河南教育信息化

HENAN EDUCATIONAL
INFORMATIZATION

— 2020 年 特别专题 —

国家网络安全宣传周
China Cybersecurity Week

主管：河南省教育厅科学技术与信息化处
主办：河南省教育科研计算机网网络中心

快来 PK! 2020 年河南省教育系统网络安全知识竞赛开启，有奖竞赛等你来！

时间：2020年9月15日-2020年9月16日
主办：河南省教育厅
承办：河南省教育信息安全监测中心
奖项设置：对成绩优秀者颁发纪念品及获奖证书
网址：https://aqjs.ha.edu.cn/

个人信息安全威胁与防护专题网站上线了！

法律法规解读、典型案例分析、安全防护支招……助力师生个人信息安全防护！

网址： http://www.ha.edu.cn

专题编前语

教育的发展离不开技术创新。云计算、物联网、人工智能、移动互联网等计算机技术的快速发展，催生着教育系统进行快速的自我革新与升级，给教育领域带来了革命性的影响以及重大的发展机遇。然而，我们也面临着勒索病毒、数据泄露等各种网络安全威胁，尤其是随着新技术与教育教学的深入融合，教育系统网络安全面临着更加严峻的挑战，其重要性更是不言而喻。那么，教育系统如何加强网络安全防护和保障能力呢？在 2020 年国家网络安全宣传周之际，《河南教育信息化》联合河南省教育信息安全监测中心共同推出本期网络安全专题，围绕 App 安全、数据安全及 IPv6 安全三大专题提供网络安全技术解决方案。

国家网络安全宣传周
China Cybersecurity Week

目录 CONTENTS

期刊简介

《河南教育信息化》立足河南，刊载行业动态、热点专题、经验交流及省内资讯等内容，多方位、多层次地探究教育信息化建设的前沿趋势、建设中的经验与问题，为教育信息化领域各级领导及从业人员提供科学、实用的决策依据。

App 安全

数据安全

IPv6 安全

河南教育信息化

2020 年 / 特别专题

主管 河南省教育厅科学技术与信息化处
主办 河南省教育科研计算机网网络中心

主编 孔繁士 王宗敏
执行主编 汪国安
编辑 吕玉玲
设计 蔡馨庆 吉祥

电话 0371-67763770
传真 0371-67763770
电子邮箱 editor@ha.edu.cn
通信地址 郑州市二七区大学路 75 号郑州大学南校区逸夫楼西 206 室
邮政编码 450052

扫一扫
关注河南教育信息化
更多精彩内容
为您呈现!

App 安全

随着移动通信和计算机科学技术的发展，智慧校园逐渐发展起来，移动应用也开始走向并广泛应用于校园。各级各类学校积极推进智慧校园建设，借助移动应用打造“互联网 + 校园”的智慧校园模式，为师生提供更加便捷的智慧校园服务。与此同时，校园移动应用的管理工作也成为信息化管理的重要组成部分。

国家网络安全宣传周
China Cybersecurity Week

App 安全

教育 App 行业规范解读

近年来，教育类 App 得到快速发展、广泛应用，在提高教育教学效率和管理水平、满足师生个性化应用等方面发挥了积极作用，但是一些学校出现了平台垄断、强制使用等现象，一些教育移动应用存在有害信息传播、广告丛生、信息违规采集、数据泄露等问题，给广大师生、家长、学校及教育机构带来了巨大的困扰，产生了极为不良的社会影响。

对此，教育部等部门重拳出击，相继发布了《关于引导规范教育移动互联网应用有序健康发展的意见》、《教育移动互联网应用程序备案管理办法》等相关政策加强对教育类 App 的监管，对符合国家监管标准的教育移动应用进行备案管理，并通过教育移动互联网应用程序，为广大学校、教育机构、师生筛选出安全、健康的教育类 App。

《八部门规范教育 App：不得与学分、成绩和评优挂钩，用未成年人信息应获授权》一文指出：

1.App 提供者应进行教育业务备案

《关于引导规范教育移动互联网应用有序健康发展的意见》（简称《意见》）明确，教育移动互联网应用程序（教育移动应用，以下简称教育 App）是指以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网 App。

《意见》要求，建立教育 App 备案制度。教育 App 提供者应当在取得 ICP 备案（涉及经营电信业务的，还应当申请电信业务经营许可）、网络安全等级保护定级备案的证明、等级测评报告后，向机构住所地的省级教育行政部门进行教育业务备案，登记单位基本信息和所开发的教育 App 信息。

对于已备案的教育 App 提供者，在上线新应用前，应当在备案单位更新相关信息。

2. 国家统一备案标准，各省份分头实施

教育部科学技术司司长雷朝滋介绍，备案按照“国家统一标准，各省份分头实施，企业属地备案”的原则开展。

国家统一标准，就是指教育部要制定教育 App 备案的管理办法，明确备案的主体、备案的时间、备案内容和备案流程；各省份分头实施，就是明确以省为单位推动备案，由省级教育行政部门组织本地区的教育 App 提供者和教育机构进行备案；企业属地备案，是指教育 App 提供者为企业的，要到注册地省级教育行政部门进行备案，通过信息共享，实现一省备案、全国有效，而教育 App 提供者为学校的，则按照属地关系到所属教育行政部门备案。

雷朝滋表示，将依托国家教育资源公共服务平台做支撑，实现“一省备案、全国有效”和全程网上办理，方便企业和学校备案。备案结果网上公示，公众和机构均可查询，为社会监督提供便利。

3. 对教育 App 审慎监管，不设置准入许可

建立备案制度是基于什么考虑？雷朝滋表示，2017 年教育部印发《关于教育网站网校审批取消后加强事中事后监管工作的通知》，建立备案制度是事中事后监管的有效手段，可准确掌握教育 App 供需双方情况，做到“底数清”、“情况明”。同时，利用大数据分析，掌握教育 App 发展的现状和存在的问题，为规范引导教育 App 有序健康发展提供决策依据。

教育部鼓励推荐优质教育 App 树立行业标杆，发挥头雁效应。鼓励购买优质教育 App 服务创新供给模式，促进产业发展。

雷朝滋称，对教育 App 实施包容审慎监管，不设置准入许可、加强事中事后监管，在严守底线的前提下为新业态发展留足空间。

4. 严控高校 App 数量禁擅自开发

教育 App 给学生学习带来不少便利，但不少学生却反映自己被 App“绑架”了，特别是在高校，打热水用一个 App，跑步用一个 App，连 WiFi 用一个，刷网课用一个，甚至湖南一所高校还曝出“扫码洗澡”的规定，让不少学生觉得“闹心”。对于高校 App 泛滥问题，教育部科学技术司司长雷朝滋回应称，要严控学校 App 数量，不得擅自开发和选用 App。

5. 学校推荐使用的教育 App，不得与教学管理行为绑定

《意见》在 App 进校合作方面明确，作为教学、管理工具要求统一使用的教育 App，不得向学生及家长收取任何费用，不得植入商业广告和游戏。对于学校推荐使用的教育 App，应当遵循自愿原则，不得与教学管理行为绑定，不得与学分、成绩和评优挂钩。

对于承担招生录取、考试报名、成绩查询等重要业务的教育 App，原则上应当由教育行政部门和学校自行运行管理。确需选用第三方应用的，不得签订排他协议，或实际由单一应用垄断业务。

《意见》指出，学校应严格选用标准、控制数量，避免造成不必要的负担。确定选用的 App 应当报上级教育行政部门进行备案。对于未经教育行政部门、学校集体决策选用的 App，不得要求学生使用。

《意见》指出，将按照“谁主管谁负责、谁开发谁负责、谁选用谁负责”的原则，建立管理责任体系。应建立 App 选用退出机制、负面清单和黑名单制度，推动将黑名单信息纳入全国信用信息共享平台，按有关规定实施联合惩戒。

6. 治理 App 信息泄露、低俗信息问题

《意见》指出，教育 App 的内容应体现素质教育导向，呈现的广告应当与提供的服务相契合。以未成年人为主要用户的应用应当限制使用时长、明确适龄范围，对内容进行严格把关；具备论坛、社区、留言等功能的教育 App 应当建立信息审核制度。

7. 教育 App 不得变相强迫收集用户信息

对于用户数据隐私的保护，《意见》指出，教育 App 提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制。应当明示收集使用信息的目的、方式和范围，并经用户同意。收集使用未成年人信息应当取得监护人同意、授权。

《意见》尤其指出，不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供服务无关的个人信息，不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人信息。（来源：教育部、《新京报》）

教育类 App 安全状况分析

2019 年 8 月，教育部、中央网信办、工业和信息化部、公安部等八部门联合印发《关于引导规范教育移动互联网应用有序健康发展的意见》，将教育 App 分为三类，一是市场竞争提供、师生自主选用；二是学校企业合作、学校组织应用；三是学校自主开发、部署校内使用，并提出了教育 App 规范发展的 4 方面 20 条工作措施。

2020 年 1 月，根据新冠肺炎疫情防控工作需要，教育部下发《关于 2020 年春季学期延期开学的通知》，并随后作出了一系列“停课不停教、停课不停学”的部署。网课，成为了大中小学、各类教育培训机构的爆款。在线授课、在线培训、在校讲座的爆炸式增长，给中国的“互联网 + 教育”带来了新的发展契机，各类教育移动互联网应用（简称教育 App）蓬勃发展，但也加大了原本存在的安全隐患。

以下为公安机关网安部门根据国家计算机病毒应急处理中心、广东移动互联网安全监测中心、北京网警、河北网警工作情况整理的关于教育类 App 的安全分析报告。

一、基本情况

目前，全国活跃的教育类 App 约 4100 余款，其中在教育部备案的约 3500 余款，约占总数的 85%。

疫情期间，有两类教育 App 成为全国大中小学校的主要选择。

一是市场竞争提供、客户自主选用的教育机构自建类 App。此类应用一般设置信息发布及网络教学等模块，展示教育机构及课程信息，提供报名渠道、缴费退费等服务，同时可作为上传相关视频课程的交流平台、在线提供教育服务的工作平台，供学习使用。此类 App 是教育类机构专门研发的学习软件，有独创知识成长体系，并有教师在线提供教育服务。

二是学校企业合作，学校组织学生应用的 App。在此类应用中，有的在网络直播平台上开辟在线教育模块，由具体开课学校注册，教师在线直播教学、互动答疑。学生根据学校授权登录使用，非本校学生不得进入直播间听课。有的借助视频平台开辟网络课堂视频模块，由教育部门或学校组织教师统一录制教学视频，上传平台供学生播放学习。在视频模块中只保留最基本观看功能，关闭了所有评论、弹幕及广告。

二、主要安全隐患

1. 部分 App 技术能力和管理制度不足

“互联网 +”政策实施为从事网络教育的企业注入了新活力，部分企业 3 至 5 年之间即完成了从初创到累计用户超过 1000 万的发展历程，但部分 App 前期准备不充分，网络安全技术防护措施及安全管理制度难以满足企业发展规模需要，抵御网络攻击、防范信息窃取能力不足，存在一定安全隐患。

2. 部分 App 存在数据违规采集的情形

多种教育类 App 通过线上答题器、多媒体课件展示、互动式小黑板等功能，采集各类用户数据，但不同程度存在超范围采集个人信息、未经用户同意采集个人信息的情况。

公安机关网安部门在检查过程中发现，部分 App 隐私协议未明示或明示过于复杂、难懂；部分 App 存在读取通话记录及短信内容、收集用户通讯录及位置信息等超范围采集用户信息违法违规行为；部分 App 通过 HTTP 非加密协议进行传输，后台数据保存也未严格加密，极易造成数据泄露。

3. 网络安全风险防范准备不足

此次新冠肺炎疫情防控客观上造成了教育类 App 用户激增，导致一些平台在风险防范等方面准备不足。如不久前媒体曾曝光出教育类 App 的授课教师在直播中抽烟、观看网上教学视频需要先观看一定时间的未成年人不宜的广告等情况。

同时，有一些教育类 App 为追求利益，广告弹出频繁、大量推荐网络游戏、广告内容过度娱乐化，甚至存在涉黄涉赌等违法有害信息，污染青少年学习环境。

4. 监管工作面临新挑战

教育类 App 平台入门门槛低、受众范围广，特别在疫情期间的爆炸式增长，给教育等主管部门、相关监管部门带来了新挑战。部分 App 应用商店、教育类 App 运营企业的安全主体责任落实不到位，部分小众网课服务应用采取二维码的推广方式脱离监管。（来源：公安部网安局）

高校校园 App 安全保护方案

校园 App 快速普及的同时，其安全问题也逐渐凸显。在技术上，开发者为高校定制校园 App 等碎片化服务而忽略安全问题；多数开发者的安全技术匮乏，无法就移动应用从设计、编码、测试、发布、更新等各个环节对安全风险进行控制。这些原因都可能导致校园 App 在防攻击、防篡改、防病毒等方面安全防护能力较低。在管理上，国内 Android 市场缺乏安全监管机制，以及 Android 平台的开源与开放性，校园 App 市场需求大等一系列因素，导致众多高校校园 App 出现诸多安全问题。

在校园 App 出现的诸多安全隐患中，程序源文件安全、本地数据存储安全、网络传输安全、内部数据交互安全、恶意攻击防范能力等，从多方面展示了校园 App 可能存在的安全风险，如图 1 所示。

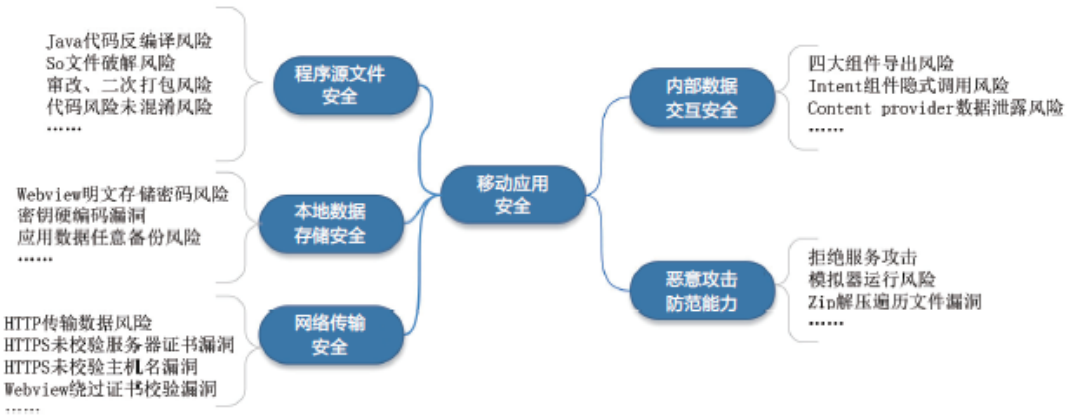


图 1 校园 App 存在的安全隐患

此外，国内外研究多是阐述如何对大批量的应用程序进行检测，但在高校校园的特殊业务场景下，针对此类碎片化业务服务，如何保护校园 App 安全的研究较少。本文根据北京大学医学部开发校园 App 时采取的措施，从应用程序源文件安全和数据安全两方面阐述校园 App 的安全保护方案。

一、校园App安全隐患研究

1. 程序源文件安全隐患

应用程序中含编码阶段的代码包和配置文件，在 Android 开源的环境下，如果未对应用程序采取有效保护措施，可能面临被反编译的风险。攻击者可能使用下载工具对未经加固保护的应用程序、可执行文件进行反汇编、反编译或动态调式等攻击，并可能通过逆向法破解应用程序的实现逻辑，如获取与服务器端的通讯方式、加解密算法、密钥、软键盘实现技术等，从而造成算法被窃取、文件被非法篡改或是程序接口被调用、篡改应用程序内容、植入恶意收费应用或广告 SDK、引诱下载其他应用程序等后果。因此，高校校园 App 的开发者需保证应用软件包的完整性和可靠性。

2. 数据存储与传输安全隐患

（1）数据存储与交互安全隐患

校园数据安全是高校信息化安全建设的重要组成部分。高校数据库一般都部署在学校内网的服务器中，并且有专门的防火墙限制，利用网络层面进行数据保护。而在使用移动应用的过程中，如果开发者在 AndroidManifest.xml 文件中权限配置不当，客户端本地静态数据如本地系统文件、本地业务数据等都可能被盗用，从而造成用户的敏感信息泄露。

Android 系统本身有四大组件：Activity、Service、Broadcast Receive 和 Content Provider。Activity 组件是 Android 程序与用户交互的界面；Service 组件是后台运行的服务进程；Broadcast Receiver 组件对外部事件进行过滤接收，并根据消息内容执行响应；Content Provider 组件是应用程序之间共享数据的容器，可以将应用程序的指定数据集提供给第三方 App。

不同的应用程序或进程之间可能存在共享数据，然而应用程序中不同的数据具有严格的访问权限。如果访问权限设置不当，应用程序中的数据可能被其他程序直接访问或修改，导致用户的敏感数据泄露，或应用程序被恶意篡改账号，盗取账号信息等。若组件中设置了导出权限，存在登录界面被绕过、敏感数据泄露、数据库 SQL 被注入的风险。

（2）数据传输安全隐患

客户端与服务器之间传输数据通常遵循通信协议指定的内容格式和内容类型，如果未对传输数据加密，传输数据很有可能被还原成网络层的数据包进行解包并分析，暴露通信过程中的各种关键数据。

在使用 HTTPS 协议时，客户端需对服务器身份进行完整性校验，即验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器进行通信链接，即造成“中间人攻击”。

当客户端的 WebView 组件访问使用 HTTPS 协议加密的 URL 时，如果服务器证书校验错误，客户端应该拒绝继续加载页面。如果重载 WebView 的 onReceivedSslError() 函数并在其中执行 handler.proceed()，客户端可以绕过证书校验错误继续访问此非法 URL，将导致“中间人攻击”。攻击者冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，充当中间人转发信息的时候，也有可能窃取手机号、账号、密码等敏感信息。

二、安全防护实践

1. 解除程序源文件安全隐患

应用开发者可以使用自己开发的加固工具或是第三方的加固工具，来强化应用程序的安全能力。

加固技术可以在不改变应用客户端代码的情况下，将针对应用程序的各种安全缺陷保护技术集成到应用客户端中，提供应用开发、打包、发布、运行全生命周期的安全，并在文件中设置防二次打包的配置，有效防止针对移动的反编译、二次打包、内存注入、动态调试等恶意攻击行为，进而全面保护应用程序安全。

北京大学医学部在开发校园 App 时，研发人员采用加固方式保护 Android 版本的程序源文件安全。

图 2 APK 文件加固方案

对 APK 文件加固后，可以有效保护 Android 应用程序不被反编译。同时，代码混淆通过将 Java 代码中的方法名、变量名、类名、包名等元素名称改成毫无关联且无意义的名字，或对简单的逻辑分支进行混淆，使攻击者难以找到函数调用的内容，无法掌控 App 内部实现逻辑，增加逆向工程和破解的难度。

除使用加固工具外，北京大学医学部还针对打包上线的应用程序，将 Android 版本应用发布在校园内的服务器上；因 iOS 应用必须通过 App Store 审核，故将 iOS 版本应用发布在 App Store 上，同时向用户公布官方下载路径。由此可以有效避免校园应用被植入其他应用程序，防止 App 被破解、被盗版，防止恶意推广安装其他应用软件，避免用户安装仿冒软件等。

2. 解除校园 App 数据安全隐患

（1）解除数据存储与交互的安全隐患

如上文所说，校园 App 在数据存储与交互时存在安全隐患。目前，高校大都使用统一身份认证，故登录时的账号和密码都不会在本地存留。应在考虑数据安全时重点考虑业务数据存储安全、交互数据安全和传输数据安全。

解除 Webview 明文存储密码风险。其他恶意程序也可能通过提权或者 root 的方式访问 Webview 数

据库，窃取用户的用户名信息及密码。北京大学医学部在开发 App 时通过设置 WebView.getSettings() 中的方法 setSavePassword(false) 关闭 Webview 组件的保存密码功能。

关闭必要组件的导出权限。限制 AndroidManifest.xml 中的 Activity、Broadcast Receiver、Content Provider、Service 组件导出权限，对于须导出的组件必须限制于授权用户或者应用组件。

采用显式方式调用 Intent 组件。Intent 通常用于 Activity、Service、Broadcast Receiver 等组件之间进行信息传递，包括发送端和接收端。当使用隐式的 Intent 调用时，并未对 intent 消息接收端进行限制，因此可能存在该消息被未知的第三方应用劫持的风险。Intent 消息被劫持，可能导致用户的敏感数据泄露，或者恶意程序执行等风险。

（2）解除数据传输安全隐患

采用 HTTPS 协议传输数据。北京大学医学部在开发校园 App 时，针对业务敏感数据，采用 HTTPS 传输协议，加入了 SSL（Secure Socket Layer）子层实现的 HTTPS 协议可确保数据在网络上加密传输，即使传输数据被截获，也无法解密和还原，保护数据在传输中的安全。

HTTPS 需校验服务器。Android 允许开发者重定义证书验证方法，重定义之后，若不对证书进行正确的校验，同样可能会导致“中间人攻击”。所以如果开发者重定义了证书验证方法，还需要对证书进行校验。

禁止 Webview 组件绕过证书校验。攻击者冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，充当中间人转发信息的时候，也有可能窃取敏感信息。所以 WebView 绕过证书校验时，也可能会造成“中间人攻击”。

采用安全加密算法并避免密钥硬编码。AES/DES 是常用的两种对称加密算法，其工作模式有 ECB、CBC、CFB 和 OFB。当其使用 ECB 或 OFB 工作模式时，加密数据可能被选择明文攻击 CPA 破解；密钥硬编码也易造成加密算法被破解，导致客户端隐私数据泄露，加密文件破解，传输数据被获取，“中间人攻击”等后果，造成用户敏感信息被窃取。

（3）提升恶意攻击防范能力

长远角度来讲，没有绝对的安全。校园 App 除了应用程序本身的问题外，还需注意防护外界的恶意攻击，即在遵守应用程序开发规范的前提下，不断提升自身防护能力，做好应用程序的安全防护工作，排除安全隐患。北京大学医学部在迭代更新校园 App 时，都会使用业界安全公司的安全检测服务对新发版的应用进行安全检测，避免因增加新的业务服务带来安全问题。（作者：魏仿，北京大学医学部信息通讯中心；来源：《中国教育网络》）

对《App 违法违规收集使用个人信息行为认定方法》的分析

继 2019 年 1 月 25 日国家互联网信息办公室、工业和信息化部、公安部、市场监管总局发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，2019 年 12 月 31 日四部门联合制定并发布了《App 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）（以下简称《认定方法》）。《认定方法》的出台，为监督管理部门认定 App 违法违规收集使用个人信息行为提供参考，为 App 运营者自查自纠和网民社会监督提供指引。

App 专项治理工作组对照《认定方法》，结合近千款 App 评估中发现的典型问题，进行具体分析，供各界参考，对于学校选用、治理 App，维护教育系统网络安全提供了参考与依据。

一、典型“未公开收集使用规则”行为

◆法律法规依据：

《网络安全法》第四十一条规定，网络运营者收集、使用个人信息时，应当公开收集、使用规则。

《消费者权益保护法》第二十九条规定，经营者收集、使用消费者个人信息，应当公开其收集、使用规则。

◆典型行为：

1. 仅在官网、应用商店中展示隐私政策而在 App 内无法找到隐私政策的，或隐私政策链接无效、文本不能正常显示的，或隐私政策中没有包含该 App 收集使用个人信息规则。

2.App 首次运行，未通过明显方式提示用户阅读个人信息收集使用规则；只在注册 / 登录界面展示隐私政策链接，进入 App 主界面后，无法找到隐私政策；刻意使用灰色字体、缩小字号、遮挡、置于边缘与背景颜色相近等方式未突出显示隐私政策链接；用户注册时，注册 / 登录界面无隐私政策链接。

3. 隐私政策访问路径设置过深，多于 4 次点击操作才能访问到；或路径设置过偏，要通过搜索、咨询客服等方式才能访问到。

4. 隐私政策文本字号、颜色、行间距、列宽、清晰度等设置造成用户阅读困难，如隐私政策文本字号过小，隐私政策文本列宽设置大于屏幕，隐私政策无法完整显示。

二、 典型“未明示收集使用个人信息的目的、方式和范围”行为

◆法律法规依据：

《网络安全法》第四十一条规定，网络运营者收集、使用个人信息，应明示收集使用个人信息的目的、方式和范围。

《消费者权益保护法》第二十九条规定，经营者收集、使用消费者个人信息，应明示收集、使用信息的目的、方式和范围。

◆典型行为：

1.App 嵌入第三方 SDK 存在收集个人信息的情况，但未在隐私政策里说明其收集使用个人信息的目的、方式、范围。

2.App 隐私政策中未完整列举逐项说明 App 实际业务功能收集使用个人信息类型、目的、方式。

3. 仅依赖系统弹窗但未在向用户申请收集个人信息的权限时告知申请的目的或未同步告知用户收集使用个人敏感信息的目的。

4.App 主动进行权限申请的二次弹窗，但仅重复申请权限而未告知目的，或目的描述不明确，用户无法得知 App 收集该类个人信息真实目的。

5. 隐私政策内容晦涩难懂、逻辑结构混乱、用语不符合通用习惯。

三、 典型“未经用户同意收集使用个人信息”行为

◆法律法规依据：

《网络安全法》第四十一条规定，网络运营者收集、使用个人信息，应经被收集者同意“且”不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。

《消费者权益保护法》第二十九条规定，经营者收集、使用消费者个人信息，应经消费者同意且不得违反法律、法规的规定和双方的约定收集、使用信息，经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

◆典型行为：

1.App 安装后，未经用户同意就收集设备 MAC 地址、应用程序列表等个人信息；用户明确表示不同意提供位置信息后，仍通过收集设备 IP 地址、通讯基站、WiFi 信息等计算出用户地理位置等个人信息。

2. 用户不同意收集非必要的个人信息或打开非必要权限，App 每次启动仍索要用户已明确拒绝提供的系统权限或个人信息；用户使用与已拒绝的系统权限或个人信息无关的功能时频繁提示用户授权同意。

3. 在申请可收集个人信息权限时，声明只使用其中与业务相关信息，实际上却收集并上传了该权限可允许的所有信息；实际收集的个人信息特别是个人敏感信息超出隐私政策等相关规则的范围；未真实披露收集使用个人信息的目的，欺骗用户打开可收集个人信息的权限。

4. 采用默认勾选同意隐私政策等非明示方式使用户略过隐私政策，注册或登录的选项与同意隐私政策的因果逻辑关系不清楚，使用户易略过隐私政策。

四、典型“违反必要原则，收集与其提供的服务无关的个人信息”行为

◆法律法规依据：

《网络安全法》第四十一条规定，网络运营者不得收集与其提供的服务无关的个人信息。

《消费者权益保护法》第二十九条规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则。

◆典型行为：

1.App 收集的个人信息类型或打开可收集个人信息的权限，超出其业务功能所需，如计算器工具类 App 申请打开位置权限、输入法类 App 申请打开通讯录权限等。

2. 强制索要的系统权限或个人信息非 App 运行所需的必要条件，如金融类 App 不同意打开通讯录和位置权限、地图类 App 不同意打开短信权限，则拒绝提供所有业务功能，中介类 App 拒绝提供银行卡号、持卡人身份证号、银行预留手机号等信息进行银行卡认证，则不允许发布任何信息等。

3.App 后台自动收集用户设备 IMEI 号、IMSI 号、地理位置等信息过于频繁，超出业务功能实际需要，如某 App 平均每秒获取 10 次 IMEI 号，非地图导航类 App 平均每秒上传 6 次 GPS 定位信息。

4. 安卓版 App 将软件安装包中的 targetSDKversion 属性值设置为低于 23，安装时，要求用户一次性打开多个可收集个人信息的权限。

五、典型“未经同意向他人提供个人信息”行为

◆法律法规依据：

《网络安全法》第四十二条规定，网络运营者未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人信息且不能复原的除外。

◆典型行为：

1. 未告知用户对外提供、转让个人信息的目的、类型及接收方身份，且数据未经处理即通过客户端或嵌入的 SDK 等代码、插件提供给了第三方。

2. 未告知用户个人信息出境情形，将数据传输至境外。

3. 未告知也未经用户同意，将个人信息直接提供给接入的小程序、公众号、服务应用等第三方主体。

六、典型“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”行为

◆法律法规依据：

《网络安全法》第四十三条规定，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

《网络安全法》第四十九条规定，网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络安全的投诉和举报。

《电信和互联网用户个人信息保护规定》第十二条规定，电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉，并自接到投诉之日起 15 日内答复投诉人。

◆典型行为：

1.App 中提供的更正、删除个人信息及注销用户账号渠道无法完成相应的操作；未在承诺时间内完成相应操作；客户端提示用户注销成功后，原账号相关信息仍保留在 App 后台服务器上。

2. 注销时，要求用户提供手持身份证正反面照片，更正个人信息时要求提供人脸认证信息等个人敏感信息。

3. 未建立并公布个人信息安全投诉、举报渠道；未按照法律法规要求或 App 承诺时限受理并处理用户个人信息投诉、举报。

以上分析为判别 App 违法违规收集使用个人信息行为提供参考，便于 App 运营者和网民了解《认定方法》，从而更有针对性地提升保护个人信息水平和能力。同时，建议对 App 违法违规收集使用个人信息行为进行认定时应当秉承科学、客观、审慎的态度，以现有法律法规为根本依据，对于发现的问题需全面分析得出结论。比如，问题是否具备典型性、是否为普遍性问题、是否已存在解决方案、对个人权益的影响程度、对产业生态可能带来的影响等。

个人信息保护的问题，已经开始步入“深水区”，而这其中对于个人信息保护与开发利用、产业生态创新与发展等方面的探讨将更加深入、复杂、具体。安全从来不是一个“孤立”的问题，如何以“治理工作”为契机，探索适应当下安全态势和舆情趋势、有利于遏制违法违规乱象、有助于保障产业高质量发展的持续监督机制，是“当务之急”，也是“长久之计”。（作者：App 违法违规收集使用个人信息专项治理工作组；来源：《中国市场监管报》）

数据安全

随着教育信息化的发展，学校积累了越来越多的教育数据。这些数据在极大地促进了教学、科研与管理质量提升的同时，由此引入各类信息系统中存储的敏感数据也越来越多，这也预示着未来越来越大的潜在数据安全风险。教育大数据直接关系到师生个人利益、校园稳定、教育系统稳定，其安全维稳工作更是至关重要。

国家网络安全宣传周
China Cybersecurity Week

数据安全

新形势下数据安全现状

新形势下数据安全内涵已发生变化

传统定义中，数据安全是指计算机网络安全中数据层面的安全，其防护主要是面向外部黑客，以对外部黑客或入侵者的防控为主要对象，以区域隔离、安全域划分为目标，以边界防护为主要安全手段，管理于技术相对分离。

新形势下，数据安全是指以数据的安全使用为目标，以数据分级分类为基础，以信息使用过程中的安全管理和技术支撑为手段，安全产品技术和流程管理深度融合的一种新的数据安全管控体系，其对数据的保护应涵盖数据的整个生命周期，满足数据安全保护、合规性和敏感数据管理。

数据安全领域主要关注的防护对象包括个人信息和重要数据。《网络安全法》指出，个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。重要数据是指不涉及国家秘密和军事数据，但与国家安全、经济发展以及公共利益密切相关的数据，包括但不限于公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的各类机构在开展业务活动中采集和产生的，不涉及国家秘密，但一旦泄露、篡改或滥用将会对国家安全、经济社会发展和公共利益造成不利影响的数据。

数据的生命周期包括：数据的采集、数据传输、数据存储、数据处理、数据共享 / 交换、数据销毁几个阶段。在定义中，数据安全保护既包括对数据的可用性、机密性、完整性等保护，也包括对数据的合规性和敏感数据管理保护。数据安全的核心是保障数据在其全生命周期的各个阶段均可实现高度可控与高度可审计，通过技术保护与高效管理尽可能隔绝各类威胁因素。

新形势下数据安全体系建设与传统数据安全的差异对比如下表所示。

表1 数据安全体系建设与传统数据安全的差异对比

对比条目	数据安全体系建设	传统数据安全
目标	数据的安全使用	数据的安全防护，不受攻击
对象	内部人员，实现对其行为的安全管控	外部黑客，实现对外部黑客或入侵者的防控
理念	以数据分级分类为基础，以信息合理、安全流动为目标	以区域隔离、安全域划分为目标
治理途径	以信息使用过程的安全管理和技术支撑为手段	以边界防护为主要安全手段
安全技术和流程管理的融合情况	深度融合	相对分离

数据安全风险日益凸显 国家出台多项标准、规范

常见的数据安全威胁包括数据泄露、勒索病毒、对数据的恶意破坏以及来自于内部人员的误操作等。随着数据和资产交易市场的形成，以及勒索病毒的演进，数据面临的风险越来越大，以勒索病毒和信息泄露为代表数据安全威胁其给企业、社会带来的严重危害。

美国安全公司 Carbon Black 发布了 2018 年勒索软件调查报告，报告显示，暗网经济中勒索软件的市场规模猛增了 2502%。2017 年，暗网上勒索软件的相关产品销售额高达 623 万美元，是 2016 年 25 万美元的 25 倍。勒索病毒等数据安全威胁给企业、社会带来严重危害的同时，也加快和促使了一系列法律、法规的出台，数据安全相关的法律、法规的制定是保障数据不被窃取、破坏和滥用的基础。

2017 年 6 月 1 日正式实施的《网络安全法》，明确了数据安全的责任部门与人员，指出应围绕数据安全构建人员管理与培训制度，对数据影响的评估与审计制度，指出各单位应明确业务调用数据的范围，建立自动化审计系统。《网络安全等级保护 2.0》则从网络安全、应用安全和数据安全层面对各数据的拥有主体提出了具体的要求和规范。

在个人数据隐私保护方面，从 2019 年开始，国家通过法律、监管和技术手段共同构建个人数据隐私保护。《App 个人信息收集与隐私政策测评报告》、四部委联合开展的《App 违法违规收集使用个人信息专项治理》行动，以及四部门联合制定并发布的《App 违法违规收集使用个人信息行为认定方法》，说明个人信息数据是企业的核心资产，企业在强调权利的同时，也应切实担负起保护用户隐私安全的责任。

《数据安全法》在今年的第十三届全国人大常委会第二十次会议通过审议，其草案 7 月在全国人大网全文公开征求意见。其中指出，国家将对数据实行分级分类保护，要求企业和组织开展数据活动必须履行数据安全保护义务，承担社会责任。

近年来，高校数据安全事件频发，师生信息泄露风波频繁上演。建立完善的数据安全体系，是高校教育信息化工作的重要内容，也是高校亟待解决的问题。（河南省教育信息安全监测中心整理）

如何进行数据安全体系建设?

针对数据安全威胁面临的新的挑战，数据安全防护具体要如何来做？数据安全的建设是否有系统化的方法，是否要沿用传统的网络安全的处理策略？数据安全的责任主体，是由数据存储所在的部门、数据处理的业务部门还是负责对数据进行运维的部门负责？这里我们结合 Gartner 数据安全治理体系，对数据安全建设的思路和具体工作中面临的问题进行相关介绍，以期对校园网的数据安全体系建设有所借鉴与启发。

数据安全治理概念最早是由国际知名咨询机构 Gartner 研究中心在 2015 年提出的。2017 年，Gartner 将数据安全治理称为数据安全中的“风暴之眼”（The eye of Storm），2018 年 Gartner 推出研究报告《如何使用数据安全治理》，将数据安全治理视作为一种系统化解决数据安全问题的合理方法论和实践工具进行推广和应用。

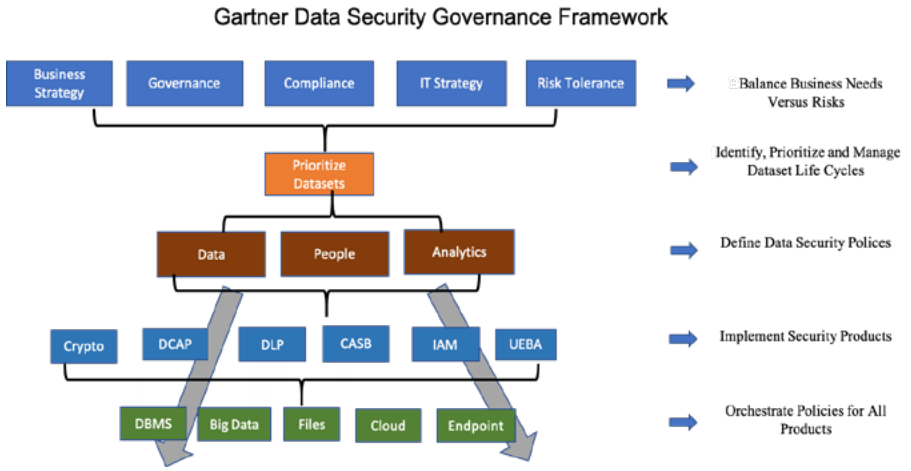


图 1 Gartner 提出的网络安全治理体系

Gartner 认为数据安全治理体系是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条，其网络安全治理体系框架如图 2 所示。其中，将数据安全建设分为 5 个阶段：业务梳理、分级分类、策略制定、技术管控、优化改进。

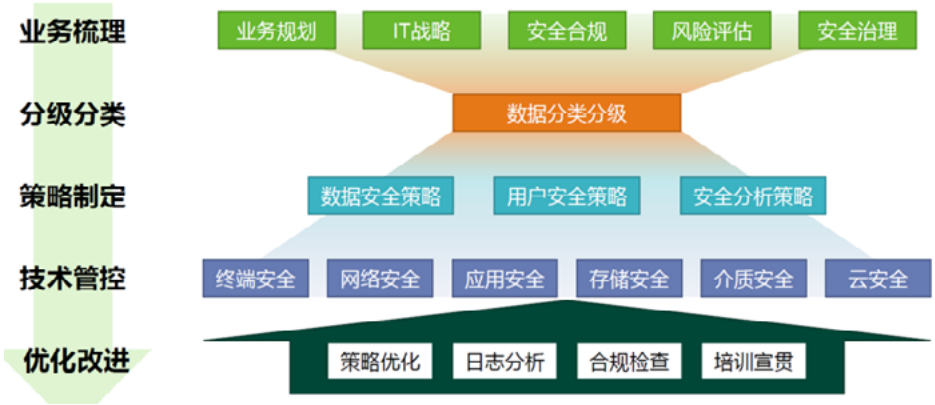


图 2 网络安全体系建设框架

（1）业务梳理。分析政策法规、梳理业务及人员对数据的使用规范，定义敏感数据。

（2）分级分类。根据定义好的敏感数据，利用工具对全网进行敏感数据扫描发现，对发现的数据进行数据定位、数据分类、数据分级。

（3）策略制定。根据敏感数据的级别，通过一系列安全策略将数据设定在全生命周期中的可用范围，利用规范和工具对数据进行细粒度的权限管控。

（4）技术管控。对数据进行监督监察，保障数据在可控范围内正常使用的同时，对非法的数据行为进行记录，为事后取证留下了清晰准确的日志信息。

（5）优化改进。指依托体系建立的系统在运行过程中，应对不断变化的数据做持续性的跟踪，并提供策略优化与持续运营的服务。

具体来讲：

1. 业务数据梳理

Gartner 数据安全治理体系指出，在业务梳理过程中，业务部门要深入参与数据资产梳理以及分级分类工作，因为业务部门是最了解数据价值与重要性的。这就需要自上而下形成高层牵头，横跨业务部门与安全部门的组织架构，并由信息安全管理团队和数据业务管理团队共同商讨建立数据安全制度流程体系，制定好制度体系应该以文档化的方式进行落地管理。从最高级的方针战略，到最细节的表格日志，都应该由不同层级的团队负责进行文档化的落地，并严格执行。在相应的业务组织与管理制度指导下，学校、教育机构才能更好的开展后续建设工作。

2. 数据分级分类

数据分级分类指基于对数据的有效理解和分析，对数据进行不同类别和密级的划分，并根据数据的类别和密级制定不同的管理和使用原则，尽可能对数据做到有差别和针对性的防护，实现在适当安全保护下的数据自由流动。数据分类分级的准确清晰，是后续数据保护的基础。由于数据类型不同，对学校、教育机构影响不同，可根据《中华人民共和国网络安全法》要求对个人信息和重要数据分开进行评估与定级，再按照就高不就低的原则对数据条目进行整体定级。

3. 数据安全策略制定

在数据分级和分类后，重要的是要了解这些数据在被谁访问，这些人是如何使用和访问数据的，从而针对不同的角色制定不同的安全访问策略。常见的角色包括：业务人员（要进一步角色细分）、数据运维人员、开发测试人员、分析人员、外包人员、数据共享第三方等。如对于开发测试人员，在开发场景下，主要需要满足对生产数据的高度仿真模拟，对于仿真数据的加密、访问控制、审计等安全措施并非重要。对于运维人员，在备份和调优场景下，并不需要访问大量底层信息，仅提供行为审计、敏感数据掩码能力即可。

在进行数据安全策略制定时，可以考虑从用户、资产和数据的行为模式出发，利用 5W1H 分析模型来进行敏感数据行为分析，并基于行为模式发现数据异常事件。需要注意的是：（1）明确数据的访问者（应用用户 / 数据管理人员）、访问对象、访问行为；（2）基于这些信息制定不同的、有针对性的数据安全策略。

4. 技术管控实现纵深防护

数据是流动的，数据结构和形态会在整个生命周期中不断变化，因此需要采用多种安全工具支撑安全策略的实施。Gartner 在数据安全治理体系中提出了实现安全和风险控制的 5 个工具：加密、以数据为中心的审计和保护、数据防泄露、身份识别与访问管理、策略配置同步，这 5 个工具对应 5 个安全领域，其中包含多种具体的技术手段。

针对数据安全的风险，应以数据为中心，向外对业务、网络、设备、用户采取“零信任”的态度，管控手段需要覆盖全部环节，任意环节失信后都能实现熔断保护。其中，用户侧、终端侧、网络侧、业务侧，以及数据中心，都要做好安全防护措施。从数据流向上，外向内防攻击防入侵防篡改，内向外防滥用防伪造防泄露。要对全部纵深防护环节进行整体控制，实现环境感知，可信控制和全面审计，整合多层次的纵深防御，及时发现问题，及时阻止安全风险。

5. 优化改进

在 Gartner 数据安全治理体系中，优化改进是指对数据安全的优化改进与持续运营。业务在变，数据也在变，因此数据安全建设也应是不断变化的，主要表现在策略配置的同步变化。因为无论访问控制、脱敏、加密亦或是令牌化技术，以上哪种手段都必须注意对数据访问和使用的安全策略保持同步下发，策略执行对象涵盖关系型数据库、大数据类型、文档文件、云端数据等多种数据类型。（河南省教育信息安全监测中心整理）

建设数据安全体系的几个关键要点

一、数据安全建设要遵循三大核心理念

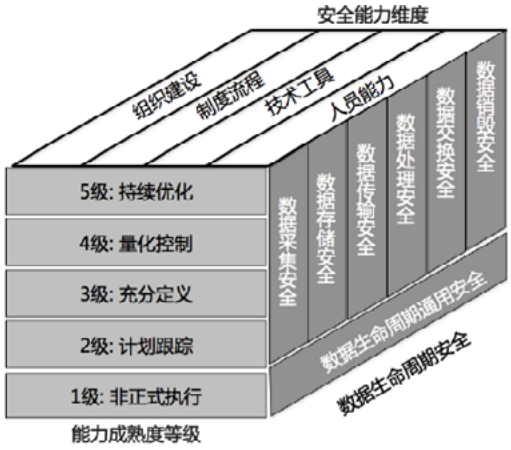
数据安全建设核心理念包括数据分级分类、角色授权、场景化安全三项内容。

1. 数据分级分类：首先，针对数据的有效理解和分析，对不同数据进行不同类别和密级的划分；其次，根据数据的类别和密级制定不同的管理和使用原则，尽可能对数据做到有差别和针对性的防护，实现在适当安全保护下的数据自由流动。

2. 角色授权：在数据分级和分类后，重要的是要了解这些数据在被谁访问，这些人是如何使用和访问数据的，要针对不同的角色制定不同的安全政策。常见的角色包括：业务人员（需要进一步角色细分）、数据运维人员、开发测试人员、分析人员、外包人员、数据共享第三方等。

3. 场景化安全：要针对不同角色在不同场景下，研究主要的数据使用需求；要在尽可能满足数据被正常使用的目标下，完成相应的安全要求和安全工具的选择。比如前面文章中提到的，对于开发测试人员，在开发场景下，主要需要满足对生产数据的高度仿真模拟，对于仿真数据的加密、访问控制、审计等安全措施并非重要。对于运维人员，在备份和调优场景下，提供行为审计、敏感数据掩码能力即可。

二、以数据安全成熟度模型评估自身数据安全能力



数据安全成熟度模型（简称：DSMM）是另一个数据安全建设中的系统化框架，是围绕数据的生命周期、结合大数据业务的需求以及监管法规的要求，持续不断的提升组织整体的数据安全能力，以数据为核心的安全框架。模型包含以下三个维度：

1. 数据生命周期安全：围绕数据生命周期，提炼出大数据环境下，以数据为中心，针对数据生命周期各阶段建立的相关数据安全过程域体系。

2．安全能力维度：明确组织机构在各数据安全领域所需要具备的能力维度，明确为制度流程、人员能力、组织建设和技术工具四个关键能力的维度。

3．能力成熟度等级：基于统一的分级标准，细化组织机构在各数据安全过程域的 5 个级别的能力成熟度分级要求。

三、采用科学有效的数据分级分类方式

数据分级分类的目的是，利用分级分类方案，在安全层面上针对数据采用更为精细化管理的措施，从而使得数据在共享使用与安全控制方面实现平衡。

1. 数据分级分类的原则：依据数据的来源、内容和用途对数据进行分类；按照数据的价值、内容敏感程度、影响和分发范围不同对数据进行敏感级别划分。

2. 数据分级分类方式：根据梳理出的备案数据资产，进行敏感数据的自动探测，通过特征探测定位

敏感数据分布在哪些数据资产中；针对敏感的数据资产进行分级分类标记，分类出敏感数据所有者（部门、系统、管理人员等）；根据已分类的数据资产由业务部门进行敏感分级，将分类的数据资产划分公开、内部、敏感等不同的敏感级别。

四、用好数据安全访问控制策略

针对数据使用的不同方面，需要完成对数据使用的原则和控制策略，一般包括如下方面：

1. 数据访问的账号和权限管理：（1）专人账号管理；（2）账号独立原则；（3）账号授权审批；（4）最小授权原则；（5）账号回收管理；（6）管理行为审计记录；（7）定期账号稽核。

2. 数据使用过程管理：（1）业务需要访问原则；（2）批量操作审批原则；（3）高敏感数据访问审批原则；（4）批量操作和高敏感数据访问指定设备、地点原则；（5）访问过程审计记录；（6）开发测试访问模糊化原则；（7）访问行为定期稽核。

3. 数据共享（提取）管理：（1）最小共享和模糊化原则；（2）共享（提取）审批原则；（3）最小使用范围原则；（4）责任传递原则；（5）定期稽核；

4. 数据存储管理：（1）涉密数据存储的网络区隔；（2）敏感数据存储加密；（3）备份访问管理；（4）存储设备的移动管理；（5）存储设备的销毁管理。（来源：安华金和《数据安全治理白皮书》）

高校个人数据的使用要进行脱敏处理

用户个人保护意识是高校个人数据安全防护中很重要的一个因素。为此，上海财经大学每年组织两次个人信息安全自检，让师生员工检查是否在处理涉密信息，有没有打开不明网址，是否遵循“涉密不上网，上网不涉密”等规定。

上海财经大学的数据中心已成立六年多，目前部门级别的系统除了少量常用数据，基本已无个人信息数据存留，在国内高校中较早完成这项工作。

数据中心作为唯一的数据源头，其所含数据都经过前期的清洗工作，具有可靠性，解决了原有不同系统中数据存在冲突的情况。此外，由于数据中心的数据比较完备，在开发新系统时不用再花费精力去开发基础数据，可减少项目工程量，缩短工期，提高效率。

由于学校数据中心成立较早，尽管在制度上还没有形成专门的个人数据安全管理办法，但数据库的运营相对成熟，相应的规范较为完备。

首先，数据库绝对保密，只有数据库管理员和各个业务系统的管理员分别可接触全部数据或部分数据。从数据中心统一对外分发数据，每次分发都会有所记录，在此基础上可定期做审计，为数据安全提供保障。

其次，与校外第三方公司合作开发新系统或新功能时，一般使用脱敏数据，学校有一套专门的脱敏产品，对数据中的证件号、联系方式、地址等比较敏感的数据进行处理。还会与这些公司签订保密协议，从法律上和技术上双管齐下，保障数据安全。

此外，校内人员使用数据时，比如学生在其研究项目中需要用学校老师或学生的统计数据，或教务处、人事处需要用其授权之外的数据，均需要走学校流程进行申请，分管校长审批通过，他们才能使用数据。

在数据中心建设过程中，我们发现，对于部门协调之类管理层面上的难题，学校的高度重视很重要。上海财经大学有一个很好的制度，分管信息化的副校长每周都会主持召开信息化协调会，相关部门的领导和信息员参加会议，遇到不好协调的问题，校长会亲自过问、拍板，有效地促进了我校的信息化进程。（作者：朱杨兴，作者系上海财经大学信息办公室党支部书记；来源：《中国教育网络》）

互联网时代如何保护个人隐私?

学校如何加强网络安全防护?

1. 禁止发布（上传）包含个人数据和敏感信息的内容。

2. 要加强对各类账号和密码的管理，定期更换密码、杜绝弱口令。

3. 各单位自建的业务信息系统要及时打补丁和封堵漏洞。

4. 禁止通过公共邮箱和微信、QQ 等公用即时通讯工具传输个人数据和敏感信息。

5. 加强对移动存储介质和笔记本电脑的管理，采取有效措施防范因失窃而造成的个人数据和敏感信息泄露。

6. 本着“谁主管，谁负责”的原则，各单位和全校师生要提高防范信息泄露的意识，加强管理和技术保障。

如何防范病毒或木马的攻击？

1. 为计算机安装杀毒软件，定期扫描系统、查杀病毒。

2. 及时更新病毒库、更新系统补丁。

3. 下载软件时尽量到官方网站或大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒。

4. 不随意打开不明网页链接，尤其是不良网站的链接，陌生人通过 QQ 给自己传链接时，尽量不要打开。

5. 使用网络通信工具时不随便接收陌生人的文件，若接收可取消“隐藏已知文件类型扩展名”功能来查看文件类型。

6. 对公共磁盘空间加强权限管理，定期查杀病毒。

7. 打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建立名为 autorun.inf 的文件夹 (可防 U 盘病毒启动)。

8. 需要从互联网等公共网络上下载资料转入内网计算机时，用刻录光盘的方式实现转存。

9. 对计算机系统的各个账号要设置口令，及时删除或禁用过期账号。

10. 定期备份，当遭到病毒严重破坏后能迅速修复。

如何防范 QQ、微博等社交平台账号被盗？

1. 账户和密码尽量不要相同，定期修改密码，增加密码的复杂度，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码。

2. 密码尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换。

3. 不同用途的网络应用，应该设置不同的用户名和密码。

4. 在网吧使用电脑前重启机器，警惕输入账号密码时被人偷看 ; 为防账号被侦听，可先输入部分账号名、部分密码，然后再输入剩下的账号名、密码。

5. 涉及网络交易时，要注意通过电话与交易对象本人确认。

如何安全使用电子邮件？

1. 不要随意点击不明邮件中的链接、图片、文件。

2. 使用电子邮件地址作为网站注册的用户名时，应设置与原邮件密码不相同的网站密码。

3. 适当设置找回密码的提示问题。

4. 当收到与个人信息和金钱相关 (如中奖、集资等) 的邮件时提高警惕。

如何保证网络游戏安全？

1. 输入密码时尽量使用软键盘，并防止他人偷窥。

2. 为电脑安装安全防护软件，从正规网站上下载网游插件。

3. 注意核实网游地址。

4. 如发现账号异常，应立即与游戏运营商联系。

如何防范社交网站信息泄露？

1. 利用社交网站的安全与隐私设置保护敏感信息 。

2. 不要轻易点击未经核实的链接。

3. 在社交网站谨慎发布个人信息。

4. 根据自己对网站的需求进行注册。

当前网络诈骗类型及如何预防？

网络诈骗类型如下四种：

一是利用 QQ 盗号和网络游戏交易进行诈骗，冒充好友借钱。

二是网络购物诈骗，收取订金骗钱。

三是网上中奖诈骗，指犯罪分子利用传播软件随意向互联网 QQ 用户、邮箱用户、网络游戏用户、淘宝用户等发布中奖提示信息。

四是“网络钓鱼”诈骗，利用欺骗性的电子邮件和伪造的互联网站进行诈骗活动，获取受骗者财务信息进而窃取资金。

IPv6 安全

2020 年 3 月，为贯彻落实《推进互联网协议第六版 (IPv6) 规模部署行动计划》（厅字〔2017〕47 号）任务要求，加快提升 IPv6 端到端贯通能力，持续提升 IPv6 活跃用户和网络流量规模，工信部印发《2020 年 IPv6 端到端贯通能力提升专项行动的通知（工信部通信函〔2020〕57 号）》，决定于 2020 年开展 IPv6 端到端贯通能力提升专项行动。

随着计划实施推行以及移动互联网、物联网等新技术的大力发展，我国整个网络环境将发生翻天覆地的变化，全产业链已蓄势待发，目前 IPv6 流量增长迅速，新的网络环境以及新兴领域均将面临着新的安全挑战。

国家网络安全宣传周
China Cybersecurity Week

IPv6 安全

IPv6 网络安全现状分析

一、IPv6攻击态势概览

1. 热点态势

随着当前 IPv6 的普及，IPv6 相关的攻击也呈现上升态势。第一起有记录的 IPv6 DDoS 攻击事件发生在 2018 年 3 月，此次攻击涉及了 1900 个 IPv6 地址。此后在 IPv6 环境下利用漏洞的攻击行为也被陆续捕获到。通过对捕获到的相关数据分析得知，目前大部分 IPv6 环境下的攻击所使用的漏洞都是应用层漏洞，与 IPv4 攻击的目标相同，暂时还未发现针对 IPv6 自身协议漏洞的攻击。

本文通过对 IPv4 环境下的远程漏洞研究发现，大多数漏洞都存在于传输层和应用层，与网络层协议无关。因此攻击者几乎没有付出代价就可以轻易地转换战场，直接使用 IPv4 环境下的攻击载荷就可以在 IPv6 环境下进行漏洞利用。

通过对 CVE 漏洞库中的漏洞进行研究发现，按 CVE 标号计算截至 2019 年 IPv6 相关协议族的漏洞共 389 个，整体占比很低。这些漏洞主要分布在 Linux 内核、Linux 发行版本系统、Windows 等系统，tcpdump、Wireshark 等应用程序和 Juniper、Cisco、Huawei 路由器等硬件产品。Linux 中出现的漏洞主要集中在 IPv6 的实现上，出现频次比较高的模块是 IPv6 的分片模块，Cisco 上的漏洞主要在 Cisco IOS 上。从漏洞涉及模块来看，IPv6 snooping 模块上出现的问题比较多，tcpdump 在 4.9.2 前版本中的 IPv6 routing header parser 模块以及 IPv6 mobility 中也连续爆出了一系列漏洞。

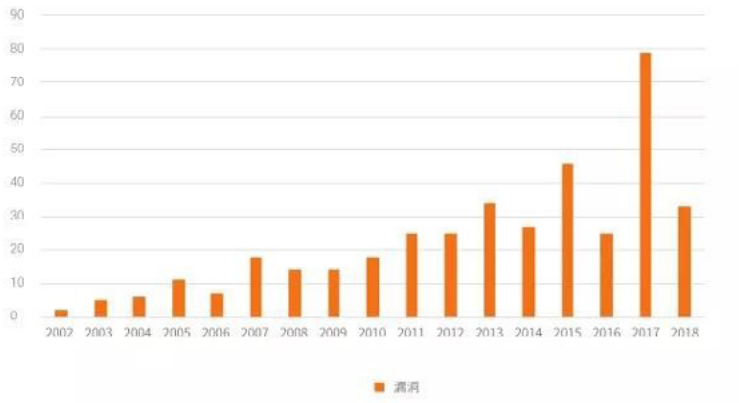


图 1 按年份来看 IPv6 相关漏洞数

其中 CVSS 小于 3 的低危漏洞占 2.6%，介于 3-7 的中危漏洞占 47.0%，大于 7 的高危漏洞占 50.4%。

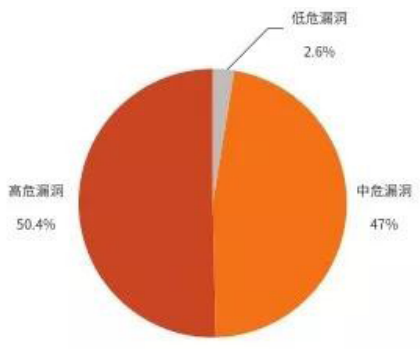


图 2 IPv6 相关漏洞的危害占比情况

2. 重要观点

观点一：2010 年后，IPv6 相关漏洞总体呈现攀升趋势，高危漏洞占比较高，值得持续关注。

观点二：在 IPv6 环境中，目前观测到的攻击主要是对传输层和应用层漏洞的利用。

观点三：当前 IPv6 网络环境中，安全威胁主要集中在僵木蠕相关攻击，以及面向 Web 服务和 Web 框架类的攻击。

观点四：运营商、教育机构、事业单位和政府的 IPv6 应用较为广泛，遭受到的攻击也最多。

二、IPv6攻击中的热点类型

据 2019 年上半年的观察，在 IPv6 环境下共出现 186 种不同的攻击告警信息。图 3 中列出的是告警数量 TOP 10 的攻击类型。

名称	数量
UDP-FLOOD 淹没拒绝服务攻击	14210
暗云木马服务器通信	12861
Webshell 后门访问控制	10865
挖矿蠕虫 WannaMine 服务器通信	9979
Web 服务 SQL 注入攻击	8710
勒索病毒 WannaCry 通信	7906
门罗币挖矿程序服务器通信	6589
Web 服务远程跨站脚本执行攻击	2540
PHP 代码执行	2242

图 3 IPv6 攻击中的 TOP 10 告警类型

从日志信息看出，IPv6 环境中的攻击大量针对的是网络层，传输层和应用层的漏洞。黑客利用一些互联网中比较流行的攻击手段，例如拒绝服务、Webshell 攻击和僵尸网络通信，其中影响最大的还是僵木蠕相关攻击。

针对图 3 中的僵木蠕攻击，将攻击内容与 IPv4 的攻击对比分析后，发现在 IPv6 和 IPv4 网络环境中，僵尸网络通信采用的方式基本相同，比如“挖矿蠕虫 WannaMine 连接 DNS 服务器通信”，都是对域名“iron.tenchier.com”发起链接请求。

三、IPv6 攻击中的行业分布

为了能够更加清楚地认识 IPv6 在国内部署、使用的情况，本文从不同行业来观察 IPv6 的情况。图 4 中表示了在不同行业中监控到的单位个数。其中的企业部分，包括了国有企业和大型私企。

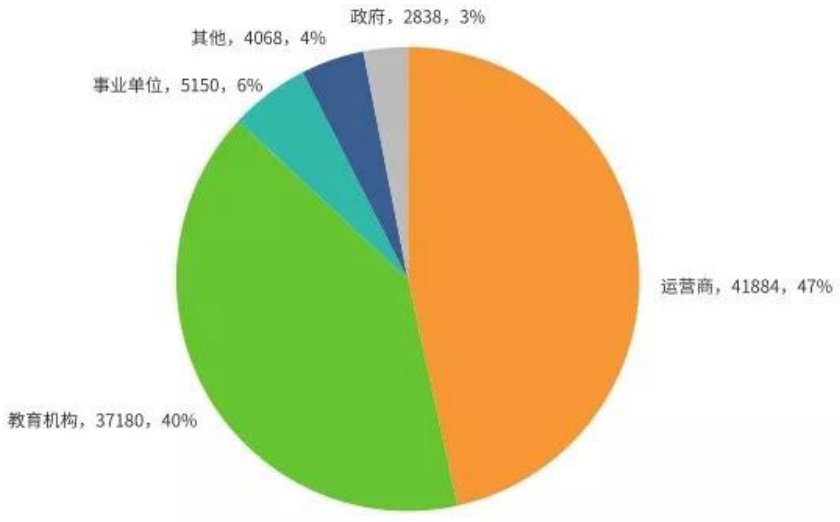


图 4 IPv6 攻击中的地域分布

从整体的 IPv6 告警分布看，排名前四为运营商、教育机构、事业单位和政府，其中运营商告警总量占 47%，教育行业占 40%，事业单位占 6%，政府占 3%，其他行业应用 IPv6 只占据很小的一部分。在 2018 年国家推出《推进互联网协议第六版（IPv6）规模部署行动计划》后，IPv6 就一直由政府主导。国家单位、事业单位、政府部门在快速推进应用的同时也更容易遭受 IPv6 环境下的网络攻击；运营商作为网络运营的基础实施和建设单位，支撑 IPv6 基础建设，是攻击者的重点目标之一；而对于教育行业来说，尤其是各大院校，也容易成为攻击者的重点目标。

四、IPv6攻击中的地域分布

2019 年上半年，我国多省观测到使用 IPv6 地址进行的攻击行为，涉及攻击类型 167 种，覆盖 20 多个省份。数量分布如下图所示（IPv4 告警数据量进行了 900：1 的比例收缩）：

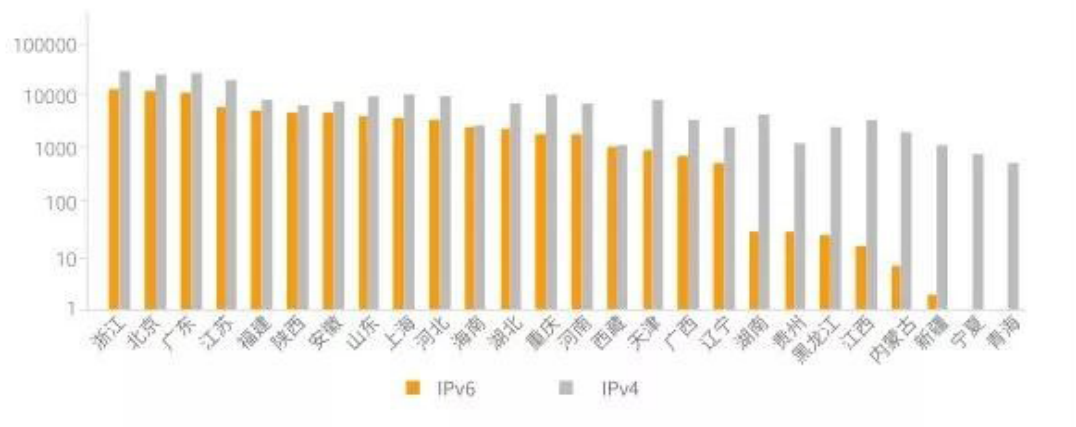


图 5 IPv6 与 IPv4 地址各省受攻击情况

上图的横坐标代表不同省份，纵坐标代表告警数量。从各省节点 IPv6 监控情况看，广东、北京、浙江等地大范围受到 IPv6 地址范围的攻击。这几个地区的院校单位大量采用 IPv6 地址。图 5 给出了 2019 上半年 IPv4 与 IPv6 的告警数量对比概览。由于 IPv4 告警数量很多，本文将 IPv4 告警数量进行了 900：1 的比例收缩后，再与 IPv6 的告警数量做对比。图 5 看出，IPv6 和 IPv4 环境中的告警数量整体分布基本保持一致。

通过分析可知：已有一些黑客和攻击组织开始使用 IPv6 进行攻击，未来有可能成为大规模攻击的风险。上图反映了各省市已经开始建设 IPv6 基础设施，并且均不同程度遭受到攻击。2019 年上半年，来自国外的攻击具体分布情况如图 6 所示，占据前四位的国家是瑞士（53.2%），罗马尼亚（20%），美国（11.2%），马来西亚（7.2%），其他国家相对占比较少，占比 3.2%。结合 Akamai 公司 IPv6 采用情况可视化结果以及 2017 年度的 IPv6 报告，可以发现告警数量排名前四的国家在国内 IPv6 覆盖度上均在全球名列前 40，其中，美国排名第 2（48%），马来西亚排名第 6（39.3%），瑞士排名第 23（21.7%），罗马尼亚排名第 37（13.1%）。

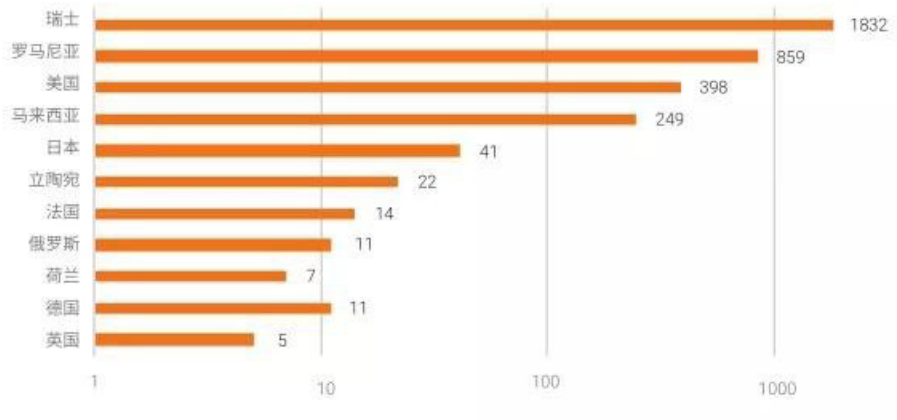


图 6 IPv6 攻击源位于国外的告警分布

在国内，从攻击目标行业分布来看，目标 IP 集中于运营商，高校及大型跨国企业，分布如下图所示。

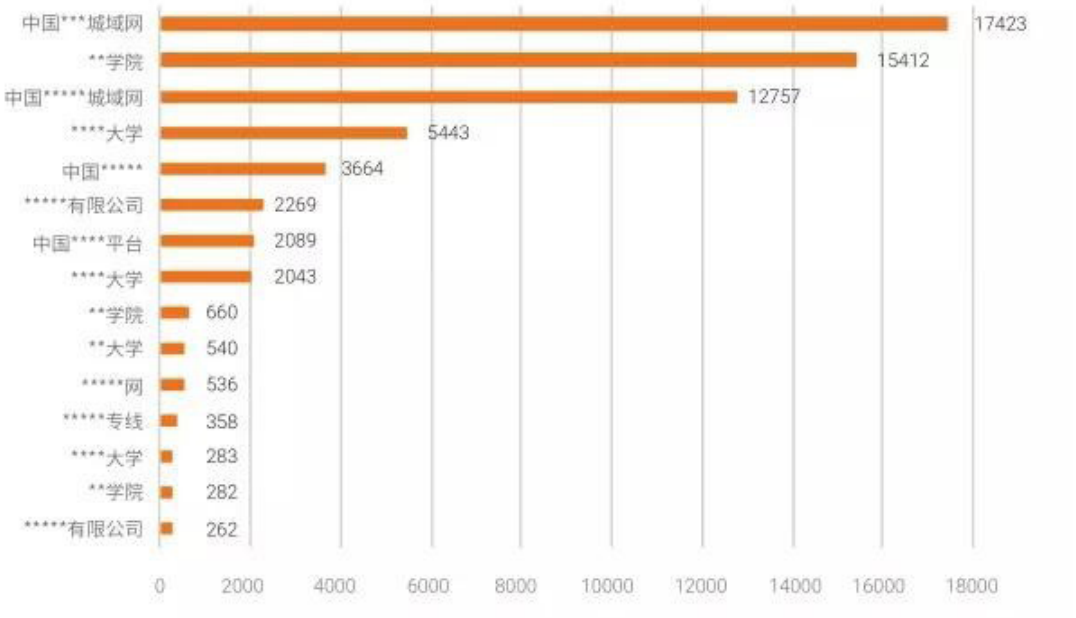


图 7 国内目的地址分布

从上图看，目标位于运营商城域网 IPv6 日志的情况要明显多于其他的单位，占日志量的 54.4%，超过一半。其次是一些高校和大型企业的日志信息。从攻击目标单位数量来看，高校是最多的，这和各大高校较早推进 IPv6 建设有关。这些高校总共受到 54 种不同的攻击，其中 Top10 分布如下。从中可以看出，在 IPv6 环境下，攻击者针对高校的攻击，往往是面向 Web 服务和数据库服务，企图获取服务器权限和进行远程命令执行，危害高校的 Web 服务安全和数据安全。

名称	数量
Webshell 后门访问控制	2674
远程 SQL 注入攻击	829
Webshell 脚本文件上传攻击	725
FCKEditor 任意文件上传漏洞	678
Web 服务远程跨站脚本执行攻击	637
PHP 代码执行漏洞	529
HTTP 服务目录遍历漏洞	404
ThinkPHP 5.x 远程命令执行漏洞	255
HTTP 命令注入攻击	194
Microsoft IIS 错误解析远程代码执行漏洞	104

图 8 攻击目标为高校的 Top10 攻击事件

大型互联网厂商攻击事件情况与高校类似，Web 服务和数据库服务也是攻击的重点。

名称	数量
Web 服务远程跨站脚本执行攻击	707
PHP 代码执行漏洞	284
Web 服务远程 SQL 注入攻击行为	180
Java 代码执行漏洞	57
Ruby on Rails 嵌套参数 SQL 注入漏洞	6

图 9 攻击目标为互联网厂商攻击事件 Top5

下图给出了一些高校中基于 IPv6 的告警情况，其横坐标表示的是不同高校，纵坐标表示告警次数。

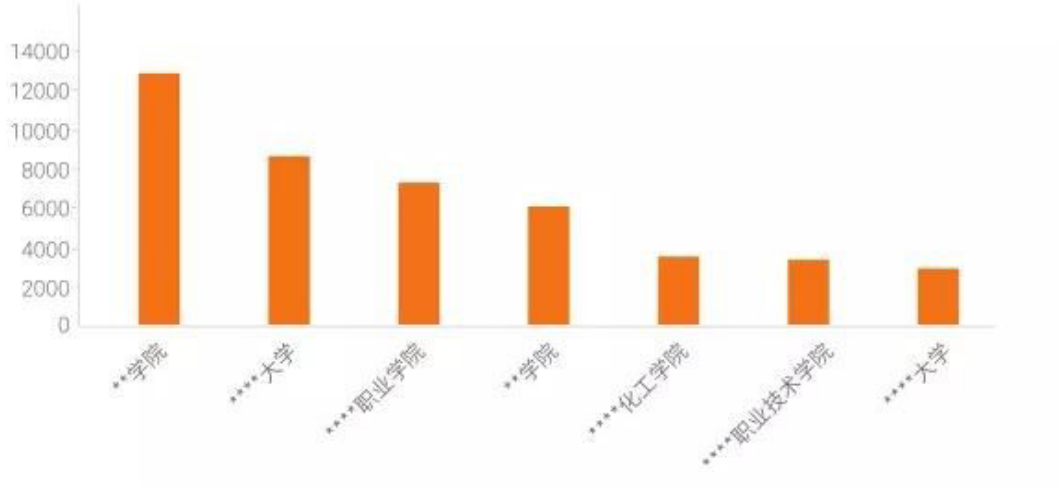


图 10 攻击源位于高校的告警情况

下面以某学院为例，分析一下针对高校中采用的攻击手法。

名称	数量
挖矿病毒 Xmrig 通信	502
挖矿程序门罗币服务器通信	308
挖矿蠕虫 WannMine 服务器通信	105
恶意程序 PowerGhost 服务器通信	62

图 11 某学院中的攻击源告警情况

从上图可以看出，该学院的告警主要源自于恶意程序与外部通信连接行为，攻击源往往是受感染主机。IPv6 环境下的僵木蠕攻击主要集中于挖矿行为。比如门罗币挖矿主要通过“minexmr.com”和“minergate.com”等地址与服务器通信连接。而这些服务地址已经由绿盟情报平台给出详细关联分析：

图 12 门罗币挖矿相关情报

攻击源地址位于三大运营商的情况如下图所示。从节点监控结果来看，攻击事件主要集中于僵木蠕攻击、Web 服务及 Web 框架类攻击和暴力攻击等，和高校基本相同，不再赘述。运营商作为网络建设的推动者，在 IPv6 建设中起到关键作用。

图 13 攻击源位于运营商的告警数量分布

（作者：绿盟科技天枢实验室 , 绿盟科技威胁情报中心；来源：《信息安全与通信保密》）

IPv6 协议中安全问题浅析

IPv6 规模部署实施在即，作为下一代互联网的关键性技术，IPv6 将逐步取代 IPv4 成为支撑互联网运转的核心协议。如何高效稳定地实现下一代互联网全覆盖，安全问题是首要焦点。

一、IPv6 存在的安全隐患

1.IPv6 扩展首部威胁

（1）逐跳选项报头

安全威胁：可利用逐跳选项报头发送大量包含路由提示选项的 IPv6 数据包，包含有路由提示选项的数据包要求所有路由器对该数据包进行处理并仔细查看该数据包的报头信息，当攻击者发送大量此类 IPv6 数据包时，将消耗链路上路由器大量资源，严重可造成 DoS 攻击。

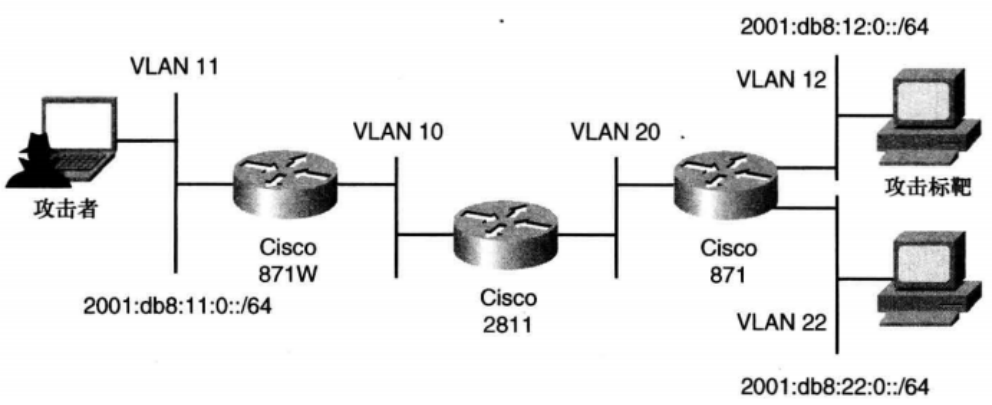


图 1 逐跳选项报头示例图

应对方式：应当限制路由器对包含路由提示选项的数据包的处理数量。

（2）目的选项报头

安全威胁：移动 IPv6 协议的数据通信以明文进行传输，因此其本身便是不安全的，攻击者可对 MIPv6 数据包进行嗅探进而识别其通信节点、转交地址、家乡地址、家乡代理等信息，并利用这些信息伪造数据包。攻击者可通过拦截类型为消息绑定更新的数据包，修改绑定关系中的转交地址。此外，移动节点标识符选项揭示了用户的家乡从属关系，攻击者可利用该选项确定用户身份，锁定特定的攻击对象。

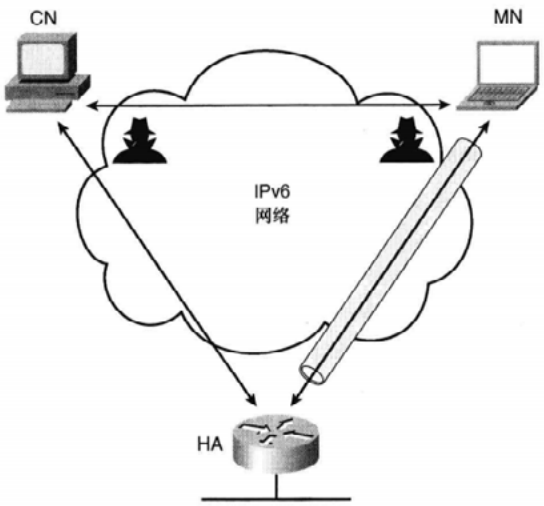


图 2 MIPv6 威胁示例图

应对方式：可尝试开启 IPSec 保证数据包不会被窃听。

（3）路由报头

安全威胁：在 RH0 路由类型（即 type 0）下，攻击者可利用路由报头选项伪装成合法用户接收返回的数据包。同时，RH0 提供了一种流量放大机制，攻击者可利用该类型进行拒绝服务攻击。虽然 RH0 已被正式弃用并启用 RH2，但旧的或未升级设备依然可能遭受 RH0 攻击。

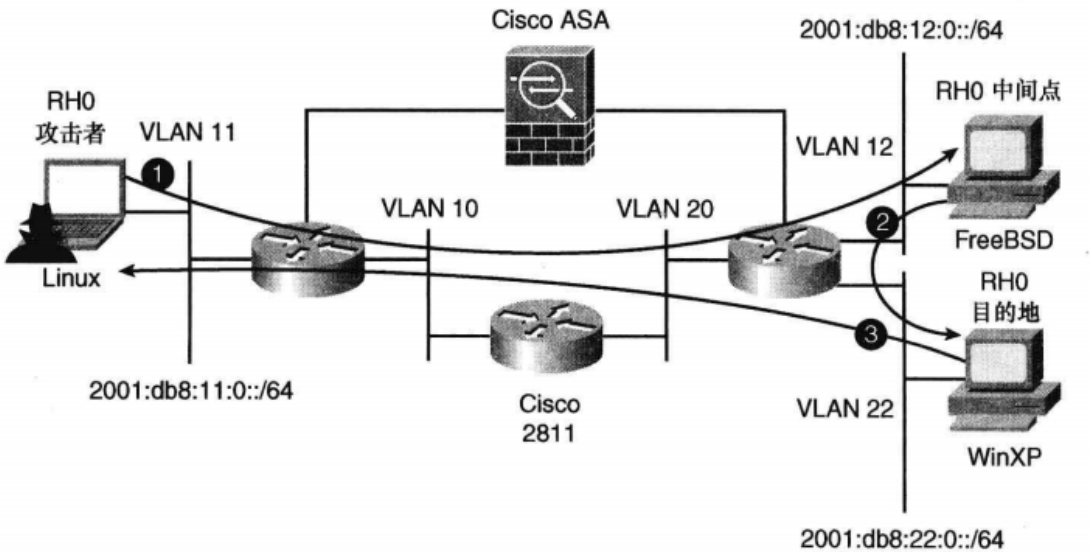


图 3 路由报头攻击示例图

应对方式：应当尽快更新安全设备并升级至最新的 IPv6 协议版本，同时对所有的 RH0 数据包进行丢弃。

（4）分段报头

安全威胁：如若将关键的报头信息切分在多个片段中，安全防护设备对关键信息进行提取与检测处理会耗费大量资源，构造大量该类数据包可能对目标主机造成 DoS 攻击。攻击者可向节点发送大量不完整的分段集合，强迫节点等待片段集合的最后片段，节点在超时时间内由于只接收到部分 IPv6 片段进而无法完成重组，最终只能将数据包丢弃，在超时等待期间，会造成存储资源的消耗。

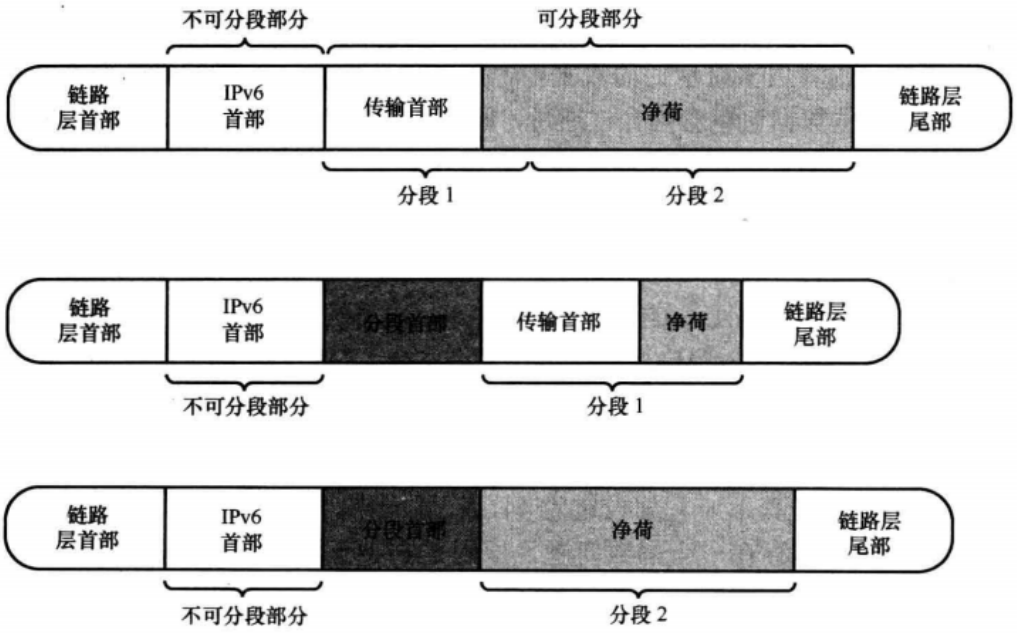


图 4 分段报头攻击示例图

应对方式：防火墙应该丢弃除最后分段外所有小于 1280 字节的所有分段。Cisco ASA 防火墙的 FragGuard 功能可以将所有的分片组装并进行整个数据包检查用以确定是否存在丢失的分段或重叠分段。根据 RFC8200，IPv6 节点已不能创建重叠分段，且在对 IPv6 报文进行重组时，如若确定一个或多个片段为重叠片段，则必须对整个报文进行丢弃。

2. 协议威胁

（1）ICMPv6 协议

安全威胁：可通过向组播地址 FF02::1 发送 Echo Request 报文，通过接收 Echo Reply 报文实现本地链路扫描，或以目标节点作为源地址向组播地址 FF02 :: 1 发送 ICMPv6 EchoRequest 消息实现 Smurf 攻击。可通过向目标节点发送 ICMPv6 Packet too big 报文，减小接收节点的 MTU，降低传输速率。可通过向目标节点发送过多的 ICMPv6 包以及发送错误消息，导致会话被丢弃，从而破坏已建立的通信，实现 DoS 攻击。可通过向主机发送格式不正确的消息刺激主机对 ICMPv6 的响应，从而发现潜在的攻击目标。

应对方式：可在交换机的每个物理端口设置流量限制，将超出流量限制的数据包丢弃。或在防火墙或边界路由器上启动 ICMPv6 数据包过滤机制，也可配置路由器拒绝转发带有组播地址的 ICMPv6 EchoRequest 报文。可尝试关闭 PMTU 发现机制，但其会影响到网络数据的传输速率。

（2）邻居发现协议（NDP）

安全威胁：

中间人攻击：由于 NDP 协议基于可信网络因此并不具备认证功能，因此可通过伪造 ICMPv6 NA/RA 报文实现中间人攻击。攻击者可以伪造 NA 报文，将自己的链路层地址并启用覆盖标志（O）作为链路上其他主机的地址进行广播。攻击者可伪造 RA 报文发送至目标节点修改其默认网关。

重复地址检测攻击：当目标节点向 FF02 :: 16 所有节点发送 NS 数据包进行重复地址检测时，攻击者可向该节点发送 NA 报文进行响应，并表明该地址已被自己使用。当节点接收到该地址已被占用消息后重新生成新的 IPv6 地址并再一次进行重复地址检测时，攻击者可继续进行 NA 响应实现 DoS 攻击。

泛洪攻击：攻击者可伪造不同网络前缀 RA 消息对 FF02 :: 1 进行泛洪攻击，接收节点将会根据不同的网络前缀进行更新，从而消耗大量的 CPU 资源。

应对方式：

安全邻居发现（SEND）协议是邻居发现协议中的一个安全扩展，其工作原理为使网络中每个 IPv6 节点都有一对公私钥以及多个邻居扩展选项。采用 SEND 协议后，各个节点的接口标识符（IPv6 地址低 64 比特）将基于当前的 IPv6 网络前缀与公钥进行计算产生，而不能由各个节点自行选择。安全邻居发现协议通过时间戳和 Nonce 选项抵御重放攻击，并引入了 CGA（密码生成地址）与 RSA 签名对数据源进行验证以解决邻居请求 / 邻居通告欺骗的问题。SEND 虽然可以解决一定的安全问题，但目前系统与设备对 SEND 的支持十分有限。

RFC7113 提出了 IPv6 安全 RA 方案 RA-Guard，其通过阻断非信任端口 RA 报文转发来避免恶意 RA 可能带来的威胁，在攻击包实际到达目标节点之前阻塞二层设备上的攻击数据包。

使用访问控制列表或空路由过滤对地址空间中未分配的部分的访问，用以防止攻击者迫使路由解析未使用的地址。

（3）DHCPv6

安全威胁：

地址池耗尽攻击：攻击者可以伪装为大量的 DHCPv6 客户端，向 DHCPv6 服务器请求大量的 IPv6 地址，耗光 IPv6 地址池。

拒绝服务攻击：攻击者可向 DHCPv6 服务器发送大量的 SOLICIT 消息，强制服务器在一定时间内维持一个状态，致使服务器 CPU 与文件系统产生巨大负担，直至无法正常工作。

伪造 DHCPv6 服务器：攻击者可伪造成 DHCPv6 服务器向目标客户端发送伪造的 ADVERTISE 与 REPLY 报文，在伪造报文中携带虚假的默认网关、DNS 服务器等信息，以此实现重定向攻击。

应对方式：对客户端所有发送到 FF02::1:2（所有 DHCPv6 中继代理与服务器）和 FF05::1:3（所有 DHCPv6 服务器）的消息数量进行速率限制。DHCPv6 中内置了认证机制，认证机制中的 RKAP 协议可以对伪造 DHCPv6 服务器的攻击行为提供防范。

二、IPv6 对安全硬件的影响

1. 防火墙

（1）IPv6 报头的影响

针对 IPv6 报文，防火墙必须对 IPv6 基本报头与所有的扩展首部进行解析，才能获取传输层与应用层的信息，从而确定当前数据报是否应该被允许通过或是被丢弃。由于过滤策略相比 IPv4 更加复杂，在一定程度上将加剧防火墙的负担，影响防火墙的性能。

（2）IPSec 的影响

如若在 IPv6 数据包中启用加密选项，负载数据将进行加密处理，由于包过滤型防火墙无法对负载数据进行解密，无法获取 TCP 与 UDP 端口号，因此包过滤型防火墙无法判断是否可以将当前数据包放行。

由于地址转换技术（NAT）和 IPSec 在功能上不匹配，因此很难穿越地址转换型防火墙利用 IPSec 进行通信。

2.IDS&IPS

面对 IPv6 数据包，倘若启用了加密选项，IDS 与 IPS 则无法对加密数据进行提取与分析，无法通过报文分析获取 TCP、UDP 信息，进而无法对网络层进行全面的安全防护。即便只允许流量启用 AH 认证报头，但认证报头内部具有可变长度字段 ICV，因此检测引擎并不能准确地定位开始内容检查的位置。

三、过渡技术的安全性

1. 双栈技术

倘若双栈主机不具备 IPv6 网络下的安全防护，而攻击者与双栈主机存在邻接关系时，则可以通过包含 IPv6 前缀的路由通告应答的方式激活双栈主机的 IPv6 地址的初始化，进而实施攻击。

2. 隧道技术

（1）隧道注入：攻击者可通过伪造外部 IPv4 与内部 IPv6 地址伪装成合法用户向隧道中注入流量。

（2）隧道嗅探：位于隧道 IPv4 路径上的攻击者可以嗅探 IPv6 隧道数据包，并读取数据包内容。

3. 翻译技术

利用翻译技术实现 IPv4-IPv6 网络互联互通时，需要对报文的 IP 层及传输层的相关信息进行改动，因此可能会对端到端的安全产生影响，导致 IPSec 的三层安全隧道在翻译设备处出现断点。

翻译设备作为网络互通的关键节点，是 DDoS 攻击的主要攻击目标。同时，翻译设备还可能遭遇地址池耗尽攻击，若 IPv6 攻击者向 IPv4 服务器发送互通请求，但每条请求都具有不同的 IPv6 地址，则每条请求都将消耗一个地址池中的 IPv4 地址，当出现大量该类请求时，便会将地址池耗尽，使得翻译设备不再接受进一步的请求。

任何协议都不是完美的，新生事物总要经过一段磨合适应期。面对 IPv6 部署中出现的各种问题，从用户角度看需要提高对网络安全的重视和网络安全知识的普及；从运营商角度看，作为下一代互联网的承建者，在建设之初就应该结合下一代互联网的特点制定相应的安全措施，包括建立完善真实源地址检

查机制，同时做好网络监管，提供事后溯源；作为设备厂商，需要紧密跟踪网络安全动态，提升设备本身的 IPv6 协议及防护的稳定性及完善相应的安全防护功能。相信通过大家的共同努力，一定可以营造一个健康、安全的下一代互联网环境。（赛尔网络河南分公司整理）

IPv6 安全建设建议

IPv6 协议在设计之初就考虑了安全性，其海量的网络地址资源、自动配置机制、集成 IPsec 协议等特性使 IPv6 在攻击可溯源性、防攻击、数据传输过程中的完整性和加密性等安全方面有所提高。

一、基于IPv6特性的安全保护

1.IPv6 拥有巨大的地址空间资源，建立了源地址验证机制，有利于攻击溯源

IPv4 没有建立起源地址验证机制，且在 IPv4 网络中，由于地址空间的不足，普遍部署 NAT，一方面破坏了互联网端到端通信的特性，另一方面隐藏了用户的真实 IP，导致事前基于过滤类的预防机制和事后追踪溯源变的尤为困难。

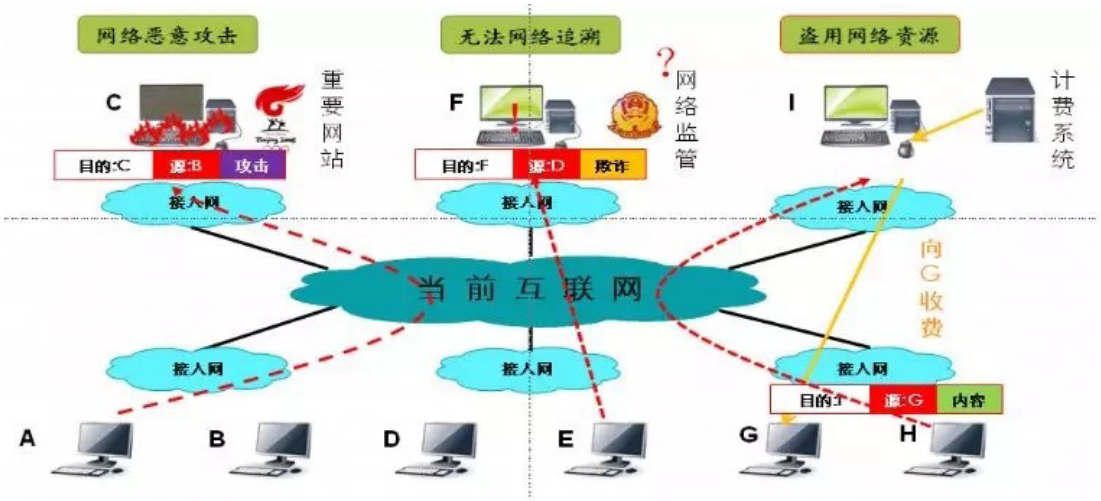


图 1 IPv4 存在的安全隐患

IPv6 则建立了可信的地址验证体系，IPv6 的地址验证体系结构（SAVA）分为接入网（Access Network）、区域内（Intra-AS）和区域间（Inter-AS）源地址验证三个层次，从主机 IP 地址、IP 地址前缀和自治域三个粒度构成多重监控防御体系，该体系一方面可以有效阻止仿冒源地址类攻击，一方面能够通过监控流量来实现基于真实源地址的计费和网管。

IPv6 拥有丰富的地址资源，且可以通过建立的地址验证机制解决网络实名制和用户身份溯源问题，在发生网络攻击事件后有利于追查溯源。同时，安全设备可以通过简单的过滤策略对节点进行安全控制，进一步提高网络安全性。

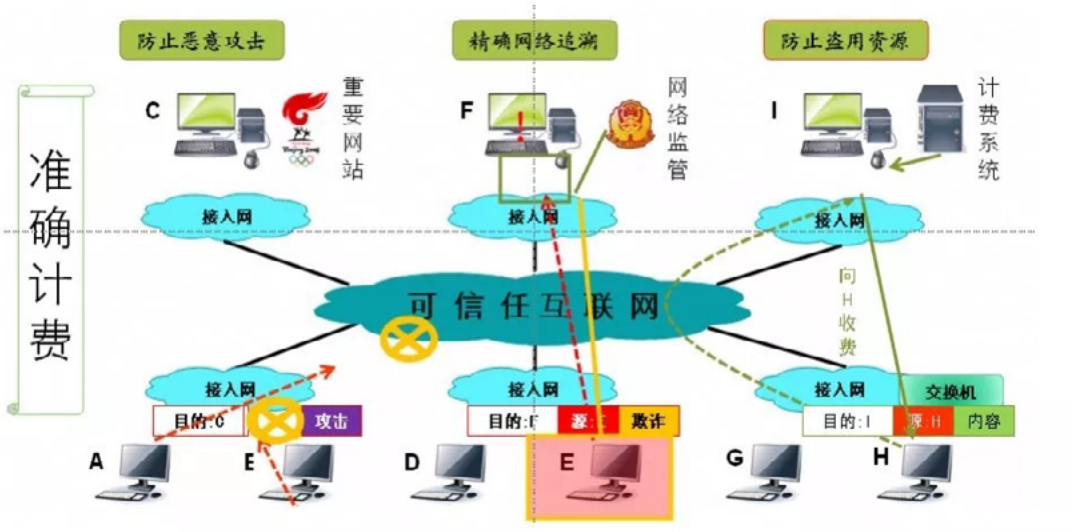


图 2 IPv6 建立可信互联网体系

此外，在 IPv4 网络中，黑客攻击的第一步通常是对目标主机及网络进行扫描搜集数据，以此推断出目标网络的拓扑结构及主机开放的服务、端口等信息从而进行针对性地攻击。在 IPv6 网络中，网络侦察的难度和代价都大大增加，从而进一步防范了攻击，提高了用户终端的安全性。

2.IPv6 协议保证了网络层的数据认证、数据完整性及机密性

IPv6 通过集成 IPsec 实现了 IP 级的安全，IPSec 可以提供访问控制、无连接的完整性、数据源身份认证、防御包重传攻击、业务流保密等安全服务，较大的提升了网络层的数据认证、数据完整性及机密性。

3.IPv6 的邻居发现协议（NDP）进一步保障传输安全性

IPv4 采用的地址解析协议（ARP），存在 ARP 欺骗等传输安全问题。IPv6 协议中采用邻居发现协议（NDP）取代现有 IPv4 中 ARP 及部分 ICMP 控制功能如路由器发现、重定向等，独立于传输介质，可以更方便地进行功能扩展，并且现有的 IP 层加密认证机制可以实现对 NDP 协议的保护，保证了传输的安全性。

4. 基于 IPv6 的新型地址结构为我国建立根服务器提供了契机

互联网的顶级域名解析服务由根服务器完成，它对网络安全、运行稳定至关重要。2013 年，中国下一代互联网国家工程中心联合日本、美国相关运营机构和专业人士发起“雪人计划”，提出以 IPv6 为基础、面向新兴应用、自主可控的一整套根服务器解决方案和技术体系。2016 年，“雪人计划”在美国、日本、印度、俄罗斯、德国、法国等全球 16 个国家完成 25 台 IPv6 根服务器架设，其中中国部署 4 台，打破我国没有根服务器的困境。

二、IPv6部署中需要重点关注的安全问题

TCP/IP 模型中，网络安全分为四个层次：物理层、网络层、传输层和应用层。IPv6 虽然增强了自身的安全机制，但 IP 协议仅是网络层的协议，IPv6 协议改变的是 IP 报头、寻址方式，提高了网络层的安全性，但对其他功能层的安全能力并未产生影响或有所提高，因此，设备仿冒接入网络、应用层攻击导致的漏洞、传输过程中的攻击等仍然存在。IPv6 发展过程中，仍然存在其他安全问题：

1. 部署 IPv6 过程中需要提高网络安全检测、维护能力

首先，庞大的地址空间会加大漏洞扫描、恶意主机检测、IDS 等安全机制的部署难度；其次，无状态地址自动配置时，攻击者可能利用冲突地址检测机制实施拒绝服务攻击（DoS）；第三，NDP（邻居发现协议）面临哄骗报文攻击、拒绝服务攻击（DoS）的安全威胁；第四，IPv6 组播所需的 MLD 等组播维护协议不能满足安全的需要，存在机密数据被窃听、对处理 MLD 报文的路由转发设备发起拒绝服务攻击（DoS）的安全隐患。

与 IPv4 网络对比，IPv6 新特性对常见网络攻击类型的影响：

表 1 IPv6 新特性对常见网络攻击的影响

攻击类型	IPv4 网络	IPv6 网络
扫描攻击	易被攻击	不易被攻击，IPv6 海量地址空间增加了扫描攻击的难度
碎片攻击	易被攻击	不易被攻击，IPv6 协议不允许碎片重叠
广播风暴	易被攻击	无法被攻击，IPv6 没有广播的概念
DHCP 攻击	易被攻击	不易被攻击，IPv6 海量地址空间增加了攻击的难度
ARP 攻击	易被攻击	易被攻击，IPv6 可以通过 ND 协议实现类似攻击
病毒和蠕虫	易被攻击	易被攻击，但因地址空间大可以延缓影响
应用层攻击	易被攻击	易被攻击
欺诈类攻击	易被攻击	易被攻击
泛洪攻击	易被攻击	易被攻击

2.IPv4 向 IPv6 过渡过程中需要关注的安全风险

在 IPv6 网络的发展过程中，面临最大的问题应该是 IPv6 与 IPv4 的不兼容性，因此无法实现二者之间的互访。

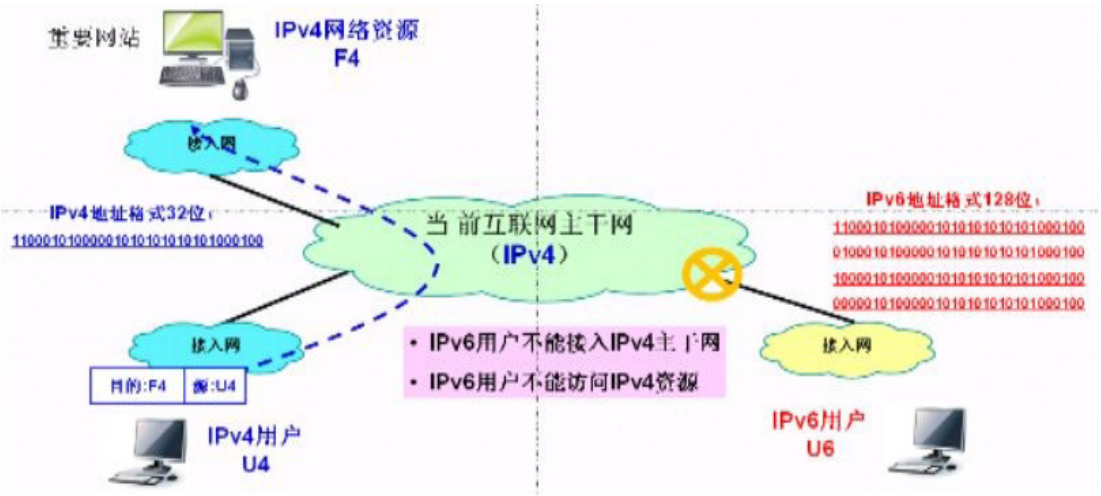


图 3 IPv6 与 IPv4 的不兼容性

IPv4 向 IPv6 过渡有三种技术：双栈技术、隧道技术、翻译（地址转换）技术。

双栈技术：双协议栈技术就是指在一台设备上同时启用 IPv4 协议栈和 IPv6 协议栈。这样的话，这台设备既能和 IPv4 网络通信，又能和 IPv6 网络通信。

隧道技术：主要有两种类型，“IPv6 over IPv4”将 IPv6 报文整个封装在 IPv4 数据报文中进行发送；“IPv4 over IPv6”，将 IPv4 报文整个封装在 IPv6 数据报文中进行发送。

翻译技术：分为 IVI 和 MAP-T 两种方式，采用地址翻译技术解决下一代互联网过渡。

目前，三种技术都存在不同的安全风险：

表 2 IPv4/IPv6 三种过渡的优劣势对比及存在的安全风险

过渡技术	优点	缺点	安全风险
双栈技术	· 互通性好 · 实现简单	· 对每个 IPv4 节点都要升级到 IPv6 · 路由器需要双寻址方案 · 不能解决 IPv4 地址短缺的困局 ——需要维护 IPv4 和 IPv6 两套路由、认证、管理系统	· 没有加强部署 IPv6 的安全策略 · 在没有部署 IPv6 的网络中，这种双栈主机也可能受到 IPv6 协议攻击
隧道技术	· 实现简单 · 技术门槛低 · 提供跨越 IPv4 实现两个 IPv6 网络的互联或跨越 IPv6 实现两个 IPv4 网络的互联	· 网络变化则需要隧道配置也实时变化 · 降低效率 · 适合小规模使用	· 没有内置认证、完整性和加密等安全功能 · 不对 IPv4 和 IPv6 地址的关系做严格的检查 · 攻击者可以通过伪造外层和内层地址伪装成合法用户向隧道中注入攻击流量
翻译技术	· 实现了两种不同协议的网络互通 · 可以有效解决 IPv4 地址短缺的问题	——需要升级地址转换设备 ——需要 DNS 的配合，对某些协议需要利用双重翻译技术实现互联	· 与上述双栈和隧道技术一样，无法对 DDoS 类型的攻击实现免疫

3. 网络安全产品对 IPv6 的支持度、产品成熟度有待提高

全球 IPv6 测试中心发布的《2017 IPv6 支持度报告》显示，目前网络安全产品 IPv6 的支持度较低，通过 IPv6 Ready Logo 认证的抗 DDoS、入侵检测、应用防火墙等安全产品数量较少。

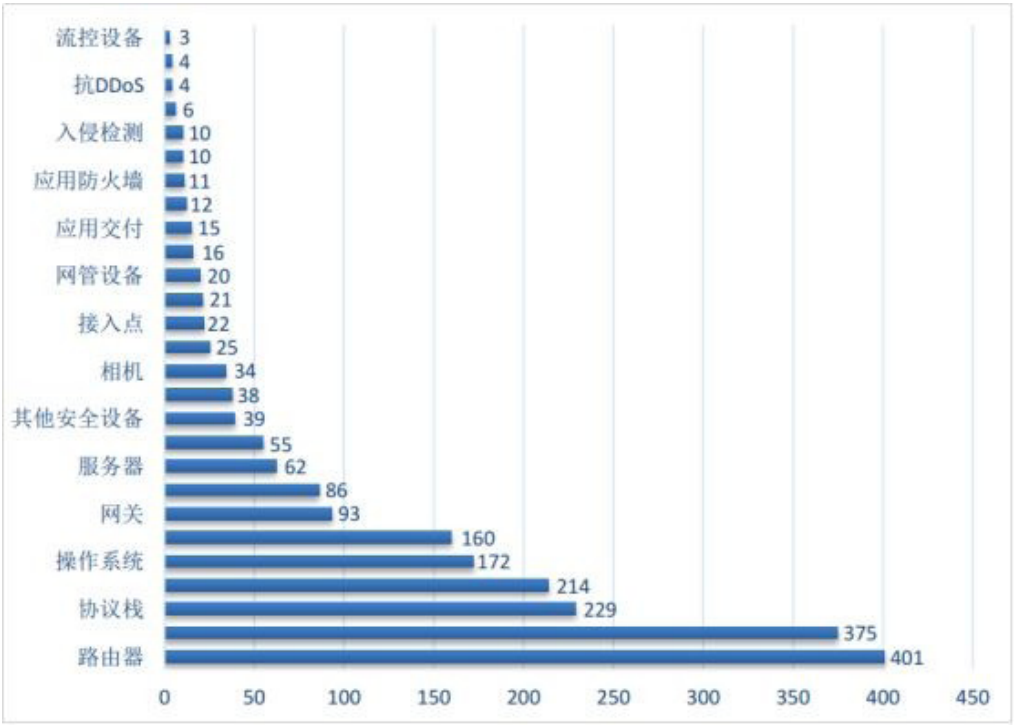


图 4 IPv6 Ready Logo 设备类型统计

此外，目前国内针对大容量安全设备、IPv6-IPv4 翻译设备研发相对薄弱，安全产品成熟度也较低。

4. 现有网络安全设备及安全系统需要进行全面升级

首先，由于 IPv6 的一些新特性，IPv4 网中现有的这些安全设备在 IPv6 网中不能直接使用，需要升级改进。其次，IPv4 向 IPv6 过渡过程中，IPv6 协议栈会挤占 IPv4 业务的 CPU 和内存等资源，导致现有的 IPv4 业务在会话表容量、吞吐率上会出现不同程度的下降。因此，对现有安全设备、安全系统处理能力的评估不够全面，设备、系统未进行全面升级，将导致 IPv6 信息安全隐患将会逐渐暴露，并被攻击者加以利用。

专家观点

北京邮电大学马严教授对 IPv6 安全建设提出了如下建议：

1．引导与管理层面

（1）政府加大对 IPv6 安全技术研究和产业发展的政策引导和支持。

（2）各界加大 IPv6 网络与信息系统安全人才培养、培训工作。

（3）加强对 IPv6 网络和信息系统安全的科普宣传。

（4）各级网络安全监管和监测机构要加强对 IPv6 网络运行安全状况的处置能力。

（5）有关检测机构对网络和软件系统的 IPv6 安全特征要加强测试和检验监管。

2．应用层面

（1）要在支持 IPv6 的安全特征研究中加强核心技术的创新与自主可控能力建设。

（2）IPv6 网络和软件提供商在生产设备和系统时加强对安全特性的支持。

（3）要大力加强网络安全设备与系统对 IPv6 特性的支持。

（4）工业互联网采用 IPv6 技术时更要对安全特性予以特别重视。

3．用户层面

IPv6 网络和信息系统使用单位在设备采购和部署时加强对安全特性的检测，工程部署时要加强对安全特性的配置与管理。（来源：高校信息化应用）

高校门户网站的 IPv6 支持数据报告

一、中国IPv6整体部署情况

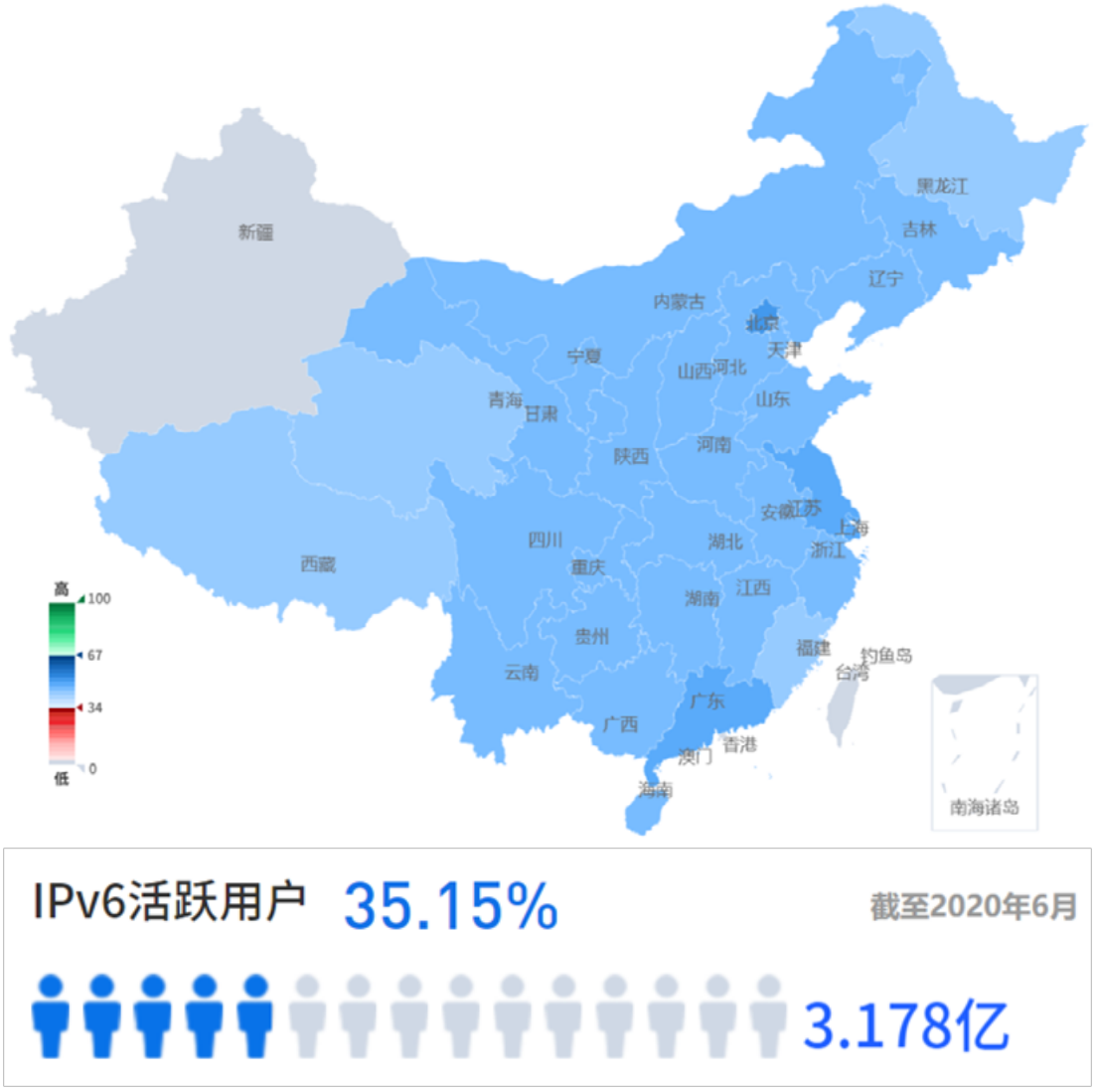


图 1 中国 IPv6 发展地图

图 2 IPv6 活跃用户与基础资源

（资料来源：国家 IPv6 发展监测平台）

二、我国网站应用IPv6支持情况

图 3 我国网站应用 IPv6 支持情况（截至 2020-08-17）

（资料来源：国家 IPv6 发展监测平台）

三、中国高校门户网站IPv6支持情况

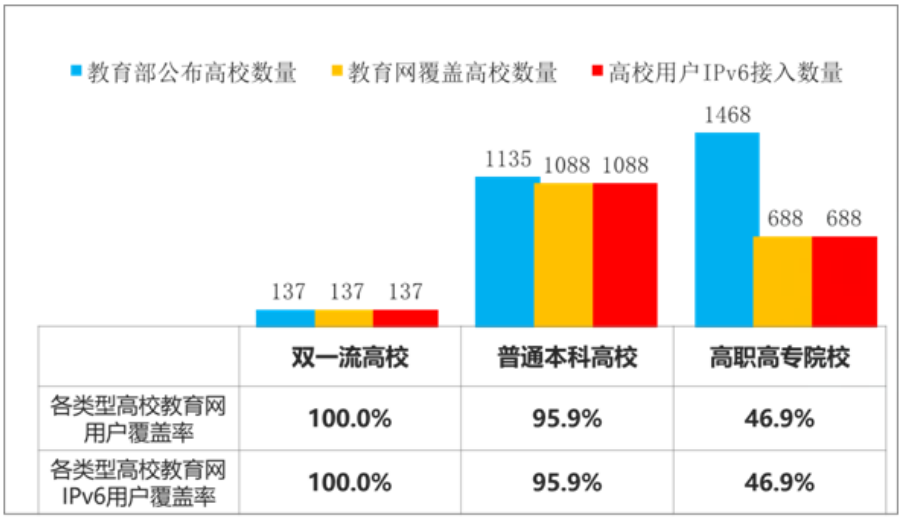
全国 1913 所高校接入教育网 IPv6，占比达 69.8%（不含成人教育）根据教育部公布的《2020 年全国高等学校名单》，截至 2020 年 6 月，全国高等学校共计 2740 所（不含成人教育）。

截至 2020 年 7 月，已有 1913 所高校接入教育网 IPv6，占比达 69.8%。

双一流高校实现 100% 接入 IPv6；

普通本科实现 95.9% 接入 IPv6；

高职高专实现 46.9% 接入 IPv6。



	双一流高校	普通本科高校	高职高专院校
各类型高校教育网用户覆盖率	100.0%	95.9%	46.9%
各类型高校教育网IPv6用户覆盖率	100.0%	95.9%	46.9%

图 4 教育网各类型高校 IPv6 用户覆盖情况

教育部公布《2020 年全国高等学校名单》显示，全国高等学校共 3005 所，其中普通高等学校 2740（含本科院校 1272 所、高职（专科）院校 1468 所），成人高等学校 265 所。

根据教育部公布的《2020 年全国高等学校名单》，截至 2020 年 6 月 30 日，全国高等学校共计 3005 所。

根据 IPv6 发展监测平台（ http://ipv6c.cngi.edu.cn ）全国各高校门户网站 IPv6 部署情况：截至 2020 年 8 月 18 日，618 所高校门户网站支持 IPv6 解析，占比达 20.6%；450 所高校门户网站支持 IPv6 访问，占比达 15%。

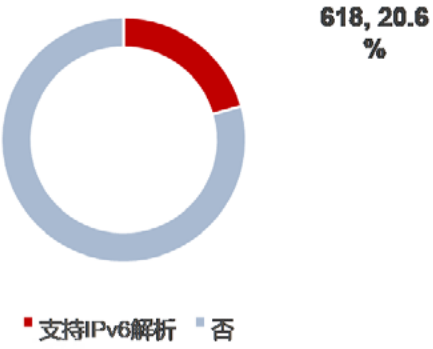


图 5 高校门户网站支持 IPv6 解析情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

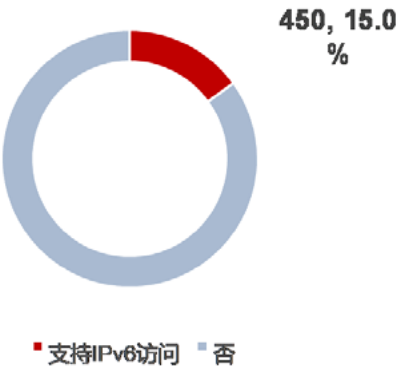


图 6 高校门户网站支持 IPv6 访问情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

四、部属院校门户网站IPv6支持情况

根据 IPv6 发展监测平台（ http://ipv6c.cngi.edu.cn ）全国高校门户网站 IPv6 部署情况：截至 2020 年 8 月 18 日，113 所部属院校（不包含国防大学和国防科技大学）中，69 所高校门户网站支持 IPv6 解析，占比达 61.1%；61 所高校门户网站支持 IPv6 访问，占比达 54%。

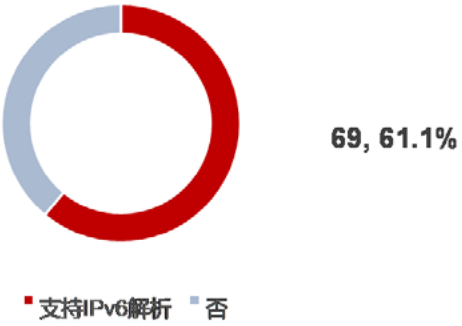


图 7 部属院校门户网站支持 IPv6 解析情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

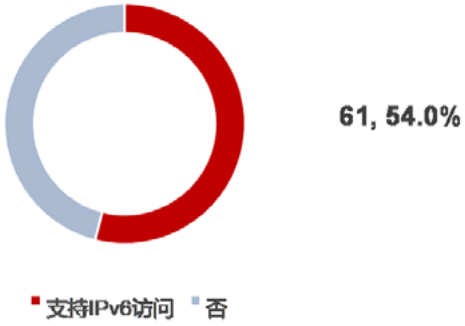


图 8 部属院校门户网站支持 IPv6 访问情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

五、各类型高校门户网站IPv6支持情况

根据 IPv6 发展监测平台（http://ipv6c.cngi.edu.cn）全国高校门户网站 IPv6 部署情况：截至 2020 年 8 月 18 日，双一流高校门户网站 IPv6 部署情况较好，70% 支持 IPv6 解析，但支持 IPv6 访问不足 60%。

另外，普通本科、高职高专以及成人教育高校门户网站 IPv6 支持率仍然较低，改造亟待加速。

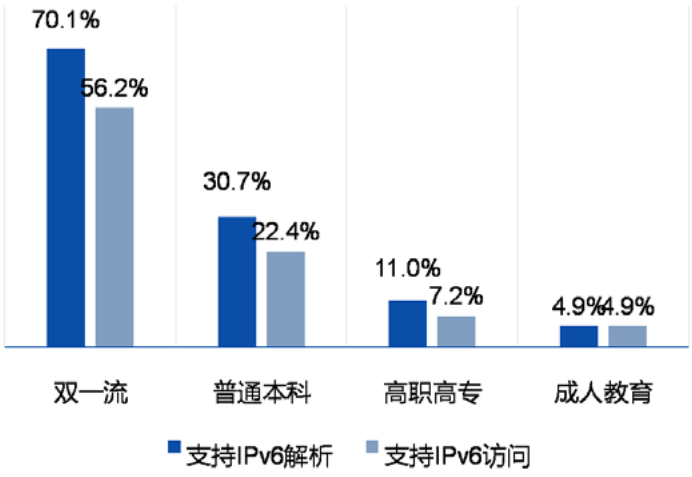


图 9 各类型高校门户网站 IPv6 支持情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

六、双一流高校网站IPv6支持情况

根据 IPv6 发展监测平台（http://ipv6c.cngi.edu.cn）全国高校门户网站 IPv6 部署情况：截至 2020 年 8 月 18 日，双一流高校中，96 所高校支持 IPv6 解析，占比 70.1%；77 所高校网站可访问，占比 56.2%。

一流大学建设高校中，34 所高校支持 IPv6 解析，占比 82.9%；29 所高校网站可访问，占比 70.7%。

一流学科建设高校中，62 所高校支持 IPv6 解析，占比 64.6%；48 所高校网站可访问，占比 50%。

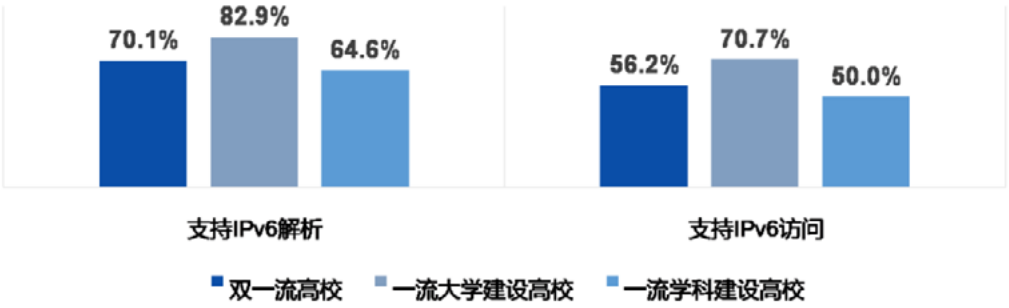


图 10 双一流高校网站 IPv6 支持情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

七、各地区高校门户网站IPv6支持情况

根据 IPv6 发展监测平台（http://ipv6c.cngi.edu.cn）全国高校门户网站 IPv6 部署情况：截至 2020 年 8 月 18 日，华南、华东北地区高校门户网站支持 IPv6 百分比 20% 以上。华北、西北、西南地区高校门户网站 IPv6 支持率较低。

备注：

华东北：江苏、安徽、山东

华北：北京、天津、河北、内蒙、山西

华东南：上海、浙江、江西、福建

华中：湖北、湖南、河南

西南：云南、贵州、重庆、四川（西藏）

华南：广东、广西、海南、深圳

东北：辽宁、黑龙江、吉林

西北：新疆、陕西（宁夏）、甘肃（青海）

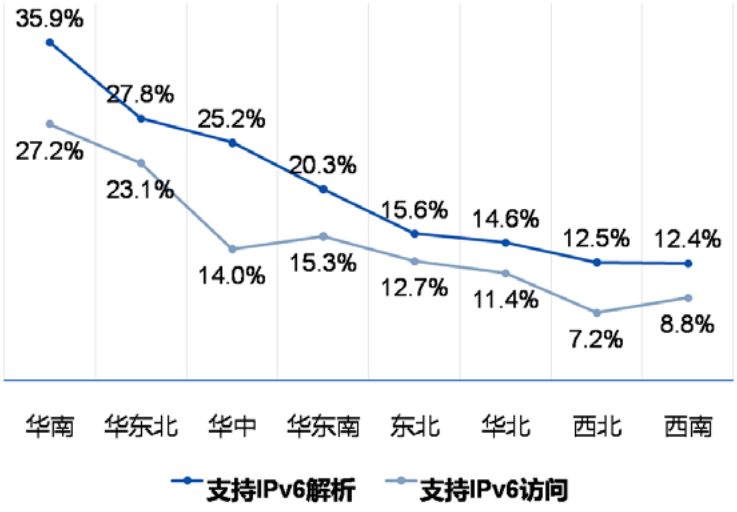


图 11 各地区高校门户网站 IPv6 支持情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

八、全国各省高校门户网站IPv6支持情况

根据 IPv6 发展监测平台（http://ipv6c.cngi.edu.cn）全国高校门户网站 IPv6 部署情况：截至 2020 年 8 月 21 日，与全国各省市相比，广东、山东、上海等省份高校门户网站支持 IPv6 情况较好，支持 IPv6 解析百分比达到 35% 以上，支持 IPv6 访问百分比达到 25% 以上；甘肃、宁夏、海南、江西、新疆等省份高校网站 IPv6 支持率较低。

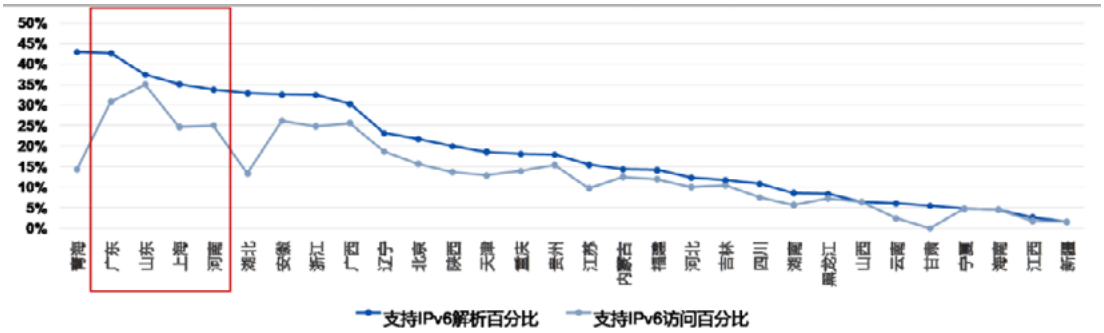


图 12 全国各省高校门户网站 IPv6 支持情况

（资料来源：IPv6 发展监测平台 http://ipv6c.cngi.edu.cn）

（来源：赛尔网络市场动态）

河南省教育信息安全监测中心（简称 HERCERT）

河南省教育信息安全监测中心（以下简称“中心”）成立于 2017 年 3 月，以郑州大学为依托，致力于提升全省教育行业信息安全管理水平。中心成立之初，先后建立了河南省教育信息安全管理云平台和各类信息安全监测系统。经过发展，中心目前具备对全省 100 余所高校提供安全、可靠的监测服务。中心不断健全完善各项运行管理制度，建立了信息安全协作通报机制，积极扩大信息获取面，不断提高中心监测能力与服务水平。

中心主要有五大职责：安全事件管理、安全预警通报、安全信息统计、安全风险评估、安全技术服务。

《河南教育信息化》征稿简则

《河南教育信息化》由河南省教育厅科学技术与信息化处主管，河南省教育科研计算机网网络中心主办。刊载行业动态、热点专题、经验交流及省内资讯等内容，多方位、多层次地探究教育信息化及教育网络建设的前沿趋势、经验与问题，为教育信息化领域各级领导及从业人员提供科学、实用的决策依据。自 2020 年，河南省教育厅将《河南教育信息化》刊发文章列入“河南省教育信息化优秀成果”评奖依据。（点击进入：河南省教育厅办公室关于开展 2020 年度河南省教育信息化优秀成果奖申报工作的通知）

来稿要求如下：

1、文章具有创新性，主题明确，数据可靠，论据充分，逻辑严密，语言简洁，图表清晰。

2、来稿附作者简介（工作单位及职务，联系电话及 E-mail）。

3、来稿请以“文章标题 + 作者姓名”为邮件标题发送电子邮件，文稿（Word 格式、宋体）及图表原图添加至附件。

4、文章结构包括：中文标题，摘要（或者核心观点），正文，参考文献（适用于学术性论文）。

文章标题应简明、具体、确切，概括论文要旨，不使用非公知的缩写词、代码等 (一般不超过 20 字)。

文中标题标示格式：

一、一级标题

1. 二级标题

（1）三级标题

5、论文中图、表和公式应通篇分别编号，图、表必须有图题、表题。

6、基金项目：若来稿有资助背景，应标明基金项目名称及编号。

7、文责自负，作者对因稿件内容所引起的纠纷或其他问题承担相应的责任。

8、依据《著作权法》的有关规定，本刊可对来稿作文字性修改。作者若不同意修改，请在来稿时注明。

9、稿件录用后，我们将支付作者适当稿酬。

附：征稿栏目

1、热点

多角度、深入探讨教育信息化热点问题。每篇稿件 1500—4000 字之间。

2、成果

分享各地各校在教育信息化工作方面的成果，有可供借鉴的思想与方法，促进交流及学习，共同提高。每篇稿件 2000—4000 字之间。

3、资讯

分享各地各校教育信息化工作相关新闻，稿件中需呈现新闻事件对实际工作的价值和意义。每篇稿件 800 字左右。

电子邮箱：editor@ha.edu.cn

河南教育信息化

回目录