新形势下的安全威胁

——中国科学院物理研究所“安全问题的行业化”主题讨论侧记

2019－11－01收到
† email: hxwei@iphy.ac.cn
DOI: 10.7693/wl20191110

时代的交替，“互联网+”、数字经济的不断深入发展，使得众多关系国家安全、国计民生和公共利益的行业和领域的运营已经高度依赖网络，信息安全的威胁和挑战日益加剧。一旦这些重要的网络系统遭到破坏或丧失功能，将带来不可估量的危害和损失。看似无懈可击的网络安全防线的背后“一点即破”，面对新形势下的安全威胁，无人可以独善其身。

2019年10月28日晚，由科技部引进国外智力管理司、中国科学院科学传播局、北京科学技术委员会支持，中国科学院物理研究所承办的第43期科学咖啡馆活动在物理所M楼咖啡厅举行，由科技部引进国外智力管理司邱成利处长主持，腾讯安全玄武实验室负责人于旸主讲。作为全球极少数因发现微软漏洞而获得十万美元大奖的顶尖黑客，于旸深度剖析安全漏洞，直指当下网络信息安全面临的严重威胁，为大家揭开安全问题逐渐行业化渗透的神秘面纱。

一击即破不容忽视

提起“安全漏洞”，我们一般想到的是偶尔从新闻上看到一些相关的话题，比如病毒、蠕虫等。通常安全漏洞是指受限制的计算机、组件、应用程序或其他联机资源无意中留下的不受保护的入口点。漏洞是硬件软件或使用策略上的缺陷，它们会使计算机遭受病毒和黑客攻击。

世界上最早的“蠕虫漏洞”出现在19世纪80年代末。1988年11月2日，由美国康乃尔大学一年级研究生编写的Morris蠕虫只用了一个现在看起来很简单的漏洞，就感染了当年整个互联网十分之一的服务器。2003年1月25日，一个仅376个字节的SQL Slammer蠕虫就拉低了全球的互联网速度，并导致多个骨干网络瘫痪。该蠕虫病毒释放后，全球受感染的机器数量每8.5秒就增加一倍。据统计，在10分钟之内，世界范围内所有抵抗能力低下的服务器中90%都被该病毒成功侵袭。2017年WannaCry勒索病毒全球大爆发，至少150个国家、30万名用户遇袭，直接损失达80亿美元，影响到金融、能源、医疗等众多行业，造成严重的危机管理问题。漏洞引发的安全问题随着全球化的步伐渗透得越来越深，波及面越来越广，表面上绝大部分漏洞只影响一个产品，或者一个产品的某个版本，但漏洞所涉及的产品如果应用广泛，就会具有极大威力。

随着第三次工业革命的快速发展，全球性的网络安全威胁不断升级，一系列的网络安全事件，影响多个国家的政府、银行、企业、电力系统。当漏洞不仅造成严重的破坏，甚至还能在国际公开市场上明码标价的时候，这已经不是简单的技术问题了，而是一个世界范围的经济问题、政治问题，为我们重重敲响了安全的警钟。

行业渗透日益严峻

对于社会公众而言，当从新闻里偶然发现安全漏洞仿佛带着“蝴蝶效应”一般，从对一个产品的破坏到产生全球性的震荡时，我们才会意识到这是个多么严重的问题。作为安全专家，于旸坦言，除了漏洞横向扩散的严重后果，在2005年的时候，出于研究两个不同公司生产的产品造成的极其相似的安全问题，他就开始思考漏洞在纵向延伸上对于一个行业的影响了。

显而易见，漏洞的渗透是一步一步深入的。在早几年对于PC安全漏洞的研究基础上，手机作为最常用的移动设备，为了规避已知的安全隐患，通过添加一些安全技术比如可信计算、漏洞缓解、权限隔离等，可以说已经被保护在了一系列

于旸主题报告现场

安全机制下。然而，相对于PC端，手机毕竟是一个新形态的产物，与PC不同的软硬件特点、长时间开启以及随时变动物理位置的时空特点，又给安全引入了很多变量，必然会产生新的安全问题。

基于这些方面的思考，于旸和他的玄武实验室在2017年时发现了“应用克隆”这种新型威胁。简单来说，就是只需向受害者通过短信、邮件、扫码等任何方式让其打开一个网页链接，就可以克隆用户手机里某个应用的账号，以该用户的身份登录相关应用，而无需知道用户的密码。玄武实验室对于国内最流行的200个应用做了检查，发现其中有27个都存在可用“应用克隆”技术攻击的漏洞，这一超过10%的渗透比例足以说明这个威胁是重磅级的。沿着这个思路，玄武实验室又研究了手机系统的漏洞情况，发现当时几乎所有手机都存在可用“应用克隆”技术攻击的漏洞!

这并非玄武实验室在行业性安全问题上的唯一发现。无论是时下最新潮的屏下指纹识别技术还是古老的条形码扫描技术，玄武实验室都发现了相关安全问题，而且不同厂商的同类产品都存在同样的问题！当你的移动设备不再安全，应用账号私人信息完全暴露，手机指纹解锁只需要“一张纸、一秒钟”就被攻破，当黑客向设备发射一束激光就能获取控制权，我们不禁反思，这是为什么?

为什么这么多常用的应用会出现同样的问题？为什么手机制造商不及时修复已知的系统漏洞？为什么指纹识别技术在成熟发展几十年后仍会出现新问题？为什么安全漏洞的问题影响了那么多企业和产品？于旸给出的答案只有四个字：信息鸿沟。试想，如果只是单纯的有人告诉你，这部手机有一个漏洞，你能理解多深层次的危险性？如果换作直接展示如何通过几秒钟就用这个漏洞以控制你的手机，你会否立刻警觉起来？往往一些漏洞的根源就是一个简单的编码错误，或者一个协议的问题，明明已经在开发者手册中写出了“不安全”、“不要做”，出于侥幸心理、从众心理，对于小BUG的忽视就造成了行业化的深入渗透。

攻守相辅共同筑防

类似上面提到的影响整个行业的安全问题数量并不多，但影响巨大、后果严重，最重要的是如果发现不及时就会难以解决。在报告接近尾声时，现场嘉宾一边惊叹于安全问题带来的巨大威胁，一边也觉得意犹未尽，纷纷展开讨论和交流。上海交通大学郁昱教授提到近年来无论是密码技术，还是生物特征扫描技术比如指纹或者面部识别，都还是在不断摸索、不断成熟的过程中，从理论认知到技术实现就很难，想要做到真正的安全又会不断出现新的问题。对于这一观点，于旸首先解释了生物特征扫描技术目前已经有很多新技术和新探索。比如面部识别不光会判断面容特征，还会判断人脸的立体结构，甚至皮肤纹理；再比如一些指纹识别的实验性技术不仅会对指纹纹路进行详细的比对，更能判断皮下是否有血管。其次，于旸认为自古以来，攻和防向来是一个此消彼长、道高一尺魔高一丈的过程，正如玄武实验室名字的由来，“玄武”是中国传统文化四象之一，由龟和蛇两种动物组成，龟和蛇恰好可以象征着网络安全两个方面——防御和攻击，这是网络安全必不可缺的一体两面。发现漏洞、修复漏洞是网络安全工作中很重要的组成部分。中国科学院科学传播局周德进局长问到，仅一个玄武实验室这几年来就发现了近千个漏洞，那全球的网络系统得有多少漏洞？于旸解答道，目前全世界每年新发现安全漏洞大约1万个，但不是所有的漏洞都那么严重，大部分漏洞只能导致软件崩溃或泄露一些不太重要的信息，再加上技术的不断提升，真正意义上严重漏洞的数量是一个稳中有降的趋势。然而随着整个网络空间复杂技术的叠加，在新形势、新挑战下，发生行业性安全问题的概率难以预估。

在于旸精彩的解答和嘉宾的热烈讨论中，本次咖啡馆科普活动结束了。最后，腾讯副总裁陈发奋先生作了总结，随着科学技术的发展，我们逐渐意识到，网络带来便利的同时，若管理不当，也会造成极大危害。面对当下仍然严峻的形势，这也就是为什么这些年有更多的呼吁，希望大家能关注到新形势下网络安全的重要性，用户们能提高安全意识，企业能保护好行业数据和资产信息，国家、企业、社会、公众共同重视，才能在安全问题的行业化中共同构筑安全防线。

(中国科学院物理研究所
田春璐　成　蒙　魏红祥　供稿)

科普活动与会嘉宾合影