中国网络卫士首登黑帽大会演讲台

今年8月，来自中国最大互联网安全公司——360公司的网络安全工程师王宇收到一份“极客”范儿十足的邀请——以中国网络卫士身份参加在美国举办的全球顶尖黑客峰会，并就其发现发表主题演讲、见证各国黑客团队“攻坚战”。

美国归来，这位“技术男”19日对记者讲述了自己亲历的网络安全“华山论剑”。

中国网络安全工程师王宇

中国网络卫士首登台

谈字体引擎的漏洞，已成这一领域顶尖高手

今年8月上旬，一年一度举行的“黑帽子技术大会”（Black Hat，简称黑帽大会）和名为“防御态势”的国际黑客大会（Def Con）再度吸引全球成千上万网络卫士和黑客高手聚首“赌城”拉斯韦加斯。

从技术培训、专家演讲到黑客大比拼，两场大会从“盾”与“矛”两个角度聚焦当下最前沿的网络安全趋势和黑客技术走向，堪称全球信息安全领域顶尖峰会。

今年，中国“网络卫士”也首次登上“黑帽大会”演讲台。

王宇介绍说，他8月7日在大会上发表题为《理解Windows内核字体引擎中的时间差问题》的主题演讲，为同业拆解他对此类安全漏洞问题的思考。

即便在全球范围内，字体引擎漏洞问题的研究者也不多，而自2011年起投入这一研究领域的王宇已算得上这一领域的顶尖高手。

王宇告诉记者，最早引起业内少数人对这一问题重视的是全球第二代国家级恶意软件——duqu，其二进制代码与第一代国家级恶意软件“震网”较为相似。

美国《华盛顿邮报》等媒体报道，“震网”及其后多个曾肆虐中东地区的网络病毒由美国和以色列联合研发，其中美国情报机构和以色列军方均参与了“震网”针对伊朗铀浓缩设备的攻击。

据王宇介绍，尽管研究者不多，从Windows XP到Windows 8.1在内的所有Windows操作系统，字体引擎时间差问题可能引发的漏洞风险却普遍存在。

今年3月，王宇向微软公司提交了由字体引擎时间差问题可能引发漏洞的详细分析材料，指出该漏洞存在被攻击者远程控制的风险。而就在拉斯韦加斯“华山论剑”落幕前夕，微软公司8月12日发布了该漏洞的补丁。

特斯拉也来招贤

汽车软件漏洞也会致命，求黑客高手们“查漏”

王宇介绍，今年大会期间受关注的安全漏洞热点话题还包括高级持续性威胁（APT）和无线领域信息安全等。

其一，APT网络攻击通常是针对高价值目标的定点打击，采取更为高端且难以监测的攻击技术，比如世界500强企业就很关注如何防范和应对此类攻击。

其二，随着移动互联技术的迅速兴起、智能手机的迅速普及，针对手机的安全漏洞问题日益凸显。

大会期间，就有黑客现场演示如何针对手机“信任区域”内的系统漏洞，仅凭很低权限切入，就能影响最高权限的功能。

比如，苹果手机iPhone 5S指纹识别技术的信息就存储于“信任区域”。

今年大会期间，顶级黑客在演示活动中再度各自施展破解大法，也更凸显现实世界的网络安全风险之剧。还有专家在会上指出，全球有超过20亿个移动设备安装了含有漏洞的远端管理程序，而黑客能借此获得权限，在移动设备上安装恶意程序或存取机密信息。

风头正劲的美国特斯拉电动汽车公司甚至特意来到大会，求助网络安全工程师和黑客高手查找特斯拉汽车软件漏洞，并借机招聘信息安全研究员。

今年7月底，360公司曾率先发现特斯拉S型汽车存在的应用程序漏洞，并第一时间提交特斯拉。

王宇说，全球进入互联网及移动互联时代，网络攻击每时每刻都在上演。无论是产业上下游各环节，还是普通消费者，都必须意识到与“网”有关的所有产品和服务都面临安全风险，手机、电视、移动设备等很容易受到攻击，生产者更应保持积极心态，及时修复、主动应对。

名词解释

黑帽大会

戴黑帽子的人被视为是恶棍或坏人。尤其是在西方的电影中，反派角色都会戴着黑色的帽子，而正派的英雄都会戴着白色的帽子。而在计算机中，这种经典措辞也成为了一种俚语，用来比喻黑客、网络入侵、计算机病毒等阴谋诡计。因此黑客们的聚会被称为黑帽子大会。

黑帽安全技术大会是一个具有很强技术性的信息安全会议，会议引领安全思想和技术走向，参会人员包括企业和政府的研究人员，甚至还有一些民间团队。为了保证会议能够着眼于实际并且能够最快最好地提出方案、问题的解决方法和操作技巧，会议环境保持中立和客观。黑帽安全技术大会是世界上最好的能够了解未来安全趋势的信息峰会，它的权威性更是独一无二的。

黑客攻防差距大

52小时黑客攻防“夺旗大赛”，美国一大学队夺冠

今年两场大会参会规模再破纪录。其中，聚焦信息安全热点话题的“黑帽大会”吸引了近万名参会人员，同比增长20%。而“黑客大会”的参与者更由去年1.2万人激增至今年近1.6万人。

王宇介绍，前者参会人员需缴纳2000美元报名费，主要吸引的是网络安全领域从业人员、美国政府安全人员等；后者入场费仅为200美元，不仅有黑客高手参与，还有不少美国相关专业的大学生也来参会。

他说，“黑客大会”丰富内容中最吸引眼球的莫过于黑客攻防“夺旗大赛”，由闯入总决赛的20支黑客队伍一边回答“考题”，一边保住自家营盘并互相攻击，持续时间为52小时。

“蓝莲花”队以清华大学学生为基础班底。王宇本人也是“蓝莲花”一员。

在这名网络“安全卫士”看来，现代社会中，网络安全攻防犹如没有硝烟的战争，深刻影响着个人安全和国家安全，而“夺旗大赛”就是一场虚拟空间短兵相接的小型演练。

据他介绍，今年比赛仍由传统强队、美国卡内基·梅隆大学的队伍PPP夺冠，美国谷歌公司派出的参赛队获得第三名。但另两大亮点更值得关注——其一，中国台湾派出的一支队伍获得第二名；其二，今年有5支韩国队伍闯进总决赛。

王宇说，他在近两年交流中获悉，韩国之所以在黑客技术领域突飞猛进，离不开韩国从中学、大学开始着力培养和储备黑客技术人才和网络安全人才的部署。

反观中国高校学生，虽学习兴趣浓厚、学习热情高涨、个人素质较高，但整体技术水平、育才政策和环境以及受重视程度尚难与之媲美。

“我们队伍成员曾在大会期间开玩笑说，要是这也能高考加分，中国队肯定能在黑客攻防比赛中拿下冠军。”王宇说。

新华社供本报特稿

两名与会者在“白帽安全”公司展台体验“黑客攻坚战” 新华/路透

叙开打“伊黎”武装 美精锐部队追捕匪首

美军飞机连日来对伊拉克境内的极端武装“伊拉克和黎凡特伊斯兰国”（“伊黎”武装）进行多轮空袭。西方媒体18日报道，叙利亚政府军也开始对境内“伊黎”武装展开空袭。分析人士称，叙利亚政府军这番行动，一是因为“伊黎”武装近期在叙利亚境内日益猖獗；二是向外界释放信号，叙利亚政府军有能力打击“伊黎”武装。

另据报道，美国已成立一支由约100名中情局人员和特种部队士兵组成的精锐部队，追捕42岁的“伊黎”首领巴格达迪。这将是美国2011年猎杀“基地”组织领袖本·拉丹以来，最大规模的反恐搜捕行动。据悉，情报专家正利用无人机和卫星影像，搜集手机通话数据，以及伊拉克和叙利亚的地面调动情况。一名消息人士说：“巴格达迪的部队分散各地，必须通过电话指挥，这是他的弱点。” 综合

利比里亚17疑似病人失踪 世卫：警惕埃博拉蔓延

利比里亚当局18日仍未找到从首都蒙罗维亚一个隔离中心逃走的17名疑似埃博拉病毒感染者。这座隔离中心16日深夜遭一群人冲击并洗劫，37名疑似感染者乘乱逃走，其中20人已被带回医院，剩余17人仍然下落不明。

世界卫生组织18日发表声明，呼吁受埃博拉疫情影响的国家立即在其所有出境机构设置检验部门，让所有出境人员接受检查，以防埃博拉病毒蔓延。世卫组织没有说明究竟哪些国家应该采取上述措施，但提及埃博拉疫情现在几内亚、利比里亚和塞拉利昂暴发，尼日利亚也有“一小部分人染病”。 据新华社

宇航员太空行走 “抛射”一颗迷你卫星

国际空间站俄罗斯籍宇航员18日“太空行走”期间徒手把一颗仅重1公斤的迷你卫星送入太空。

国际空间站拍摄的画面中，一名宇航员喊出“一、二、三”后，这颗边长10厘米左右的立方体形迷你卫星离开宇航员之手，经历些许波动后慢慢远离空间站尾部，在镜头中越来越小，预计不久后进入自身轨道飞行。

这颗卫星由秘鲁国家工程大学学生研发，以印加文化中含义为信使的Chasqui命名，以太阳能为动力，外置可视灯、红外线摄像头和感应仪，用以拍摄地球照片并记录飞行轨道的气温和气压。 据新华社

青年遭枪杀视频曝光 美司法部长前往调查

8月18日，有目击者首次公开美国黑人青年布朗遭警员威尔逊枪杀的视频。19岁的女子克伦肖声称当时从家中目睹事件部分过程，她说当时布朗疑似被警员推上警车，期间布朗想逃走，但被追上，转身面对警员时，身中多枪。克伦肖公开的视频，应该是开完枪的情况，视频显示布朗中枪后倒卧在地上，警员威尔逊在布朗身边踱步。

18日，奥巴马呼吁，非裔和白人之间应寻求和解而不是互相伤害。他宣布，司法部长霍德20日前往弗格森市，布朗死亡已成立联邦独立调查组，霍德会与调查官员和其他官员会面。 据《中国日报》