基于动态系统画像的漏洞风险遏制方案研究

Research on Vulnerability Risk Containment Scheme Based on Dynamic System Security Portrait

杨丽丽[1]，刘　果[1]，李发财[2]，戚大强[1]，张　彬[1]，高贯银[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Yang Lili[1]，Liu Guo[1]，Li Facai[2]，Qi Daqiang[1]，Zhang Bin[1]，Gao Guanyin[1]（1. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China；2. China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：

针对信息系统漏洞的直接修复方案带来的一系列问题，提出了基于动态系统画像的漏洞风险遏制方案。方案通过对系统资产以及漏洞的统一管控，分析漏洞的风险以及风险路径，对系统的风险进行动态画像。针对画像中的风险以及风险路径，结合修复操作、风险影响面进行决策分析，形成从风险控制到消除的一组风险遏制方案。再通过运维人员对方案的实施，完成画像中风险点的消除，形成对风险的一套闭环管理方案。

关键词：

系统安全画像；决策分析；风险遏制；动态调整

doi：10.12045/j.issn.1007-3043.2022.09.005

文章编号：1007-3043（2022）09-0019-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In view of the series of drawbacks brought by the direct repair scheme for information system vulnerabilities，it proposes a vulnerability risk containment scheme based on dynamic system security portrait.Through the unified management of the system's assets and vulnerabilities，the scheme analyzes the risks and risk paths of the vulnerabilities，and dynamically profiles the risks of the system. According to the risks and risk paths in the portrait ，and combined with the repair operation and risk impact surface，the decision-making analysis is made，which forms a set of risk containment schemes from risk control to elimination. Then through the implementation of the scheme by the operation and maintenance personnel，the elimination of the risk points in the portrait is completed，and a set of closed-loop management schemes for risks is formed.

Keywords：

System security portrait；Decision analysis；Risk containment；Dynamic adjustment

引用格式：杨丽丽，刘果，李发财，等. 基于动态系统画像的漏洞风险遏制方案研究[J]. 邮电设计技术，2022（9）：19-23.

0　前言

随着信息技术产业的蓬勃发展，信息系统的软硬件也不断涌入互联网，由此产生的软硬件漏洞以及公网暴露面给信息系统带来了诸多安全风险。轻者使得系统信息被泄露，重者导致系统被控制，甚至使整个系统以及网络瘫痪。

面对漏洞的诸多安全威胁，信息系统的漏洞修复一直是各主体单位的重点关注对象，但是目前漏洞的闭环管理工作大部分还是以漏扫工具和人工修复判断为主。一般通过漏扫发现漏洞，经过维护人员的评估，在业务闲时对其进行修复，漏洞的评估和修复通常以一个独立的漏洞孤岛来看待。这种模式能从根本上解决漏洞本身的风险，但也存在很多弊端，比如，带来系统可用性以及兼容性问题，修复操作以及修复效果不透明，修复方案的移植性较差，运维人员需要全面了解业务环境的相关性以及漏洞的危害。

从以上场景看，为了减小和防范系统漏洞风险，需要高度依赖人工经验，这不可避免地带来一些其他负面问题。通过一些技术手段对系统的基本信息进

收稿日期：2022-07-14

行统一管理，结合漏洞扫描、渗透测试等技术，动态地发现漏洞以及漏洞被利用的风险；之后，通过对漏洞的风险评估和业务影响的决策分析，形成从路径阻断到完全修复的过渡方案，实现系统在安全性和可用性方面的平衡，降低因片面的漏洞评估产生的负面影响。从该角度出发，提出基于动态系统画像的漏洞风险遏制方案。

1 整体方案

本方案是以信息系统的资产管理为脉络，通过动态调度漏扫、渗透测试、攻防专家经验库为系统进行安全画像，安全画像主要暴露系统漏洞引入的风险点以及可能利用的风险路径。经过对画像中风险阻断以及系统的业务影响决策，产生适用于当下的风险遏制操作，经过遏制策略以及动态分析的迭代调整，逐步完成漏洞根本问题的修复，从而使系统安全画像的风险点位处于收敛趋势。整体方案如图1所示。

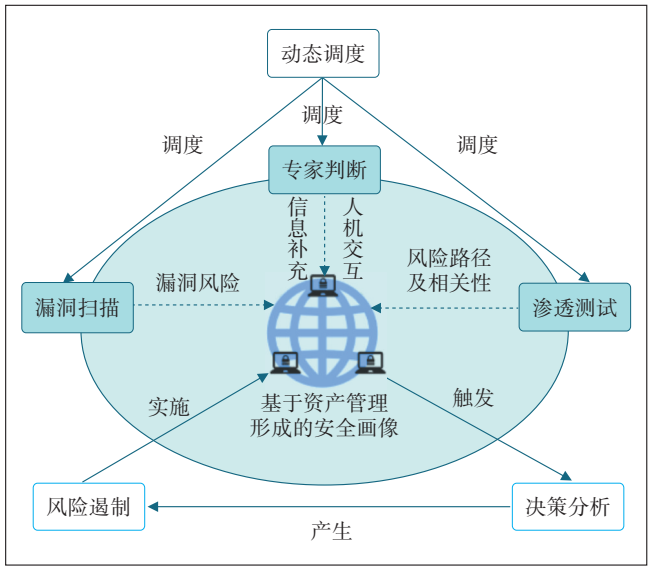

图1　整体方案示意图

其中，资产管理的安全画像为动态计算的过程，随着资产管理内的资产范围、边界以及漏洞库等因素的变化，自动触发评估工具，从而更新安全画像的信息。随着安全画像中的新风险暴露，自动触发决策分析，通过决策分析得到是否产生新的风险遏制手段以及可能的影响范围。风险的遏制策略在决策分析中需要综合考虑对系统业务可用性以及当前威胁的程度。随着风险遏制策略的实施，安全画像的整体风险会减小。

就方案的设计思路（见图2）做如下介绍。

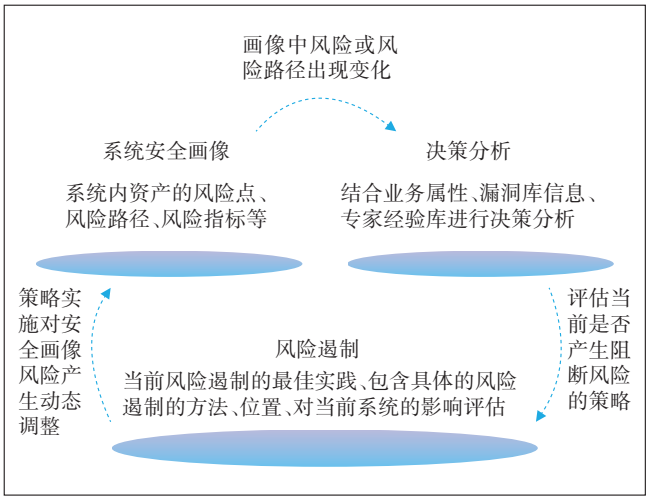

图2　方案的设计思路

a）系统安全画像是将系统内资产的漏洞风险进行统一管理，除了单个资产的漏洞风险，还对漏洞风险的影响面进行评估，从而建立资产与资产之间的风险关键路径。资产管理的基础信息（操作系统、软件版本、业务属性）、网络拓扑、安全边界等为系统安全画像的过程提供了基本的数据支撑，同时也为下一步的决策分析提供了全面的分析维度。

b）决策分析是针对系统安全画像的风险以及风险的影响路径进行全端点、全路径覆盖分析，通过加入风险权重、资产的保护等级、业务影响的接受程度、业务闲时/忙时的数据统计等多因素进行决策，生成针对客观条件下业务影响范围最小、风险阻断效率较高的风险遏制策略。该策略包含按不同时段、不同优先级的多项操作步骤，为系统运维人员的操作提供详细指南。

c）风险遏制是运维人员按照决策分析结果进行风险遏制的实施环节。运维人员通过选择系统安全画像的风险点或者风险路径进行实施，操作完成后相应的风险点以及路径在安全画像上随之消失或风险处于减小趋势，修复效果在系统画像中得到充分体现。

以上3个环节从风险的发现评估、遏制策略分析和策略实施操作对漏洞风险进行了有效的闭环管理。同时，随着调度算法的调优将会极大地提高系统漏洞风险的暴露速度以及系统画像的准确度，策略分析算法的优化将逐步降低策略建议的复杂度并减少无效操作。

2 详细设计

2.1 系统安全画像

系统安全画像是以资产管理为基础，加入对资产的漏洞动态评估过程，利用知识图谱技术将资产漏洞评估产生的安全风险以及风险发生的相关路径进行关系定义而形成的一张系统安全全景图。采用知识图谱直观地呈现资产与风险，资产与资产，风险与风险的关系网络。在图谱中的每一个资产的安全风险的评估结果都不是独立产生的，其需要从关系网中的相互影响评估获得。系统安全画像示意图如图3所示。

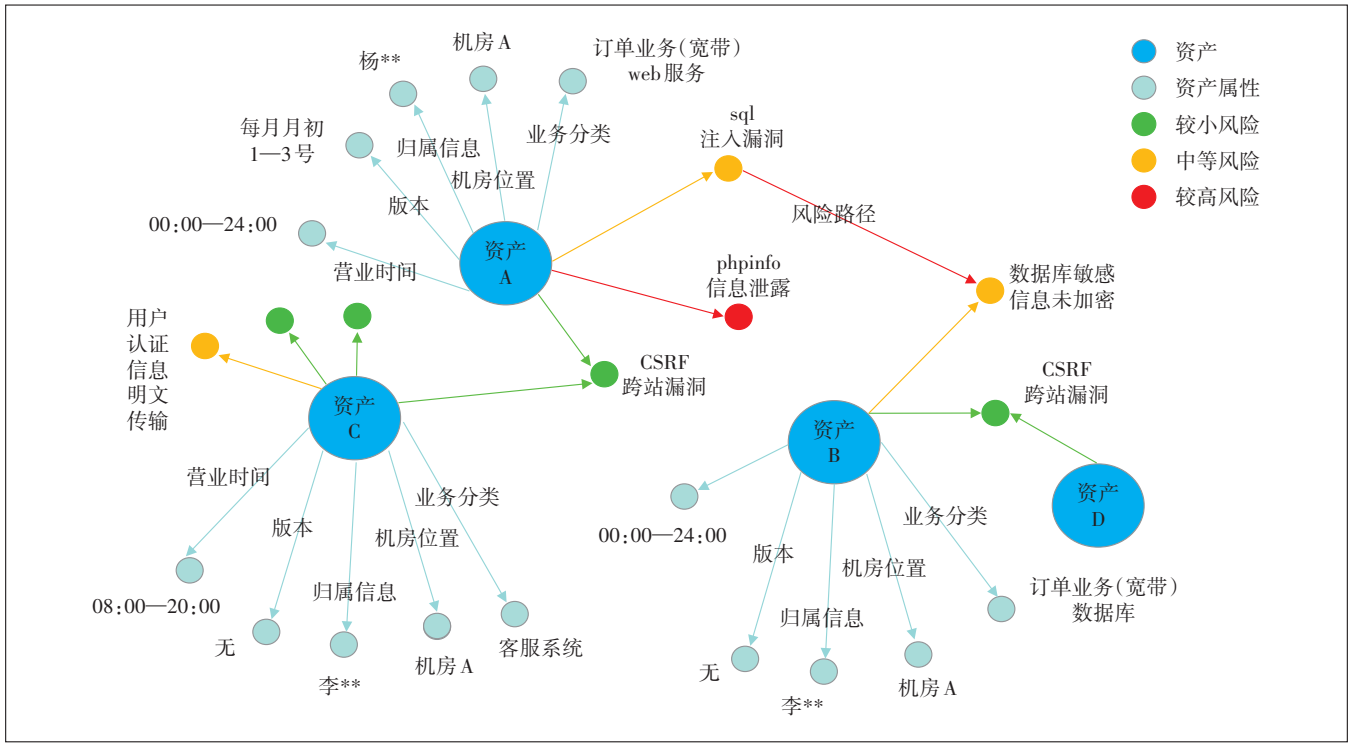

图3　系统安全画像示意图

2.1.1 目标

a）建立基于系统的知识图谱体系，为系统安全画像提供风险附着点、风险影响路径、风险严重程度的可视化，方便系统运维人员对系统安全概况进行全局了解。

b）通过资产变化以及资产关联关系的变化，动态调度检测工具对资产进行实时评估和数据收集，使系统安全画像的时效性得到保障。

c）对系统安全画像中的风险进行全流程闭环管理，方便回溯系统漏洞从发现到遏制过程的合理性和有效性，为系统安全画像以及决策分析提供评价指标。

2.1.2 设计方法

系统安全画像的形成大致总结为以下4个环节，如图4所示。

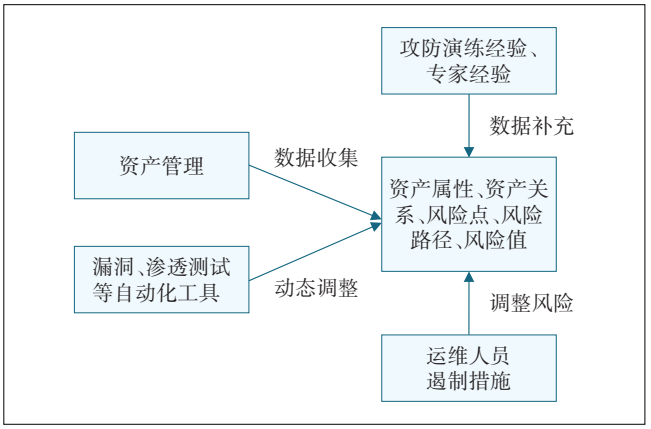

图4　系统安全画像过程

a）资产管理的数据收集阶段。通过系统历史台账、资产发现工具、开放录入渠道等作为系统资产搜集的来源，搜集的资产属性主要包含业务属性、网络拓扑、安全策略信息、资产保护等级等。以上属性中网络拓扑和安全策略信息会在系统画像建立知识图

谱的过程中发挥重要作用，由于网络的连接以及安全策略的开放，不同资产的漏洞可能会被联合利用或者迭代利用，从2个低危漏洞演变成系统的1个高危风险。而业务属性（业务闲时/忙时、业务的功能属性、迭代版本时间等）、资产等级保护等会在决策分析环节起关键作用。

b）系统安全画像的数据形成。资产范围的新增会自动触发漏洞检测工具和自动化渗透测试工具的动态调度。从漏洞扫描中获得单个资产的漏洞信息以及指纹信息，完成对单个漏洞或资产的风险评估。通过渗透测试对漏洞的利用价值进行评估，生成系统可能被攻击的路径以及漏洞利用的路径。在此过程中，通过对漏洞的组合利用和关联分析，可以形成新的风险点。在系统渗透的过程中根据漏洞的利用价值给予攻击路径一定的权重信息，该权重直观地反映了风险的严重程度。通过知识图谱对上述基础信息以及风险信息进行组织，形成具有关联关系的网络图谱。

c）系统安全画像的数据补充。通过系统定期的攻防演练，收集攻防专家经验以及成果，加强系统安全性。虽然此种活动的持续性较低，但对系统的安全性提升会有较大突破，尤其是系统风险点以及风险路径的发现得到进一步丰富，使系统的安全画像更具真实性。

d）系统安全画像的风险闭环管理。运维人员基于安全画像的风险点或风险路径进行相应的风险遏制操作。随着操作的实施，画像中风险点以及风险路径的权重会随之减弱或消除。直到一系列的风险遏制策略实施完成，风险点会从安全画像中消失，从而实现风险闭环管理。查看资产管理节点时可查看该资产出现的所有历史风险遏制操作数据。

2.2 决策分析

2.2.1 目标

决策分析基于系统安全画像中的多维属性，通过决策算法规划出从控制风险到消除风险的一些遏制点，同时动态调度安全策略知识库，提取针对风险或风险路径的最优遏制方法，经过遏制点和遏制策略的组合生成一组遏制策略方案。

2.2.2 设计方法

决策分析的建模环节大致需要经过以下4个步骤，如图5所示。

a）识别系统安全画像中参与决策分析的属性，比

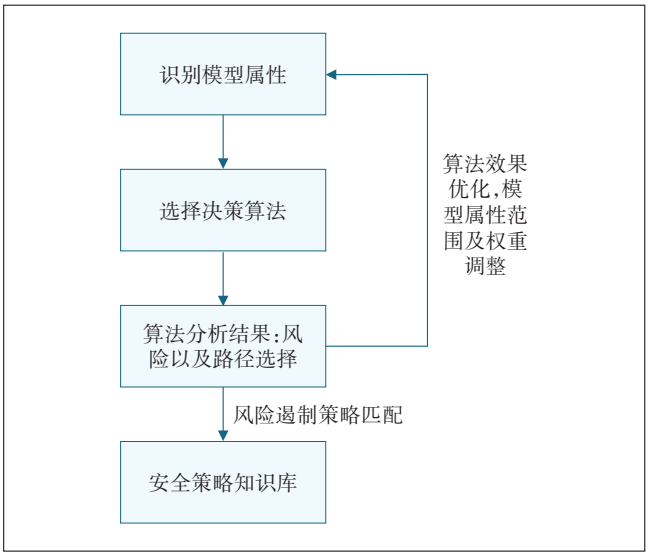

图5　决策分析过程

如重点关注的风险点、风险关联路径及权重、风险值、系统业务属性、资产保护等级等属性。随着模型的训练，根据属性在模型中的贡献度调整模型涉及的属性范围。

b）建立决策算法，优先采用加权决策树预测每一个风险决策路径的结果，决策树的路径选择方法是模拟人工判断风险决策的过程。决策树中的叶子节点即为每一个风险点或风险路径，而其他属性即为子节点的特征。对于决策算法中的已知风险，风险的相关特征相对比较稳定，决策算法的预测结果会比较准确。而对于新的未知风险，影响因素的特征值估算不准可能会对模型造成干扰，将列入异常边界数据进行处理。随着不断的测量，将未知风险转化为已知风险，从而提高算法的预测准确度。

c）决策算法中针对一个节点（即风险）出发进行计算，得到每一轮决策的最佳的阻断方案。而对于同一风险，其起始决策结果很大程度对业务的特征依赖度较高，故从风险的角度只是减小漏洞最大可能利用的概率，大概率并未根除。随着决策路径覆盖范围变广，待参与决策树的路径变短以及噪声数据的减少，消除风险方案的形成也趋于稳定和集中，风险的消除方案必然会产生。

d）建立决策分析中的安全策略知识库，决策分析的过程需要依赖调度对应风险的安全策略知识库。该知识库收集了大量的风险类型的控制和消除方案，一般来自于官方漏洞库的解决方案和系统维护人员处置风险的经验积累。

2.3 风险遏制

2.3.1 目标

风险遏制是基于决策分析产生的策略方案，运维人员进行实施操作的过程，此过程在遏制风险的同时，快速提升运维人员对系统架构的熟悉程度。而人工对策略方案的分析，可能找到更加合理的策略方案，从而有利于系统的回归优化。

2.3.2 设计方法

风险遏制的实施过程及对整体方案的影响如图6所示。

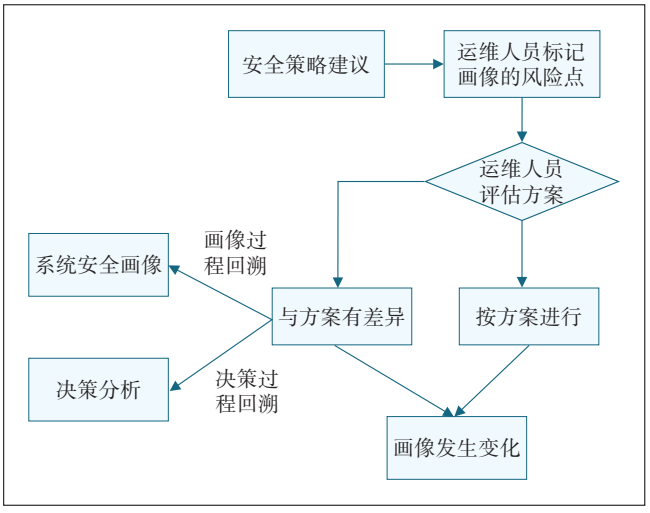

图6　风险遏制过程及影响

a）系统运维人员根据遏制风险策略方案，基于系统画像找到操作的风险点或风险路径，实施对画像中对应风险点的标记操作。

b）标记的风险点自动触发画像的触点关联性重评估，评估运维人员实施效果有效性。如运维人员误操作，风险遏制并未达到预期效果，此时在画像中给予特殊标记提醒。如运维人员的操作达到效果，但与推荐方案预期不符，则系统记录差异。如运维人员操作方案以及结果与模型相符，则对应的风险点从画像中消失，该风险点的处置处于闭环状态。

c）风险遏制的操作结果即为对系统整体流程的验证环节，验证漏洞风险以及路径设计的合理性，以及策略规划的有效性。

3 总结

本文从信息系统漏洞带来的风险出发，考虑安全运维团队对漏洞修复普遍存在的问题，提出基于系统安全画像的漏洞风险遏制方案，权衡风险修复操作的利弊问题，在保障风险可控的同时，兼容系统可用性、可靠性方面的要求。

另外随着时间的推移，由于大部分信息系统的业务复杂度逐步提升以及人员的更替问题，无法保证漏洞评估和修复的时效性以及有效性。而通过系统安全画像使系统基础信息以及风险程度可视化，运维人员在处理系统风险的同时了解了系统的基本架构及周边关系，通过系统决策分析产生的风险遏制方案使运维人员的日常工作变的规范化、简单化。

参考文献：

[1] PEROZZI B，AL-RFOU R，SKIENA S. DeepWalk：online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining. New York：Association for Computing Machinery，2014：701-710.

[2] 赵尚儒，李学俊，方越，等. 安全漏洞自动利用综述[J]. 计算机研究与发展，2019，56(10)：2097-2111.

[3] 李如平. 数据挖掘中决策树分类算法的研究[J]. 东华理工大学学报(自然科学版)，2010，33(2)：192-196.

[4] 肖岩军，王津，陈震杭，等. 基于知识图谱的APT组织追踪治理[R/OL]. [2022-04-25]. https://copyfuture.com/blogs-details/9fe0b964307f26f25af624709e0f97ef.

[5] 王铮. 计算机网络安全漏洞分析及防范对策探讨[J]. 电脑知识与技术，2020，16(29)：55-56.

[6] 张志一. 网络安全技术研究[J]. 中小企业管理与科技，2009(33)：268.

[7] 李江灵. 计算机网络安全中漏洞扫描技术的研究[J]. 电脑编程技巧与维护，2021(6)：168-169.

[8] 莫媛淇，陈智慧. 信息通信网络安全威胁与漏洞分析[J]. 电子元器件与信息技术，2021，5(7)：247-248.

[9] 李琪. 解析工业互联网网络安全渗透测试技术[J]. 中国新通信，2021，23(15)：113-114.

[10] 邓泽. 计算机网络安全的漏洞及防范措施[J]. 数码世界，2021(3)：256-257.

[11] 徐宁，常亮. 浅谈计算机网络安全漏洞及防范措施[J]. 网络安全技术与应用，2021(2)：160-161.

[12] 樊营. 试论计算机网络安全与漏洞扫描技术的运用[J]. 科学与信息化，2020(31)：56.

作者简介：

杨丽丽，毕业于合肥工业大学，学士，主要从事网络安全技术研究工作；刘果，毕业于武汉理工大学，学士，主要从事网络安全技术研究工作；李发财，毕业于北京交通大学，硕士，系统架构师，主要从事网络安全产品研究、技术选型及架构与实现方案设计工作；戚大强，毕业于中国药科大学，学士，主要从事网络安全技术研究工作；张彬，毕业于昆明理工大学，硕士，主要从事大数据组件及相关安全技术研究工作；高贯银，毕业于北京师范大学，硕士，主要从事网络安全相关系统的研发及研究工作。