新疆大学本科论文

新疆大学
Xinjiang University

论文题目：	浅谈网络空间安全对高校校园安全的影响与对策
学生姓名：	刘宇诺
学　　号：	20201210207
所属院系：	信息科学与工程学院
专　　业：	计算机科学与技术
班　　级：	计算机科学与技术 20-1
指导老师：	海拉提·克孜别克
日　　期：	2022 年 9 月 20 日

声　明

本人郑重声明，本论文是在导师的指导下独立完成，除加注和致谢外，文中不包含他人所发表或撰写的成果。本人拥有自主知识产权，没有抄袭、剽窃他人成果，对于参考的文献已经加注并表示感谢。若有不实之处，本人愿意承担相关法律责任。

作者签名：刘宇诺

签字日期：2022 年 9 月 20 日

摘　要

随着信息技术的告诉发展，各大高校利用校园网络积极推进校园信息化管理。通过信息化数据可以更高效的管理校园，促进校园发展，增强校园的综合实力。校园里的大量有价值的数据上传到网络上，也成为了很多不法分子的网络攻击目标。网络空间被称为第五空间，没有网络安全就没有国家安全。高校网络数据有学生信息、科研成果、教学数据等很多重要的信息，一旦遭遇网络攻击将会有重大损失。所以网络空间安全对高校校园安全至关重要，各大高校在进行信息化建设的同时也要高度重视网络安全建设。本文将对高校的信息化建设和不法分子攻击的目的进行分析，概述高校网络安全建设存在的难点，并提出增强高校网络安全建设的对策。

关 键 词：信息化建设；网络安全；网络攻击；校园安全；网络空间

ABSTRACT

With the telling development of information technology, major universities are actively promoting campus informatization management by using campus networks. The informatized data can manage the campus more efficiently, promote the campus development and enhance the comprehensive strength of the campus. The large amount of valuable data on campus uploaded to the network has also become the target of cyber attacks by many lawless elements. Cyberspace is known as the fifth space, and without cyber security there is no national security. The network data of colleges and universities have student information, research results, teaching data and many other important information, which will have significant losses once they encounter cyber attacks. Therefore, cyberspace security is crucial to the security of college campus, and major universities should pay great attention to network security construction while carrying out information construction. In this paper, we will analyze the information construction of colleges and universities and the purpose of unlawful elements' attacks, outline the difficulties of college network security construction, and propose countermeasures to enhance college network security construction.

Key words: information construction; network security; network attack; campus security; cyberspace

目　录

1 绪论

随着大数据、人工智能、云计算、物联网和区块链等新一代网络技术的发展，我国已经发展成为一个科技强国。各大高校也积极推进校园信息化，通过利用新技术和网络信息化来更方便的管理校园，同时也能更好制定出适合自己学校学生的培养方案。高校信息化所要解决的核心问题是建立数字化校园，在大学校园内组建数字化的网络环境。通过网络多元化、共享化的特征，建立一个开放性的新型现代教育模式，以达到高校教育资源的共享和高校教育过程优化的目的。[1]高校的信息化发展不仅有有利于高校的发展，也有利于社会的进步，对于推动我国信息化发展有重要作用。但与此同时，一些危害网络安全的病毒、木马、恶意软件、钓鱼邮件等网络威胁也层出不穷，对高校数字化发展和信息化变革带来了很大挑战。高校的学生信息、科研成果、测试数据、教师信息、教务系统、财务系统等都在校园网中进行处理或者保存，这些都是很重要的信息，如果被不法分子窃取，将会对校园造成巨大的损失，也会危害国家安全。所以网络空间安全和高校校园安全紧密相连。高校在进行数字化发展的同时也要重视网络安全建设。所谓校园网络安全就是保证校园网络的软件、硬件和网络数据安全，避免校园的网络受到恶意、偶然的攻击，最终导致校园的系统受到信息泄露、修改与破坏等，进而保证校园网络系统的安全稳定运行。[2]高校应高度重视网络安全建设和保障工作，最大限度降低网络安全事件发生的概率，保障教学、科研和办公的正常进行。[3]

2 分析高校遭到网络攻击

2.1 高校为何成为网络攻击的主要目标

随着高校信息管理的推进，高校越来越多的事物要在网络中进行，并且越来越多的数据进行数字化后保存于网络之中。高校校园网络具有开放，覆盖面广，主机和带宽 资源丰富，用户群体活跃，盗版资源泛滥等特点，从而使得校 园网络很容易成为网络攻击和入侵的目标。[4]高校的校园服务器中存储着大量师生的个人信息和敏感数据，不法分子可以窃取到这些信息后进行贩卖以达到获利的目的；高校的数据中心有这很多高性能的计算机，不法分子可以通过攻击来获取这些资源，用这些高性能的计算机进行“挖矿”活动，通过虚拟货币来获利；高校的教务系统、财务系统、学工系统这些信息都保存在网络中，不法分子通过攻击财务系统进行非法获利；高校还有科研数据、核心专利、考试数据，黑客通过攻击获取到数据，进行非法售卖；还有很多高校和公司有科研项目，和政府有基础设施建设活动，和军队有联合研发项目，被他国通过网络攻击非法获取数据，危害我国国家安全。一些不法分子为了获取利益对高校进行非法攻击，一些国家对高校攻击获取国家数据危害国家安全。这些原因使得高校成为网络攻击的主要目标。高校进行信息化给高校带来了效率和便利，同时外部的风险和危害也增加了，所以高校要重视网络空间安全，网络空间安全与我们每一个使用网络的公民也息息相关。

2.2 网络攻击

在高校中每天都有很多学生使用电脑，通过 U 盘进行数据拷贝或者存储。很多同学网络完全意识相对较薄弱，在使用是没有查杀病毒的习惯，如果 U 盘携带病毒进入终端，同学之间用 U 盘拷贝数据、学生将 U 盘插入学校机房进行数据下载、师生之间通过 U 盘传资料，这将导致病毒成链式传播，最终会造成大规模的终端中病毒，校园网络可能也会遭受攻击。

以破坏校园网络为目的的黑客用 DOS 攻击破坏校园的服务器，致使校园网络瘫痪。DOS 攻击原理：首先攻击者向服务器发送众多的带有虚假地址的请求，

服务器发送回复信息后等待回传信息，由于地址是伪造的， 所以服务器一直等不到回传的消息，分配给这次请求的资源 就始终没有被释放。[5]等服务器因超时切断一次请求后，攻击者会再次发起新的攻击，这样频繁的攻击会大量的占用服务器的资源，最终会导致服务器的资源占尽，而校园中师生的正常的网络请求无法完成。DOS 攻击只要一台单机和一个 modem 就可实现，而 DDOS 攻击是利用一批受控制的机器向一台机器发起攻击， 这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。[6]所以黑客利用 DOS 攻击会对校园的管理和用户使用造成很大的破坏性作用。

在链路层的破坏。网络接口层在 TCP/IP 网络参考模型中的主要作用是实现数据的传输，将网络层的数据包封装上 MAC 地址最后一比特流的形式在网络中传输到达目的地。黑客能通过监听方式对传输的数据进行获取、篡改和破坏。黑客通过发送大量的假的 MAC 地址，从而使 MAC 地址无法正常的工作；在桥接过程中，通过分析桥接数据来获取校园数据传输过程中的隐私数据；攻击者通过分析传输数据获取目的 MAC 地址，然后将自己的 MAC 地址伪装成目的 MAC 地址，从而使数据传输出现问题;ARP 协议攻击最常见的攻击方式为攻击者通过修改 ARP 表的 网络目标地址，以此来实现中间人攻击、服务拒绝攻击等[7-8]。

恶意应用软件的破坏。有些大学生的网络安全意识淡薄，在使用网络时可能会安装了包含恶意病毒的应用软件，从而导致电脑中病毒，病毒可以通过网络在校园中大量传播。恶意病毒传播途径还有文件夹共享，在局域网中的病毒会搜索本地网络存在的共享，通过口令猜想获得安全访问权限，然后将自身复制到网络共享文件夹中，并进行伪装诱导用户执行，从而感染病毒；网络下载或者浏览，先在越来越多的伪装的很多好恶意浏览网页和链接，从而使用户访问恶意网页，下载捆绑病毒，点击恶意链接成为病毒传播的主要途径；电子邮件传播，不法分子将制作好的病毒放到附件中然后大量的发送给众多用户，利用邮件内容引用用户打开带有病毒的附件，从而使用户的电脑中病毒。计算机病毒一旦传人内网，病毒\恶意软件通过网络在极短时间可感染整个内网，轻则导致计算机速度减慢、死机、数据丢失；重则引起网络阻塞导致网络瘫痪，影响正常工作。[9]

3 高校网络安全提升对策

3.1 高校网络安全建设存在的难点

高校的信息化建设程度不同，有的高校信息化建设程度很高，其网络空间安全意识较高，网络安全建设也相对较全面；而信息化建设相对较弱的高校，其对网络空间安全的认识程度较弱一些，对网络安全建设的迫切程度也相对低一些。网络空间安全建设需要人、物、财三个方面的投入，需要网络安全方面的人才提供技术支持，需要加大网络空间安全建设的财政投入比例，在网络设备方面也需要较好且更安全的设备来维护校园网络系统的运行。网络技术在不断更新进步，黑客的恶意攻击手段也在不断更新变化。部分高校的安全系统是几年前的 老旧安全系统，面对今天的黑客攻击，其安全性会折扣很多。一套网络安全系统可能在今天情况下是合适的，但是随着技术的更迭，它的安全性能也会逐渐下降。

3.2 高校网络空间安全提升对策

各个高校联合开展网络空间安全交流会，不同的高校之间分享彼此在网络安全方面的看法和见解，帮助信息化建设程度相对低的高校增加网络安全意识，进行信息交流有利于实现信息互通，针对不同给的网络攻击进行安全部署。西北工业大学遭受境外网络攻击，西北工业大学公开发布遭受境外网络攻击，积极采取防御措施的行为值得其他遭受网络攻击的受害者学习，这将成为世界各国有效防范境外网络攻击行为的有力借鉴。

高校要重视网络安全方面的人才培养，为社会和国家培养网络安全技术人才，在培养过程中也会增强学校网络安全技术综合实力。学校要定期对学生进行网络安全方面的知识宣讲、进行防范网络攻击的教学和安全防范意识的培养。尤其要重视新生的网络安全教育。

学生要提高自己的网络安全意识，在个人电脑上安装个人版软件查杀病毒，进行定期的病毒查杀和漏洞修补，不给恶意软件和木马病毒趁虚而入的机会。在使用 U 盘等其他截止进行资源传递时，要提前进行病毒扫描，以降低感染病毒的风险。面对不熟悉的网页、来源不明的链接、陌生人发来的邮件，都不要进行

随意打开和转发，把病毒侵袭的风险讲到最低，保证了自己网络的安全，同时也促使校园网络更加安全。

高校网络安全是以保护现有业务系统为基础，利用成熟的防御技术来保障网络安全。[10]网络安全技术主要有防火墙、数据加密、入侵检测技术、身份认证技术、病毒防护技术等。高校要及时学习和使用现有的成熟技术，对高校网络安全进行防护，并且定期进行网络病毒查杀。随着科技的进步和技术的迭代更新，也要及时更行网络安全防护技术，应对网络攻击手段的更新。

4 总结与展望

科技给校园的信息化发展带来的便利和高效，同时也有网络攻击的风险。不同高校面对的网络攻击风险可能不同，但都要高度重视网络空间安全，加强自己的网络攻击防御能力。本文分析了高校成为网络攻击的主要目标的原因以及网络攻击的手段，在未来中可能会有更过潜在的未被发现的网络攻击手段，各高校要重视网络攻击的危害性，将这些潜在危害扼杀在萌芽中。希望各高校共同联合，为我国校园网络安全共同构筑起网络空间防护的钢铁长城，为国家培养更多的网络空间人才，提高我国的网络安全防护能力。

参考文献

[1] 张凤梅,袁亮环. 高校信息化建设[J]. 中国管理信息化,2016,19(8):159. DOI:10.3969/j.issn.1673-0194.2016.08.115.

[2]韩晓露,刘云,张振江,等. 网络安全态势感知理论与技术综述及难点问题研究[J]. 信息安全与通信保密,2019(7):61-71. DOI:10.3969/j.issn.1009-8054.2019.07.010.

[3]刘鹏飞,王铁柱,韩佳乐,等. 高校网络安全发展实践与研究[J]. 网络安全技术与应用,2022(3):86-87. DOI:10.3969/j.issn.1009-6833.2022.03.051.

[4] 梁亮. 高校校园网络安全浅析[J]. 科学咨询,2018(32):20. DOI:10.3969/j.issn.1671-4822.2018.32.016.

[5] 谢小红. 校园网典型攻击的特征分析及防范措施[J]. 河南教育学院学报（自然科学版）,2004,13(2):67-69. DOI:10.3969/j.issn.1007-0834.2004.02.026.

[6]于泠,陈波.分布式拒绝服务攻击工具 Trinoo 的分析[J].计算机工程与应用,2002(3):152-154,231.

[7]韩雨桥,范宏.校园网中网络安全技术的应用策略[J].网络安全技术与应用,2016(3):91-91.

[8]韩红光.校园网网络安全策略构建与应用研究——以浙江农业商贸职业学院为例[J].电脑知识与技术,2016(3X):57-59.

[9]高军,肖卫. 试述内网计算机病毒/恶意软件的防范[J]. 长江工程职业技术学院学报,2011,28(1):35-36,39. DOI:10.3969/j.issn.1673-0496.2011.01.014.

[10] 彭明,刘建峰. 高校校园网络安全问题分析与对策[J]. 现代信息科技,2022,6(3):116-118. DOI:10.19850/j.cnki.2096-4706.2022.03.031.