

基于零信任架构的高校校园网络安全体系研究与实践

成洋¹ 钟珞²

1.湖北孝感美珈职业学院, 中国·湖北 孝感 432000

2.武汉理工大学, 中国·湖北 武汉 430000

摘要: 高校校园网是教学科研、管理服务的主阵地, 移动接入、资源上云、跨域协作使得传统的边界防护越来越无效。本文对身份信息分散、终端状态不同、资源边界弱化、管理权责衔接不紧密等状况展开剖析, 创建起以统一身份为中心、设备状态为限制, 结合细粒度授权和持续评价的零信任安全架构。实践当中, 经由资产梳理来确定改造的对象与顺序, 依靠策略编排来保证业务的连续性, 依靠持续运营以及组织治理来修正安全策略。研究认为高校应该分阶段推进改造, 把验证要求嵌入到资源访问的全过程之中, 把安全控制从位置判断转变为以身份、状态、行为证据为基础的动态决策。

关键词: 零信任架构; 校园网络; 持续验证; 最小权限; 安全治理

Research and Practice of University Campus Network Security System Based on Zero Trust Architecture

Cheng Yang¹, Zhong Luo²

1. Meiga Polytechnic Institute Hubei, China Hubei Xiaogan 432000

2. Wuhan University of Technology, China Hubei Wuhan 430000

Abstract: The campus network of universities is the main battlefield for teaching, research, and management services. Mobile access, cloud based resources, and cross domain collaboration have made traditional boundary protection increasingly ineffective. This article analyzes the situation of dispersed identity information, different terminal states, weakened resource boundaries, and loose connection of management rights and responsibilities, and creates a zero trust security architecture centered on unified identity, limited by device status, combined with fine-grained authorization and continuous evaluation. In practice, the objects and sequence of transformation are determined through asset sorting, business continuity is ensured through strategy orchestration, and security policies are revised through continuous operation and organizational governance. Research suggests that universities should promote transformation in stages, embedding verification requirements into the entire process of resource access, and transforming security control from location judgment to dynamic decision-making based on identity, status, and behavioral evidence.

Keywords: Zero trust architecture; Campus network; Continuous verification; Least privilege; Security governance

0 引言

高校校园网已经成了教学科研、管理服务的共同基础。师生借助无线网络、互联网以及个人终端去获取资源, 业务系统还延伸到了云平台 and 校外的合作环境之中, 网络的位置已经很难再对可信主体做出明确的划分。账号被冒用、终端被攻击或者权限积攒之后, 攻击者会利用合法的连接来扩大影响。零信任架构把内网位置默认的信任取消了, 用身份认证、状态检查、最小权限控制来验证每一次的访问^[1]。国内的研究已经探索了校园网零信任的应用, 但是技术控制同高校治理流程的衔接还不到位。本文首先分析校园网络信任风险, 然后讨论面向校园场景的体系设计, 从资产改造、策略执行、持续治理等几个方面说明实

践路径。

1 高校校园网络的信任风险重构

1.1 身份关系的碎片化困境

学生身份会随着学籍状态的改变而变化, 教师还会同时承担教学、科研或者管理工作, 访客和合作人员一般只在一段时间内参与业务。各部门各自维护账号时, 身份源之间没有稳定的映射关系, 账号生命周期很容易和真实人员的关系脱离。同一人会在不同的系统里拥有多个账号, 角色记录以及身份属性也不一定同时更新, 从而造成长期累积的权限。人员离职、毕业或者项目结束之后, 若有关权限不能及时收回, 那么历史身份仍然可以访问现有的资源; 共享账号也会降低操作行为和责任主体之间的对应关

系。因此问题不是认证次数不够,而是身份信息分散、变化不能及时传递,系统不能持续确认访问者的身份和职责,也不能判断现有的授权是否有依据。身份链条一旦失真,后续访问决策就会缺少可靠基础。

1.2 资源边界的持续消解

高校数字资源已经从本地机房发展为云服务、实验网络、校际合作平台等,访问方式也不再是校园内固定的网络,而是可以通过互联网或者应用接口直接建立。传统的防护依靠网络区域来判定可信程度,主体进入内网之后会看到比较大的范围的资源,因此单个账号或者终端一旦被攻破,横向传播就很容易发生。随着资源上云、跨境协作的不断增多,网络位置与资源归属之间联系越来越弱,校园网内外边界也变得模糊起来^[2]。同时一些遗留的服务以及临时开放的接口会脱离统一的管理视线之外,使得实际暴露面不能被完全识别出来。在此时,静态网段已经不能准确地表示出真正需要保护的范围,边界弱化还会进一步加大账号或者终端失陷后传播的风险。

1.3 管理责任的协同障碍

零信任策略要依靠业务部门给出判断依据,也要依靠信息化部门执行技术任务,还需要由安全管理岗位来监督。业务部门最清楚人员的职责以及数据的用途,信息化部门负责身份平台和策略系统的运行,但是这些职责往往分散在不同的流程中。如果技术部门脱离业务语境直接决定权限,就会出现过度授权或者误阻断的情况;如果业务部门只强调功能的可用性,那么账号回收和接口开放就很容易失去必要的约束。外部服务方参与远程维护后,责任链还会进一步拉长。合同主体、实际操作者和技术账号之间如果不能一一对应,那么相关的操作就很难追查到责任人。

跨部门授权、临时访问等很容易暴露出协同问题。当出现紧急业务的时候,如果审批责任以及处理时限没有事先规定,那么例外权限就会在业务结束后仍然保留下去。另一方面,业务紧急性和安全风险之间没有统一的标准来判断,会带来两种相反的结果,即合理的需要会被长期搁置,或者为了方便而不断放宽控制。由此产生的协同障碍,会导致策略不能及时地随着人员、业务、资源关系的变化而进行调整,从而造成责任不能准确地落实到具体的环节上。

2 面向校园场景的零信任体系设计

2.1 统一身份驱动访问决策

统一身份的目的不是简单的合并账号,而是给访问决策提供可信主体信息。学校应该以权威人员的数据为依据,

把学籍或者聘用状态同岗位、项目联系起来,然后由身份治理平台给业务系统提供一致的认证依据。账号生命周期也要跟随真实人员关系的变化而变化,不能让身份失效之后权限还保留着。当一个访问请求到达时,策略决策点除了要检验用户的身份是否合法之外,还会根据用户的职责、所用的资源是否敏感、当前会话环境等来决定是否开启连接。认证通过只是证明了主体的身份已经被确认,但是并不能保证可以访问所有的资源。授权范围要与当前的任务相适应,并且要有期限的限制,短期的教学合作、科研合作以及外部运维等工作不再依靠长期的账号^[3]。

2.2 设备状态约束的连接控制

校园终端包含学校统一管理的办公设备、师生个人终端以及专用实验设备,其系统版本及安全配置存在着较大的差别,管理能力也有所不同。连接建立前控制系统要先辨别设备身份,再检查与当前资源访问有关的完整性以及防护状态。会话维持期间,如果设备风险发生变化,就要触发补充验证,按照变化程度缩小权限或者终止连接。个人终端不能纳入统一管理的时候,可以将访问限制在受控的应用入口上,必要时采用隔离浏览或者只读模式,使终端所拥有的访问能力与资源风险相匹配。对于交互能力较差的实验仪器、物联网终端,用设备证书来确认身份,利用接入网关对它的通信对象进行限制。设备控制的目的在于给访问判断提供可靠的依据,而不是要求所有的终端都采用相同的配置。

2.3 资源粒度支撑的微隔离

微隔离就是对连接在资源之间继续传播进行限制。保护对象不再只是宽泛的网段,而是细化到具体的资源,即应用、接口、数据库以及管理端口等,划分标准也从原来的业务逻辑走向了实际的业务调用关系。学校要识别出资源依赖,规定主体在一定条件下可以发起怎样的交互。控制点可以设置在应用代理、访问网关或者主机附近,使得未经许可的横向通信在接近目标资源的时候被阻断。软件定义边界把资源入口隐藏起来,在主体经过验证之后再建立连接,给校园网收敛暴露面提供了一条实现路径^[4]。暂时不能改造的遗留系统可以先接入统一网关,然后细化到接口、操作权限。系统升级、服务迁移或者项目结束之后,应该及时对微隔离规则进行调整,防止出现过期依赖造成的通道留空。

2.4 行为证据贯通的动态评估

持续验证要求访问决定可以随会话状态的变化而改变,行为证据就成为权限修正的依据。安全平台应当将认

证记录同终端状态联系起来,把应用和网络日志也纳入到安全平台的跟踪体系当中,对主体访问资源的时间、路径以及操作的敏感程度等各方面进行持续的记录。校园业务具有周期性、灵活性等特点,一个异常特征不能直接对应风险,僵化阈值会增加误报。动态评价要根据异常程度和资源影响来确定处置强度。证据不足时可以申请重新鉴定;风险持续增大时暂停敏感作业,重大事项由人手复核。评估结果应立即对后续的策略产生影响。

3 零信任校园网络的实践路径

3.1 资产梳理牵引的分阶段迁移

高校系统建设时期不同,技术架构、归属部门也不同,因此零信任改造不能在全网同时切换。实施之前要创建一个可以长久保持更新的资产目录,明确资源所属方和服务接收者,记入身份产生途径,主要访问路线,关键依赖等信息,依照业务影响力与暴露情况来安排改造顺序。初期可以从身份关系明确、入口集中度高的业务入手,主要验证统一认证可以同策略决策、访问代理稳定联动,然后逐步扩展到需要依赖关系更加复杂的系统上。遗留应用不能识别现代的身份协议时,代理可以承担认证,但是共享账号仍然需要映射到真实的主体上。每一个阶段都应事先设定回退条件,防止策略失误造成选课或者考试等重要业务受到影响。迁移成效不能用已经部署了多少个组件来衡量,而应该关注资源责任是否已经明确、访问是否真正纳入统一决策、历史权限是否得到有效收敛。

3.2 策略编排保障的业务连续性

零信任策略直接影响到访问过程,规则的好坏会对安全效果以及业务体验造成影响。策略编排要从可以理解的业务条件入手,使决策表达能体现主体职责和访问目的,把设备状态和目标资源可能造成的后果纳入判断。新策略上线之前,可以在观察模式下与真实的访问进行比较,找出遗漏的依赖和确有必要例外。进入执行阶段之后,应该先控制敏感的操作,然后根据运行情况逐渐扩大控制的范围。集中报到、选课或者考试时,对可用性有较高要求的场合,策略的改变要避开重要的时段,而且要留有被授权的应急途径。应急权限要明确可以访问的资源,并设置有效的期限,只有在达到预定条件的时候才能启用,使用过程中还要自动留痕,在事后还要进行复核。

3.3 运营闭环推动的能力演进

零信任体系上线之后,安全工作就进入到持续运行的状态。安全团队不能只看告警数量,还要判断关键资源是否真正被策略覆盖,异常会话是否可以得到正确的处理,

临时权限能否按时收回。发现问题之后,首先要判断它的来源。身份信息滞后时要修正数据同步,设备状态判断不准时重新检查检测条件,资源依赖遗漏就补充资产关系;确认属于恶意活动之后再进入相应的安全响应流程。对于误报、误拒绝,应该按照原因来修正判断条件,并且保留变更的依据。对于不能解释的高风险结果不能直接自动处置,而应该转入人工审核。当证据充分并且可以被恢复的时候,系统就会自动要求重新认证,必要时会暂时停止会话或者收回到期权限。身份服务、策略引擎和执行节点也要具有故障监测和必要的降级能力,防止控制平台变成单点风险。

3.4 治理规则嵌入的组织协同

技术控制要进入到学校已有的管理流程当中,才能产生稳定的约束作用。账号管理、系统上线、采购验收、外包运维均要按零信任要求执行。新系统立项时需要说明身份接入方式和权限模型,采购环节要约定必要的日志和接口能力,服务退出后还要有相应的处理要求。外部人员到校内资源处申请,得到校内责任人的同意后,在授权期之内才给予其必要性确认。持续监测包含日志使用时,还要说明安全目的,限定有关数据的访问人员和保存期限,避免个人信息使用范围失控。组织分工要同访问决策相适应,资源所有者说明访问目的和期限,技术团队据此形成规则,安全监督岗位检查实际执行情况。跨部门的争议或者临时授权需要明确审批责任和结束条件,保证例外可以追溯^[5]。培训应该以岗位责任为出发点,治理评价则关注规则是否可以及时更新、责任是否可以被追查、例外授权是否能按时关闭。

4 结语

高校校园网络出现开放接入、混合部署的情况之后,物理位置已经不能再作为稳定的信任基础了。本文从身份关系失真、资源边界弱化和治理协同不足三个方面进行分析。在体系的设计上,用统一的身份作为访问决策的基础,把设备的状态纳入到连接控制当中去,对横向传播的风险用资源粒度的微隔离来约束,用行为证据不断修正访问判断。实践上首先要进行资产梳理来确定改造对象和推进顺序,然后用策略编排来减少改造给正常业务带来的影响,最后依靠持续运营和治理机制来不断校正体系运行。零信任并不是对现有的网络进行完全的替换,它不能依靠单一的产品一次性完成。高校应该按照资源重要程度以及系统改造条件分阶段推进,在保持必要的传统防护能力的基础上,慎重处理业务连续性和个人信息保护之间的关系。

参考文献:

- [1] 郭军利, 许明洋, 原浩宇等. 引入内生安全的零信任模型[J]. 郑州大学学报(理学版), 2022,54(6):51-58.
- [2] 李静元. 基于零信任架构的校园网安全访问研究[J]. 微型电脑应用, 2023,39(9):60-62.
- [3] 李益发, 孔雪曼, 耿宇等. 零信任体系架构的可跨域连续身份认证[J]. 郑州大学学报(理学版), 2024,56(4):41-47.
- [4] 林思一. 基于零信任 SDP 的高校网络安全体系架构[J]. 网络安全技术与应用, 2022(8):80-81.
- [5] 姚军光. 高校零信任安全防护架构的设计与实践[J]. 网络安全技术与应用, 2025(7):89-91.

作者简介: 成洋(1981.12-), 男, 汉族, 湖北武汉人, 本科, 湖北孝感美珈职业学院, 讲师, 研究方向: 网络安全、智能方法与系统。