化,性能优化主要从以下两个方面分析:

(1) 博弈模型的状态空间随着资产数量的增加而指数增加,当网络的资产数量很多时,首先进行资产缩减,合并一些连接紧密功能相似的节点,剔除一些影响不大的资产;

(2) 评估过程对每个威胁都要建立博弈模型,同一个威胁可能在多次评估时遇到.每一次的博弈模型是相似的,可将每个威胁对目标网络的每个可能状态的一步损害静态地存储,在每次评估时通过查表的方式取得;以类似的方式将管理员每个行为对目标网络的每个可能状态的一步报酬静态地存储,在评估时通过查表方式获取,虽然增加了存储空间的损耗,但是提高了算法的执行速度,能够做到实时评估.

本文在实现态势感知系统时采用这两种优化方法,评估时间得到有效控制,做到了实时评估分析.

4 结 论

本文系统分析了目前存在的网络安全态势感知算法,提出一种基于 Markov 博弈分析的网络安全态势感知模型及其实现方法.以威胁传播分析为基础,以威胁、管理员、普通用户三方博弈为核心,综合分析三方行为选择对网络安全的动态影响,并给出最佳加固方案.并根据态势感知模型实现了相应的态势感知系统,对有关的算法进行了优化分析,使得测评过程能够实时运行.通过对目标网络的测评分析发现,基于 Markov 博弈分析的态势评估过程能够很好地描述资产、威胁的脆弱性的定量关系,评估结果全面、客观、准确,提供的安全加固方案能很好地找到针对某个威胁危害程度最大的节点和路径,有效地抑制了威胁的扩散,提高了系统的安全性.

本文建立的 Markov 博弈模型还存在一些问题:首先,状态空间很大,对大规模网络的评估效率低,需要一定的近似处理;其次,本文只讨论了最大最小策略下的态势评估过程和加固方案生成过程,接下来需要对混合策略的均衡做深入讨论,并比较不同策略下系统的均衡状态;最后,模型的各个参数需要在真实的网络环境中不断地

© 中国科学院软件研究所 http://www.jos.org.cn

测试和完善,最终建立适合多个行业需要的网络安全态势感知系统.

致谢 真诚感谢各位指导老师对本文提出的宝贵意见.

References:

[1] Endsley MR. Situation awareness global assessment technique, In: NAECON, ed. Proc. of the IEEE '88 National Aerospace and Electronics Conf. (NAECON'88). Dayton: IEEE, 1988. 789−795.

[2] Bass T, Gruber D. A glimpse into the future of ID. http://www.usenix.org/publications/login/1999-9/features/future.html

[3] Bass T. Intrusion detection systems and multi-sensor data fusion: Creating cyberspace situation awareness. Communications of the ACM, 2000,43(4):99−105. [doi: 10.1145/332051.332079]

[4] Stephen L. The spinning cube of potential doom. Communications of the ACM, 2004,47(6):25−26. [doi: 10.1145/990680.990699]

[5] Lakkaraju K, Yurcik W, Lee AJ. NVisionIP: NetFlow visualizations of system state for security situational awareness. In: Proc. of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security. 2004. 65−72. [doi: 10.1145/1029208.1029219]

[6] Yin XX, William Y, Michael T. VisFlowConnect: NetFlow visualizations of link relationships for security situational awareness. In: Proc. of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security. 2004. 26−34. [doi: 10.1145/1029208.1029214]

[7] AS Internet Graph. http://www.caida.org/research/topology/as_core_network/AS_Network.xml

[8] Steinberg AN, Bowman CL, White FE. Revisions to the JDL data fusion model. In: SPIE, ed. Proc. of the Sensor Fusion: Architectures, Algorithms, and Applications, SPIE 3719. Orlando: SPIE, 1999. [doi: 10.1117/12.341367]

[9] Endsley MR. Toward a theory of situation awareness in dynamic systems. Human Factors Journal, 1995,37(1):32−64. [doi: 10.1518/001872095779049543]

[10] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. Journal of Software, 2006,17(4):885−897 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/885.htm [doi: 10.1360/jos170885]

[11] Hu W, Li JH, Shi JJ. A novel approach to cyberspace security situation based on the vulnerabilities analysis. In: WCICA, ed. Proc. of the 6th World Congress on Intelligent Control and Automation. 2006. [doi: 10.1109/WCICA.2006.1713284]

[12] Zhao GS, Wang HQ, Wang J. Study on situation evaluation for network surivability based on grey relation analysis. MINI-MICRO Systems, 2006,27(10):1861−1864 (in Chinese with English abstract).

[13] Seddigh N, Pieda P, Matrawy A, Nandy B, Lambadaris J, Hatfield A. Current trends and advances in information assurance metrics. In: Proc. of the 2nd Annual Conf. on Privacy, Security and Trust. 2004. 197−204.

[14] Zhang Y, Tan XB, Xi HS. A novel approach to network security situation awareness based on multi-perspective analysis. In: Proc. of the 2007 Int'l Conf. on Computational Intelligence and Security (CIS 2007). 2007. 768−772. [doi: 10.1109/CIS.2007.160]

[15] Zhang YZ, Fang BX, Chi Y, Yun XC. Risk propagation model for assessing network information systems. Journal of Software, 2007,18(1):137−145 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/137.htm [doi: 10.1360/jos180137]

[16] GB/T 20984-2007. Information security technology — Risk assessment specification for information security. General Administration of Quality Supervision, Inspection and Quarantine of P.R.C, 2007 (in Chinese).

[17] Hou GM, Li CJ. Managerial Game Theory. Beijing: Beijing Institute of Technology Press, 2004 (in Chinese).

[18] Liu K. Applied Markov Decision Processes. Beijing: Tsinghua University Press, 2004 (in Chinese).

[19] Sallhammar K, Knapskog SJ, Helvik BE. Using stochastic game theory to compute the expected behavior of attackers. In: Proc. of the 2005 Symp. on Applications and the Internet Workshops. 2005. [doi: 10.1109/SAINTW.2005.1619988]

[20] Shen D, Chen G, Cruz JB, Haynes JL, Kruger M, Blasch E. A Markov game theoretic approach for cyber situational awareness. In: Dasarathy BV, ed. Proc. of the Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Vol.6571, 65710F. 2007.

[21] Cui XL, Tan XB, Zhang Y, Xi HS. A Markov game theory—Based risk assessment model for network information system. In: Proc. of the 2008 Int'l Conf. on Computer Science and Software Engineering. 2008. [doi: 10.1109/CSSE.2008.949]

© 中国科学院软件研究所 http://www.jos.org.cn

[22] Tan XB, Qin GH, Zhang Y, Liang P. Network security situation awareness using exponential and logarithmic analysis. In: Proc. of the 5th Int'l Conf. on Information Assurance and Security. 2009. 149−152. [doi: 10.1109/IAS.2009.38]

附中文参考文献:

[10] 陈秀真,郑庆华,管晓宏,林晨光.层次化网络安全威胁态势量化评估方法.软件学报,2006,17(4):885−897. http://www.jos.org.cn/1000-9825/17/885.htm [doi: 10.1360/jos170885]

[12] 赵国生,王慧强,王健.基于灰色关联分析的网络可生存性态势评估研究.小型微型计算机系统,2006,27(10):1861−1864.

[15] 张永铮,方滨兴,迟悦,云晓春.用于评估网络信息系统的风险传播模型.软件学报,2007,18(1):137−145. http://www.jos.org.cn/1000-9825/18/137.htm [doi: 10.1360/jos180137]

[16] GB/T 20984-2007.信息安全技术——信息安全风险评估规范.国家质量监督检验检疫总局发布,2007.

[17] 侯光明,李存金.管理博弈论.北京:北京理工大学出版社,2004.

[18] 刘克.实用马尔可夫决策过程.北京:清华大学出版社,2004.

张勇(1984－),男,安徽阜阳人,博士生,主要研究领域为网络安全,风险评估,安全性分析.

崔孝林(1981－),男,硕士生,主要研究领域为网络态势评估,网络风险评估.

谭小彬(1973－),男,博士,副教授,主要研究领域为网络安全,入侵检测,安全评估.

奚宏生(1951－),男,教授,博士生导师,主要研究领域为离散事件动态系统,信息网络性能分析与优化.

© 中国科学院软件研究所 http://www.jos.org.cn