智慧校园总体框架网络安全风险评估的运用

周雅馨

（河海大学　江苏　南京　210098）

[摘　要]近年来，互联网事业飞速发展，国内外多数技术领域将互联网技术和网络技术应用到实际操作当中，企业技术更加倾向于智能化、自动化。国家在注重科技发展的同时，加大教育力度，为祖国建设培养人才。由于计算机时代的到来，传统校园架构缺点日益凸显，因此，智慧校园是为了推动高校实行智能化、自动建设而产生的新概念。网络安全则是确保用户使用安全的重要影响因素，也直接影响着智慧校园能否正常设置和使用。本文将详细分析智慧校园总体构建过程中的网络安全，探讨当前智慧校园发展现状等问题，为高校构建智慧校园体系贡献一份力量，为相关工作人员提供合理参考。

[关键词]智慧校园；总体框架；网络安全风险评估

【DOI】10.12252/j.issn.2096-6261.2021.07.523

一、智慧校园概要

所谓智慧校园是近年来互联网技术、物联网技术、云计算等技术有机结合的产物。对校园内的物理空间进行数字化建设，校园内人员可以随时随地进行资源获取和信息化服务。利用相关技术对学校现有教学、设备、日常等各类系统进行整合，提高系统应用的灵活性，保障日常工作的完成质量，构建全面、多角度、综合管理服务，推动校园智能化，构建智慧化教学生活一体化。

“智慧校园”是校园信息化、智能化发展的阶段性产物。智慧校园在使用过程中需要具备基础建设平台，另外需要对校园进行全网络覆盖，需要通过有线和无线保障校内网络畅通，在整体操作前期需要对校园内设施进行数字化处理，随着国家相关政策颁布，标志着智慧校园进入了一个新阶段。

智慧校园是实现基础在于通信基础和网络技术是否全面，是否适用于人口数量大的场所使用，所以通信网络技术建设将成为智慧校园未来发展的基石。智慧校园建设方便了学生日常生活和教师办公，例如学生可以通过校园网络进行选课、退课操作，可以自主缴纳杂费，利用一卡通可以完成门禁、就餐等问题，方便学生整体生活。

二、智慧校园建设过程中造成网络安全风险的影响因素

国家在2018年颁布了智慧校园构建标准，意味着我国教育事业将进入一个新的发展方向，智能化校园建设也将进入新阶段。在经济新常态发展下，各行业都意识到了互联网技术所带的便捷，能够有效提高工作效率和质量，智慧校园成为未来校园发展的必然趋势。国内各个高校很早就制定了数字化校园建设目标，近年来，互联网、云计算、物联网等相关技术兴起，将智慧校园建设带入了新阶段，目前国内高校在指挥校园建设上已经取得显著成果，基本上具备全覆盖的网络体系，在日常办公、学习、图书馆等方面都形成了统一型管理系统，推动智慧校园发展。智慧校园将公共基础设施利用网络技术进行管理，将实体进行虚拟化控制，让师生可以随时随地完成工作任务，随时随地的获取校内资源和服务。智慧校园涉及方面非常广泛，所以从层次角度来看，在建设过程中需要严格把控网络安全问题。

（一）基础建设方面

基础建设方面主要包括实体、“云服务”、教学信息化三个方面，基础建设是为了确保应用层能够灵活地连接、操作，为用户提供强大的便捷服务体系创造条件。在基础建设过程中，首先需要明确数据处理中心、网络管控中心的设立位置，要充分考虑防火、防潮以及供电电源稳定等问题，本层是智慧校园整体构建的重要基石，为上层服务平台提供有效的技术支持，本层是上层信息的获取层，其所需要处理的信息需要在本层进行采集，为之后的数据库分析、处理等过程提供数据支持，同样本层构建过程中需要使用一些通讯协议和传感器，作为采集工具，在位置选择过程中，要结合设备特点，确定环境因素是否会影响数据采集效果、是否会对设备造成损坏，严格把控相关特性。

（二）支撑平台方面

智慧校园在整体构建过程中，需要严格把控信息安全问题，另外由于一些硬件设施存在信息处理不兼容的问题，在连接过程中需要确保数据传输正常，接口驱动符合网络安全标准。目前，在高校内常见支撑平台主要具备基础业务处理、数据共享和分析的能力，所需要考虑数据交换的可靠性、精准性以及安全性。高校在建设过程中要尽可能保证数据处理具有统一性，保证数据交换的高效性，数据处理能力为整个体系结构云计算的提供保障，该层主要是通过虚拟信号完成数据的传输、交换的工作，具有一定的抽象性。本层主要存在的问题就是信息传递是否可靠、数据结构协议是安全，数据收发是否准确等问题。

（三）应用平台方面

本层主要包括师生日常学习或办公所需要应用的服务系统，根据涉及方面不同分成不同种类、例如教学服务平台、信息查询平台等不同方面管理系统，具体涉及方面有一卡通、信息门户、教务系统、移动校园等服务方面。该层主要包括校园内部日常所需的基本业务管理系统平台，能够高效的帮助师生完成日常事务处理工作、获取海量网络资源以及便民服务。该层涉及用户信息的保密问题，常见的网络威胁有木马病毒、DDos攻击等。

（四）移动终端方面

移动终端是为了保障师生能够正常访问平台数据的方法和工具，校内人员能够通过各种服务终端获取资源和服务，常见终端既有早期的自助服务终端，也有现代化的手持设备。由于近年来网络十分发达，一些网络黑客利用终端设备上的漏洞恶意获取用户信息、发送诈骗短语或者引诱用户消费，对涉事人员造成巨大损失。

通过上述分析，在当前智慧校园建设体系结构中，信息传播设备和资源、服务获取设备逐渐增加，各种应用软件、平台、终端种类不断增加，呈现多样化、碎片化趋势，随着科技种类增多，也为智慧校园带来了安全挑战，所以在智慧校园的建设过程中需要及时进行风险评估，制定相应的解决方案和预防措施，避免造成实质性危害。

三、智慧校园建设过程中的网络安全风险评估

风险评估主要是在事件发生前后对造成的影响和损失进行量化评估过程。量化分析能够推测某一事件对主体造成影响和损失的可能程度。在智慧校园构建过程中，合理运用风

险评估能够保障校园网络安全和使用人员信息安全问题。对智慧校园网络安全评估过程能够及时发现风险存在位置，推算出该风险对系统造成损坏程度，管理人员要根据风险等级尽早对风险问题进行管理，根据实际需求制定应急预案。本小节将从风险认知、风险评估、风险处理以及风险控制四个方面进行探讨，确保智慧校园框架能够安全有效实行，方便管理人员及时应对网络所出现的安全事件，并对因素进行深入分析。

（一）风险认知

风险认知主要是从上述分析的四个层级出发，通关研究人员测评以及建设经验分析，确认每一层次存在风险影响因素，根据层次逐步、全面深入，确保清晰掌握风险因素，及时筛选，有利于技术人员进行层次化管理。表1为各个层次部分常出现的风险情况。

表1 风险认知结果

层次	风险内容
基础建设层	线路质量差、设备陈旧，机房等位置不符合环境安放标准 …
支撑平台层	身份信息泄漏、接口传输不安全、数据交换不安全 …
应用平台层	黑客入侵、系统病毒、文件丢失 …
应用终端层	诈骗信息、破坏用户数据 …

（二）风险评估

目前风险评估方法具有多样化，例如安全查表法、危险和可操作性研究、矩阵法等相关方法。该篇选用测试方法为格雷厄姆风险评估法，简称LEC法，此方法作为定量风险评估法，它整体利用三个标识来衡量风险危害性（见图1-3），L为“风险项”发生可能性，其取值范围在0.1～10之间，风险发生的可能越大，值越大；E为风险发生频繁度，其取值范围0.5～1之间，风险发生频率越高，值越大；C为发生风险后造成的后果，其取值范围在1～100之间，风险造成后果越严重，值越大；专家根据风险评估标准对三个指标赋值，得到风险危险值D。

D=L×E×C

L 取值	风险发生的可能性
10	必然会发生
6	非常可能
3	可能，但不会频繁发生
1	可能性小
0.5	很不可能
0.2	极不可能
0.1	实际不可能

图1 “风险项”发生可能性L

10	持续发生
6	在工作时间内发生
3	每周偶尔发生
2	每月发生一次
1	每年发生几次
0.5	非常罕见发生

图2 风险发生频繁度E

C 值	风险发生的频繁程度
100	大灾难
40	灾难
15	非常严重
7	严重
3	重大
1	引人注目

图3 发生风险后造成的后果

（三）风险处理

当L、E、C赋值后，三者相乘即可获得风险发生的危险程度D，根据图4可知，风险发生造成危害性越大，对应的D值就越高，技术人员将风险项根据LEC方法计算并且按照D值进行等级划分，针对不同危险等级制定应急方案和解决措施，具体见图5，管控措施能够高效降低损坏程度。

D 值	风险的危险程度	风险等级
>320	极其危险，不能允许风险发生，必须采取措施	5
160~320	高度危险，需要立即整改	4
70~160	显著危险，需控制和监控	3
20~70	一般危险，需要引起注意，经评审后可适当接受	2
<20	稍有危险，可接受的风险，不经评审即可接受	1

图4 风险发生的危险程度D

低风险等级：1，2级为低风险等级需要相关管理部门和责任部门做好日常风险观测记录，合理安排工作人员进行观测。

中、高风险等级：针对2级以上的风险等级，受对应风险体系条款制约，根据条款严格执行，加强管控力度，如果没有符合风险管理合同体系，应该派专业技术人员制定管控计划，将风险后果危害程度降到最低。

等级	应对措施
1	改进造成风险的原因，尽量消除风险的发生
2	采取措施减轻风险造成的危害
3	购买运维、保险服务，转移风险造成的后果
4	改变功能目标或计划，规避风险
5	了解相关信息，寻求机遇承担风险

图5 风险应急方案和解决措施

（四）风险控制

当技术人员完成风险识别和评估后，需要根据实际情况对风险项安排专门人员负责风险监控，当风险扩大到一定程度，必须向负责人上报，及时制定防护措施。智慧校园各个层次需要将设备、系统等工具进行监控方案和应急预案的制定，当发生异常现象时，应该及时做出响应，提示相关负责人。要合理科学的利用智慧校园的大数据技术，对于发生异常问题及时查询使用日志，当达到了风险预警状态，应该立即通知负责人。

结束语

通过上述分析，随着科技发展，智能化校园模式发展已经成为必然趋势。在智慧校园体系架构下，高校各个方面都向信息化、智能化、数据精准化方向发展，为师生处理日常事务、获取资源提供了便捷。为了确保师生正常使用设备、系统，高校管理人员需要提高网络安全建设，对网络安全风险及时评估，根据评估等级，制定相关的解决方案和应急措施，相关技术人员需要具有应变能力确保网络安全结构稳定，网络安全的稳定和可靠，能够促进智慧校园建设，推动社会经济发展。

参考文献

[1]刘海龙，张刚刚.浅谈智慧校园总体框架网络安全风险评估的运用[J].网络安全技术与应用，2020（05）：97-99.

[2]张顺利.《智慧校园总体框架》标准的网络安全防护[J].信息与电脑（理论版），2019，31（20）：204-205.

[3]符睿.智慧校园环境下网络安全体系设计与建设研究[J].网络安全技术与应用，2021（05）：111-112.