“互联网+”时代的个人隐私保护

● 王 晔 / 扬州市邗江区保密局

随着我国“互联网+”产业的发展，各种新兴互联网应用在给人们带来便捷的同时，也对个人隐私安全带来风险。近期，IBM公司对全球范围100个国家的8000多名客户进行监测并发布报告指出，2016年个人隐私泄露同比增长566%，泄露超过40亿条个人信息[1]，其中国内由于隐私泄露所带来的电信诈骗等违法犯罪案件数量由10万件增长至60万件[2-3]。本文对常见的隐私泄露途径进行了归纳总结，并初步思考了应对策略。

常见的个人隐私泄露途径

设备指纹追踪

设备指纹（Device Fingerprint）追踪技术首先被各大网络广告商采用，用于向用户投放更有针对性的广告，同时这些数据也将被收集起来用于对用户个人行为的研判[4]。最常见的设备指纹追踪手段是通过植入Cookie实现。通常情况下，Cookie被认为是定位用户的有效手段之一。广告商与各大门户网站或流量较高的社交网站以广告合作的形式，通过嵌入框架网页（Iframe Page）、隐藏跟踪图片（Hidden Image）和JavaScript脚本从而实现向用户浏览器发送Cookie，并持续跟踪用户访问习惯的目的。由于Cookie的易失性，现在设备指纹追踪技术已不仅依赖于Cookie，多种手段的设备指纹追踪技术正在被应用。Evercookie 脚本正是此类型的追踪技术[5]，该脚本通过在浏览器产生难以删除的僵尸Cookie从而牢牢地锁定特定用户。除此之外，通过在页面追踪用户鼠标轨迹、停留时长和点击方位生成热图（Heatmap）也成为标识用户行为的一种新型设备指纹追踪手段之一。

应用程序接口权限审查不严

开放形式的应用程序接口如Web API，正成为分布式云计算的一个重要入口方式，但由于管理疏忽和权限审查不严，容易给不法分子以可乘之机。通常第三方网站通过集成采用OAuth规范的Web API可轻松实现类似“使用QQ账户登录”“使用微信账户登录”等功能，以进一步吸引用户资源并简化开发流程，但由于第三方网站管理疏忽或被恶意攻击从而导致用户相关账户资料的泄露。其中部分内部应用接口为了调用方便，甚至没有进行有效的身份认证，导致内部接口暴露，从而可直接输出用户隐私数据，造成数据泄露。例如，某电信运营商通过内部应用接口显示访问用户的上网账号和用户名，但此接口未做权限判断导致任意网站可调用获取当前访问用户的隐私信息。

网络应用漏洞

“互联网+”产业的发展带来了层出不穷的各类应用，无论是Web应用还是手机APP，在给人们生活带来便捷的同时其隐含的安全问题也不容忽视。各种形如SQL注入攻击（SQL Injection Attack）、跨站脚本攻击（XSS

Attack）、任意文件上传漏洞攻击等，易实施和高度自动化的网络攻击形式给应用部署带来风险。同时，互联网企业为了抢占先机而缩短互联网应用开发的周期，可能导致应用设计上的粗制滥造，缺乏安全防护给攻击者大开方便之门。除此之外，部分用户有将所有账户都设置为同一密码的习惯，这为黑客攻破其所关联的其他系统带来了方便。随着大量隐私资料的泄露而衍生出的地下黑市，让不法分子通过交易互换便可掌握用户个人隐私，甚至逐步且立体地掌握用户的全部相关资料[6]。

流氓软件偷传隐私

流氓软件源于英文“Badware”一词，国外对“Badware”的定义为：一种跟踪用户上网行为并将其个人信息反馈给幕后市场利益集团的软件[7]。流氓软件处于病毒和正规软件之间的灰色地带，其最显著特征是隐蔽安装、占用资源、窃取隐私，干扰用户正常使用计算机且难以被卸载。通常流氓软件进驻系统后，不仅会在后台偷偷采集用户数据，还会下载安装其他恶意软件，扩大用户隐私泄露范围。部分流氓软件打着大公司的旗号，以正规软件功能为幌子，未经用户许可偷偷上传用户通信录、地理位置、设备信息、软件安装与使用情况、分析网络流量，甚至采用自签名的根数字证书拦截并分析加密传输的网络流量，然后利用这些非法获取的隐私数据进行大数据分析与处理从而达到获利目的。

明文数据传输

超文本传输协议（HyperText Transfer Protocol，HTTP）被普遍应用于互联网数据传输，但由于设计原因，HTTP协议自身并不具有加密特性，这就导致用户隐私数据极有可能在网络中因明文传输而被第三方窃取。攻击的主要方式为中间人攻击（Man in the Middle Attack，MITM Attack）。目前，通过对HTTP协议数据采用安全套接层（Secure Sockets Layer，SSL）进行加密形成HTTPS连接，可有效避免中间人流量分析拦截。国外对于HTTPS的采用率要明显高于国内，尤其是在政务网站领域。2016年10月1日，英国政府要求所有政务网站强制使用HTTPS加密连接，在这之前美国政府也曾发布HTTPS Only标准，并要求所有政务网站在2016年年底前强制使用HTTPS[8]。而国内大部分网站，尤其是关系国计民生的政务服务网站，在涉及用户登录凭据等隐私数据时则采用明文传输，这给个人隐私保护带来风险。

加密措施存在隐患

国内大部分网站的SSL加密数字证书采用国外产品[9]，对于这些网站的第三方认证完全由国外公司实现，且数字证书私钥也由国外公司存档，因此话语权完全掌握在国外公司手里，信息安全难以保障。

国内自主商用加密算法普及率尚不高，大部分应用依然采用国外的加密算法。有报道显示，国外有些数据加密服务商与美国国家安全局（NSA）合作在内置加密算法中设置后门[10]，而此加密算法被广泛应用于国内的商业软件中，使得软件用户的个人隐私安全受到威胁。

钓鱼网站

钓鱼网站（Phishing Site）是指，通过伪造正规网站界面诱使用户访问并输入个人隐私信息进行窃取行为的陷阱网站。近几年，这一类网站尤其是涉及金融类网站的钓鱼网站数量呈现上升趋势，其中银行类网站属于重灾区；此外，是以中奖为诱饵的热门综艺节目类型钓鱼网站，如假冒《我是歌手》和《奔跑吧兄弟》等节目[11]。这一类网站迷惑性较大，尤其是与官方网站地址（URL）较为接近使用户难以分辨。传统钓鱼网站散布方式主要包括垃圾

邮件和即时通信聊天工具，现在已出现通过伪基站假冒官方号码发送短信的传播形式，可谓形式多样、迷惑性较强，用户如果不加以分辨登录钓鱼网站，极易被诱惑输入隐私信息，造成信息泄露。

流量劫持

流量劫持（Traffic Hijack）是一种常见的中间人攻击手段，攻击常常发生于关键的网络设备，如路由器、网关及入侵检测系统（IDS），尤其以HTTP流量和DNS查询流量劫持较为常见。国家互联网应急中心曾表示，有多家路由器厂商的产品存在“后门”[12]。不法分子可通过攻击路由器获得管理权限，进而部署流量劫持行为。另一种较为常见的劫持手法是在网络中相对靠近用户的旁路节点部署攻击行为。这些攻击手段隐蔽性较强，但可通过在应用层和传输层之间部署SSL对服务器身份进行验证加以避免。

个人隐私保护建议

个人层面

1.提高个人隐私保护意识。一是不向来历不明或存在风险的组织或个人提供个人信息，不在“朋友圈”、微博等社交网络发布可能暴露隐私的照片或文字；二是培养积极健康的个人兴趣，只浏览正规网页、下载官方软件，不运行来历不明的程序，不安装不必要的浏览器插件；三是妥善处理废弃手机、电脑、存储卡、U盘和移动硬盘等个人设备，必要时交由具有保密资质的专业组织回收或销毁；四是保管好银行凭据、快递单据、车票等包含个人信息的文件，丢弃前可采取对关键信息进行涂抹或粉碎等手段进行处理。

2.养成良好的行为习惯。一是安全防护方面，在设备中安装杀毒软件并合理配置防火墙，定期进行病毒查杀；二是上网习惯方面，及时清理上网痕迹，开启浏览器防跟踪标识，必要时使用浏览器的“隐私浏览”保护模式，移动上网设备不要连接未经加密或来历不明的公共Wi-Fi；三是网络账户方面，使用账户登录网站之前，核实网站URL网址是否为官网地址，不在未进行加密的HTTP连接上提交个人信息，对于HTTPS加密的网站要核实网站数字证书是否由可信机构颁发，定期修改登录账户密码，采用8位以上无规律复杂密码，不要使用生日、电话号码、身份证号码等易获取的信息作为密码，多个账户不要设置相同的用户名和密码，尤其是涉及找回密码的认证邮箱密码要单独设置；四是信息存储方面，不要使用网盘、电子邮箱等互联网应用存储个人信息，如有需要可采取专用移动存储设备脱机单独存储并杜绝外借；五是手机使用方面，对于手机APP只授予软件正常运行的最小权限，不对手机操作系统进行“越狱”或ROOT操作，卸载不需要的APP且只在官方手机软件市场下载安装APP，不随意用手机扫描未知二维码；六是检查维护方面，定期检查计算机和手机上软件安装列表、操作系统进程列表和系统启动项等关键位置，及时发觉可疑项目并处理，随时关注网络安全信息资讯并及时修补系统漏洞。

国家层面

1.扶持并推广自主知识产权的加密产品研发与使用。国家层面继续出台相关政策支持和鼓励国内数字证书产品和自主商用密码算法的研发，深化网络安全企业与各大院校和科研院所合作，建立产学研一站式服务机制，加快科研成果转化为实际产品的速度，突破国外技术壁垒，打破对国外软件的依赖。

推广自主国产商用密码产品，结合全国科普日、科普下基层等活动将保密常识、国产商用密码产品等以清晰易懂的科普形式展现

以提高公众知晓度。结合“七五”普法规划，加大国家密码管理政策和法律法规的宣传力度。进一步与企业合作降低商用密码使用门槛和经济成本，让普通用户也能使用商用密码保护个人隐私。

做好商用密码监管，依据我国《商用密码管理条例》第十四条规定：任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。进一步落实对境外流入密码产品的管理，强制凡是涉及公民个人信息处理的企事业单位、政府部门采用经过认可的自主国产商用密码产品。

2.提高行业门槛并探索自律机制。提高互联网网站、手机APP接入准入门槛，通过对用户个人隐私进行分级并审计互联网服务商所能接受的用户隐私范围，颁发个人信息处理许可，公示相关信息并通过官方平台邀请用户进行监督和举报，保障用户知悉权，在互联网应用获取用户信息前在醒目位置进行提示，让用户选择可以提供的信息。加强行业自律，成立互联网个人信息保护协会，自我监督、自我约束，并通过与政府部门合作，建立保护联动机制。

3.完善相关立法并加强法律监管。政府等相关机构进一步加大对公民个人信息的保护力度，完善并制定有关公民个人信息保护的法律法规，明确主体、责任到人，多举措、全方位防止个人信息的泄露和滥用。对公民隐私进行分级管理，划分信息保护范围，加强涉及泄露公民隐私犯罪的打击力度；加大清理未备案的网站力度，进一步遏制钓鱼网站等恶意网站的蔓延趋势；加强对电信运营商、互联网提供商的监管力度，建立自查自纠机制。

在信息安全形式日益严峻的今天，个人隐私泄露已成为一个严重问题，如果我们不注重保护自己的隐私，那么个人隐私的泄露不仅会带来生活上的骚扰、经济上的损失甚至是个人名誉的损害，不法分子还可能利用这些隐私信息进一步威胁个人所任职单位的网络安全。END

参考文献：

[1] TechRepublic.IBM Report: Leaked Records Hit 4B, Up 566% Since Last Year[EB/OL].(2017-3-29)[2017-4-7].http://www.techrepublic.com/article/ibm-report-leaked-records-hit-4b-up-566-since-last-year/.

[2] 张末冬.中国个人信息安全和隐私保护报告发布[N].金融时报,2016-11-22(003).

[3] 案件数量四年飙升六倍 破案难致电信诈骗猖獗[EB/OL].(2016-9-4)[2017-4-9].http://it.sohu.com/20160904/n467557348.shtml.

[4] Peter Eckersley.How Unique Is Your Web Browser?[C].Electronic Frontier Foundation. 2010.

[5] Wikipedia. Evercookie[EB/OL].(2010-10-23)[2017-4-9].https://en.wikipedia.org/wiki/Evercookie.

[6] 揭秘个人信息泄露网上贩卖"黑市"可实现精准实时定位[EB/OL].(2010-9-4)[2017-3-10].http://tech.sina.com.cn/i/2017-02-16/doc-ifyarrcc7401951.shtml.

[7] Wikipedia. Badware[EB/OL].(2002-1-4)[2017-3-10].https://en.wikipedia.org/wiki/Badware.

[8] 英美政府网站强制要求HTTPS加密[EB/OL].(2016-7-22)[2017-3-10].http://www.gov.cn/wzpc/2015/2016-07/22/content_5094643.htm.

[9] Datanyze. Analytics Market Share Report[EB/OL].(2016-12-31)[2017-3-10].https://www.datanyze.com/market-share/ssl/.

[10] NSA在RSA加密算法中设置了第二个后门程序[EB/OL].(2014-4-1)[2017-3-10].http://tech.qq.com/a/20140401/001158.htm.

[11] 2016钓鱼网站排名出炉:你被钓鱼了吗?[EB/OL].(2016-5-10)[2017-3-10].http://mt.sohu.com/20160510/n448652008.shtml.

[12] 业内爆路由器厂商人为留"后门"多用户存安全隐患[EB/OL].(2014-4-1)[2017-3-10].http://news.163.com/14/0401/07/9ONRBN0F00014JB6.html.