ISSN：3078-8994
EISSN：3104-4492

网络异常行为检测与密码动态调整联动策略

王舒婷

联通数字科技有限公司，北京 100176

摘　要：网络异常行为检测技术可以通过对用户访问行为、网络流量和系统运行状态等信息进行分析来达到发现潜在安全威胁的目的，但是检测结果和身份认证机制缺乏有效的联动，制约了安全防护的效果。为解决以上问题，提出了将网络异常行为检测和密码动态调整相结合，并通过对异常行为的感知、风险等级评估等环节进行整合的联动策略，密码动态调整和多因素认证技术构建了一个以风险变化为导向的动态安全防护体系。该策略能依据网络行为的异常程度对密码安全策略进行自动调整，增强了身份认证的灵活性与安全性，从而为复杂网络攻击的处理提供了有效的保证。

关键词：网络异常检测；密码动态调整；风险感知；多因素认证

DOI：10.64649/yh.shfzykjcx.issn3078-8994.202608003

0 引言

网络攻击的手段也在不断地演变，攻击方通过异常登录、暴力破解、账号窃取、权限滥用和隐蔽式流量攻击打破了传统的安全防护体系，使得网络安全管理受到了更高的挑战。传统的网络安全机制大多依赖于防火墙、入侵检测系统和静态密码认证，但是这些方法一般都是建立在已知的规则或者固定的安全策略之上，不可知的攻击行为很难被及时的发现，防护措施不能随着风险的变化而迅速的调整。网络异常行为检测技术从网络访问数据、用户行为特征和系统运行状态等方面分析可以检测出偏离正常模式存在的威胁，从而为安全事件的报警提供技术支撑。现有的异常检测系统大多只处于风险发现的阶段，其检测结果和用户身份认证环节缺乏有效的衔接，使得攻击者即使被发现而继续使用泄露的账号非法访问。

1 网络异常行为检测技术分析

1.1 网络异常行为的类型与特征

网络异常行为指网络主体访问资源、数据传输和系统操作等方面偏离正常运行规律的行为，一般和网络攻击、账户泄露或者内部违规操作有关[1]。网络异常按行为的来源分为外部攻击行为、内部异常操作和异常访问行为三类。其中外在攻击行为有暴力破解、恶意扫描、流量攻击以及漏洞利用；内部的异常行为涵盖了超出权限的访问和对敏感数据的异常采集等方面。网络中的异常行为一般具有隐蔽性、动态性以及复杂性等特征，攻击者倾向于通过模仿正常用户的行为来减少被发现的可能性。随着网络环境的日益改变，异常行为模式呈多样化发展趋势，这使得依赖固定规则进行检测的传统模式很难适应安全防护需求。

1.2 基于规则匹配的异常检测方法

以规则匹配为核心的异常检测方法作为传统网络安全检测技术之一，主要根据事先构建的攻击特征库以及安全规则来分析与判断网络行为。检测系统能够在用户的接入行为、网络流量特征或者系统的操作方式满足现有的异常检测规则的情况下发现潜在的安全威胁[2]。这种方法具有执行简单、检测速度快，对已知攻击识别精确等优点，在入侵检测和防火墙策略管理等安全领域具有广泛的应用前景。通过对持续多次登录失败、异常端口访问和恶意数据包特征的规则设定，能够迅速检测出常见的攻击行为。规则匹配方法主要依靠人工维护，在新的攻击方式多变的情况下检测能力欠缺。同时对未知攻击以及变种攻击的行为会因为缺乏相应规则的支持而导致系统不能及时的检测出来。

1.3 基于机器学习的异常行为识别方法

基于机器学习网络异常行为识别方法在海量网络数据的训练下，使得模型能自动地学习到正常行为模式和异常行为的区别，以达到智能化检测的目的。这种方法一般由数据采集、特征提取、模型训练和异常分类组成，并通过对用户的登录时间、访问频率、数据流量和操作习惯的特征分析来判断其当前行为的危险程度。常见的机器学习算法主要有支持向量机、决策树、随机森林和聚类算法，其中分类算法能基于现有样本对异常行为进行识别，聚类算法能检测出与正常数据分布存在偏差的未知异常情况。与传统的规则检测方法相比较，机器学习拥有更强大的数据分析能力与未知威胁发现能力，并能适应复杂网络环境的改变。但是这种方法对于训练数据的质量有很高的要求，如果样本不充分或者出现偏差就会影响检测的精度。有些模型解释能力不强，算法结构有待

ISSN：3078-8994
EISSN：3104-4492

进一步优化，检测结果可靠性有待提高。

1.4 基于深度学习的网络异常检测方法

基于深度学习网络异常检测方法，利用神经网络较强的特征提取能力从深层次上分析复杂网络行为数据以达到更准确地识别异常的目的。对比传统机器学习方法，深度学习能自动地完成对高维数据的特征提取，降低了人工进行特征设计的流程，适合大规模网络环境中的安全检测[3]。现阶段，深度学习的常见模型有卷积神经网络（CNN）、循环神经网络（RNN）、长短期记忆网络（LSTM）和自动编码器（AE）等几种。其中 CNN 能够有效地抽取网络流量的空间特征，而 LSTM 适用于时间连续性用户行为变化的分析。深度学习方法可以发现更深层次的隐藏攻击模式，对于未知攻击的检测和异常流量分析有着明显的优势。这种方法一般所需训练数据多、计算资源多，而模型复杂度高、检测结果解释能力尚有欠缺。

2 传统密码管理方式存在的问题

2.1 静态密码机制安全防护能力不足

传统密码管理方式主要依赖固定密码作为用户身份验证依据，用户在注册账户后通常长期使用同一组密码完成身份认证。尽管该静态密码机制具有执行简单、部署费用低廉的优点，但是它的安全防护能力已经很难满足目前复杂的网络环境。伴随着网络攻击技术的日益进步，攻击者可通过暴力破解、密码泄露和撞库攻击来获取用户的密码，当密码被盗用时攻击者可长时间使用合法身份获取系统资源。同时静态密码缺乏实时变化的能力，不能根据用户行为变化及网络风险情况对安全策略进行及时调整，甚至当系统已发现异常访问时也很难迅速降低账户遭受进一步攻击的可能性。

2.2 用户密码使用习惯导致安全风险增加

用户密码的使用习惯，是网络身份安全最主要的影响因素。在实践中，很多用户出于便于记忆的考虑，往往会设置简单的密码或反复使用同一密码进行多平台的操作，这一行为大大增加了账户泄露的风险。一旦某个网站的数据被泄露，攻击者会尝试使用已获得的密码信息登录其他相关账户，从而触发一系列的安全问题。一些用户在长时间内没有对密码进行修改或采用含有个人信息的密码组合也会导致密码防护能力下降。由于普通用户安全意识不足，难以主动发现密码管理存在的风险，导致传统密码机制面临社会工程攻击和钓鱼攻击时防御能力受到限制。

2.3 密码管理缺乏动态感知与风险响应能力

传统密码管理体系一般都是使用固定策略来设置、修改及验证密码，安全控制方式多依赖于事先制定好的规则，缺乏实时感知用户行为及网络环境改变情况的能力。传统的密码系统在用户账户发生异常登录、异地访问或者高风险操作的情况下，一般不能根据风险程度的大小自动调节认证的力度，仍按原密码验证流程进行身份确认。这种动态响应能力不足的管理方式使得攻击者获得密码之后可以继续使用账户来执行非法操作。同时传统的密码管理不能有效地与网络异常检测的结果相结合，使得安全检测和身份认证形成了信息隔离的现象，从而降低了整体防御的效率。

2.4 传统认证方式难以应对复杂网络攻击环境

网络攻击手段日益更新，传统的单一密码认证方式已很难有效处理复杂化和多阶段网络攻击。攻击者在密码破解中不仅能获得账户权限，而且会使用木马程序、钓鱼网站和会话劫持来绕开传统的身份验证机制。在这种情况下，即便用户密码自身复杂度很高，但仍不能完全规避账户非法获取的危险。传统认证方式一般缺乏对用户行为环境进行全面分析，仅仅根据密码正确与否来判定身份合法性而不能确定是否存在已被窃取合法账户的行为。当攻击者从异常位置用正确的密码登录系统后，传统的认证机制也许仍然允许进入。

3 网络异常检测与密码动态调整联动策略设计

3.1 联动策略总体架构设计

网络异常检测和密码动态调整的联动策略意在构建以风险感知为动力，网络安全检测和身份认证机制有效配合的主动防御体系[4]。策略的整体架构由异常行为检测层、风险评估层、密码动态调整层和安全认证响应层四个部分组成。其中异常行为检测层主要收集用户的访问日志、网络流量、设备信息及操作行为，通过规则匹配、机器学习及深度学习技术发现的异常事件；风险评估层基于检测结果综合分析用户的行为以判断账户当前的安全状态，产生风险等级；密码动态调整层，用于依据风险等级，自动进行密码强化、密码更新或者认证策略的调整；安全认证响应层采用多因素认证和动态验证码的方法，对用户的身份进行进一步认证。

3.2 异常行为感知与风险等级划分机制

异常行为感知和风险等级划分机制作为网络中异常检测和密码动态调整相联系的关键环

ISSN：3078-8994
EISSN：3104-4492

节，主要功能在于实时监控用户的行为，根据异常情况决定对应的安全响应策略。该机制通过收集用户登录位置、访问时间、设备状态、操作频率、资源访问范围和网络流量特征的多维数据来构建用户正常行为模型。在实际行为与正常模式存在偏差的情况下，该系统利用异常检测算法对行为的风险值进行统计，同时结合历史行为记录做出综合判断。从风险等级的划分上看，用户的行为风险可分为低、中、高三个级别。低风险一般体现在轻微的行为偏差上，而系统只记录并不断监控；中风险说明账户有隐患，需加强身份验证或者对某些操作进行约束；高风险是指账户有被攻击的风险，立即引发密码调整和强制重新认证的安全措施。

3.3 风险驱动的密码动态调整流程

风险驱动密码动态调整过程是将异常检测结果转换为身份安全控制的重要途径，该过程的核心思想就是基于账户风险状态对密码安全策略进行自动调整。网络异常检测系统在检测到用户的行为出现异常时，先将检测结果发送给风险评估模块，由风险评估模块对当前账号的风险等级进行统计，根据风险等级开始相应的密码调整过程[5]。对风险较小的用户，在强化行为监控的前提下，该系统能够保持原密码策略；对中风险用户可请求用户修改密码，提高密码复杂度的需求，也可启用附加身份验证；对高风险用户立即实施强制密码更新，暂时冻结账户和限制访问权限以防止攻击行为的继续扩展。系统在动态调整时也能综合考虑用户历史行为及攻击趋势智能调整密码有效周期，实现密码管理从固定周期更新到以风险状态为主的动态管理。

3.4 多因素认证与动态密码协同机制

多因素认证和动态密码协同机制对增强联动安全策略的可靠性至关重要，它通过综合运用各种身份验证方式来增强账户接入时的安全保障。传统的密码认证只依赖于用户输入的固定密码来判定身份是否合法，易遭受密码泄露与窃取攻击，多因素认证是通过与密码相结合的方式进行的、综合考虑动态验证码、生物特征，设备信息和行为特征来评判用户的身份。当系统在网络异常检测中识别到潜在风险时，它能够依据风险的级别自动增强认证的严格性。正常接入状态时只需完成普通密码的验证即可；在发现有异常登录或者高风险操作的情况下，需要用户键入动态密码并配合短信验证码、身份令牌或者生物识别等二次验证。同时动态密码机制可以根据时间变化或者风险状态产生新认证信息，减少了固定密码因长时间使用而存在的安全隐患。

4 结论

信息化应用日益深入，网络安全威胁也呈现愈加复杂多变的趋势，仅靠传统密码认证与被动防御方式已很难保障用户账户与系统资源的安全。为解决传统密码管理静态化，风险响应不充分和难以处理智能攻击的问题，本文提出一种网络异常行为检测和密码动态调整联动策略。该策略通过采用异常检测技术对用户行为特征进行实时分析，结合风险等级评价结果对密码策略进行动态调整，从而将安全检测和身份保护有效地结合起来。同时引入多因素认证机制进一步加强账户访问控制，提升系统在异常登录、密码泄露和复杂网络攻击等情况下的防御水平。

参考文献：

[1] 刘昉 . 基于人工智能的网络信息安全异常行为检测方法 [J]. 信息与电脑 ,2026,38(9):160-162.
[2] 崔妍 . 人工智能驱动的油田网络异常行为检测技术研究 [J]. 电脑知识与技术 ,2026,22(12):22-24.
[3] 金鑫 . 网络异常行为的多模态融合检测方法及自适应响应机制 [J]. 中国宽带 ,2026,22(5):92-94.
[4] 刘荣云 . 基于人工智能技术的网络信息安全威胁检测系统 [J]. 软件 ,2026,47(2):19-21.
[5] 霍莉莉 . 基于人工智能的网络异常行为检测方法研究 [J]. 网络安全技术与应用 ,2026,(1):10-13.

作者简介：王舒婷（1998.11—），女，汉族，新疆人，本科，研究方向：网络安全，数据安全。