软件定义边界安全模型在电网企业系统中的应用*

文　星

（中国南方电网超高压输电公司信息通信运维中心，广东 广州 51066）

摘　要：针对电网企业在内网环境下应用系统访问出现安全问题，结合传统访问控制机制，提出了一种基于软件定义边界（Software Defined Perimeter，SDP）的用户多维度数据身份验证模型。首先分析了当前电网企业应用系统中访问控制模型存在的不足，然后对现有的模型引入信任的属性，依照最小化授权方式，建立每个人与公司业务系统的对应关系，创建千人千面的安全软边界网关。实际应用和理论分析表明，该模型可以实现用户只能看到被授权访问的应用，建立强信任、强可控、强防护的新安全架构，有效保护电网企业的各类应用系统。

关键词：电网企业；访问控制；最小化授权；软件定义边界

中图分类号：TP391　　**文献标识码**：A　　DOI：10.19358/j.issn.2096-5133.2020.01.007

引用格式：文星.软件定义边界安全模型在电网企业系统中的应用[J].信息技术与网络安全，2020，39(1)：38-41，49.

Application of software definition boundary security model in power grid enterprise system

Wen Xing

（China Southern Power Grid EHV Power Transmission Company Information and Communication Center，Guangzhou 510663，China）

Abstract：Aiming at the security problem of application system access in power grid enterprises under intranet environment，a user multi-dimensional data authentication model based on Software Defined Perimeter（SDP）is proposed in combination with traditional access control mechanism. Firstly，the shortcomings of access control model in current power grid enterprise application system are analyzed. Then，the attribute of trust is introduced into the existing model. According to the minimal authorization method，the corresponding relationship between each person and the company business system is established，and a secure soft boundary gateway with thousands of people and thousands of faces is created. Practical application and theoretical analysis show that the model can achieve the application that users can only see authorized access，and establish a new security architecture with strong trust，strong control and strong protection，which can effectively protect various application systems of power grid enterprises.

Key words：grid enterprise；access control；minimizing authorization；software definition boundary

0　引言

目前随着云计算和移动互联网等新兴技术的普及，对于电网企业来说，信息化水平越来越高，企业经营和管理都离不开各类应用系统，但是在生产信息化管理中，存在信息安全问题，特别是在内网环境下，系统访问几乎不受任何身份校验约束，网络攻击者可以轻易通过流量攻击、安全渗透等网络攻击手段破坏应用系统，且无法通过任何防火墙设备进行快速拦截[1]。系统一旦被攻击将给电网企业造成不可估量的损失和无法预料的后果。因此，通过对现有网络架构分析，通过引入软件定义边界架构可以设计更安全的权限管理、身份验证机制，建立符合电网企业自身安全的用户访问控制模型，具有重要的意义和价值，有效提升电网企业各级各类应用系统的安全性。

文献[2]设计了一种专门应用于企业级系统移动智能终端访问控制框架，该框架在一定程度上可以增强访问的安全性能，对于访问的用户来说能够得到访问授权，对于获取的执行权限可以完成安全

*基金项目：2019 年南方电网超高压公司信中心职工技术创新项目阶段性成果（CGYKJXM20190297）

范围内操作，不过缺陷就是操作相对负载，需要依靠人工进行处理，工作效率不高。文献[3]介绍了数据库安全访问强制控制模型，对数据库操作制定一系列规则，对客体进行安全级别指定策略，缺点是扩展性不高，在更多用户连接和跨多云实例部署情况下，在应用系统的复杂多元环境下无法做出灵活处理。文献[4]提出了基于角色进行安全访问控制机制，该机制可以将用户级别、设备类别、权限层级进行一定程度的匹配，并且针对实际需求，可以满足日常需求，不足之处是以传统的边界防护为核心的防护理念和措施，有可能带来系统安全隐患。

本文根据现有传统网络安全模型的研究和分析，针对电网企业在信息化管理中出现的防护策略不能适应多变的信息安全问题，提出了一种基于软件定义边界的用户多维度数据身份验证模型，该模型在现有基于角色基础上将身份认证和行为认证相结合，可根据用户行为数据、访问数据、内容数据动态调整用户权限，建立起强信任、强可控、强防护的新安全架构，可以有效保护电网企业的各类应用系统。

1 相关技术研究

系统访问控制是信息安全技术重要内容，用户通过对各类应用系统制定相应的访问控制策略，使得用户在访问系统时得到授权，能够获取相应网络资源的操作权限，可以对资源进行访问和处理[5]。通过科学、规范的用户访问控制模型的设计，可以保护系统、限制用户访问，使得系统资源的安全性和完整性得到保证。

在访问控制模型中，通常包括了三个重要要素，分别是主体 S(Subject)、客体 O(Object) 和控制策略 A (Attribution)，对上述三个要素制定出不同的策略，形成了三种相关访问控制机制，包括了自主访问控制(DAC)、强制访问控制(MAC) 和基于角色访问控制(RBAC)[6]。目前大部分的系统采取的是 RBAC 机制，该机制能够针对不断变化的需求将用户、角色、权限形成映射，使得用户映射到角色，对角色进行授权，使得用户具有委派获得的访问权限，因此，管理员就可以将不同的需求进行一定的组合和映射，进行系统权限的处理[7]。RBAC 模型具体如图 1 所示。

在上述的 RBAC 模型中，在一定程度上解决了由于用户多造成的操作复杂和繁琐问题，但存在一定安全隐患，不足之处包括如下[8]两点：

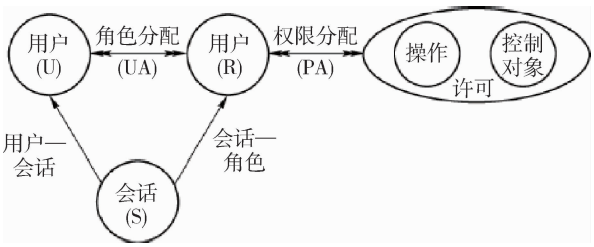

图 1 RBAC 模型示意图

(1)模型中各类的操作和规则制定是通过系统管理员完成的，因此，权限获取是静态过程，通过系统管理员的委派所获得。

(2)用户一旦获取了权限，可能存在无限制的使用，甚至出现滥用的情况，违背最小权限原则。

针对上述 RBAC 模型不足和对传统访问控制模型的研究分析，结合电网企业对应用系统安全性要求，提出了基于软件定义边界的用户多维度数据身份验证(SDP-BAC)模型，该模型在对用户身份验证、访问控制的基础上引入软件定义边界，使得模型可以根据用户行为数据、访问数据、内容数据动态调整用户权限，保障企业应用系统的安全。

2 身份验证访问控制模型

通过前面分析，模型设计重点是需要对用户行为数据、访问数据、内容数据等进行分析，从而获得该用户访问系统的权限，在这个过程中需要对用户的行为进行认证和评估。在模型中，用户在开始阶段具有一定的初始信任度，用户在后续的使用过程中，模型将会对用户的行为、用户的访问进行数据的记录，并且根据用户行为情况进行动态的评估，对用户信任度动态计算与调整，因此，用户在系统模型中的信任度是不断变化的，随着信任度的变化而自动调整[9]。只有获取相应阈值的用户，才能拥有对电网企业系统的访问。一旦用户信任度结果低于某阈值时，模型做出反应，用户失去系统的访问权限，这样系统就可有效掌握安全态势，及时发现安全威胁。

2.1 计算信任度

身份验证访问控制模型需要对用户的信任度进行计算和评估，在评估过程中主要考虑如下的因素：

(1)用户历史行为。记录和评估以往操作情况，用户的操作数据是进行信任度计算重要的参数，直接影响到系统对用户信任度作出评估分析，并且不会随着用户退出和消失[10]。

(2)用户当前行为。分析用户在目前阶段的操作,并且对此进行记录和监控,对操作的数据结果作出分析,分析其访问和处理系统数据资源和内容,一定程度上避免恶意操作的发生[11]。

定义 1　信任度衰减函数:计算以往操作中行为对目前信任度的影响,其结果受到时间 t 影响,计算公式如(1) 所示。

$$\Phi(t) = e^{-pt} \tag{1}$$

式中 p 是信任度衰减值。

定义 2　惩罚项:对用户的恶意操作或不当操作作出记录和处理,某个用户 a 在系统中的惩罚项表示为 $P(a)$,惩罚项计算公式如式(2) 所示。

$$P(a) = 0.2 \times e^{\frac{1}{t-1}} \tag{2}$$

式中,n 表示的是系统访问数据流量。

定义 3　奖励项:对于用户符合正常操作,可以增加用户的信任度,并且给予一定的奖励,计算的具体公式如式(3) 所示。

$$R(a) = e^{-(0.2m+4)} \tag{3}$$

式中,m 表示的是正常访问数据流量。

定义 4　访问信任度:对前面历史的操作数据,计算得到的历史信任度和当前访问的信任度进行一定处理,完成加权计算从而获取得到访问信任度,具体计算如式(4) 所示。

$$\mathrm{Cur}(a) = \mathrm{History}(a) \times \Phi(t) + \mathrm{Entiro}(R(a), P(a)) \times \varphi(t) \tag{4}$$

式中,History(a)表示的是历史信任度的结果,Entrio($R(a)$,$P(a)$)表示的是用户在当前信任度的结果,$\Phi(t) + \varphi(t) = 1$。

2.2　动态授权

在模型中,对于用户的权限设置不是静态的,而是根据用户的行为、用户的访问进行数据的记录从而动态持续地调整,数据包层级为用户或设备持续认证,具有较强的安全性能。从前面的分析中可以看到,传统的 RBAC 模型实现依赖的是身份认证,用户完成认证后就可以持续获取到相应的权限。改进后的用户多维度数据身份验证(SDP-BAC)模型在原来基础上引入软件定义边界和用户行为机制,使得对用户的访问可以实时监控,具有动态授权的特性。用户行为评估机制工作示意图如图 2 所示。

通过用户行为进行动态授权的计算过程如下。

(1)进行用户的访问身份验证,取得初始权限。

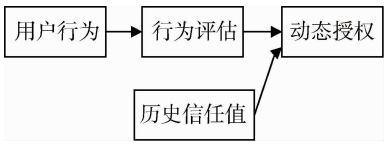

图 2　用户行为评估示意图

(2)计算用户访问控制函数 G,将其重新分解为 G_1 和 G_2,其中 $G_1: U \to T, T \in [0,1]$,$T$ 表示的是信任度;$G_2: T \to R, R \in \{0,1]$,$R$ 表示的是角色,通过上述映射函数进行分解。

(3)对用户行为进行评估,分析是否存在严重违规行为、历史行为记录是否良好。如果用户出现违规,用户信任度指数就会下降,下降后将采用慢启动策略上升。计算当前信任度的值,结合历史行为重新计算当前访问信任度。

(4)一旦用户当前访问信任度低于某个设定的阈值,用户就不能赋予高一级的权限,甚至自动失去系统访问的权限。

动态授权的计算流程如图 3 所示。

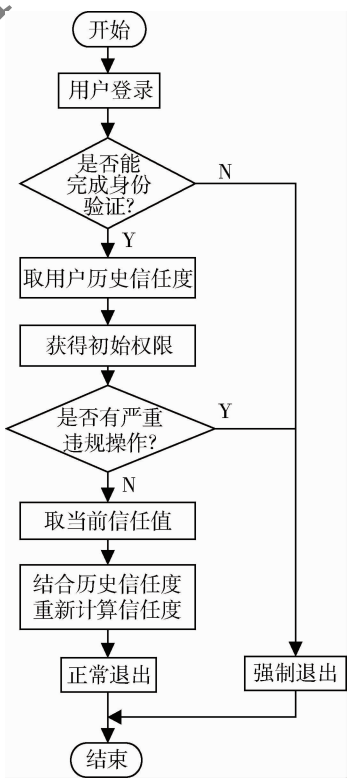

图 3　模型流程图

3　在电网企业系统中的应用

3.1　电网企业系统访问控制要求

以中国某公司的 ERP 系统应用为例进行研究和分析,在公司中的各类应用系统主要划分为几个

类别,分别是 Web 服务平台、调度应用平台、分析平台和专业数据存储平台。因此,目前公司网络架构通过建立区域边界将内部网络与外部网络(互联网)、内部网络之间进行隔离,这个边界制作手段往往是一组防火墙策略。防火墙策略是非敏捷的,管理颗粒度仅为 IP 与端口,且只能通过人工下发策略。随着移动互联网的快速发展,用户或设备的身份属性、地理属性、网络属性都在随时随地地发生变化,确定“我真的是我”这件事变得极其重要。特别是在内网环境下,系统访问几乎不受任何身份校验约束,网络攻击者可以轻易通过流量攻击、安全渗透等网络攻击手段破坏应用系统,且无法通过任何防火墙设备进行快速拦截。

3.2 模型工作流程

从系统安全访问为出发点,通过软件定义边界理念,采取多维度数据建模验证身份,并依照最小化授权方式,建立每个人与公司业务系统的对应关系,对于上述的各类系统需要进行用户访问控制,通过改进后的安全模型进行处理。在公司内部对于角色的划分主要有如下几个类别:系统管理员、公司领导、部门领导、工程技术人员、普通职工。对于不同的用户角色其要求不同,达到不同安全目标。

针对传统模型中出现的依赖于 RBAC 授权机制,在改进后的模型中,对用户身份验证不是立即将权限授予,不能即时获取到角色权限。接着安全模型将对用户操作日志和数据进行查询和分析,计算其信任度,对其相应的权限等级进行划分。下面以某电网超高压输电公司作为例子,公司内部信任值等级处理具体如表 1 所示。

表 1 公司内部信任等级划分表

	可信	一般可信	弱可信	不可信	完全不可信
系统管理员	7	5	3	1	0
公司领导	6	5	3	1	0
部门领导	5	4	2	1	0
工程技术人员	4	3	2	1	0
普通职工	2	1	0	0	0

在上述信任等级划分和处理表中可以看到整个等级划分为八个等级。对用户来说,其等级越高相应获取的权限就越大,最高等级的用户(系统管理员),具有最大的操作权限。对于等级数值为 1 的,那么其只能浏览基本内容。对于信任度等级为 0,说明其信任度是最低的,甚至违规操作如盗用公司用户账号,可以强制退出或无法访问。

3.3 模型特征分析

动态性。在前面分析中,可以看到模型采用基于身份的联网技术在数据包层级为用户或设备持续认证。安全不存在侥幸,所有网络流量都有日志可供审计和调查,该模型具有动态性。

双重控制机制。基于预设策略是就具体应用的访问,而不是对整个网络的访问。在身份验证上,首先是登录的验证,其次是登录后根据用户行为的信任度的计算,进行第二重的控制,通过双重的控制访问技术可以有效提升系统安全性。

细粒度的访问控制。在用户和资源间实现单对单的定制网络访问策略。未授权用户看不到资源,减少了潜在攻击面。此外,根据用户的等级进行访问控制的授权。

4 结论

本文根据电网企业应用系统安全的设计需求,针对传统网络安全模型、以边界防护为核心的防护理念和措施存在的不足,建立了一种基于软件定义边界的用户多维度数据身份验证模型。该模型可以解决以往用户静态赋权限的缺陷,根据用户历史和当前行为进行用户角色的动态授权,实现了身份认证和行为认证相结合的双重访问控制机制。通过电网企业应用系统的实例,验证了模型在电网企业应用系统在网络隐身、最小授权方面的作用。该模型适用于云计算和移动时代的电网企业访问控制方案,从而建立强信任、强可控、强防护的新安全架构。

参考文献

[1] 余洋,孙林夫,马亚花. 基于属性的云制造协同平台访问控制模型[J]. 计算机集成制造系统,2017(1):340-346.

[2] 黄健,黄建文,黄志新,等. 企业级系统移动智能终端访问控制技术研究[J]. 微型机与应用,2014(7):34-46.

[3] 魏立峰,孟凯凯,何连跃. 面向用户角色的细粒度自主访问控制机制[J]. 计算机应用,2018(12):208-214.

[4] 李凤华,陈天柱,王震. 复杂网络环境下跨网访问控制机制[J]. 通信学报,2018(2):109-118.

[5] MATTOS D M F, DUARTE O C M B. AuthFlow:authentication and access control mechanism for software defined networking[J]. Annals of Telecommunications,2016(12):349-246.

(下转第 49 页)

[11] 汪海萍,赵晶晶. 隐藏访问结构的密文策略的属性基加密方案[J]. 计算机科学,2016,43(2):175-178.
[12] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]. Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 456-465.
[13] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]. International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2011:53-70.
[14] 刘西蒙,马建峰,熊金波,等. 云计算环境下基于密文策略的权重属性加密方案[J]. 四川大学学报(工程科学版),2013 (6):21-26.
[15] TSAI C Y, HO P F, HWANG M S. A secure group signature scheme [J]. IJ Network Security, 2018, 20 (2): 201-205.
[16] 张兴兰,崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报,2019,5(1):15-21.
[17] 范运东,吴晓平. 基于策略隐藏属性加密的云存储访问控制方案[J]. 计算机工程,2018 (7):24.

(收稿日期:2019-10-30)

作者简介:

朱林(1995 -),男,硕士,主要研究方向:网络安全、密码学。

张伟(1964 -),通信作者,女,硕士,副教授,主要研究方向:网络安全、密码学。E-mail:283186823@ qq. com。

谢宝文(1993 -),男,硕士,主要研究方向:网络空间安全、可信计算。

(上接第 41 页)

[6] ALBERTINI D A, CARMINATI B, FERRARI E. An extended access control mechanism exploiting data dependencies[J]. International Journal of Information Security, 2017 (2):107-115.
[7] SOMAVARAPU A K, KEPP K P. The dynamic mechanism of presenilin-1 function: sensitive gate dynamics and loop unplugging control protein access[J]. Neurobiology of Disease, 2016(5):78-82.
[8] 陆佳炜,吴斐斐,徐俊. 基于动态授权机制的自适应云访问控制方法研究[J]. 计算机应用与软件,2017(11):203-211.
[9] 廖大强. 基于云计算的密集型数据库资源快速检索方法研究[J]. 内蒙古民族大学学报(自然科学版),2019(5):215-220.
[10] 邹德清,杨凯,张晓旭. 虚拟域内访问控制系统的保护机制研究[J]. 山东大学学报(理学版),2014(8):96-104.
[11] 赵坤,方鹏. 数据库的安全机制及访问控制策略分析[J]. 通讯世界,2016(12):81-90.

(收稿日期:2019-07-20)

作者简介:

文星(1987 -),男,硕士研究生,工程师,主要研究方向:电力信息化技术。

版权声明